

Symantec™ Client Management Suite 8.1 powered by Altiris™ technology User Guide



Symantec™ Client Management Suite 8.1 powered by Altiris™ technology User Guide

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

Legal Notice

Copyright © 2017 Symantec Corporation. All rights reserved.

Symantec, the Symantec Logo, the Checkmark Logo and Altiris are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

The product described in this document is distributed under licenses restricting its use, copying, distribution, and decompilation/reverse engineering. No part of this document may be reproduced in any form by any means without prior written authorization of Symantec Corporation and its licensors, if any.

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

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

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

<http://www.symantec.com>

Technical Support

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

Symantec's support offerings include the following:

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

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

support.symantec.com

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level
- Hardware information

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

Asia-Pacific and Japan	customercare_apac@symantec.com
------------------------	--

Europe, Middle-East, and Africa	semea@symantec.com
---------------------------------	--

North America and Latin America	supportsolutions@symantec.com
---------------------------------	--

Contents

Technical Support	4	
Chapter 1	Introducing Client Management Suite	10
	About Client Management Suite	10
	Components of Client Management Suite	11
	Where to get more information	14
Chapter 2	Getting started with Client Management Suite	17
	About installing Client Management Suite	17
	Preparing managed computers for evaluating Client Management Suite	17
	Symantec Management Agent for Windows installation prerequisites	19
	Installing the Symantec Management Agent for Windows with a manual push	20
	Configuring the Symantec Management Agent settings for evaluation use	22
	Installing the Inventory and Application Metering plug-ins	23
	Upgrading the Inventory and Application Metering plug-ins	25
	Installing or upgrading the Software Management Solution plug-in	26
Chapter 3	Metering application usage and creating custom reports	28
	Metering application usage and creating custom reports	28
	Gathering inventory with predefined inventory policies	30
	Enabling application usage metering for Adobe applications	31
	Creating a custom audit report for Adobe using plain-text SQL	33
	Creating a custom audit report for Adobe using Query Builder	36
	Creating a drill-down computer report	44
	Other methods of viewing software usage data	49

Chapter 4	Managing software licenses in ITMS Management Views	52
	Managing licensed software in ITMS Management Views	52
	Manually creating the managed software products	55
	Tracking usage of the managed software products	56
	Tracking the software license compliance	58
	Creating a task to uninstall software	60
	Removing unused software from client computers	60
	Creating a custom license usage report for multiple software products	61
	Customizing a license report	62
Chapter 5	Delivering a new version of software using Software Workspace Virtualization	64
	Delivering a new version of software using Software Workspace Virtualization	64
	About Workspace Virtualization	66
	Installing the Workspace Virtualization Agent	67
	Delivering Mozilla Firefox 11 software into a virtual layer	68
	Creating a task that toggles layers	71
	Delivering Firefox 12 and toggling the layers	72
	Viewing delivery reports	74
Chapter 6	Managing power scheme settings	75
	About managing power scheme settings	75
	Preparing target computers for power scheme management	77
	Installing the Power Scheme Task Plug-in	77
	Upgrading the Power Scheme Task Plug-in	78
	Uninstalling the Power Scheme Task Plug-in	78
	Collecting power scheme inventory data	79
	Creating a Power Scheme Task	80
	Editing and deploying power scheme settings	80
	Viewing power scheme inventory data	81
Chapter 7	Symantec Remote Access Connector	82
	About Symantec Remote Access Connector	82
	Symantec Remote Access Connector configuration file	83
	Creating the Remote Access Connector configuration file template	84
	Importing the Remote Access Connector configuration file	85

Enabling right-click menu to use the Remote Access Connector options	86
Index	87

Introducing Client Management Suite

This chapter includes the following topics:

- [About Client Management Suite](#)
- [Components of Client Management Suite](#)
- [Where to get more information](#)

About Client Management Suite

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 [“Components of Client Management Suite”](#) on page 11.

See [“Where to get more information”](#) on page 14.

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 10.

Table 1-1 Components of Client Management Suite

Component	Description	Link to User Guide
Symantec Management Platform	<p>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.</p> <p>Symantec Management Platform provides the following services:</p> <ul style="list-style-type: none">■ 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 <p>Symantec Management Platform includes the following components:</p> <ul style="list-style-type: none">■ 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	DOC9469

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

Component	Description	Link to User Guide
Deployment Solution	<p>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.</p> <p>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.</p> <p>For the Deployment Solution 8.1 release notes, see the link at the following URL:</p> <p>http://www.symantec.com/docs/DOC9583</p>	DOC9496
Inventory Solution	<p>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.</p> <p>After you gather inventory data, you can analyze it using predefined or custom reports.</p>	DOC9616
Inventory for Network Devices	<p>Inventory for Network Devices gathers inventory data from the devices that are not managed through the Symantec Management Agent.</p> <p>You can gather inventory on the devices that are already discovered and exist as resources in the CMDB.</p>	DOC9605
IT Analytics	<p>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.</p> <p>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.</p>	<p>Client Server Management content pack:</p> <p>DOC9690</p>

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

Component	Description	Link to User Guide
Patch Management Solution	<p>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.</p> <p>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.</p> <p>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.</p>	<ul style="list-style-type: none"> ■ Patch Management Solution for Linux: DOC9606 ■ Patch Management Solution for Mac: DOC9607 ■ Patch Management Solution for Windows: DOC9608
Real-Time System Manager	<p>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.</p> <p>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.</p>	DOC9304
Software Management Solution	<p>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.</p> <p>Software Management Solution supports software virtualization technology, which lets you install software into a virtual layer on the client computer.</p> <p>Software Management Solution also lets users directly download and install approved software or request other software.</p>	DOC9609

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

Component	Description	Link to User Guide
Workflow Solution	<p>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.</p> <p>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.</p> <p>For the Workflow Solution release notes, see the link at the following URL:</p> <p>http://www.symantec.com/docs/DOC9624</p>	DOC9625

Where to get more information

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

Table 1-2 Documentation resources

Document	Description	Location
Release Notes	Information about new features and important issues.	<p>The Supported Products A-Z page, which is available at the following URL:</p> <p>https://www.symantec.com/products/products-az</p> <p>Open your product's support page, and then under Common Topics, click Release Notes.</p>
User Guide	Information about how to use this product, including detailed technical information and instructions for performing common tasks.	<ul style="list-style-type: none">■ The Documentation Library, which is available in the Symantec Management Console on the Help menu.■ The Supported Products A-Z page, which is available at the following URL: https://www.symantec.com/products/products-az Open your product's support page, and then under Common Topics, click Documentation.

Table 1-2 Documentation resources (*continued*)

Document	Description	Location
Help	<p>Information about how to use this product, including detailed technical information and instructions for performing common tasks.</p> <p>Help is available at the solution level and at the suite level.</p> <p>This information is available in HTML help format.</p>	<p>The Documentation Library, which is available in the Symantec Management Console on the Help menu.</p> <p>Context-sensitive help is available for most screens in the Symantec Management Console.</p> <p>You can open context-sensitive help in the following ways:</p> <ul style="list-style-type: none"> 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.	<p>The links to various groups on Connect are as follows:</p> <ul style="list-style-type: none"> ■ 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

Getting started with Client Management Suite

This chapter includes the following topics:

- [About installing Client Management Suite](#)
- [Preparing managed computers for evaluating Client Management Suite](#)

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 11.

