Use cases of Symantec™ Client Management Suite 8.5

Use cases of Symantec™ Client Management Suite 8.5

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

https://www.symantec.com

Symantec 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/

Contents

Chapter 1

Introducing Client Management Suite

This chapter includes the following topics:

About Client Management Suite

Note: Current documentation applies to the most recent version of the product.

Client Management Suite combines the tools that help you deploy, manage, secure, and troubleshoot your desktop and laptop client computers.

Client Management Suite is a collection of solutions that run on the Symantec Management Platform. The platform and solutions of the Client Management Suite provide the following key features:

- Discovery and inventory
  The suite lets you gather inventory of all hardware and software on your client computers.
- Imaging and deployment
  The suite lets you deploy standardized and hardware-independent images on your client computers.
- Software distribution and patch management
  The suite lets you control the software configurations of your client computers. The automated policies for software and patch management help you distribute the latest

software and operating system updates. You can ensure that the required software remains installed, is in a working state, and is correctly configured on the client computers.

- Remote Management

See "Where to get more information" on page 10.

Components of Client Management Suite

Client Management Suite is a collection of solutions that run on the Symantec Management Platform. The following table lists all the solutions in Client Management Suite and also provides a short description of each.

See "About Client Management Suite" on page 6.

Table 1-1 Components of Client Management Suite

Component	Description	Link to User Guide
Symantec Management Platform	Symantec Management Platform provides a set of services that IT-related solutions can leverage. By leveraging these services, the solutions that are built on the platform can focus on their unique tasks. They also can take advantage of the more general services that the platform provides. The platform services also provide a high degree of consistency between the solutions, so that users do not need to learn multiple product interfaces. Symantec Management Platform provides the following services: ■ Role-based security ■ Client communications and management ■ Execution of scheduled or event-triggered tasks and policies ■ Package deployment and installation ■ Reporting ■ Centralized management through a single, common interface Symantec Management Platform includes the following components: ■ Configuration Management Database (CMDB) ■ Notification Server ■ Symantec Management Console ■ Symantec Management Agent for Windows ■ Symantec Management Agent for UNIX, Linux, and Mac ■ Network Discovery ■ Software Management Framework	DOC11091

Table 1-1 Components of Client Management Suite *(continued)*

Component	Description	Link to User Guide
Deployment Solution	Deployment Solution helps to reduce the cost of deploying and managing servers, desktops, and notebooks from a centralized location in your environment. It offers operating system deployment, configuration, personality migration of computers, and software deployment across different hardware platforms and operating systems. Deployment Solution provides integrated provisioning, disk imaging, and personality migration from the Symantec Management Console. Using Symantec Ghost™, you can perform initial computer deployment using standard images and migrate user data and application settings to new computers. For the Deployment Solution 8.5 release notes, see the link at the following URL: http://www.symantec.com/docs/DOC11089	DOC11083
Inventory Solution	Inventory Solution lets you gather inventory data about the computers, users, operating systems, and installed software applications in your environment. You can collect inventory data from the computers that run Windows, UNIX, Linux, and Mac. After you gather inventory data, you can analyze it using predefined or custom reports.	DOC11109
Inventory for Network Devices	Inventory for Network Devices gathers inventory data from the devices that are not managed through the Symantec Management Agent. You can gather inventory on the devices that are already discovered and exist as resources in the CMDB.	DOC11110
IT Analytics	IT Analytics Solution software complements and expands upon the traditional reporting that is offered in most Altiris solutions. It brings exciting new features and capabilities to Notification Server because it incorporates multi-dimensional analysis and robust graphical reporting and distribution features. This functionality allows users to explore data on their own, without advanced knowledge of databases or third-party reporting tools. It empowers users to ask and answer their own questions quickly, easily, and effectively.	Client Server Management content pack: DOC11099

Table 1-1 Components of Client Management Suite *(continued)*

Component	Description	Link to User Guide
Patch Management Solution	Patch Management Solution for Linux lets you scan Red Hat and Novell Linux computers for security vulnerabilities. The solution then reports on the findings and lets you automate the download and distribution of needed errata, or software updates. The solution downloads the required patches and provides wizards to help you deploy them. Patch Management Solution for Mac lets you scan Mac computers for the updates that they require. The solution then reports on the findings and lets you automate the downloading and distribution of needed updates. You can distribute all or some of the updates. Patch Management Solution for Windows lets you scan Windows computers for the updates that they require, and view the results of the scan. The system lets you automate the download and distribution of software updates. You can create filters of the computers and apply the patch to the computers that need it.	■ Patch Management Solution for Linux: DOC11111 ■ Patch Management Solution for Mac: DOC11112 ■ Patch Management Solution for Windows: DOC11113
Real-Time System Manager	Real-Time System Manager provides you detailed real-time information about a managed computer, and lets you remotely perform different administrative tasks in real time. Real-Time System Manager also lets you run some of the management tasks on a collection of computers. You can run the tasks immediately, or on a schedule.	DOC11105
Software Management Solution	Software Management Solution provides intelligent and bandwidth-sensitive distribution and management of software from a central Web console. It leverages the Software Catalog and Software Library to ensure that the required software gets installed, remains installed, and runs without interference from other software. Software Management Solution also lets users directly download and install approved software or request other software.	DOC11114

Table 1-1 Components of Client Management Suite *(continued)*

Component	Description	Link to User Guide
Workflow Solution	Symantec Workflow is a security process development framework that you can use to create both automated business processes and security processes. These processes provide for increased repeatability, control, and accountability while reducing overall workload. The Symantec Workflow framework also lets you create Workflow processes that integrate Symantec tools into your organization's unique business processes. Once deployed, Workflow processes can respond automatically to environmental variables. Workflow processes can also allow for human interface points when a process calls for someone to make a decision with accountability. For the Workflow Solution release notes, see the link at the following URL: http://www.symantec.com/docs/DOC11090	DOC11087

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 ■ User Guides	■ Information about new features and important issues. ■ Information about how to use this product, including detailed technical information and instructions for performing common tasks.	IT Management Suite (ITMS) 8.5 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: ■ Click the page and then press the F1 key. ■ Use 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.	Knowledge Base
Cloud Unified Help System	All available IT Management Suite and solution guides are accessible from this Symantec Unified Help System that is launched on cloud.	Unified Help System

Table 1-3 Symantec product information resources *(continued)*

Resource	Description	Location
Symantec Connect	An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products.	The links to various groups on Connect are as follows: ■ Deployment and Imaging ■ Discovery and Inventory ■ ITMS Administrator ■ Mac Management ■ Monitor Solution and Server Health ■ Patch Management ■ Reporting ■ ServiceDesk and Workflow ■ Software Management ■ Server Management ■ Workspace Virtualization and Streaming

Chapter 2

Getting started with Client Management Suite

This chapter includes the following topics:

About installing Client Management Suite

To install Client Management Suite, you use Symantec Installation Manager. You can download the installation files directly to your server or you can create offline installation packages.

For more information, see the *Installing IT Management Suite* chapter in the *IT Management Suite Planning for Implementation Guide*.

After you install the Suite, refer to the individual solution documentation for information on how to configure and use it.

See "Components of Client Management Suite " on page 7.

Preparing managed computers for evaluating Client Management Suite

The following is the process to prepare the computers in your environment for evaluating Client Management Suite.

Symantec recommends that you evaluate Client Management Suite on an isolated group of computers in a lab environment.

Table 2-1 Process for preparing target computers for evaluating Client Management Suite

Step	Action	Description
Step 1	(Optional) Discover computers in your environment.	You can discover the computers that are not yet managed by Symantec Management Agent. If you know the host names or the IP addresses of the computers on which you want to evaluate Client Management Suite, the discovery is optional. For more information about discovering computers, see the *IT Management Suite Administration Guide*.
Step 2	Configure your Windows computers to allow Symantec Management Agent to push installation.	You can configure computers manually for evaluation. You can also use a group policy to configure the firewall and other settings on all or a group of computers in your network. See "Symantec Management Agent for Windows installation prerequisites" on page 15.
Step 3	Install Symantec Management Agent	Symantec Management Agent establishes communication between Notification Server and the computers in your network. Notification Server interacts with Symantec Management Agent and lets you monitor and manage each computer from the Symantec Management Console. See "Installing the Symantec Management Agent for Windows with a manual push" on page 16. For evaluation, you can also use another method of installing Symantec Management Agent, such as pull install. For more information on the methods of installing the Symantec Management Agent, see the *IT Management Suite Administration Guide*.
Step 4	(Optional) Configure the Symantec Management Agent settings for evaluation use.	To ease the configuration and evaluation of Client Management Suite, make Symantec Management Agent request the configuration from Notification Server more frequently. See "Configuring the Symantec Management Agent settings for evaluation use" on page 18.

Table 2-1 Process for preparing target computers for evaluating Client Management Suite *(continued)*

Step	Action	Description
Step 5	Install or upgrade the plug-ins.	In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**. In the left pane, under **Agents/Plug-ins**, locate and turn on the installation or upgrade policies for the plug-ins, according to your needs. See "Installing the Inventory and Application Metering plug-ins" on page 19. See "Upgrading the Inventory and Application Metering plug-ins" on page 20. See "Installing or upgrading the Software Management Solution plug-in" on page 21.

After you prepare the client computers, you can do the following:

- Collect application usage data and create custom reports to view the collected data.
  See "Metering application usage and creating custom reports" on page 24.
- Enable software usage tracking, and then uninstall the software from the managed computers that do not use it.
- Deploy the required plug-ins, and then run tasks to collect inventory information and change power scheme settings on the managed computers.
  See "About managing power scheme settings" on page 59.

Symantec Management Agent for Windows installation prerequisites

Before you can install Symantec Management Agent, you need to configure the computers and verify that they meet the installation prerequisites.

This task is a step in the processes for installing Symantec Management Agent manually on Windows computers.

Table 2-2 Symantec Management Agent for Windows installation prerequisites

Prerequisite	Description
Operating system	Symantec Management Platform and Altiris Solutions Support Matrix
Hard disk space	60 MB minimum
RAM	64 MB minimum (128 MB recommended)

Table 2-2 Symantec Management Agent for Windows installation prerequisites *(continued)*

Prerequisite	Description
Internet Explorer	Version 6.0 or later
Access rights	Local administrator rights
Firewall	The computer must be able to communicate with Symantec Management Platform through the computer's firewall. Perform any of the following: ■ Enable **File and Printer Sharing** in the firewall settings. ■ Add port UDP 138, TCP 445, TCP 80 (or TCP 443 for HTTPS) and ICMP type 8 as inbound port exceptions. You can add the ports by using a group policy. ■ Turn off the firewall.
Simple file sharing (Windows XP in non-domain only)	For non-domain client computers running Windows XP, you must also disable **Use simple file sharing** in **Folder Options** in Windows XP.
UAC (Windows Vista and Windows 7 in non-domain only)	For non-domain client computers running Windows Vista or Windows 7, you must also turn off the User Access Control (UAC).

Installing the Symantec Management Agent for Windows with a manual push

You can push Symantec Management Agent to any Windows computers. Before you can manually install or uninstall Symantec Management Agent from the **Symantec Management Agent Install** page, you need to choose the target computers. You can enter the computer names manually, choose the computers that have been discovered with resource discovery, or import the computers from a CSV file. The CSV file is a comma-delimited text file. The file includes the DNS names or the IP addresses of the client computers on which you want to install Symantec Management Agent. For Windows computers, the CSV file is a list of computer names or IP addresses that are imported into the **Symantec Management Agent Install** page. Items are interpreted as the names of computers or the IP addresses of computers (for the entries that are in the appropriate format). No spaces are allowed: any item that contains a space is ignored.