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.	<p>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.</p> <p>For more information about discovering computers, see the <i>IT Management Suite Administration Guide</i>.</p>
Step 2	Configure your Windows computers to allow Symantec Management Agent to push installation.	<p>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.</p> <p>See “Symantec Management Agent for Windows installation prerequisites” on page 19.</p>
Step 3	Install Symantec Management Agent	<p>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.</p> <p>See “Installing the Symantec Management Agent for Windows with a manual push” on page 20.</p> <p>For evaluation, you can also use another method of installing Symantec Management Agent, such as pull install.</p> <p>For more information on the methods of installing the Symantec Management Agent, see the <i>IT Management Suite Administration Guide</i>.</p>
Step 4	(Optional) Configure the Symantec Management Agent settings for evaluation use.	<p>To ease the configuration and evaluation of Client Management Suite, make Symantec Management Agent request the configuration from Notification Server more frequently.</p> <p>See “Configuring the Symantec Management Agent settings for evaluation use” on page 22.</p>

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.	<p>In the Symantec Management Console, on the Actions menu, click Agents/Plug-ins > Rollout Agents/Plug-ins.</p> <p>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.</p> <p>See “Installing the Inventory and Application Metering plug-ins” on page 23.</p> <p>See “Upgrading the Inventory and Application Metering plug-ins” on page 25.</p> <p>See “Installing or upgrading the Software Management Solution plug-in” on page 26.</p>

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 28.
- Enable software usage tracking, and then uninstall the software from the managed computers that do not use it.
- Install software into a virtual layer with the Software Workspace Virtualization technology.
See [“Delivering a new version of software using Software Workspace Virtualization”](#) on page 64.
- 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 75.

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)
Internet Explorer	Version 6.0 or later
Access rights	Local administrator rights
Firewall	<p>The computer must be able to communicate with Symantec Management Platform through the computer's firewall.</p> <p>Perform any of the following:</p> <ul style="list-style-type: none"> ■ 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 **Rollout 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 **Rollout 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.	<p>Select the computer in the list and click the Edit icon.</p> <p>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.</p> <p>The fields under the Resolved fields section are automatically filled with the data of a matched entry in database. These fields are not editable.</p>
Rediscover the selected entries.	<p>Select the computers in the list, and then click the Rediscover selected computer details icon.</p> <p>Rediscovering lets you search for additional information about the selected computers. For example, domain, operating system details, etc.</p>
View different selections of entries in the grid.	<p>In the View drop-down list, click the selection that you want to view.</p> <p>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.</p>

- 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 **Rollout 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: Software-based usage tracking and application metering are Windows-only features and are supported on Windows XP and above managed computers only. Software-based usage tracking and application metering are not supported on Windows 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.
- For MSI-based software, the dynamic association of files and components does not work properly until the information about file properties is gathered.
- 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 > Rollout 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 30.

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.

Upgrade from a 6.x version of Software Management Solution plug-in is not supported. You must upgrade Symantec Management Agent first, and then use the **Software Management Solution Plug-in Install** policy to install the plug-in.

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 or if you upgraded from the 6.x version 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**, on the toolbar, click **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:

Run once ASAP Lets you run the policy as soon as possible, and only once.

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.

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 notify 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**.

Metering application usage and creating custom reports

This chapter includes the following topics:

- [Metering application usage and creating custom reports](#)
- [Gathering inventory with predefined inventory policies](#)
- [Enabling application usage metering for Adobe applications](#)
- [Creating a custom audit report for Adobe using plain-text SQL](#)
- [Creating a custom audit report for Adobe using Query Builder](#)
- [Creating a drill-down computer report](#)
- [Other methods of viewing software usage data](#)

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 is 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.	<p>You must have Symantec Management Agent installed on the client computers.</p> <p>See “Preparing managed computers for evaluating Client Management Suite” on page 17.</p>
Step 2	Install the Inventory and Application Metering plug-ins.	<p>See “Installing the Inventory and Application Metering plug-ins” on page 23.</p> <p>For more detailed information, see the <i>Preparing managed computers for inventory and metering</i> topic in the <i>Inventory Solution User Guide</i>.</p> <p>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</p>
Step 3	Collect full inventory.	<p>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.</p> <p>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.</p> <p>You can configure the policy schedule according to your needs.</p> <p>See “Gathering inventory with predefined inventory policies” on page 30.</p>

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

Step	Action	Description
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 31.
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: <ul style="list-style-type: none"> ■ Plain text SQL See “Creating a custom audit report for Adobe using plain-text SQL” on page 33. ■ The Symantec Management Console Query Builder See “Creating a custom audit report for Adobe using Query Builder” on page 36. 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 44.
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 49.

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 36.

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 44.

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 33.

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

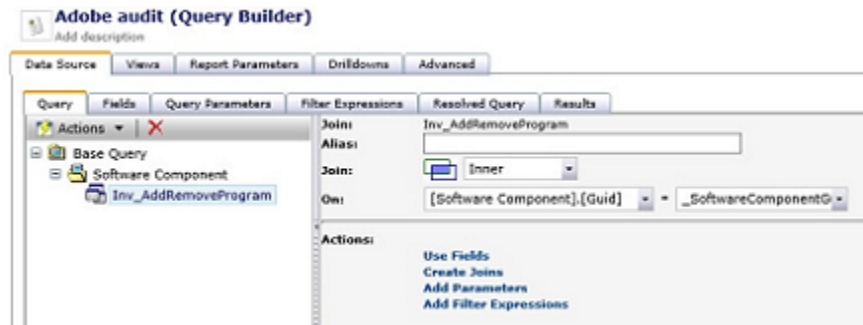
Note: Symantec recommends that you save the report regularly while making changes to the report. This reduces the chances of the Symantec Management Console timing out and losing your changes. To save the changes you made to the report, you can click either **Save Changes** or **Apply**. To return to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

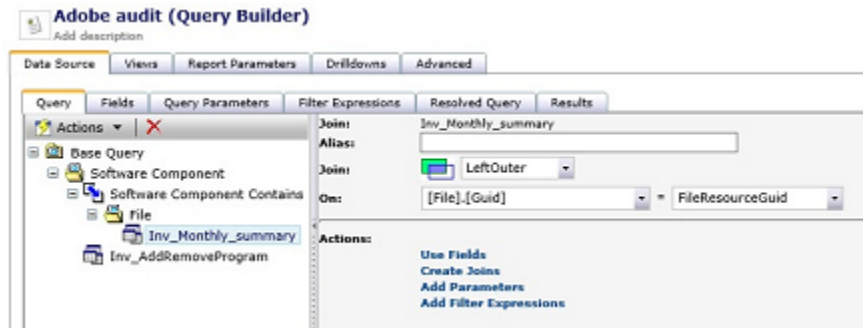


Click **OK**.

- 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:

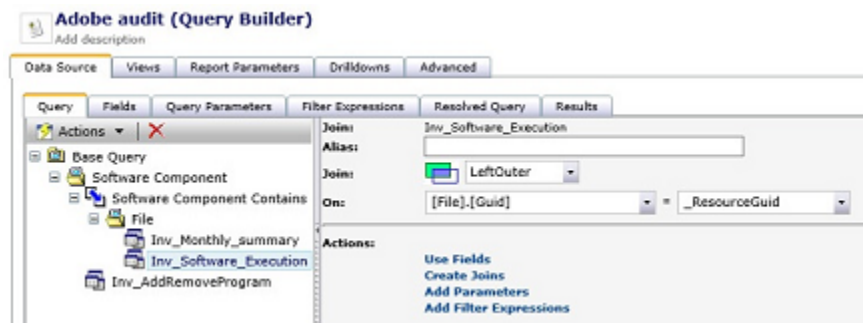
Left Outer join **Inv_Monthly_summary** on **[File].[Guid]** = **FileResourceGuid**.



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.

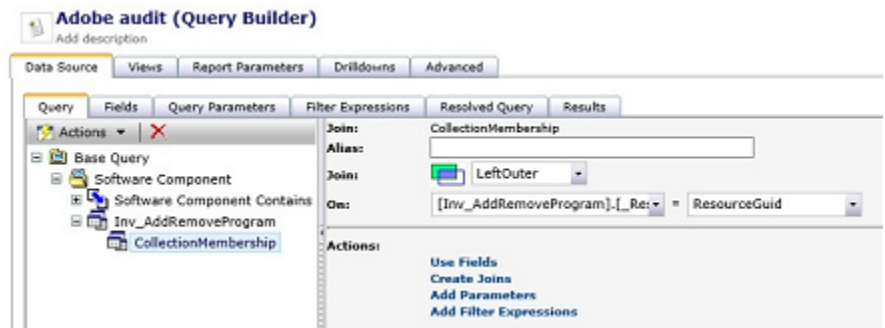
In this example, you filter the results by GUID

f5758af1-e777-436f-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**.

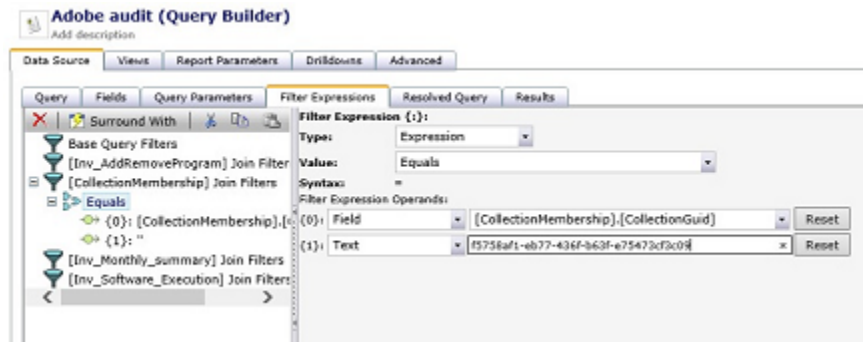
- 3 On the **Filter Expressions** tab, click **Switch to Advanced Mode**.
- 4 In the left pane, click **[CollectionMembership] Join Filters**.
- 5 In the right pane, in the drop-down list, click **Equals**.

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]**.

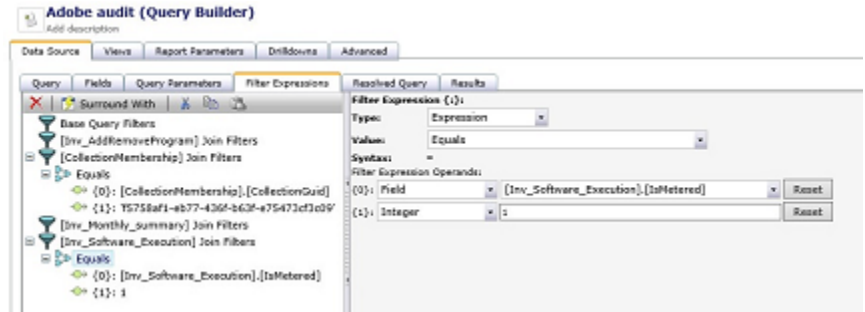
For the second operand, under **Filter Expression Operands**, in the {1}:: drop-down list, click **Text**, and then, to the text box on the right, paste the following GUID:

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**.

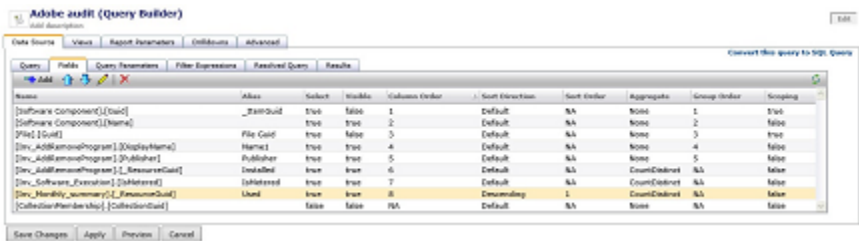
- [Inv_Monthly_Summary].[_ResourceGuid] Displays the count of workstations on which the software has been run.
- In the **Alias** box, type **Used**.
- In the **Aggregate** drop-down list, click **Count Distinct**.
- (Optional) In the **Sort Direction** drop-down list, click **Descending**.

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

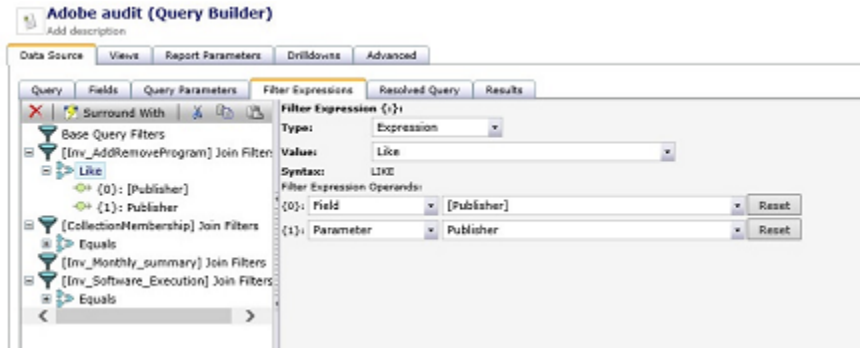
- 1 Open the report you want to edit, and then click the **Report Parameters** tab.
- 2 On the **Report Parameters** tab, on the toolbar, click **Add > New Parameter**.
- 3 In the **Editing Parameter** dialog box, fill in the following text boxes:

Name	Type Publisher .
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, 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 44.

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

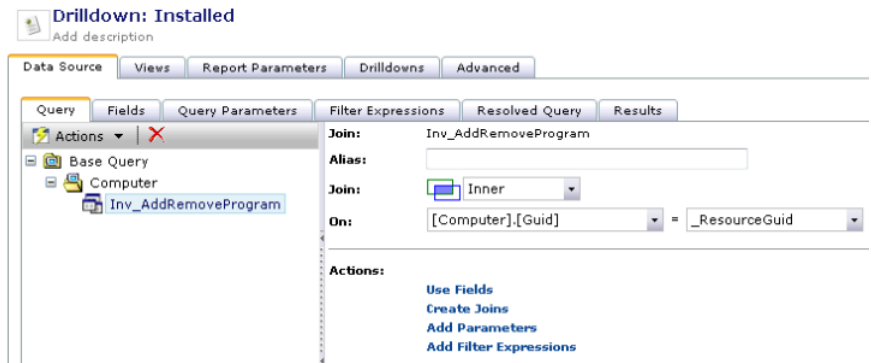
- 1 In the Symantec Management Platform, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, under **Reports**, expand **Discovery and Inventory > Inventory > Cross-platform > Software /Applications**, right-click **Software**, and then click **New > Report > Computer Report**.

- 3 On the **New Computer Report** page, click the report name and type a new name.