Note: You can manually install Symantec Management Agent only on the computers that were discovered using **Domain Resource Discovery** or **Network Discovery**.

This task is a step in the processes for installing the Symantec Management Agent on Windows computers.

To install the Symantec Management Agent for Windows with a manual push

1. In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Push Symantec Management Agent**.
2. On the **Symantec Management Agent Install** page, on the **Install Agent** tab, under **Roll out Agent to Computers**, choose the computers on which to install Symantec Management Agent, and then click **Install**.

To manually add a computer.	In the text box, type the IP Address, FQDN, name, or name@domain of the computer, and then click **Add**. When you type **name@domain**, the system splits the name into two and tries to match the existing resource by both fields. If the full match is not found, the rest of the fields are not populated for this entry.
To choose from the available computers.	1 Click **Select Computers**. 2 In the **Select Computers** dialog box, add the appropriate computers from the **Available computers** list to the **Selected computers** list, and then click **OK**.
To import computers from a CSV file.	1 Under **Roll out Agent to Computers**, on the toolbar, click the **Import computers from a selected file** symbol. 2 In the **Select file to import** dialog box, choose the appropriate CSV file, and then click **Open**.

3 (Optional) Under **Roll out Agent to Computers**, using the icons on the toolbar, you can do the following:

View or edit a selected entry.	Select the computer in the list and click the **Edit** icon. In the **Edit entry** dialog box, the fields under the **Entry fields** section are editable and let you update the data in the **AgentPushData** table. The fields under the **Resolved fields** section are automatically filled with the data of a matched entry in database. These fields are not editable.
Rediscover the selected entries.	Select the computers in the list, and then click the **Rediscover selected computer details** icon. Rediscovering lets you search for additional information about the selected computers. For example, domain, operating system details, etc.
View different selections of entries in the grid.	In the **View** drop-down list, click the selection that you want to view. You can view the computers that are manually added, the computers that are automatically added when the **Scheduled Push to Computers** is enabled, or both.

4 In the **Symantec Management Agent Installation Options** dialog box, configure the installation settings according to your needs, and then click **Proceed With Install**.

For more information, click the page and then press **F1**.

On the **Symantec Management Agent Install** page, under **Roll out Agent to Computers**, in the computer list, the **Status** column shows the success or failure of the installation on each computer. Note that the newly installed Symantec Management Agent reports its status back to the originating Notification Server, even if it is going to be managed by another Notification Server.

Configuring the Symantec Management Agent settings for evaluation use

(Optional)

By default, Symantec Management Agent requests new configuration from Notification Server once per hour. This means that it can take up to one hour for a rollout policy to reach the target computer.

If you are evaluating this solution in a lab environment, you can change the configuration request interval to speed up the evaluation process.

The next time Symantec Management Agent downloads configuration information, these settings take effect. If you used the default agent configuration settings before the change, updates can take up to one hour before these changes are effective.

To configure the Symantec Management Agent for evaluation use

1. In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > Targeted Agent Settings**.
2. In the left pane, under **Policy Name**, click the policy that you want to configure.
3. In the right pane, on the **General** tab, in the **Download new configuration every** box, change the value to 5 minutes.

   This forces the agent to check for changes more frequently.
4. In the **Upload basic inventory every** box, change the value to 15 minutes.

   This forces inventory data to be sent more frequently.
5. Click **Save changes**.

Installing the Inventory and Application Metering plug-ins

To gather inventory data on managed computers, you must install Inventory Plug-in on them.

To meter applications on managed computers, you must install Application Metering Plug-in. These plug-ins work with Symantec Management Agent to perform tasks on the managed computers and communicate with Notification Server.

If you have Inventory Pack for Servers, you can also use the Inventory Pack for Servers Plug-in.

Note: You can track usage of managed software products, meter, and deny Win64 and Win32 applications on Windows XP and above managed client computers.

You can track usage of managed software products on Mac client computers.

Software-based usage tracking and application metering are not supported on Windows and Mac servers.

To install a plug-in, you configure the policy that installs the plug-in on managed computers. You choose the group of computers on which the policy runs, and when it runs. If you choose a group that contains a computer that already has the plug-in installed, the task is ignored on that computer. When you turn on the policy, the plug-in is automatically installed on any new computer that is a member of the target group.

By default, no plug-in installation policies are turned on. If you install Inventory Solution for the first time, you must manually turn on the policies to install the Inventory and Application Metering plug-ins.

You can install Inventory plug-in and Application Metering plug-in separately. However, if only Application Metering plug-in is installed on the client computer, but the Inventory plug-in is not, there are the following limitations:

- You cannot gather information about installed software and files using Inventory policies and tasks.
- You cannot track software products if information about installed software is not gathered on these computers.
- The **Underutilized Software** report only shows the information about client computers on which metered software has been recognized as installed.

Before you perform this task, you must install Symantec Management Agent on target computers.

This task is a step in the process for preparing managed computers for inventory and metering.

To install the Inventory or Application Metering plug-ins

1. In the **Symantec Management Console**, on the **Actions** menu, click **Agents/Plug-ins > Roll out Agents/Plug-ins**.
2. In the left pane, under **Agents/Plug-ins**, expand **Discovery and Inventory > Windows/UNIX/Linux/Mac**, and then click the policy for the plug-in that you want to install.
3. In the right pane, on the toolbar, click **Apply to** to choose the computers on which you want to install the plug-in.

   For more information, see the topics about specifying the targets of a policy and specifying filtering rules in the *IT Management Suite Administration Guide*.
4. Under **Schedule**, on the toolbar, click **Add schedule**, and then schedule the policy to run on managed computers.
5. On the plug-in install page, turn on the policy.

   At the upper right of the page, click the colored circle, and then click **On**.
6. Click **Save changes**.

The next step is to gather inventory on your client computers.

See "Gathering inventory with predefined inventory policies" on page 26.

Upgrading the Inventory and Application Metering plug-ins

If you upgrade from a previous version of Inventory Solution, and you previously installed the Inventory or Application Metering plug-ins, you must upgrade the plug-ins on client computers.

To upgrade a plug-in, you turn on an upgrade policy that is located with the plug-in installation policy.

This task is a step in the process for preparing managed computers for inventory and metering.

To upgrade the Inventory or Application Metering plug-ins

1. In the **Symantec Management Console**, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**.
2. In the left pane, expand **Discovery and Inventory > Windows/UNIX/Linux/Mac**, and then click the policy for the plug-in that you want to upgrade.

   The upgrade policy for x64 plug-in is received by 64-bit client computers. The x86 plug-in policy is received by 32-bit computers. You cannot install a 32-bit plug-in on a 64-bit client computer.

   Note: The cloned policies that you have created with Inventory Solution 7.5 SP1 and earlier still attempt to install or upgrade 32-bit plug-ins on 64-bit client computers. These policies fail due to the change introduced in Inventory Solution 7.6.

3. On the plug-in upgrade page, turn on the policy.

   At the upper right of the page, click the colored circle, and then click **On**.
4. Click **Apply to** to select the computers on which you want to upgrade the plug-in.

   For more information, see the topics about specifying the targets of a policy and specifying filtering rules in the *IT Management Suite Administration Guide*.
5. Schedule the policy to run on managed computers.

   For more information, see the topic about adding a schedule to a policy, task, or job in the *IT Management Suite Administration Guide*.
6. Click **Save changes**.

Installing or upgrading the Software Management Solution plug-in

Before you can deliver or manage software on client computers with Software Management Solution, you must install the Software Management Solution plug-in on those computers.

If you upgraded from a 7.x version of Software Management Solution, you must upgrade the Software Management Solution plug-in that is installed on the managed computers.

For more information about upgrade and data migration, see the *IT Management Suite Installation and Upgrade Guide*.

You install the Software Management Solution plug-in to Windows and non-Windows computers using the **Software Management Solution Plug-in Install** policy.

This task is a step in the process for implementing Software Management Solution.

To install or upgrade the Software Management Solution plug-in

1. In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > All Agents/Plug-ins**.
2. In the left pane, under **Agents/Plug-ins**, expand **Software > Software Management**, and then click one of the following policies:
   - **Software Management Solution Plug-in Install**
     Click if it is a new installation of the product.
   - **Software Management Solution Plug-in Upgrade**
     Click if you upgraded from the 7.x version of the product.
3. In the right pane, check or uncheck **Enable Verbose Reporting of Status Events** according to your needs.

   This option records the detailed events that are related to the installation and posts them to the Notification Server computer.
4. Under **Applied to**, on the toolbar, click **Apply to**, and then choose where to install the agent.

   For more information, see the *IT Management Suite Administration Guide*.
5. Under **Schedule**, next to **Run**, select the method to run the policy as follows:
   - To run the policy once and as soon as possible, click **Once ASAP**.
   - To run the policy once while maintenance window is open, click **Once at next maintenance window**.
   - To schedule the policy, click **By schedule**, on the toolbar, click **Add schedule**, and then configure the schedule for the policy.

   Note that if you turn off and then turn on the policy, it cannot run on the same computer again. To run a policy on the same computer again, you must configure it to run on a schedule.

6 (Optional) Under **Extra schedule options**, configure following options:

User can run	Allows the user on the client computer to run the policy manually.
Notify user when the task is available	Displays a message to notify the user that new software is available. When the user clicks the message, the **New Software is Available** dialog box opens. The user can start, dismiss, or defer the policy. If you do not choose to prompt the user, the **New Software is Available** dialog box does not appear. The **New Software is Available** dialog box appears only if **Show popup notifications** is checked. This option does not apply to UNIX and Linux.
Warn before running	Displays the **Starting Task** dialog box to notifiy the user before the policy runs. Unless you let the user defer the policy, the policy starts 60 seconds after the **Starting Task** dialog box appears. A progress bar shows the amount of time that remains. The user can dismiss the **Starting Task** dialog box but cannot cancel the policy unless you checked **User can run**. The **Starting Task** dialog box appears only if the **Show popup notifications** is checked in the client computer's Symantec Management Agent settings. This option does not apply to UNIX or Linux.

7 Turn on the policy.

At the upper right of the page, click the colored circle and then click **On**.

8 Click **Save changes**.

Chapter 3

Metering application usage and creating custom reports

This chapter includes the following topics:

Metering application usage and creating custom reports

Client Management Suite lets you collect various data from the managed computers, store the data in the Configuration Management Database (CMDB), and then create custom reports that display that data.

Below is a sample process for creating a custom report that displays the collected Adobe software inventory and usage data. You can use this report for a software audit or to determine the computers on which the software in not used. You can then use Software Management Solution to uninstall the software from these computers and reclaim licenses.

In the following example, you use Inventory Solution to collect data about installed Adobe software, and then track the software usage with the application metering feature of Inventory Solution.

Note: Application metering is supported for Windows only. The software usage information is limited to Windows XP and above.

Table 3-1 Process for application usage metering and creating custom reports

Step	Action	Description
Step 1	Meet the prerequisites.	You must have Symantec Management Agent installed on the client computers. See "Preparing managed computers for evaluating Client Management Suite" on page 13.
Step 2	Install the Inventory and Application Metering plug-ins.	See "Installing the Inventory and Application Metering plug-ins" on page 19. For more detailed information, see the *Preparing managed computers for inventory and metering* topic in the *Inventory Solution User Guide*. Note that you use policies to install the plug-ins on the client computers. If you use default settings, it can take up to one hour for Symantec Management Agent to request the configuration update, receive the policy and install the plug-in. You can request configuration manually from the Symantec Management Agent GUI, or by running the **Update Client Configuration** client task
Step 3	Collect full inventory.	The predefined inventory policies are enabled by default and configured to run ASAP on every computer with the Inventory plug-in installed. Then, policies run daily , weekly or monthly to send the updated inventory information to Notification Server. For example, the **Collect Full Inventory** policy is set by default to run once on every computer ASAP, and then every Monday at 18:00. You can configure the policy schedule according to your needs. See "Gathering inventory with predefined inventory policies" on page 26.
Step 4	Create an application metering policy for the software.	The application metering policy records application start and stop events, and sends the application usage data to Notification Server. See "Enabling application usage metering for Adobe applications" on page 27.