For example, type **Drilldown: Installed**.

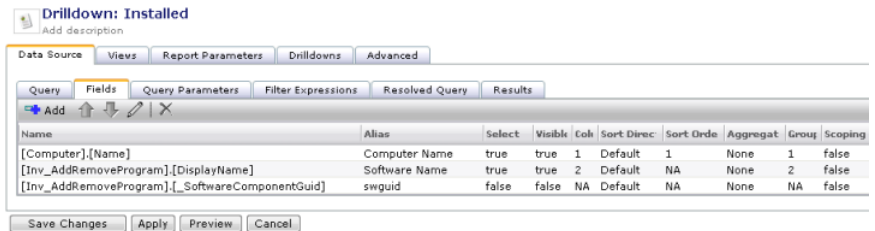
- 4 On the **Query** tab, under **Base Query**, click **Computer**, and then, in the left pane, under **Actions**, click **Create Joins**.

- 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**.



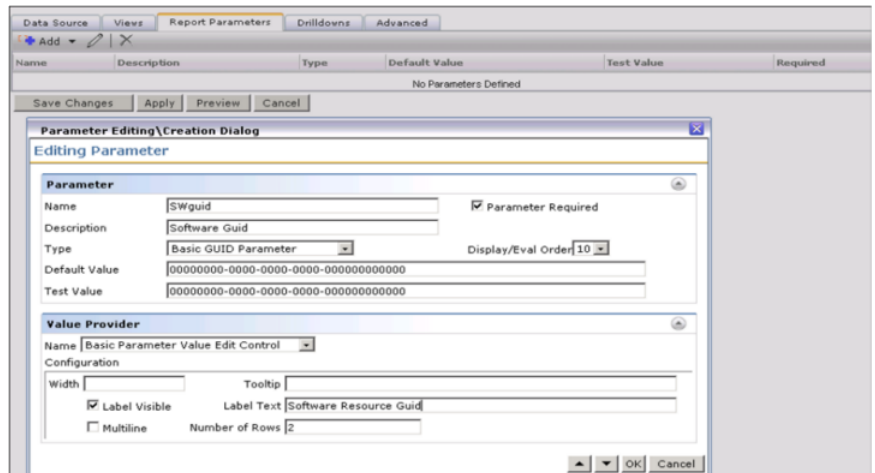
- 6 On the **Fields** tab, on the toolbar, click the **Add** symbol, and then add the fields that are shown below.

Configure the fields as shown.

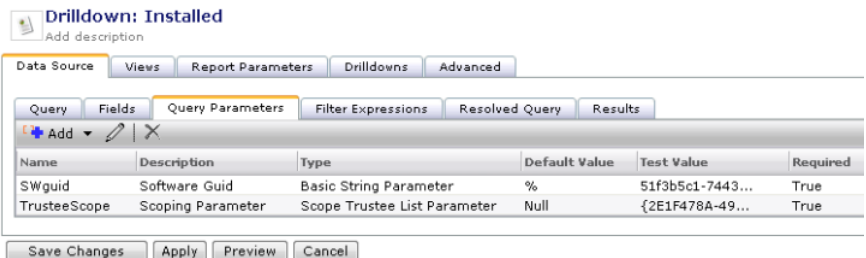


- 7 On the **Report Parameters** tab, on the toolbar, click **Add > New Parameter**, and then, in the **Editing Parameter** dialog box, configure the parameter as follows:
 - In the **Name** box, type **SWguid**.
 - In the **Description** box, type **Software Guid**.
 - In the **Type** drop-down list, 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**.

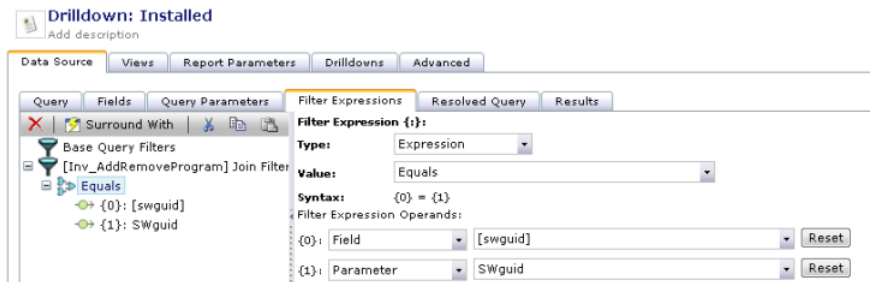


- 8 On the **Data Source** tab, click the **Query Parameters** tab, and then, on the toolbar, click **Add > Software Guid**.



- 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.

```
<implementation>
<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	<p>To access the Software view, in the Symantec Management Console, on the Manage menu, click Software.</p> <p>In the left pane, under Metered Software, click Usage Tracking. Then view the usage data in the right pane.</p> <p>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.</p> <p>For more information about Software Catalog and managed software, see the <i>Software Management Solution User Guide</i>.</p>
Application metering reports	<p>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.</p> <p>The following reports and several others are available for file-level application metering:</p> <ul style="list-style-type: none"> ■ Executable Usage <p>For more information about application metering, see the <i>Inventory Solution User Guide</i>.</p> <p>The following reports are available for software product-level usage tracking:</p> <ul style="list-style-type: none"> ■ Underutilized Software <p>For more information about tracking software usage, see the <i>Inventory Solution User Guide</i>.</p>
Installed software reports	<p>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.</p> <p>The following reports and several others are available:</p> <ul style="list-style-type: none"> ■ Audit Software Search report ■ Installed Software ■ Disk Usage by File Extension <p>For more information about viewing inventory data in reports, see the <i>Inventory Solution User Guide</i>.</p>

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*.

Managing software licenses in ITMS Management Views

This chapter includes the following topics:

- [Managing licensed software in ITMS Management Views](#)
- [Manually creating the managed software products](#)
- [Tracking usage of the managed software products](#)
- [Tracking the software license compliance](#)
- [Creating a task to uninstall software](#)
- [Removing unused software from client computers](#)
- [Creating a custom license usage report for multiple software products](#)
- [Customizing a license report](#)

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.	<p>The following components must be installed on the client computers:</p> <ul style="list-style-type: none"> ■ Symantec Management Agent 8.0 (or a later version). ■ Asset Management Suite 8.0 (or a later version). <p>If you install IT Management Suite 8.0 (or a later version), the Asset Management Suite is automatically installed with it.</p> <p>See “Preparing managed computers for evaluating Client Management Suite” on page 17.</p>
Step 2	Install Software Management Solution plug-in.	<p>Software Management Solution lets you deliver and manage software.</p> <p>See “Installing or upgrading the Software Management Solution plug-in” on page 26.</p>
Step 3	Install Inventory and Application Metering plug-in and gather software inventory.	<p>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.</p> <p>Note that it can take up to one hour for Symantec Management Agent to receive the installation policy and install the plug-ins.</p> <p>See “Installing the Inventory and Application Metering plug-ins” on page 23.</p> <p>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.</p> <p>See “Gathering inventory with predefined inventory policies” on page 30.</p>

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.	<p>To track the usage of a software product, do the following:</p> <ul style="list-style-type: none"> ■ 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 55. ■ Enable the software-based usage tracking option for the managed software product. See “Tracking usage of the managed software products” on page 56. <p>Before you move on to the next step, you need to wait for 24 hours.</p> <p>Note: The software usage tracking is only supported for Windows operating systems.</p>
Step 5	Add licenses to the software products.	<p>You use the Asset Management Suite to add and configure software licenses. For more information, see the <i>Asset Management Suite User Guide</i>.</p> <p>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.</p>
Step 7	View the license information report.	<p>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.</p>
Step 8	Manage software, licenses and reports.	<p>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.</p> <p>In this example, the following scenarios are described:</p> <ul style="list-style-type: none"> ■ Removing unused software from client computers. See “Removing unused software from client computers” on page 60. ■ Creating a custom license usage report for multiple software products. See “Creating a custom license usage report for multiple software products” on page 61. ■ Customizing the license report to gather additional information. See “Customizing a license report” on page 62.

Manually creating the managed software products

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

Note: You can track usage of managed software products, meter, and deny Win64 and Win32 applications on Windows XP and above computers only. Software-based usage tracking and application metering are not supported on Windows servers.

Inventory Solution provides the list of predefined software products. If discovered software component matches software product from the list, the task **NS.Nightly schedule to associate Software component to software product** automatically associates software component with the relevant predefined software product so you may manage it.

If the software component that you want to track does not match filtering rules 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 the managed software products

- 1 In the **Symantec Management Console**, on the **Manage** menu, click **Software**.
- 2 In the **Software** pane, under **Software Filters**, 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 the **Create Software Product** icon.
- 5 In the **Software Product** dialog box, view or edit the name, company, and version of the software product.
- 6 (Optional) On the **Identify inventory** tab, perform the following actions:
 - To edit filtering inventory rules, enter new criteria in the **Software name**, **Company**, or **Version** filters.

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.

Note that when using the **Company** filter, you must first enter criteria in the **Software name** filter. Otherwise, the **Company** filter does not work.

- 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 yellow.

7 Click **OK**.

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

See [“Tracking usage of the managed software products”](#) on page 56.

Tracking usage of the managed software products

Software usage tracking is only available on Windows computers.

Inventory Solution provides the software-based usage tracking option to help you track application usage and prepare for managing software licenses.

You enable the software-based usage tracking option for the managed software products and view gathered usage tracking data in the Symantec Management Console **Software** views.

You can track usage of a managed software product only if at least one software component in the software product has the association with one or more key program files. Otherwise, when you try to enable the software-based usage tracking option by checking **Turn on metering / usage tracking for this software product** in the **Software Product** dialog box, you get the following error message:

"Associate at least one program to meter / track usage."

The key program files that are installed with an MSI-based installer get automatically associated with the relevant software components.

For the following program files, you create associations manually when you enable the software-based usage tracking option in the **Software Product** dialog box:

- The program files that are installed with non-MSI-based installers.
- The program files that are not determined as key program files and have no component-to-file association.
- The program files that do not match any key program files that are already associated with the software component of a metered software product.

When you associate key program files to software components of the software product, the best practice is to use a more granular approach to usage tracking. To use this method, each software component must be associated with the correct key program file. The version of the associated key program file should correspond to the version of the relevant software component. As a result, you can view the usage of all components and versions of the metered software product.

For example, in the software product **Adobe Reader 9**, you add the program file `AcroRd32.exe` with the version 9.5.0.270 to the software component **Adobe Reader 9.5.0 English** with the version 9.5.0. You add the program file `AcroRd32.exe` with the version 9.0.0.2008061200. to the software component **Adobe Reader 9 English** with the version 9.0.0.

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

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 55.

To track usage of the managed software products

- 1 In the **Symantec Management Console**, on the **Manage** menu, click **Software**.
- 2 In the **Software** pane, in the **Favorites** folder, click **Installed Products**.
- 3 In the **Installed Products** pane, double-click the software product that you want to track.
- 4 In the **Software Product** dialog box, click the **Meter / track usage** tab.
- 5 On the **Meter / track usage** tab, perform one or both of the following actions:
 - To add a key program file to the software component with no associations to any program files, click **Add Program** next to the relevant software component.
 - To add a new key program file to the software component that already has associations to program files, click any associated program file next to the relevant software component.
- 6 In the **Add Program** dialog box, under **Available programs**, type the name of the program file that you want to track to filter the results.
- 7 In the **Available programs** list, select the program file that you want to track, click the arrow to move the selected program file to the **Associated programs** list, and then click **OK**.
- 8 On the **Meter / track usage** tab, in the **Count software as used if run in the last ... days** box, type the number of days.

9 Check **Turn on metering / usage tracking for this software product**.

10 Click **OK**.

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 60.
- 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.