Table 3-1 Process for application usage metering and creating custom reports *(continued)*

Step	Action	Description
Step 5	Create a custom audit report and view inventory data.	You create a report that displays data about the number of software components that are installed on the client computers and the number of times the software has been used. You can use the following methods to create a custom report: ■ Plain text SQL See "Creating a custom audit report for Adobe using plain-text SQL" on page 29. ■ The Symantec Management Console Query Builder See "Creating a custom audit report for Adobe using Query Builder" on page 32. Using plain text SQL gives you more flexibility, but if you don't have extensive SQL language knowledge, you can use Query Builder to build a custom report. However, using Query Builder requires the knowledge of the CMDB tables and the data that they contain.
Step 6	(Optional) Create a drill-down report.	You can create a drill-down report. For example, you can create reports that show the list of computers on which a particular software product is installed. See "Creating a drill-down computer report" on page 40.
Step 7	(Optional) Use other methods to view software inventory and application metering data.	Client Management Suite provides reports and dashboards that let you view software inventory, application metering data, and other types of data. See "Other methods of viewing software usage data" on page 45.

Gathering inventory with predefined inventory policies

You can gather inventory data from managed computers with predefined inventory policies. You can also configure the predefined policies to meet your needs. If you want to configure a predefined policy, Symantec recommends that you clone it, and then configure the copy.

Note: You can manually run an original or modified predefined inventory policy on the managed Windows computers. You can do it after the policy automatically runs on the computer at least once.

Before you perform these steps, ensure that you have prepared the managed computers for inventory.

To turn on predefined inventory policies

1. In the **Symantec Management Console**, on the **Manage** menu, click **Policies**.
2. In the left pane, expand **Discovery and Inventory > Inventory**, and then click the predefined inventory policy that you want to use.
3. On the inventory policy page, turn on the policy.

   At the upper right of the page, click the colored circle, and then click **On**.
4. Click **Save changes**.

To clone and configure predefined inventory policies

1. In the **Symantec Management Console**, browse to the predefined inventory policy that you want to clone.
2. Right-click the policy, and then click **Clone**.
3. Give the cloned policy a unique name, and then click **OK**.
4. On the inventory policy page, configure the policy options according to your needs.

   For more information about the options, click the page, and then press the **F1** key.
5. On the inventory policy page, turn on the policy.

   At the upper right of the page, click the colored circle, and then click **On**.
6. Click **Save changes**.

The next step is to wait for the client computers to receive the new policy and report the inventory results, and then view the data that is stored in the Configuration Management Database (CMDB).

Enabling application usage metering for Adobe applications

To meter application usage, you create an application metering policy. On the policy page, you create application definitions for the software that you want to meter. For each metering policy, you can define one or more software components. Application metering functionality is a component of the Client Management Suite.

Inventory Solution also lets you track software usage on the software product level.

In the example below, you create an application metering policy that monitors start events for the executables with the file properties containing "Adobe".

Note: Depending on how you configure the application metering policy, it can take some time for the application usage data to arrive to Notification Server and be stored in the Configuration Management Database (CMDB).

To enable usage metering for Adobe applications

1. In the Symantec Management Console, on the **Manage** menu, click **Policies**.
2. In the left pane, expand **Software**, right-click **Application metering**, and then click **New > Application metering policy**.
3. On the **New Application metering policy** page, give the policy a unique name and description.
4. On the policy page, on the **Software** tab, on the toolbar, click **Add > Rule**.
5. In the **Add Application Rule** dialog box, in the **Definition name** box, type **Adobe**. In the **Product name** box, type ***Adobe***, and then click **OK**.
6. On the **Options** tab, check **Record usage events**, and then, in the drop-down lists on the right, click **Start** and **Daily**.

   These settings instruct the policy to record application startup events and send the summary data to Notification Server daily.
7. Click **Save changes**.

The following is the procedure for testing the application metering rule.

To test the application metering rule

1. On client computer that belongs to the **Windows Computers with Application Metering Plug-in** targets, open the Symantec Management Agent GUI.

   For example, double-click the Symantec Management Agent icon on the taskbar.
2. In the Symantec Management Agent GUI, on the toolbar, click **Settings**, and then click **Update Configuration** to request configuration policies from Notification Server.
3. Verify that the new application metering policy has arrived to the client computer.

   If the policy arrived, you can see the name of the policy in the client configuration policy XML file at the following location: `C:\Program Files\Altiris\Altiris Agent\Client Policies`.

   In this example, look for *Adobe*.

4 Run an Adobe application.

5 The application usage information is sent to the Notification Server computer according to the interval that you specified for the Record usage events option.

In this example, the data is sent to the Notification Server daily.

Creating a custom audit report for Adobe using plain-text SQL

After you enable application metering, you can create a custom report using a plain-text SQL query. You can also add parameters to an SQL query-based report.

You can use the Symantec Management Console Query Builder to create custom reports.

See "Creating a custom audit report for Adobe using Query Builder" on page 32.

Note: Symantec recommends that you save the report regularly while making changes to the report. This reduces the chances of the Symantec Management Console timing out and losing your changes. To save the changes you made to the report, you can click either **Save Changes** or **Apply**. To return to the report, click **Edit**.

The query that you use in this example is as follows:

```
SELECT

ifd.DisplayName,

ifd.Publisher,

COUNT(DISTINCT ifd._ResourceGuid) AS 'Installed',

COUNT(DISTINCT cm.Metered) AS 'Metered',

COUNT(DISTINCT eas._ResourceGuid) AS 'Used'

FROM ( SELECT DISTINCT _ResourceGuid, DisplayName, Publisher,
ParentResourceGuid, ChildResourceGuid FROM Inv_AddRemoveProgram iarp JOIN
ResourceAssociation ra ON iarp._SoftwareComponentGuid = ra.ParentResourceGuid
WHERE Publisher LIKE '%Adobe%' ) ifd

LEFT JOIN ( SELECT DISTINCT ResourceGuid AS Metered FROM CollectionMembership
WHERE CollectionGuid = 'f5758af1-eb77-436f-b63f-e75473cf3c09' ) cm ON cm.Metered
= ifd._ResourceGuid

LEFT JOIN ( SELECT DISTINCT _ResourceGuid, FileResourceGuid FROM
Evt_Application_Start ) eas ON eas.FileResourceGuid = ifd.ChildResourceGuid
AND eas._ResourceGuid = ifd._ResourceGuid
```

```
GROUP BY

ifd.Publisher,

ifd.DisplayName

ORDER BY

Used DESC,

Publisher ASC
```

This query selects all software resources that display Adobe as the publisher in the Windows **Add/Remove Program** dialog box (`WHERE Publisher LIKE '%Adobe%`). The count of computers with this software will be displayed in the **Installed** column. You will replace the `%Adobe%` substring with a report parameter later in the process.

In the `LEFT JOIN` statement that follows, the query gets the count of computers that can be metered. Inventory Solution can collect inventory from both server and workstation operating systems, but application metering is available for workstations only. When you run the report, the count of workstations with this software is displayed in the **Metered** column. This particular example uses the collection that is used by the default application metering policy. Note that if you use a non-default target to meter Adobe software, the data in the **Metered** column will be inaccurate. If the data is inaccurate, you can further customize the report.

The last `LEFT JOIN` statement gets the count of computers on which an application from Adobe was executed and displays it as **Used**.

Note: This is a simplified query and it does not let you specify a time interval for which to display metering data. You can add these parameters later.

To create a custom audit report for Adobe using plain-text SQL

1. In the **Symantec Management Console**, on the **Reports** menu, click **All Reports**.
2. In the left pane, under **Reports**, expand **Discovery and Inventory > Inventory > Cross-platform > Software/Applications**.
3. Under **Software/Applications**, right-click the **Software** folder, and then click **New > Report > SQL Report**.
4. On **New SQL Report** page, rename the report.

   For example, rename the report to **Adobe audit (SQL)**.
5. Click the **Parameterised Query** tab, and then, in the text box, delete all the default query text.
6. Copy the SQL query that is provided in this topic and paste it into the text box.
7. Click **Save Changes**.

To add a parameter to the plain-text SQL report

1 On the report page, click the **Report Parameters** tab.

2 On the toolbar, click **Add > New Parameter**.

3 In the **Editing Parameter** dialog box, configure the following settings:

Name	Type **Publisher**.
Description	Type **Publisher**.
Default Value	Type **%**.
Test Value	Type **%Adobe%**.

4 Under **Value Provider**, in the **Name** drop-down list, click **Basic Parameter Value Edit Control**, and then, under **Configuration**, in the **Label Text** box, type **Publisher**.

5 Click **OK**.

6 On the report page, click the **Data Source** tab, and then click the **Query Parameters** tab.

7 On the toolbar, click **Add > Publisher**.

8 Click the **Parameterised Query** tab.

9 In the text box, before the query, add the following lines:

```
DECLARE @v3_Publisher nvarchar(max)

SET @v3_Publisher = N'%Publisher%'
```

10 In the SQL query, locate the following string:

```
LIKE '%Adobe%'
```

and replace it with the following:

```
LIKE @v3_Publisher
```

11 Click **Save Changes**.

To test the report, you can type **%oracle%** in the **Publisher** box. Then refresh the report, and see if it displays the list of Oracle software that is discovered by Inventory Solution.

See "Creating a drill-down computer report" on page 40.

Creating a custom audit report for Adobe using Query Builder

After you enable application metering, you can use Query Builder to create a custom report in the Symantec Management Console.

You can also build a custom report using a plain-text SQL query.

See "Creating a custom audit report for Adobe using plain-text SQL" on page 29.

For more information, see the topics about creating custom Notification Server reports in the *IT Management Suite Administration Guide*.

Note: Symantec recommends that you save the report regularly while making changes to the report. This reduces the chances of the Symantec Management Console timing out and losing your changes. To save the changes you made to the report, you can click either **Save Changes** or **Apply**. To return to the report, click **Edit**.

To create a new report and add tables and associations

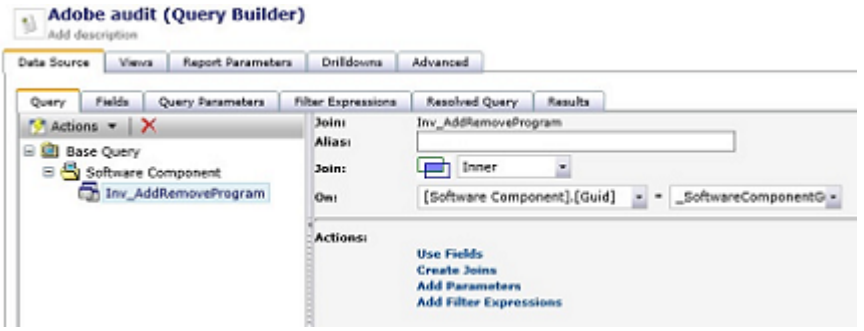
1. In the **Symantec Management Console**, on the **Reports** menu, click **All Reports**.
2. In the left pane, expand **Discovery and Inventory > Inventory > Cross-platform > Software/Applications**.
3. Under **Software/Applications**, right-click **Software**, and then click **New > Report > Computer Report**.
4. On the **New Computer Report** page, type a new name for this report.