Delivering a new version of software using Software Workspace Virtualization

This chapter includes the following topics:

- [Delivering a new version of software using Software Workspace Virtualization](#)
- [About Workspace Virtualization](#)
- [Installing the Workspace Virtualization Agent](#)
- [Delivering Mozilla Firefox 11 software into a virtual layer](#)
- [Creating a task that toggles layers](#)
- [Delivering Firefox 12 and toggling the layers](#)
- [Viewing delivery reports](#)

Delivering a new version of software using Software Workspace Virtualization

Client Management Suite lets you remotely deliver software into virtual layers. You can achieve this by using the functionality that is provided by Software Management Solution and the Symantec Workspace Virtualization software.

Software Management Solution provides intelligent and bandwidth-sensitive distribution and management of software from a central Web console. Software Management Solution lets you make sure that the correct software gets installed, remains installed, and runs without interference from other software.

For more information, see the *Software Management Solution User Guide*.

The Symantec Workspace Virtualization software lets you place applications and data into managed units, called Virtual Software Layers. It lets you instantly activate, deactivate, or reset virtual layers together with the applications that are installed in them.

Client Management Suite integrates Software Management Solution with Symantec Workspace Virtualization and lets you perform managed software deliveries into virtual layers using the Symantec Management Console.

You can deliver a newer version of software into a new virtual layer and then swap the layers on the next computer restart. Mozilla Firefox is used as the example here. Firefox has a built-in auto-update feature, so it may not be necessary to update this kind of software using Client Management Suite. However, the automatic updates may be disabled by an administrator. Also, the autoupdate feature is not available to non-administrative users. In this case, you can update Firefox in the production environment.

Symantec recommends to first perform this process in a test environment.

Warning: Make sure that Mozilla Firefox is not already installed on the client computer. Installing another version of Firefox in a virtual layer may conflict with this software installation. If you cannot uninstall Firefox, choose a different software for this procedure.

The following procedure introduces the functionality that is available in Client Management Suite. If unexpected issues occur, please ignore them if possible.

Table 5-1 Process for delivering a new version of a software using Software Workspace Virtualization

Step	Action	Description
Step 1	Meet the prerequisites.	You must have Symantec Management Agent installed on the client computers. The client computers must be registered with Notification Server. See “Preparing managed computers for evaluating Client Management Suite” on page 17.
Step 2	Learn about Workspace Virtualization.	Symantec Workspace Virtualization software lets you install software into virtual layers then enable, disable, and reset the layers. See “About Workspace Virtualization” on page 66.
Step 3	Install the Software Management Solution plug-in.	This plug-in lets you deliver and manage software, and it lets you check compliance on the endpoints. See “Installing or upgrading the Software Management Solution plug-in” on page 26.

Table 5-1 Process for delivering a new version of a software using Software Workspace Virtualization (*continued*)

Step	Action	Description
Step 4	Install the Symantec Workspace Virtualization Agent.	This agent lets you create and manage virtual layers. See “Installing the Workspace Virtualization Agent” on page 67.
Step 5	Deliver Firefox 11.	For example, deliver Mozilla Firefox 11 to your test computers. After that, you upgrade this software with a newer version. See “Delivering Mozilla Firefox 11 software into a virtual layer” on page 68.
Step 6	Create a task that toggles the layers.	You can use the SVSCmd.exe command-line tool to manage virtual layers. Create a command script task that uses this tool to toggle virtual layers. See “Creating a task that toggles layers” on page 71.
Step 7	Deliver Firefox 12 and toggle the layers.	Use managed delivery policy to deliver a newer version of Firefox into a new virtual layer and then toggle the layers on next computer restart. See “Delivering Firefox 12 and toggling the layers” on page 72.
Step 8	View delivery reports.	Software Management Solution provides reports that let you view the managed software delivery results. See “Viewing delivery reports” on page 74.

About Workspace Virtualization

Workspace Virtualization places applications and data into managed units, called Virtual Software Layers. This lets you activate, deactivate, or reset applications. You can also completely avoid conflicts between applications without altering the base Windows installation.

Symantec's application virtualization technologies integrate virtualized applications to preserve the user experience. Virtualized applications act like normal applications, ensuring normal behavior and full functionality.

Workspace Virtualization also lets you do the following:

- Reset the damaged applications to a known state and instantly repair them.
- Run two versions of the same program side by side.
- Add and remove software with zero impact on the underlying operating system.
- Turn applications on and off instantly.

Workspace Virtualization is based on Symantec's patented core technology, Symantec WorkspaceVirtualization (SWV) File System Filter driver. An application

or set of data is virtualized by using a capture process that creates a Virtual Software Package (VSP). A VSP contains all the files and registry settings of the application or data. It can be used on a client computer that has the Workspace Virtualization Agent. After the VSP is activated through the Workspace Virtualization Agent, the application becomes visible along with its files, folders, and settings.

Installing the Workspace Virtualization Agent

To virtualize software on the endpoints, you install the Symantec Workspace Virtualization Agent. By default, only the command-line tool is installed. Symantec recommends that you also install the Admin tool on the client computers. The Admin tool lets you view and manage layers using the GUI program, and verify the changes that you make to the layers. You can install the Admin tool in the following ways:

- In the Symantec Management Console, modify the command line in the **Install SWV agents** managed delivery policy before you install the Workspace Virtualization Agent.
- Install additional components using the **Programs and Features** dialog box on the Control Panel on the client computer. For example, you can use this method if the Workspace Virtualization Agent is already installed on a client computer.
- Install the SWV agent manually, and choose to install Admin tool in the Wizard. For more information on this method, see the *Symantec Workspace Virtualization User Guide*.

This task is a step in the process for installing software into a virtual layer.

See [“Delivering a new version of software using Software Workspace Virtualization”](#) on page 64.

To install the Workspace Virtualization Agent using the Symantec Management Console

- 1 In the Symantec Management Console, on the **Actions** menu, click **Agents/Plug-ins > Rollout Agents/Plug-ins**.
- 2 In the left pane, expand **Software > Software Management > Workspace Virtualization**, and then click **Install SWV agents**.
- 3 (Optional) In the right pane, configure the settings according to your needs.
For example, under **Schedule**, you can modify the compliance check schedule so that the agent is deployed sooner; and under **Applied to**, you can change the target so that the agent is deployed only to the computers in your test environment or a pilot group.

- 4 Turn on the policy.

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

- 5 Click **Save changes**.

Note: If you are using Client Management Suite earlier than 7.6, you can use the managed software delivery process to upgrade the Symantec Workspace Virtualization Agent.

For more information, refer to the following article:

<http://www.symantec.com/docs/HOWTO107267>

For Client Management Suite 7.6 or later, you can use the existing Software Management Solution agent upgrade policies.

Delivering Mozilla Firefox 11 software into a virtual layer

The following is an example of how to deliver Mozilla Firefox 11 to the client computers and install this software into a virtual layer. First, you create a new software resource in the Software Catalog, and then you use Software Management Solution to create a managed delivery policy for this software resource. Software Management Solution is a component of Client Management Suite.

This is an optional step in the production environment if you already have the software that you want to update installed on the endpoints.

Before performing this task, download the Mozilla Firefox 11 setup file (Firefox Setup 11.0.exe) from the following URL:

<ftp://ftp.mozilla.org/pub/firefox/releases/11.0/win32/en-US/>

This task is a step in the process for installing software into a virtual layer.

See “[Delivering a new version of software using Software Workspace Virtualization](#)” on page 64.

To create a new software resource for Mozilla Firefox 11

- 1 In the Symantec Management Console, on the **Manage** menu, click **Software Catalog**.
- 2 In the **Software Catalog** dialog box, on the toolbar, click **Import**.

- 3 In the **Import Software: Specify Software** dialog box, in the **Software type** drop-down list, click **Software release**, and then use one of the four available methods to import the software.

For more information on the methods, click the dialog box and then press **F1**.

If more than one file is in the package source, make sure that you set the installation file. The installation file is highlighted with bold font. To do this, click the file, and then, on the toolbar, click **Set installation file**.

- 4 Click **Next**.
- 5 In the **Import Software: Software Details** dialog box, choose to create a new software resource for Firefox 11.
- 6 Click **OK**.
- 7 In the dialog box that opens, on the **Package** tab, under **Command lines**, double-click **Install**.
- 8 In the **Add or Edit Command Line** dialog box, in the **Command line** box, replace