   For example, type **Adobe audit (Query Builder)**.
5. On the **Query** tab, click **Base Query**, and then, on the right, in the **Base Resource Type** drop-down list, click **Software Component**.

   When a dialog box opens, click **OK**.
6. On the **Query** tab, under **Base Query**, click **Software Component**, and then, under **Actions**, click **Create Joins**.

7 In the **Joins** dialog box, create a table join as follows:

Inner join **Inv_AddRemoveProgram** on **[Software Component].[Guid]** = **_SoftwareComponentGuid**.



Click **OK**.

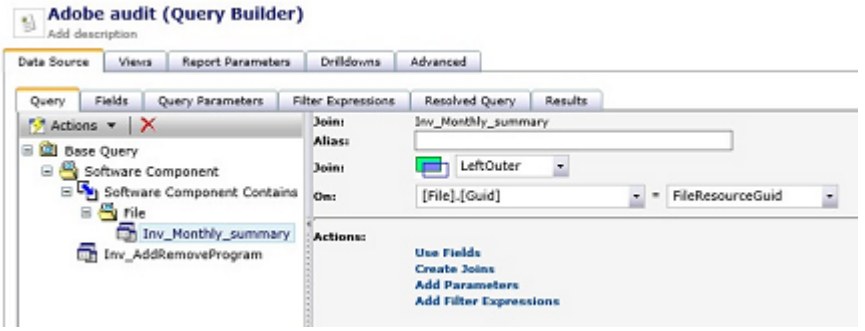
8 On the **Query** tab, under **Base Query**, click **Software Component**, and then, on the right, under **Actions**, click **Use Resource Type Associations**.

9 In the **Resource Type Associations** dialog box, in the drop-down list, click **[Software Component Contains File] to [File]**, and then click **OK**.

10 On the **Query** tab, under **Software Component Contains**, click **File**, and then, on the right, under **Actions**, click **Create Joins**.

11 In the **Joins** dialog box, create a table join as follows:

Left Outer join **Inv_Monthly_summary** on **[File].[Guid]** = **FileResourceGuid**.

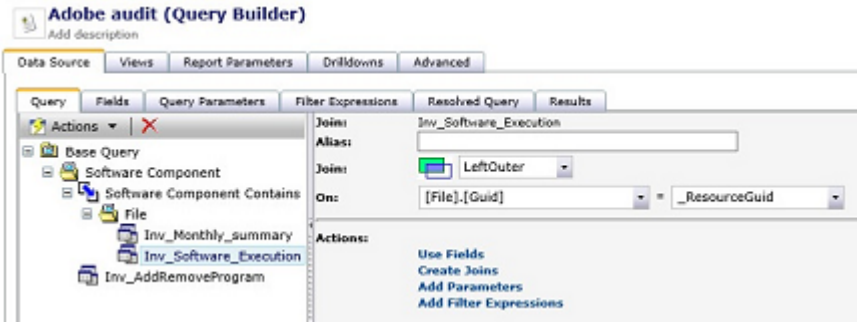


Click **OK**.

12 On the **Query** tab, under **Software Component Contains**, click **File**, and then, on the right, under **Actions**, click **Create Joins**.

13 In the **Joins** dialog box, create a table join as follows:

LeftOuter join **Inv_Software_Execution** on **[File].[Guid]** = **_ResourceGuid**.



Click **OK**.

14 Click **Save Changes**.

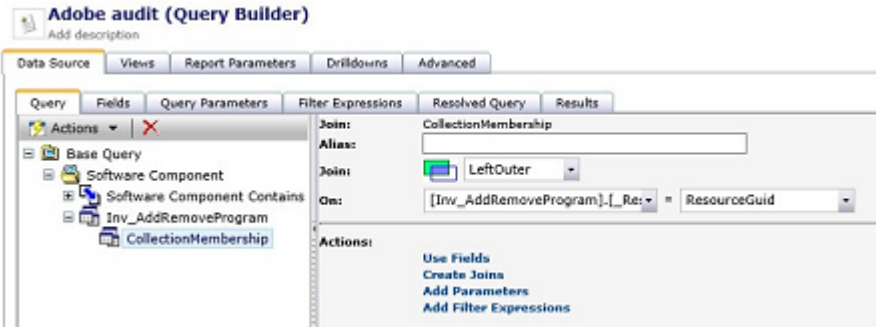
Next, add the third table, which will be used to get the count of computers that can be metered. You must then add a filter expression that lets you exclude the operating systems that are not supported by the Application Metering Plug-in.

In this example, you filter the results by GUID `f5758af1-eb77-436f-b63f-e75473cf3c09`, which is a GUID of the **Windows Computers with Application Metering plug-in**.

To join the CollectionMembership table and add a filter expression

1. On the **Query** tab, under Base Query, click **Inv_AddRemoveProgram**, and then, in the right pane, under **Actions**, click **Create Joins**.
2. In the **Joins** dialog box, create a table join as follows:

   Left Outer join **CollectionMembership** on **[Inv_AddRemoveProgram].[_ResourceGuid] = ResourceGuid**.



   Click **OK**.

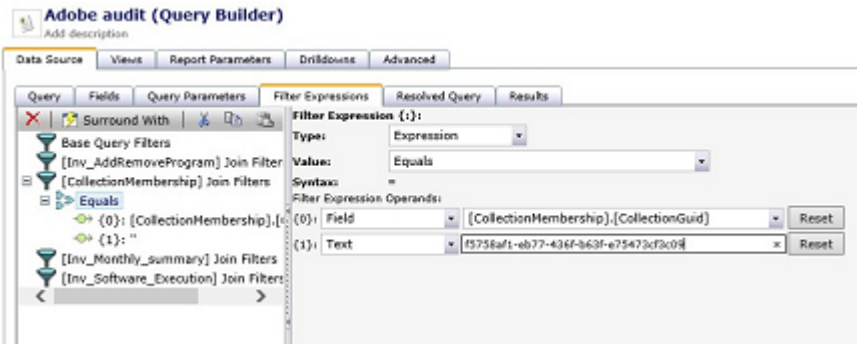
3. On the **Filter Expressions** tab, click **Switch to Advanced Mode**.
4. In the left pane, click **[CollectionMembership] Join Filters**.
5. In the right pane, in the drop-down list, click **Equals**.

   When a dialog box opens, click **OK**.

6 For the first filter operand, under **Filter Expression Operands**, in the **{0}:**: drop-down list, click **Field**, and then, in the right drop-down list, click **[CollectionMembership].[CollectionGuid]**.

For the second operand, under **Filter Expression Operands**, in the **{1}:**: drop-down list, click **Text**, and then, to the text box on the right, paste the following GUID:

```
f5758af1-eb77-436f-b63f-e75473cf3c09
```



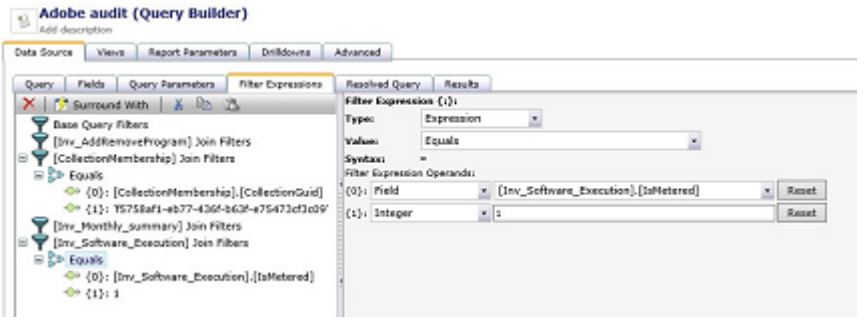
7 In the left pane, click **[Inv_Software_Execution] Join Filters**.

8 In the right pane, in the drop-down list, click **Equals**.

When a dialog box opens, click **OK**.

9 For the first filter operand, under **Filter Expression Operands**, in the **{0}:** drop-down list, click **Field**, and then, in the right drop-down list, click **[Inv_Software_Execution].[IsMetered]**.

10 For the second operand, under **Filter Expression Operands**, in the **{1}:** drop-down list, click **Integer**, and then, to the text box on the right, type **1**.



11 Click **Save changes**.

In the next step, you choose the table fields that will appear in the report. You also aggregate data and choose the sort order.

The following list shows the fields that you must add to the report when you perform the next procedure.

[Inv_AddRemoveProgram].[DisplayName]	Displays the software name, as shown in the Windows Add/Remove Programs window. In the **Alias** box, type **Name**.
[Inv_AddRemoveProgram].[Publisher]	Displays the software publisher, as shown in the Windows Add/Remove Programs window. In the **Alias** box, type **Publisher**.
[Inv_AddRemoveProgram].[_ResourceGuid]	Displays the count of computers (both servers and workstations) with this software installed. In the **Alias** box, type **Installed**. In the **Aggregate** drop-down list, click **Count Distinct**.
[Inv_Software_Execution].[IsMetered]	Displays the count of workstations with this software installed. In the **Alias** box, type **IsMetered**. In the **Aggregate** drop-down list, click **Count Distinct**.
[Inv_Monthly_Summary].[_ResourceGuid]	Displays the count of workstations on which the software has been run. In the **Alias** box, type **Used**. In the **Aggregate** drop-down list, click **Count Distinct**. (Optional) In the **Sort Direction** drop-down list, click **Descending**.

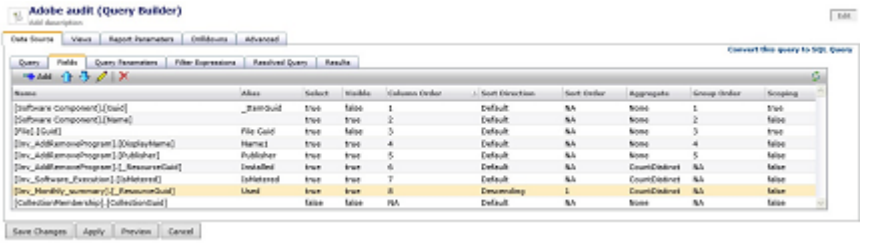
To add fields to the report

1 Open the report that you want to edit, and then click the **Fields** tab.

2 On the **Fields** tab, on the toolbar, click the **Add** symbol, and then add the fields that are shown in the left column in the table on the **Fields** tab.

Note: You can add fields one by one. You can also check **Select Multiple Fields**, and then add multiple fields from the drop-down list.

After you add the fields, you can configure them as shown in the table below.



3 On the **Fields** tab, remove all other fields except for **[CollectionMembership].[CollectionGuid]** that are not part of this list. Click a row, and then, on the toolbar, click the **Delete** symbol.

4 Click **Save changes**.

Note: [CollectionMembership].[CollectionGuid] is a required hidden field in this example, and it cannot be removed.

You can add a parameter to the report that lets you filter the results by the software publisher. First, you add a new parameter text box to the report, and then you configure the report query.

To add a parameter using Query Builder

1 Open the report you want to edit, and then click the **Report Parameters** tab.

2 On the **Report Parameters** tab, on the toolbar, click **Add > New Parameter**.

3 In the **Editing Parameter** dialog box, fill in the following text boxes:

Name	Type **Publisher**.
Descrpiption	Type **Publisher**.
Default Value	Type **%**.
Test Value	Type **%Adobe%**.

4 Under **Value Provider**, in the **Name** drop-down list, click **Basic Parameter Value Edit Control**, and then, in the **Label Text** box, type **Publisher**.