```
"Firefox_Setup_11.0.exe"
```

with

```
"Firefox_Setup_11.0.exe" -ms
```

The `-ms` switch lets you install Firefox so that the installation wizard will not be displayed on the client computer at the time of installation.

- 9 (Optional) In a production environment, configure a detection rule on the **Rules** tab. The detection rule ensures that the managed delivery policy does not run on the computers where the software is already installed.

For example, create a smart **Static File Expression** detection rule that checks if the `mozilla firefox\firefox.exe` file version equals or is larger than 11.

- 10 Click **OK**.
- 11 Click **OK**.
- 12 Click **Close**.

To deliver Mozilla Firefox 11 into a virtual layer

- 1 In the Symantec Management Console, on the **Manage** menu, click **Software**.
- 2 Under **Deliverable Software**, click **Software Releases**.
- 3 In the middle pane, right-click **Firefox 11**, and then click **Actions > Managed Software Delivery**.

- 4 In the **Managed Software Delivery** Wizard, on the **Select software** page, under **Additional delivery options**, check **Install this policy's software into a virtual layer**.
- 5 In the **Layer Name** box, type **firefox11**.
- 6 Click **Next**.
- 7 On the **Select destinations** page, specify the computers to which you want to deliver Firefox 11.

Symantec recommends that you first perform this task in a test environment. You can choose one of the existing targets or groups, or you can build a new resource target. For help, click the page on which you want to get more information, and then press **F1**.

- 8 Click **Next**.
- 9 On the **Schedule delivery** page, under **Choose when to check the compliance**, on the toolbar, click **Add schedule > Scheduled time**, and then configure a schedule. For example, set a schedule 10 minutes ahead of current time.

Note that by default, Symantec Management Agent requests new configuration from Notification Server once every hour. If you set a schedule only 10 minutes ahead of the current time, you must then use the Symantec Management Agent GUI on the client computer to request configuration soon after you complete this wizard. You can also run the managed delivery policy manually from the Symantec Management Agent GUI.

- 10 Click **Next**, and then, on the **Specify dependencies and updates** page, click **Deliver software**.

You can view and edit the managed delivery policy that you just created at **Manage > Policies > Software > Managed Software Delivery**.

To verify that Firefox 11 is installed in a virtual layer

- 1 On the client computer to which you want to deliver the software, open the Symantec Management Agent GUI.

You can use the **Start** button to launch this program.

- 2 Ensure the **Firefox 11 - Install** managed delivery policy has arrived to the client computer and has run successfully.

If necessary, update the configuration manually. You can run the managed delivery policy manually from the Symantec Management Agent GUI.

- 3 (Optional) If installed, run the Symantec Workspace Virtualization admin tool using **Start > All Programs > Symantec > Workspace > Virtualization > Symantec Workspace Virtualization Admin**.

- 4 Make sure that the **firefox11** layer appears in the Symantec Workspace Virtualization admin tool.

If necessary, click **View > Refresh** to refresh the window.

- 5 (Optional) In the Symantec Workspace Virtualization admin window, click **firefox11**, and then click **Layer > Activate on system startup**.

Creating a task that toggles layers

After you install a newer version of Firefox, you must disable the old layer and activate the new one. To toggle layers at the next computer restart, you must change the **Activate on system startup** option. To do this remotely from the Symantec Management Console, create a new **Run script** task with the following command-line script:

```
SET exitcode=0

cd "%programfiles%\Symantec\Workspace Virtualization"

:: Check if layer is already activated

SVSCmd.exe firefox12 P -v | findstr /R /c:"Active on start:.*No"

goto %errorlevel%

:0

echo not active

:: Deactivate new layer until next startup

SVSCmd.exe firefox12 D

:: Turn off autostart for old layer

SVSCmd.exe firefox11 AUTO -N

:: Turn on autostart for new layer

SVSCmd.exe firefox12 AUTO -Y

SET exitcode=%errorlevel%

:1

echo active

:: For testing purposes sleep 10 seconds before closing the command
window

ping 1.1.1.1 -n 1 -w 10000 > nul

:: Exit
```

```
exit /b %exitcode%
```

This script uses the SVSCmd.exe command-line utility to modify settings. First, this script checks if the new layer exists and is already configured to activate on startup. The follow-up tasks in managed delivery policies always run, regardless of the compliance check results. This check is required to make sure the script does not run in case the managed delivery policy is executed again by mistake.

Then the script disables the autostart option for the **firefox11** layer and enables it for the new **firefox12** layer. When the computer is restarted, the **firefox12** layer is activated.

For more information on the SVSCmd.exe command line parameters, see the *Symantec Workspace Virtualization User Guide* or run the SVSCmd.exe utility from the command-line prompt.

Do not run the **Run script** task after you create it. Instead, run it as part of the managed delivery policy in the next step of this tutorial.

This task is a step in the process for installing software into a virtual layer.

See [“Delivering a new version of software using Software Workspace Virtualization”](#) on page 64.

To create a task that toggles layers

- 1 In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
- 2 In the left pane, right-click any folder, and then click **New > Task**.
For example, right-click **System Jobs and Tasks**.
- 3 In the **Create New Task** dialog box, in the left pane, click **Run Script**.
- 4 In the right pane, type a name for the task.
For example, type **Toggle layers**.
- 5 Under **Script Details**, in the **Script type** drop-down list, click **Command Script**, and then copy and paste the script sample from this topic into the text box.
- 6 Click **OK**.

Delivering Firefox 12 and toggling the layers

You can deliver Mozilla Firefox 12 to the client computers and install this software into a new virtual layer. You create a new software resource in the Software Catalog for Mozilla Firefox 12. Then, you use Software Management Solution to create a managed delivery policy that delivers the software and then runs the **Toggle layers** task that you created earlier.

Before performing this task, download the Mozilla Firefox 12 setup file (`Firefox Setup 12.0.exe`) from the following URL:

<ftp://ftp.mozilla.org/pub/firefox/releases/12.0/win32/en-US/>

This task is a step in the process for installing software into a virtual layer.

See “[Delivering a new version of software using Software Workspace Virtualization](#)” on page 64.

To deliver Firefox 12 and toggle layers

- 1 Create a new software resource for Mozilla Firefox 12.
 Use the instructions that are provided for Firefox 11, but type **12** instead of **11** where appropriate.
 See “[Delivering Mozilla Firefox 11 software into a virtual layer](#)” on page 68.
- 2 In the Symantec Management Console, on the **Manage** menu, click **Software**.
- 3 In the left pane, under **Deliverable Software**, click **Software Releases**.
- 4 In the middle pane, right-click **Firefox 12**, and then click **Actions > Managed Software Delivery**.
- 5 In the **Managed Software Delivery** Wizard, on the **Select software** page, under **Additional delivery options**, check **Install this policy's software into a virtual layer**.
- 6 In the **Layer Name** box, type **firefox12**, and then click **Next**.
- 7 On the **Select destinations** page, specify the computers to which you want to deliver Firefox 12, and then click **Next**.

Symantec recommends that you first perform this task in a test environment. You can choose one of the existing targets or groups, or you can build a new resource target. For help, click the page on which you want to get more information, and then press **F1**.

- 8 On the **Schedule delivery** page, specify when to check for compliance.
 For example, click **Add schedule > Scheduled time**, and then specify a schedule. You can specify a schedule 10 minutes ahead of the current time.

Click **Next**.

Note that by default, Symantec Management Agent requests a new configuration from Notification Server once every hour. If you set a schedule only 10 minutes ahead of the current time, you must then use the Symantec Management Agent GUI on the client computer to request configuration soon after you complete this Wizard. You can also run the managed delivery policy manually.

- 9 On the **Specify dependencies and updates** page, configure the settings according to your needs, and then click **Deliver software**.
- 10 In the Symantec Management Console, on the **Manage** menu, click **Policies**.
- 11 In the left pane, click **Software > Managed Software Delivery > Firefox 12 - Install**.
- 12 On the **Firefox 12 - Install** page, on the **Software** tab, on the toolbar, click **Add > Task**.
- 13 In the **Select Task** dialog box, click the **Toggle layers** task that you created earlier.
- 14 Click **OK**.

After the managed delivery policy runs, and you restart the client computer, you should see that **firefox11** is disabled and **firefox12** is enabled. Verify that when you launch Firefox from the **Start** menu, browser version 12 is launched.

Viewing delivery reports

You can view the managed delivery policies compliance and remediation information in the Software Management Solution compliance reports.

This task is a step in the process for installing software into a virtual layer.

See [“Delivering a new version of software using Software Workspace Virtualization”](#) on page 64.

To view delivery reports

- 1 In the Symantec Management Console, on the **Reports** menu, click **All Reports**.
- 2 In the left pane, expand **Software > Compliance**.
- 3 Click a report.

Managing power scheme settings

This chapter includes the following topics:

- [About managing power scheme settings](#)
- [Preparing target computers for power scheme management](#)
- [Installing the Power Scheme Task Plug-in](#)
- [Upgrading the Power Scheme Task Plug-in](#)
- [Uninstalling the Power Scheme Task Plug-in](#)
- [Collecting power scheme inventory data](#)
- [Creating a Power Scheme Task](#)
- [Editing and deploying power scheme settings](#)
- [Viewing power scheme inventory data](#)

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 77.

Table 6-1 Power Scheme Task features

Feature	Description
Edit and deploy power schemes.	<p>You can edit and deploy different predefined power schemes.</p> <p>See “Editing and deploying power scheme settings” on page 80.</p> <p>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.</p>
Create power scheme management tasks.	<p>You can create custom power scheme management tasks, and you can specify the power scheme settings according to your requirements.</p> <p>See “Creating a Power Scheme Task” on page 80.</p>
Inventory power schemes on client computers.	<p>You can collect information about the power scheme settings that are currently active on your Windows computers.</p> <p>See “Collecting power scheme inventory data” on page 79.</p>
View power schemes data.	<p>You can use a predefined report to see the power scheme settings that are currently active on your Windows computers.</p> <p>See “Viewing power scheme inventory data” on page 81.</p>

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 77.

See [“Upgrading the Power Scheme Task Plug-in”](#) on page 78.

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 75.

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 75.

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 75.

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 77.

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 75.

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 77.

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 81.

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 75.

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 75.

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 77.

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 75.

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 79.

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 75.

Symantec Remote Access Connector

This chapter includes the following topics:

- [About Symantec Remote Access Connector](#)
- [Symantec Remote Access Connector configuration file](#)
- [Creating the Remote Access Connector configuration file template](#)
- [Importing the Remote Access Connector configuration file](#)
- [Enabling right-click menu to use the Remote Access Connector options](#)

About Symantec Remote Access Connector

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 [“Enabling right-click menu to use the Remote Access Connector options”](#) on page 86.
- You can install Remote Access Connector individually or as a part of Client Management Suite.

For the first-time user

As a first-time user, you must perform the following actions to use the Remote Access Connector:

Table 7-1 Options for the first-time Remote Access Connector user

Actions	Topics
Create a configuration file based on the suggested template or modify the default file as per your requirements.	<ol style="list-style-type: none">1 See “Symantec Remote Access Connector configuration file” on page 83.2 See “Creating the Remote Access Connector configuration file template” on page 84.
Import the updated configuration file to enable the right-click menu options in the Symantec Management Console.	<ol style="list-style-type: none">1 See “Importing the Remote Access Connector configuration file” on page 85.2 See “Enabling right-click menu to use the Remote Access Connector options” on page 86.

See [“Symantec Remote Access Connector configuration file”](#) on page 83.

See [“Creating the Remote Access Connector configuration file template”](#) on page 84.

See [“Importing the Remote Access Connector configuration file”](#) on page 85.

See [“Enabling right-click menu to use the Remote Access Connector options”](#) on page 86.

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.

Table 7-2 The following table lists the tags used in the configuration file

Attributes	Description
remoteTool Name	<p>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.</p> <p>Warning: If this attribute is not present or the value is empty, the system will not import the configuration file and display an error.</p>

Table 7-2 The following table lists the tags used in the configuration file
(continued)

Attributes	Description
API type	<p>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.</p> <p>For Bomgar API URL, refer to the Bomgar API Programmer's Guide at the following location:</p> <p>https://www.bomgar.com/docs/content/integrations/api/index.htm</p> <p>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.</p> <p>The default file contains configuration for Microsoft® Remote Desktop Connection application.</p> <p>Warning: If this attribute is not present or the value is empty, the system will not import the configuration file and display an error.</p>

See “[Creating the Remote Access Connector configuration file template](#)” on page 84.

Creating the Remote Access Connector configuration file template

The default Remote Access Connector configuration file is available to you when you install IT Management Suite. The location of the default file is `<install directory>\Program Files\Altiris\Notification Server\NSCap\bin\Win32\X86\RemoteTemplate`. 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 configuration file template

- 1 From the Symantec Management Console, open **Settings > Console > Remote Tool Integration** and click **Create Template Configuration**.
- 2 Save the `RemoteToolTemplate.config` file at an accessible location.

See “[Symantec Remote Access Connector configuration file](#)” on page 83.

See “[Importing the Remote Access Connector configuration file](#)” on page 85.

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.

To import the remote access connector configuration file

- 1 From the Symantec Management Console, open **Settings > Console > Remote Tool Integration** and click **Import Configuration**.
- 2 In the **Import configuration of remote tool** dialog box, click **Choose File**, select and open the modified `.config` file, and then click **Import**.

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

XML validation checks while importing the file

Symantec Remote Access Connector does the following validation checks while importing 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 [“About Symantec Remote Access Connector”](#) on page 82.

See [“Symantec Remote Access Connector configuration file”](#) on page 83.

See [“Enabling right-click menu to use the Remote Access Connector options”](#) on page 86.

Enabling right-click menu to use the Remote Access Connector options

When you install IT Management Suite and Symantec Remote Access Connector, you must import the configuration file to enable the right-click menu in the Symantec Management Console for remote access.

To use a remote connection tool from Symantec Management Console

- 1 Click **Manage > Computers**.
- 2 To launch a remote session with a computer, right-click the computer and select **Remote Access** and then the tool of your choice. For example, select MS RDP or Bomgar.
- 3 For using Microsoft Remote Desktop, save the file on Notification Server to start using the remote connection tool.

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.

See [“Importing the Remote Access Connector configuration file”](#) on page 85.

Index

A

- Application Metering Plug-in
 - installing 23
 - upgrading 25

C

- Client Management Suite
 - about 10
 - components 11
 - Release Notes 11
 - User Guides 11
- computer
 - prerequisites for installing Symantec Management Agent 19
 - pushing Symantec Management Agent 20
 - selecting for Symantec Management Agent installation 20
- configuring
 - Symantec Management Agent 22
- context-sensitive help 14
- CSV file
 - importing computers 20

D

- documentation 14

H

- help
 - context-sensitive 14

I

- installing
 - Software management solution plug-in 26
- Inventory Plug-in
 - installing 23
 - upgrading 25
- inventory policies
 - predefined 30

M

- managed software
 - metering and usage tracking 56
- managed software installed with a non-MSI-based installer
 - metering and usage tracking 56
- managed software products
 - creating manually 55
- metering
 - managed software products 56

P

- power scheme management
 - preparing managed computers 77
- power scheme settings
 - deploying 80
 - editing 80
 - inventory 79
 - inventory data 81
 - report 81
- Power Scheme Task
 - about 75
 - creating 80
 - features 75
 - Power Scheme Task Plug-in 77
 - settings 80
- Power Scheme Task Plug-in
 - installing 77
 - uninstalling 78
 - upgrading 78
- predefined inventory policies
 - cloning 30
 - using 30
- prerequisites
 - Symantec Management Agent installation 19

R

- Release Notes 14

S

- software components to software products
 - associating 55
- software license compliance
 - tracking 58
- software licenses
 - tracking 58
- Software management solution plug-in
 - installing 26
 - upgrading 26
- Symantec Management Agent
 - configuration request interval 22
 - configuring 22
 - importing computers from CSV file 20
 - installation requirements 19
 - installing on selected Windows computers 20
 - prerequisites 19
 - pushing to Windows computers 20
 - selecting computers for installation 20
- Symantec Management Agent for Windows
 - importing computers from CSV file 20
 - selecting computers for installation 20
- Symantec Management Agent manual installation
 - selecting computers 20

T

- tracking usage
 - of managed software products 56
 - of managed software products installed with a non-MSI-based installer 56

U

- upgrading
 - Software management solution plug-in 26
- usage tracking
 - component and version level 57
 - software-based 56