5 Click **OK**.

6 Click the **Data Source** tab, and then click the **Query Parameters** tab.

7 On the **Query Parameters** tab, on the toolbar, click **Add > Publisher**.

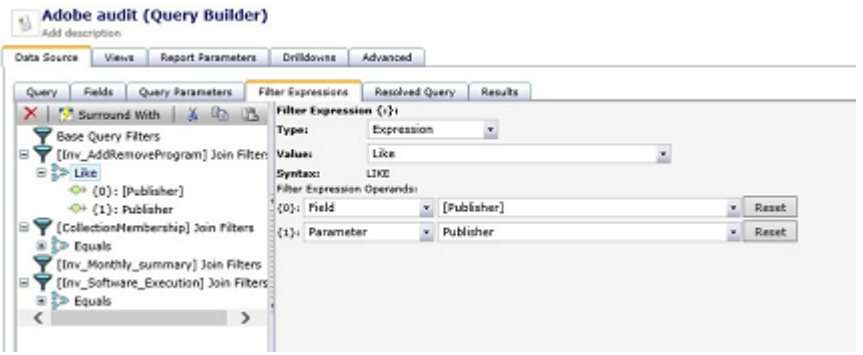
8 On the **Filter Expressions** tab, in the left pane, click **[Inv_AddRemoveProgram] Join Filters**.

9 In the right pane, in the drop-down list, click **Like**.

When a dialog box opens, click **OK** to confirm.

10 For the first filter operand, in the **{0}:** drop-down list, click **Field** and then, in the right drop-down list, click **[Publisher]**.

For the second operand, in the **{1}:** drop-down list, click **Parameter**, and then, in the right drop-down list, click **Publisher**.



11 Click **Save changes**.

See “Creating a drill-down computer report” on page 40.

Creating a drill-down computer report

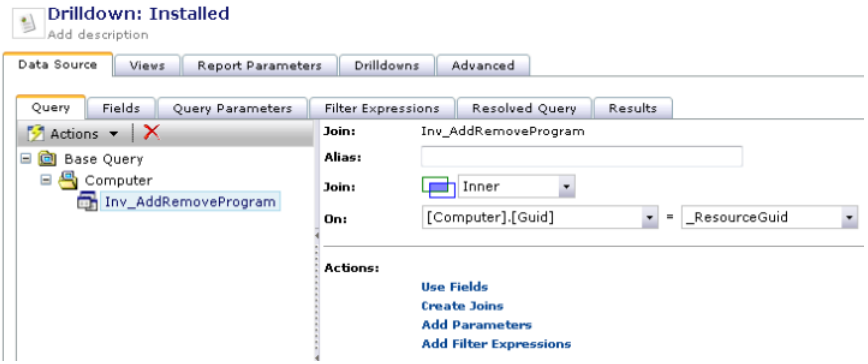
You can create a custom drill-down report and add it as a right-click menu action to the audit report that you created.

The following is an example of how to create a drill-down report that shows the list of computers that have the software installed. You can create any other report according to your needs.

To create a drill-down computer report

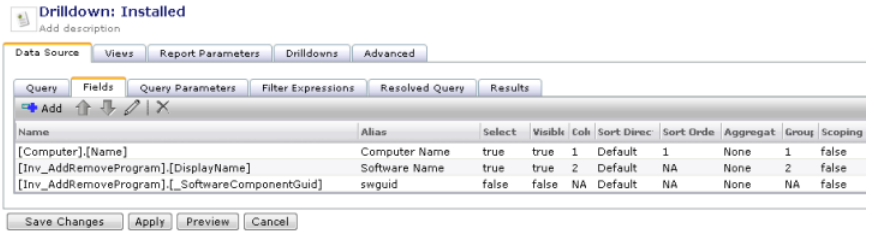
1. In the Symantec Management Platform, on the **Reports** menu, click **All Reports**.
2. In the left pane, under **Reports**, expand **Discovery and Inventory > Inventory > Cross-platform > Software /Applications**, right-click **Software**, and then click **New > Report > Computer Report**.
3. On the **New Computer Report** page, click the report name and type a new name.

   For example, type **Drilldown: Installed**.
4. On the **Query** tab, under **Base Query**, click **Computer**, and then, in the left pane, under **Actions**, click **Create Joins**.
5. In the **Joins** dialog box, create a table join as follows:
   - In the **Join** drop-down list, click **Inner**.
   - In the middle drop-down list, click **Inv_AddRemoveProgram**.
   - In the bottom drop-down lists, click the following:
     On **[Computer].[Guid]** = **_ResourceGuid**.
   - Click **OK**.



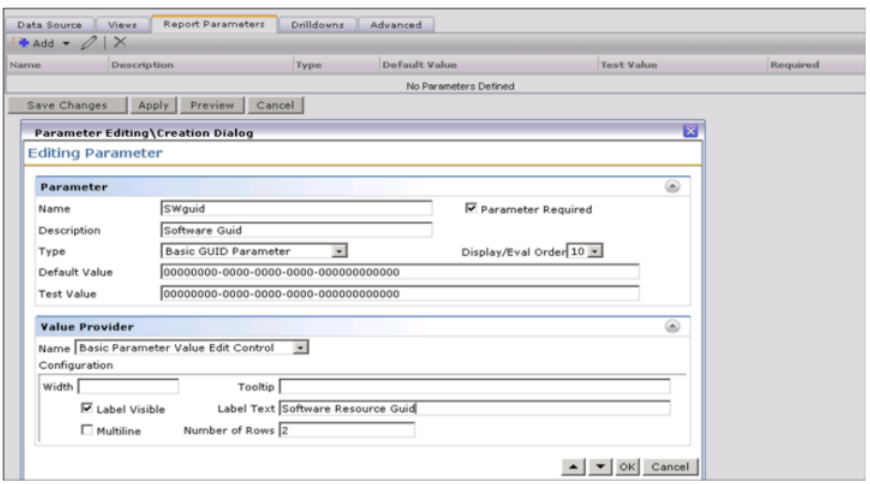
6 On the **Fields** tab, on the toolbar, click the **Add** symbol, and then add the fields that are shown below.

Configure the fields as shown.

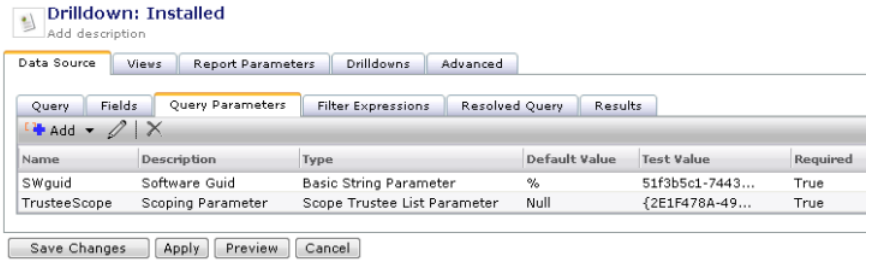


7 On the **Report Parameters** tab, on the toolbar, click **Add > New Paramater,** and then, in the **Editing Parameter** dialog box, configure the parameter as follows:

- In the **Name** box, type **SWguid**.
- In the **Description** box, type **Software Guid**.
- In the **Type** drop-down list, click **Basic GUID Parameter**.
- Check **Parameter Required**.
- Under **Value Provider**, in the **Name** drop-down list, click **Basic Parameter Value Edit Control**.
- In the **Label Text** box, type **Software Resource Guid**.
- Click **OK**.



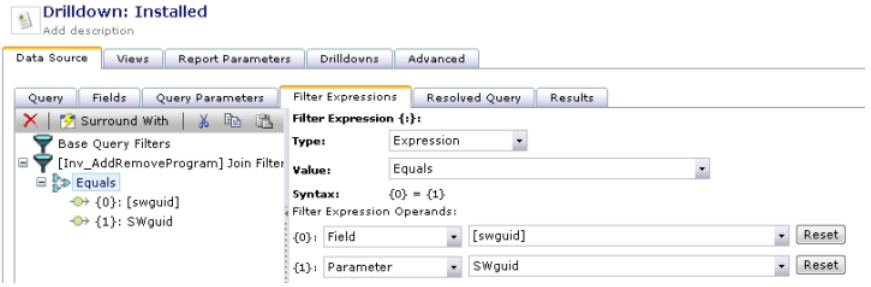
8 On the **Data Source** tab, click the **Query Parameters** tab, and then, on the toolbar, click **Add > Software Guid**.



9 On the **Filter Expressions** tab, click **Switch to Advanced Mode**, and then click **[Inv_AddRemoveProgram] Join Filters**.

10 In the right pane, do the following:

- In the top drop-down list, click **Equals**.
  When a dialog box opens, click **OK**.
- Under **Filter Expression Operands**, for the first filter operand, in the **{0}:** drop-down list, click **Field** and then, in the right drop-down list, click **[swguid]**.
- For the second filter operand, in the **{1}:** drop-down list, click **Parameter**, and then, in the right drop-down list, click **SWguid**.



11 Click **Save Changes**.

To create a right-click drill-down menu

1 Open the report that you created with Query Builder.

2 Add a new **[Inv_AddRemoveProgram].[_SoftwareComponentGuid]** field to the report, and make it invisible.

3 On the **Drilldowns** tab, click **Remove** to remove the default **ShowContextMenu** drilldown.

4 Click **Add**.

5 In the **Name** box, type **Show Installed**.

6 In the **Performs** drop-down list, click **Drilldown To Report**.

7 Under **Action Configuration**, click **No report selected**, and then search for and select the drill-down report that you created.

8 Under **Passing Parameter**, click the **Add** symbol.

9 In the **Pass Drilldown Parameter** dialog box, configure the fields as follows:

Pass from source	Click **Data field**, and then, in the drop-down list below, click **_SoftwareComponentGuid**.
Name at destination	Type **SWguid**. This string must match the input parameter name of the drill-down report.
Transform to type	Click **Basic GUID Parameter**.

10 Click **OK**.

11 Click **Add**.

12 Create a new drill-down as follows:

Name	Type **ContextMenu**.
Available On	Click **DefaultDataView**.
Event	Click **Right-click**.
Performs	Click **Show context menu**.
Action Configuration	Skip and do not configure.
Passing Parameters	Skip and do not configure.

13 Click **Save changes**.

The right-click action that you created is not available in the right-click menu by default. You must edit the source of the report manually, as follows:

To enable the custom right-click menu

1 In the left pane, right-click the **Adobe audit (Query Builder)** report, click **Export**, and then save the file.

2 Open the saved XML file in a text editor.

3 In the XML file, under `<viewingControl>`, in the `<link>` element with the `name="ContextMenu"` attribute, locate the following string:

```
<action id="ContextMenu" />
```

4 Replace this string with the following text:

```
<action id="ContextMenu">

<arguments>

<argument name="MenuFactories" list="true">

<value>LinkMenu</value>

</argument>

</arguments>

</action>
```

Also, add the `visible="false"` attribute to the `link` element.

```
    <viewingControl>
      <implementation classGuid="a967db13-cd5f-4246-8fc1-29959ee5046f">
        <customAttributes /><configuration><base><id><![CDATA[DefaultReportView__2]]
></id><linking><links><link id="Link1" name="Show Installed" sourceId="view"
targetId="DefaultReportView__2"><action id="Drilldown"><arguments><argument
name="MoveToReport"><![CDATA[c100e168-1036-4c10-b833-c0e95feb017f]]
></argument></arguments></action><parameterMappings><map
sourceParameter="SelectedRow[_SoftwareComponentGuid]" destinationParameter="SWguid"
destinationTypeAlias="ptype-guid" /></parameterMappings></link><link id="Link2"
name="ContextMenu" sourceId="view" targetId="DefaultReportView__2"
event="ContextMenu" visible="false">
<action id="ContextMenu">
        <arguments>
                <argument name="MenuFactories" list="true">
                        <value>LinkMenu</value>
                </argument>
        </arguments>
</action>
<parameterMappings
/></link></links></linking></base></configuration></implementation>
    </viewingControl>
```

5 Save and close the file.

6 In the Symantec Management Console, right-click the folder in which your report is located (in this example, **Software**), click **Import**, then and import the report back into the CMDB.

The right-click menu is now available. Test the report. To go back to the parent report, use the breadcrumb bar above of the right pane.

7 (Optional) To hide the drill-down report from the left pane, in the XML, replace `<itemAttributes>Normal</itemAttributes>` with `<itemAttributes>Hidden</itemAttributes>`.

Other methods of viewing software usage data

The software usage data appears in reports and views after you collect full inventory, enable usage tracking or create application metering policies, and after the usage information is sent to Notification Server by the Application Metering plug-in.

Software view

To access the **Software** view, in the Symantec Management Console, on the **Manage** menu, click **Software**.

In the left pane, under **Metered Software**, click **Usage Tracking**. Then view the usage data in the right pane.

This data can be displayed only for the software that is defined in the Software Catalog and is added to the list of managed software products. You must also enable tracking for the software that you want to appear in this view.

For more information about Software Catalog and managed software, see the *Software Management Solution User Guide*.

Application metering reports

To view application metering reports, in the Symantec Management Console, on the **Reports** menu, click **All Reports**, and then, in the left pane, under **Reports**, expand **Software > Application Metering**.

The following reports and several others are available for file-level application metering:

- **Executable Usage**

For more information about application metering, see the *Inventory Solution User Guide*.

The following reports are available for software product-level usage tracking:

- **Underutilized Software**

For more information about tracking software usage, see the *Inventory Solution User Guide*.

Installed software reports

To view the installed software reports, in the Symantec Management Console, on the **Reports** menu, click **All Reports**, and then, in the left pane, under **Reports**, expand **Discovery and Inventory > Inventory > Cross-platform > Software/Applications**.

The following reports and several others are available:

- **Audit Software Search report**
- **Installed Software**
- **Disk Usage by File Extension**

For more information about viewing inventory data in reports, see the *Inventory Solution User Guide*.

Resource Manager

Resource Manager lets you view information and perform numerous tasks on a Configuration Management Database (CMDB) resource. A CMDB resource can be a computer, software, network device, and so on.

You can access Resource Manager if you double-click a resource in the Symantec Management Console.

For more information about viewing inventory data in Resource Manager, see the *Inventory Solution User Guide*.

Chapter 4

Managing software licenses in ITMS Management Views

This chapter includes the following topics:

Managing licensed software in ITMS Management Views

In IT Management Views you can see detailed reports about software and license usage on your client computers. For example, you can see how many licenses there are, if they are under- or overutilized and if any of them are used without authorization. You can then uninstall the unused software products and reclaim licenses.

Software and license usage information is collected during Inventory scan of the client computers on which software usage metering and tracking is enabled.

You use the features of Asset Management Suite to add and manage purchased software licenses. Asset Management Suite combines licensing data with software usage tracking data.

Before you can manage the licenses, you need to set up your environment and gather the information about software usage from your client computers.

Table 4-1 Process for managing licensed software in ITMS Management Views

Step	Action	Description
Step 1	Meet the prerequisites.	The following components must be installed on the client computers: ■ Symantec Management Agent 8.0 (or a later version). ■ Asset Management Suite 8.0 (or a later version). If you install IT Management Suite 8.0 (or a later version), the Asset Management Suite is automatically installed with it. See "Preparing managed computers for evaluating Client Management Suite" on page 13.
Step 2	Install Software Management Solution plug-in.	Software Management Solution lets you deliver and manage software. See "Installing or upgrading the Software Management Solution plug-in" on page 21.
Step 3	Install Inventory and Application Metering plug-in and gather software inventory.	Inventory Solution lets you gather inventory data on your client computers. To collect information about your software and licenses, you need to install Application Metering plug-in. Note that it can take up to one hour for Symantec Management Agent to receive the installation policy and install the plug-ins. See "Installing the Inventory and Application Metering plug-ins" on page 19. The predefined Inventory policies are enabled by default and configured to run ASAP on every computer with the Inventory plug-in installed. You can configure the policy settings and schedule according to your needs. See "Gathering inventory with predefined inventory policies" on page 26.

Table 4-1 Process for managing licensed software in ITMS Management Views *(continued)*

Step	Action	Description
Step 4	Manage your software products and enable software usage tracking.	To track the usage of a software product, do the following: ■ Associate at least one software component with the product. After that, the product becomes managed and its usage can be tracked. See "Manually creating the managed software products" on page 50. ■ Enable the software-based usage tracking option for the managed software product. Before you move on to the next step, you need to wait for 24 hours. **Note:** The software usage tracking is only supported for Windows operating systems. Starting from 8.1 Release Update 1, you can track usage of managed software products on Mac OS X.
Step 5	Add licenses to the software products.	You use the Asset Management Suite to add and configure software licenses. For more information, see the *Asset Management Suite User Guide*. To open the software license editor from ITMS Management Views, on the **Software** View page, in the **Software Product Summary** flipbook, click the **License type**. In the **Software Product** dialog box that opens, on the **Licenses** tab, click **Add license**.
Step 7	View the license information report.	After you add and configure licenses, you can see the software usage and license utilization information on the color-coded charts on the **Software** view page.

Table 4-1 Process for managing licensed software in ITMS Management Views *(continued)*

Step	Action	Description
Step 8	Manage software, licenses and reports.	Based on the information for the charts, you can, for example, remove software from client computers, create a custom report or customize an existing license utilization report to get specific information. In this example, the following scenarios are described: ■ Removing unused software from client computers. See "Removing unused software from client computers" on page 56. ■ Creating a custom license usage report for multiple software products. See "Creating a custom license usage report for multiple software products" on page 56. ■ Customizing the license report to gather additional information. See "Customizing a license report" on page 57.

Manually creating the managed software products

On Windows XP and above client computers, you can track usage of managed software products, meter, and deny applications.

On Mac client computers, you can track usage of managed software products.

Software usage tracking and application metering are not supported on Windows and Mac servers.

You can track usage of a software product only if the software product is managed.

Inventory Solution provides the list of predefined software products. If discovered software component matches software product from the list, software component is automatically associated with the relevant predefined software product so you may manage it.

If the software component that you want to track does not match filtering criteria of any predefined software product, you can manually create a managed software product for this software component.

This task is a step in the process for tracking usage of the managed software products.

To manually create a managed software product for a discovered software component

1. In the **Symantec Management Console**, on the **Manage** menu, click **Software**.
2. In the **Software** pane, click **Favorites > Discovered Unreviewed Software**.

3 In the content pane, select the software component for which you want to create a software product.

4 In the right pane, under **Software Release Summary**, click **Manage this software**.

5 In the **Manage Software Component - Define Product** dialog box, click one of the following options, and then perform the required actions:

Create a new software product for this software component	1 View the software component details, and then click **Next**. 2 In the **Manage Software Component - Define Product Properties** dialog box, view or edit the software component properties, and then click **Next**.
Associate this software component with an existing software product	Select an existing software product that you want to associate with the software component, and then click **Next**.

6 (Optional for a new product) In the **Manage Software Component - Define Product Inventory** dialog box, perform the following actions:

- To edit filtering criteria, enter new criteria in the **Software name**, **Company**, or **Version** filters.

  Note that the **Company** filter works only after you enter criteria in the **Software name** filter.

  The filtering inventory rules define the software product and the software components that can be associated to it. The filtering inventory rules are dynamic. Any software component that comes into your environment and matches these rules is automatically associated to this software product. For example, you can change the **Software name** from **Adobe Reader** to **Adobe**, and the details in the **Identify inventory** tab change to display software components for all Adobe products.

  If your software component does not match the filter criteria of the selected existing software product, the component is highlighted in red. To proceed with associating the component with the selected product, you need to edit the filtering inventory rules of the product.

Warning: If you modify filter criteria of a predefined software product, the product will not be updated with future product definitions provided by Symantec.

If the product already has associated software components that do not match the modified filter criteria, such components are grayed out. After you save the changes, such components are excluded from product associations.

- To include the software components that are associated with other software products, check **Include components associated with other products**. The components that are associated with other software products are highlighted in yellow.

7 Click **Create** or **Save**.

The next step is to track the usage of the managed software products.

Tracking usage of the managed software products

Software tracking is only available on Windows and Mac computers.

Inventory Solution provides the usage tracking option to help you track software usage at the product level and prepare for managing software licenses.

You can track usage of a software product only if the software product meets the following requirements:

- A software product is installed and discovered in your environment.
- A software product is managed in the Software Catalog and has at least one software component that is associated to it.
- The usage tracking option is enabled for a software product.
- (Windows only) A software product has at least one usage tracking rule.

Note: You can configure tracking usage of a newly created managed software product before the inventory data for this product is gathered in your environment.

This task is a step in the process for software usage tracking.

Before you perform this step, ensure that the managed software product that you want to track has the software components that are associated to it.

See "Manually creating the managed software products" on page 50.

You view the managed software products in the **Symantec Management Console**, when you click **Manage > Software Catalog > Managed Products**.

To track usage of the managed software products

1 In the **Symantec Management Console**, on the **Manage** menu, click **Software Catalog**.

2 In the **Software** pane, in the **Software Catalog** folder, click **Managed Products**.

3 In the **Managed Products** pane, click the software product that you want to track.

4 In the right pane, in the software details flipbook, click **Product Summary > Usage Tracking**.

5 On the **Usage Tracking** page, enable the usage tracking option.

6 In the **Count software as used if run in the last ... days** box, type the number of days.

7 (Windows only) To add a usage tracking rule for the software product that you want to track, perform the following steps in order:

- In the upper left corner of the table, click the **Add usage tracking rule** icon.
- In the **Add Usage Tracking Rule** dialog box, click one of the following options, and then preform the required actions:

Specify a custom usage tracking rule for the software product	A usage tracking rule consists of program file data. Define the file data as follows: ■ Type a valid program file name (.exe). Note that the file name cannot contain the following characters: \/:*?"<>| ■ Type a program file version. **Note:** For usage tracking, Inventory Solution uses the **binary** representation of the file version in the program file. You can use wildcards ('*') in the **Version** field to broaden the scope of the rule. If you do not specify a version, Inventory Solution uses wildcards by default.
Select at least one predefined usage tracking rule for the software product	Select one or many predefined usage tracking rules. The predefined usage tracking rules are based on the key program files that are automatically associated with the software components of the new or already metered software products.

- Click **OK**.

8 (Windows only, optional) To edit an added usage tracking rule, on the **Usage Tracking** page, double-click the rule, in the **Edit Usage Tracking Rule** dialog box, edit the program file name or version, and then click **OK**.

9 On the **Usage Tracking** page, click **Save**.

The next step is to wait for the client computers to report the specified software usage, and then view the data that is stored in the Configuration Management Database (CMDB).

Tracking the software license compliance

After you insert all necessary data and create the associations, you can track the software license compliance in your environment.

Note: Software products are linked to one or more software resources. The purpose and benefit of a software product is not fully realized until Asset Management Suite is installed. Installation of Asset Management Suite is a pre-requisite for creating a licensed software product.

You can use the **Software** view or Resource Manager to check the software license compliance of a single software. In the **Licensing Reports** Web Part, on the **Software Product Licensing Compliance** tab, you can view the software license compliance report for all your software.

To see the most accurate data in Resource Manager and in the **Software Licensing** portal, the **Software Product Licensing Recalculation Operation Task** must run. By default, this task is scheduled to run during off-peak hours. You can access the task on the **Jobs / Tasks** page, under **Jobs and Tasks > System Jobs and Tasks > Service and Asset Management > Contract Management**.

This task is a step in the process for managing your software license compliance using the Software view.

You can also track the software license compliance by location using the **Software Product Licensing Compliance By Location** report. To view the report, ensure that the installation location is associated with the software purchase and the computers. Ensure that you run the **Software Product Licensing Recalculation Operation Task** before generating the report to get the updated data.

To track your software license compliance in the Software view

1. In the Symantec Management Console, on the **Manage** menu, click **Software**.
2. In the navigation pane, under **Licensed Software**, click **Licensed**, and then select a software product in the list pane.
3. In the software details pane, you can view the information about software usage and software licenses.

   For more information, click the page and then press **F1**.

   Note that the software license compliance graphic does not include non-inventoried, borrowed, or upgraded licenses. It only shows the count of purchased licenses as compared to the count of software product installs detected in the environment.

To track your software license compliance in Resource Manager

1. In the Symantec Management Console, on the **Home** menu, click **Service and Asset Management > Software Licensing**.
2. In the left pane, click **Software Product**.
3. In the **Software Product** list, right-click the software product, and then click **Resource Manager**.
4. In Resource Manager, on the **Summaries** menu, click **Software Product Licensing Summary**.

To track your software license compliance in the Software Licensing portal

1. In the Symantec Management Console, on the **Home** menu, click **Service and Asset Management > Software Licensing**.
2. In the right pane, in the **Licensing Reports** Web Part, click the **Software Product Licensing Compliance** tab.

To track your software license compliance by location in the Software Licensing portal

1. In the Symantec Management Console, on the **Reports** menu, click **All reports**.
2. In the **Reports** pane on the left, click **Service and Asset Management > Contract Management > Software Licensing > Software Product Licensing Compliance By Location** to view the software license compliance by location report.

   Alternatively, on the **Home** menu, click **Service and Asset Management > Software Licensing**. In the left pane, click **Service and Asset Management Reports > Contract Management > Software Licensing > Software Product Licensing Compliance By Location.**

   Alternatively, on the **Home** menu, click **Service and Asset Management > Manage Configuration Items**. In the left pane, click **Service and Asset Management Reports > Contract Management > Software Licensing > Software Product Licensing Compliance By Location.**

Creating a task to uninstall software

To uninstall software, you can create a custom **Run Script** task.

To create a task to uninstall software

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, navigate to the folder in which you want to create a new task.

   For example, click **System Jobs and Tasks > Software**.
3. Right-click **Quick Delivery**, and then click **New > Task**.
4. In the **Create New Task** dialog box, in the left pane, click **Run Script**.
5. In the right pane, type a new task name.

   Under **Script Details**, type a script or a command line that uninstalls the software product.

   Configure other options according to your needs, and then click **OK**.

Removing unused software from client computers

In ITMS Management Views, you can view the software usage and license utilization report. According to the report results, you can uninstall the unused software products from your client computers.

To remove unused software from client computers

1. In the Symantec Management platform, on the **Manage** menu, click **Software**.
2. In the left pane, under **Software Filters**, click a filter, and then, in the content pane, click the software that you want to view the license report for.
3. On the right, in the **Software Product Summary** flipbook, under **Details**, you can see the number of **Unused** licenses (licenses belonging to unused software products that were discovered during software inventory).
4. Under **License Usage**, click **Unused**, or click the corresponding section in the pie chart. The **Computers with software installed** list below is updated to show the client computers with this license state.
5. Under **Computers with software installed**, on the toolbar, click the **Save results as filter** symbol.
6. In the **Save Filter as** dialog box, type the name of the new filter, choose where to save it, and then click **OK**.
7. Open the **Computers** view and, under **Filters**, navigate to the filter that you have created.

   Right-click the filter, and then click **Create Target from Filter**.

   In the dialog box that opens, type the name for the new target and click **OK**.
8. Under **Targets**, right-click the target that you have created, and then click **Assign to > Task**.
9. In the **Assign Target to Task** dialog box, click the custom task for uninstalling the software, and then click **OK**.

   See "Creating a task to uninstall software" on page 55.
10. In the **New Schedule** dialog box, configure the schedule for the task, and then click **Schedule**.

Creating a custom license usage report for multiple software products

In ITMS Management Views, you can create a custom license usage report based on a software filter that includes multiple software items.

To create a custom license usage report for multiple software products

1. In the Symantec Management platform, on the **Manage** menu, click **Software**.
2. In the left pane, under **Software Filters**, click a filter, and then, in the content pane, click a software filter.

   Add filter criteria.

   For example, in the **Add Filter Criteria** drop-down list, click **Manufacturer**, and then, in the text box, type **Microsoft**.
3. Click **Update**.
4. Click **Save Filter as**.

   In the dialog box that opens, type a new name for the filter, choose where to save the filter, and then click **OK**.
5. Open the filter that you have created and click the **View filter results report** symbol.
6. In the **Filter Results Report** dialog box, using Data Classes and Views, configure the report parameters according to your needs.

   For example, under **Data Classes**, click **License Calculation Results**, and then check the **Active** and **Consumed** boxes.
7. (Optional) To save the reports as a CSV file, click **Export**.

   In the dialog box that opens, type the file name, choose where to save the report, and then click **Save**.
8. Click **Save as Report**.

   In the dialog box that opens, type the report name, choose where to save it, and then click **OK**.

   This report is automatically updated according to the state of your software.

Customizing a license report

In ITMS Management Views, you can customize a report to gather additional information about the software and license usage. For example, you can create a dynamic report that shows the unused licenses for a software product.

To customize a license report

1. In the Symantec Management Platform, on the **Manage** menu, click **Software**.
2. Under **Software Filters**, click a filter, and then, in the content pane, click a software product.

3 On the **Software Product Summary** flipbook page, under **License Usage**, click a license usage parameter.

For example, click **Unused**.

4 (Optional) To add or remove filter parameters, under **Computers with software installed**, click **Filter by Usage**, and then check the boxes to gather the information that you need.

5 On the toolbar, click the **Save result as report** symbol.

6 In the **Save as Report** dialog box, choose where to save the new report, type the name of the report, and then click **OK**.

This report is automatically updated according to the state of your software.

Chapter 5

Managing power scheme settings

This chapter includes the following topics:

About managing power scheme settings

Power scheme is a collection of settings that manage the power usage of the computer. The settings define after what period of inactivity to turn off the computer display and hard drives to save power, put the computer to standby, in hibernation, or shut the computer down.

The Altiris Power Scheme Task component helps you discover and remotely configure the power scheme settings of your Windows computers. The Power Scheme Task component is installed when you choose to install Client Management Suite in the Symantec Installation Manager. It is not installed if you install individual solutions.

The Power Scheme Task component includes a **Power Scheme Inventory** task and a collection of predefined tasks with different power scheme settings. According to your requirements, you can configure the settings of the predefined tasks according to your needs or create custom power scheme management tasks.

The Power Scheme Task that you run does not change the power schemes that Windows or other applications install. It creates and activates the **Altiris Power Scheme** with the power scheme settings that you specify.

See "Preparing target computers for power scheme management" on page 60.

Table 5-1 Power Scheme Task features

Feature	Description
Edit and deploy power schemes.	You can edit and deploy different predefined power schemes. See "Editing and deploying power scheme settings" on page 64. The Power Scheme Task that you run does not change the power schemes that Windows or other applications install. It creates the Altiris Power Scheme with the power scheme settings that you specify.
Create power scheme management tasks.	You can create custom power scheme management tasks, and you can specify the power scheme settings according to your requirements. See "Creating a Power Scheme Task" on page 63.
Inventory power schemes on client computers.	You can collect information about the power scheme settings that are currently active on your Windows computers. See "Collecting power scheme inventory data" on page 63.
View power schemes data.	You can use a predefined report to see the power scheme settings that are currently active on your Windows computers. See "Viewing power scheme inventory data" on page 64.

Preparing target computers for power scheme management

To run the power scheme management tasks, you must install or upgrade the Power Scheme Task Plug-in on the target computers.

See "Installing the Power Scheme Task Plug-in" on page 61.

See "Upgrading the Power Scheme Task Plug-in" on page 62.

The Power Scheme Task Plug-in works with Symantec Management Agent to perform the power scheme management tasks. The Power Scheme Task Plug-in lets you configure the power scheme settings on your managed Windows computers. The Power Scheme Task Plug-in also lets you collect information about the power scheme settings that are currently in use on the managed computers.

You can identify computers with not up-to-date plug-ins in the overall **Agent Health** status report. The **Agent Health** status is displayed in the filter summary view flipbook. To access the flipbook, in Symantec Management Console, on the **Manage** menu, click **Computers**, and then in the upper left corner of the content pane (center), click the **Expand Summary View** symbol.

If you want to view the status of the Power Scheme Task Plug-in for a particular computer, in Symantec Management Console, on the **Manage** menu, click **Computers**, on the **Computers** view page, in the content pane (center), click the computer name, and then in the computer details flipbook (right), click **General > Plug-in Versions**.

See "About managing power scheme settings" on page 59.

Installing the Power Scheme Task Plug-in

The Power Scheme Task Plug-in lets you configure the power scheme settings on your managed Windows computers. The agent installation process can take some time to start, depending on the update intervals that you set for Symantec Management Agent.

To install the Power Scheme Task Plug-in

1. In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**.
2. In the left pane, under **Agents/Plug-ins**, click **Power Scheme > Power Scheme Task Plug-in Install**.
3. In the right pane, configure the installation policy according to your needs.

   For more information about policy configuration options, click the page and then press **F1**.
4. Turn on the policy.

   At the upper right of the page, click the colored circle, and then click **On**.
5. Click **Save changes**.

See "About managing power scheme settings" on page 59.

Upgrading the Power Scheme Task Plug-in

If you upgrade from a previous version of the Client Management Suite, you must also upgrade the Power Scheme Task Plug-in to the latest version. To upgrade the Power Scheme Task Plug-in, you must turn on the upgrade policy.

To upgrade the Power Scheme Task Plug-in

1. In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**.
2. In the left pane, under **Agents/Plug-ins**, click **Power Scheme > Power Scheme Task Plug-in Upgrade**.
3. In the right pane, configure the upgrade policy according to your needs.

   For more information about policy configuration options, click the page and then press **F1**.
4. Turn on the policy.

   At the upper right of the page, click the colored circle, and then click **On**.
5. Click **Save changes**.

See "About managing power scheme settings" on page 59.

Uninstalling the Power Scheme Task Plug-in

If you do not perform the power scheme management tasks on your computers over an extended period of time, you can uninstall the Power Scheme to lessen the unnecessary network traffic. To uninstall the Power Scheme Task Plug-in, you must turn on the uninstall policy.

Note: Before you uninstall the Power Scheme Task Plug-in, make sure that you turn off the **Power Scheme Task Plug-in Install** policy.

See "Installing the Power Scheme Task Plug-in" on page 61.

To uninstall the Power Scheme Task Plug-in

1. In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**.
2. In the left pane, under **Agents/Plug-ins**, click **Power Scheme > Power Scheme Task Plug-in Uninstall**.

3 In the right pane, configure the uninstall policy according to your needs.

For more information about policy configuration options, click the page and then press **F1**.

4 Turn on the policy.

At the upper right of the page, click the colored circle, and then click **On**.

5 Click **Save changes**.

See "About managing power scheme settings" on page 59.

Collecting power scheme inventory data

The **Power Scheme Inventory** task lets you collect power scheme settings inventory from managed computers.

To perform this task, you must install the Power Scheme Task Plug-in on the target computers.

See "Preparing target computers for power scheme management" on page 60.

After you run the inventory task, you can view the collected power scheme settings data in a predefined report.

See "Viewing power scheme inventory data" on page 64.

To collect power scheme inventory data

1 In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.

2 In the left pane, under **Jobs and Tasks**, click **System Jobs and Tasks > Power Scheme Tasks > Power Scheme Inventory**.

3 On the **Power Scheme Inventory** page, configure the task according to your needs.

See "About managing power scheme settings" on page 59.

Creating a Power Scheme Task

You can create custom power scheme management tasks and specify the power scheme settings according to your requirements.

For more information, see the topic about creating a task in the *IT Management Suite Administration Guide*.

To create a Power Scheme Task

1 In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.

2 In the left pane, under **Jobs and Tasks**, click **System Jobs and Tasks**, right-click **Power Scheme Tasks**, and then click **New > Task**.

3 In the **Create New Task** dialog box, in the left pane, click **Power Scheme Settings Task**.

4 In the right pane, configure the task according to your needs.

5 Click **Ok**.

See "About managing power scheme settings" on page 59.

Editing and deploying power scheme settings

Power Scheme Tasks let you create and activate different power scheme settings on your managed Windows computers.

To perform the power scheme management tasks, you must install the Power Scheme Task Plug-in on target computers.

See "Preparing target computers for power scheme management" on page 60.

Note that only one power scheme can be active on a computer at a time. When you run more than one Power Scheme Task on a target computer, the task that runs last sets the active power scheme. For example, you may run the **Always On Power Scheme** task on all your computers. Later, you can run the **Portable/Laptop Power Scheme** task on your notebook computers.

Note: The power scheme that the specified Power Scheme Task creates and activates, is always named **Altiris Power Scheme** on the target computers. For example, when you run **Always On Power Scheme** task, the created and activated power scheme is named **Altiris Power Scheme** on the target computers.

To edit and deploy power scheme settings

1 In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.

2 In the left pane, under **Jobs and Tasks**, click **System Jobs and Tasks > Power Scheme Tasks**.

3 In the right pane, click a Power Scheme Task that you want to run and configure the task settings according to your needs.

4 Click **Save changes**.

See "About managing power scheme settings" on page 59.

Viewing power scheme inventory data

You can use a predefined report to view the power scheme inventory data. The report lets you see the power scheme settings that are active on the client computers.

To collect the power scheme inventory data, you must run the **Power Scheme Inventory** task on target computers.

See “Collecting power scheme inventory data” on page 63.

To view power scheme inventory data

1. In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
2. In the left pane, under **Reports**, click **Power Scheme > Power Scheme Settings**.

See “About managing power scheme settings” on page 59.

Chapter 6

Symantec Remote Access Connector

This chapter includes the following topics:

Setting up Symantec Remote Access Connector

Symantec Remote Access Connector is an IT Management Suite application that lets you configure and integrate the following third-party remote connection tools with IT Management Suite:

- Microsoft Remote Desktop Connection
- Bomgar Remote Support Solution
- XVUE Remote Desktop Client
- SimpleHelp Remote Support
- Splashtop Business for Remote Support

You can then use the third-party tool to connect to a client computer.

The Remote Access Connector tool has the following highlights:

- You do not require a license to use the Remote Access Connector tool. However, you do require a license for the third-party remote connection tool that you want to integrate with IT Management Suite.
- You can integrate more than one remote connection tool. The multiple tools can be accessed from the right-click option in Symantec Management Console.
  See "Using a remote connection tool from Symantec Management Console" on page 72.
- You can install Remote Access Connector individually or as a part of Client Management Suite.

To use the Remote Access Connector, you must create or configure the Remote Access Connector configuration file and then import it to enable the right-click menu options in the Symantec Management Console.

Table 6-1 Setting up Remote Access Connector

Step	Action	Description
Step 1	Create the configuration file.	Create a configuration file based on the suggested template. You can also modify the default file according to your requirements. See "Symantec Remote Access Connector configuration file" on page 67. See "Creating the Remote Access Connector configuration file template" on page 71.
Step 2	Import configuration file.	Importing the configuration file enables the right-click menu options in the Symantec Management Console. See "Importing the Remote Access Connector configuration file" on page 71. See "Using a remote connection tool from Symantec Management Console" on page 72.

Symantec Remote Access Connector configuration file

The Symantec Remote Access Connector configuration file lets you add or modify the configuration details to enable the use of a third-party remote connection tool.

You can edit the configuration file, an XML-based file, to add information to connect with the following third-party remote tools:

- Microsoft Remote Desktop Connection
- Bomgar Remote Support Solution

- XVUE Remote Desktop Clien
- SimpleHelp Remote Support
- Splashtop Business for Remote Support

The content of the default configuration file is the following:

```
xml version="1.0" encoding="utf-8" ?>
<remoteTools>
     <remoteTool Name="MS RDP">
         <API type="EXE">
               <exeFullPath>%windir%\system32\mstsc.exe</exeFullPath>
                <parameters>-v [HOSTNAME]</parameters>
         </API>
     </remoteTool>

<!--
<remoteTool Name="Bomgar Remote">
<API type="HTTP">
<URL>https://support.example.com/api/client_script?type=rep&amp;operation=generate&amp
</API>
</remoteTool>
<remoteTool Name="Bomgar Connect">
<API type="HTTP">
<URL>https://support.example.com/api/client_script?type=rep&amp;operation=generate&amp
</API>
</remoteTool>
<remoteTool Name="SimpleHelp">
<API type="HTTP">
<URL>simplehelp://?JW_machine_filter=</URL>
</API>
</remoteTool>
<remoteTool Name="XVUE">
<API type="HTTP">
<URL>xvue://?JW_machine_filter=</URL>
</API>
</remoteTool>
<remoteTool Name="Splashtop">
<API type="HTTP">
<URL>st-business://com.splashtop.business/?account=username@company.com&amp;autologin=
</API>
</remoteTool>
-->
</remoteTools>
```

Note: By default, Microsoft RDP tool is enabled and rest tools are commented. To use any tool, user can remove the comment of the required tool node and provide the details.

1. For Bomgar tool, replace the valid Bomgar instance URL with support.example.com value in <URL> node.

2. For Splashtop, replace the valid SplashTop user account details with username@company.com value in <URL> node.

Table 6-2 Tags used in the configuration file

Attributes	Description
remoteTool Name	You can provide a short name of the remote tool. The short name is seen in the right-click menu option when you try to access the remote tool from the Symantec Management Console. **Warning:** If this attribute is not present or the value is empty, the system will not import the configuration file and display an error.
API type	This tag describes the type of API connection. The values can be HTTP or EXE. For the HTTP type, you must provide the API URL for the third-party tool. If you update the third-party tool, you must verify the URL. For Bomgar API URL, refer to the Bomgar API Programmer's Guide at the following location: https://www.bomgar.com/docs/content/integrations/api/index.htm For the EXE type, you must provide the full path of the remote tool that is available on the Notification Server computer. You can also add the path as an environment variable for ease of use. If you access Symantec Management Console from a different computer, ensure that the remote tool is installed on the computer. The default file contains configuration for Microsoft® Remote Desktop Connection application. **Warning:** If this attribute is not present or the value is empty, the system will not import the configuration file and display an error.

To include the details of a third-party tool in the configuration file, add the required syntax before the `</remoteTools>` XML tag.

Table 6-3 Syntax for supported third-party remote connection tools

Remote Tool Name	Syntax
Microsoft Remote Desktop Connection **Note:** Present by default	<remoteTool Name="MS RDP"> <API type="EXE"> <exeFullPath>%windir%\system32\mstsc.exe</exeFullPath> <parameters>-v [HOSTNAME]</parameters> </API> </remoteTool>
Bomgar Remote Support Solution	<remoteTool Name="Bomgar"> <API type="HTTP"> <URL>https://*support.example.com*/api/client_script?type=rep&operation=generate&action=start_pinned_client_session&search_string=</URL> </API> </remoteTool>
XVUE Remote Desktop Client	<remoteTool Name="XVUERDC"> <API type="HTTP"> <URL>xvue://?*JW_machine_filter*=</URL> </API> </remoteTool>
SimpleHelp Remote Support	<remoteTool Name="SimpleHelp"> <API type="HTTP"> <URL>simplehelp://?*JW_machine_filter*=</URL> </API> </remoteTool>
Splashtop Business for Remote Support	<remoteTool Name="Splashtop"> <API type="HTTP"> <URL>st-business://com.splashtop.business/?*account=username@company.com*&autologin=1&mac=</URL> </API> </remoteTool>

See "Creating the Remote Access Connector configuration file template" on page 71.

Creating the Remote Access Connector configuration file template

The default Remote Access Connector configuration file is available after the installation of IT Management Suite at the following location:

`<install directory>\Program Files\Altiris\Notification Server\NSCap\bin\Win32\X86\RemoteTemplate`

See "Symantec Remote Access Connector configuration file" on page 67.

However, if required, you can recreate the default configuration file template and save it at another location.

The default file contains configuration for Microsoft Remote Desktop Connection application.

To create the Remote Access Connector configuration file template

1. In the Symantec Management Console, on the **Settings** menu, click **Console > Remote Tool Integration > Create Template Configuration**.
2. Save the `RemoteToolTemplate.config` file at an accessible location.

Importing the Remote Access Connector configuration file

You can customize the default configuration file template if required and import the modified file to access the third-party remote connection tool.

The following validation checks are performed while you import the configuration file:

- The `<remoteTools>` and `<remoteTool>` nodes are present.
- The `<remoteTool>` attribute `Name` is present and the value is not empty.
- The `<API>` node is present.
- The `<API>` attribute `<type>` is present and the value is either `HTTP` or `EXE`.
- If the `<API>` attribute `<type>` is `HTTP`, then the child node `<URL>` is present and the value is not empty.
- If the `<API>` attribute `<type>` is `EXE`, then the child node `<exeFullPath>` is present and the value is not empty.
- If the `<API>` attribute `<type>` is `EXE`, then the second child node is `<parameteres>`.

See "Setting up Symantec Remote Access Connector" on page 66.

See "Symantec Remote Access Connector configuration file" on page 67.

See "Using a remote connection tool from Symantec Management Console" on page 72.

To import the Remote Access Connector configuration file

1. In the Symantec Management Console, on the **Settings** menu, click **Console > Remote Tool Integration > Import Configuration**.
2. In the **Import configuration of remote tool** dialog box, click **Browse...**, select the `.config` file, and then click **Import**.

Warning: If the configuration file size exceeds 4 MB, then the application displays an error.

Using a remote connection tool from Symantec Management Console

To enable the right-click menu in the Symantec Management Console for remote access, you must import the configuration file.

See "Importing the Remote Access Connector configuration file" on page 71.

To use a remote connection tool from Symantec Management Console

1. In the Symantec Management Console, on the **Manage** menu, click **Computers**.
2. In the computers list, right-click a computer, click **Remote Access**, and then select the tool that you want to use. For example, select Microsoft Remote Desktop Connection or Bomgar Remote Support Solution.
3. For using Microsoft Remote Desktop Connection tool, save the file on Notification Server to start using it.

   This `.bat` file contains the information that Notification Server requires to access the third-party remote tool.

   For other third-party remote connection tools, you can directly start the application.

Index

T

U