Altiris Inventory Solution™ 7.1 SP2 from Symantec™ User Guide

Altiris Inventory Solution™ 7.1 SP2 from Symantec™ User Guide

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

Legal Notice

Symantec and the Symantec Logo, Altiris, and any Altiris or Symantec trademarks used in the product 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.

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

See "*Altiris Inventory Solution™ 7.1 SP2 from Symantec™ Third-Party Legal Notices*" on page 163.

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, "Rights in Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

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

Symantec's support offerings include the following:

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

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

www.symantec.com/business/support/

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

Contacting Technical Support

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

www.symantec.com/business/support/

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

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

- Product release level

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

Licensing and registration

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

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

Support agreement resources

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

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

Contents

Chapter 1

Introducing Inventory Solution

This chapter includes the following topics:

About Inventory Solution

Obtaining and analyzing accurate inventory data is an important part of managing and securing your network. Inventory Solution lets you gather inventory data about computers, users, operating systems, and installed software applications in your environment. An application metering feature also lets you monitor and deny the usage of applications on your network. You can collect inventory data from the computers that are running the following platforms: Windows, UNIX, Linux, and Mac.

See “About supported Inventory Solution platforms” on page 17.

You use policies and tasks to perform inventory and application metering functions. The policies and tasks are easily configured and managed using a central Web console.

The inventory data is stored in the Configuration Management Database (CMDB). The CMDB provides a central store of data that is used across the Symantec Management Platform.

For more information, see the topics about the CMDB in the *Symantec Management Platform User Guide*.

After you have gathered inventory data or metered applications, you can analyze the data using predefined or custom reports.

See “About viewing inventory data” on page 155.

You can collect the following kinds of inventory data:

- Hardware and operating system.
- Software.
- File properties.

See “About inventory types” on page 15.

See “About components of Inventory Solution” on page 19.

See “About methods for gathering inventory” on page 22.

Predefined inventory policies let you gather inventory with little effort.

See “About predefined inventory policies” on page 45.

To help maximize your investment, Inventory Solution does more than gather data. By providing a Web-based management console, policies to alert you about critical information, and professional quality Web reports, Inventory Solution includes the tools that you need to transform your inventory data into useful information.

Inventory Solution also has the following features:

- Supports zero-footprint configuration.
- Operates in always connected, sometimes connected, and stand-alone computing environments.
- Can be installed to run on a recurring basis with the Symantec Management Agent.
- Posts data through SMB and/or HTTP.

You can use the application metering feature within Inventory Solution to monitor and control the use and availability of applications on managed computers. You can meter applications that are running on Windows-based managed computers. When metering applications, you define the applications you want to monitor or deny by creating application definitions. You can use broad or specific product definitions. For example, you can use one definition to meter all Microsoft applications or you can use a specific definition to meter Word version 12. The rules for metering applications are controlled through Notification Server policies. The Application Metering Plug-in runs within the Symantec Management Agent on the managed device and enforces the properties of the policies. An application metering policy can meter one or more applications.

You can use the application metering features of Inventory Solution to do the following:

- Discover applications.
  Application metering records the first time an application starts. This lets you identify the software, including its version, that is used on managed computers. You can use the information about discovered applications when you create monitoring policies.
- Monitor specific applications.
  You can create policies to monitor applications. The policies let you perform the following actions:

Monitor activity	You can track when an application is started, stopped, or both to determine duration.
Deny usage	You can deny the use of an application. You can have a denial event sent to Notification Server.
Harvest unused software licenses	Determine unused applications, so that you can reuse licenses elsewhere. For more information, see the topics about managing software licenses in the *Asset Management Suite User Guide*.

See “About metering and denying applications” on page 106.

You can use Inventory Pack for Servers, which is a separate product that lets you gather server-based inventory data from servers.

See “About Inventory Pack for Servers” on page 14.

You can also use additional Symantec products to gather inventory data from handheld computers, network devices, and Windows, UNIX, Linux, and Mac servers.

See “Where to get more information” on page 29.

About Inventory Pack for Servers

Inventory Pack for Servers is a separate product with a separate license that gathers server-based inventory data from servers. It runs on top of Inventory Solution and uses the Inventory Pack for Servers Plug-in.

You can gather the following types of server-based inventory data:

- Microsoft Windows server operating systems
- Red Hat Enterprise Linux
- SUSE Linux Enterprise Server
- VMware ESX
- ORACLE
- Microsoft SQL Server
- Microsoft SQL Server clusters
- MySQL
- Microsoft Exchange Server
- Microsoft DHCP server
- Microsoft DNS server
- Microsoft RAS server
- Microsoft IIS
- Apache
- Network load balancing
- System DSN

For a complete list of supported platforms and versions, see the *Inventory Pack for Servers Release Notes* at the following URL:

http://www.symantec.com/business/support/overview.jsp?pid=55266

See “Where to get more information” on page 29.

See “About supported Inventory Solution platforms” on page 17.

You can use predefined inventory policies to gather inventory with little effort.

See "Using predefined inventory policies" on page 49.

See "About Inventory Solution" on page 11.

About inventory types

You can gather different types of inventory data. Inventory data is stored in the data classes that are stored in the CMDB.

See "About custom inventory data classes" on page 77.

Table 1-1 Inventory types

Type	Description
Basic inventory.	The data that you can gather when the Symantec Management Agent is installed on the managed client computer. This inventory is a core function of the Symantec Management Platform and does not require Inventory Solution. Basic inventory gathers information about the computer that the Symantec Management Agent is installed on. For example, its name, domain, installed operating system, MAC and IP address, primary user account, and so on. This information is updated on a regular basis as long as the Symantec Management Agent is installed on the computer.
Standard inventory.	The expanded data that you can gather using Inventory Solution. Standard inventory collects information about the following characteristics of a client computer: ■ **Hardware and operating system**: The hardware components of the client computer. For example, the processor, memory devices, disk controllers, storage disks, and partitions. Operating system: The operating system that is installed on the client computer. For example, the version of the operating system, countrycode, serial number, and total swap space size. User accounts: The details about the user accounts and groups on a computer. For example, the primary user, all installed local accounts, installed email profiles, and membership of the local admin group. ■ **Software**: The software that is installed on a client computer and the virtual software layers that are created on a client computer. For example, the names of the applications that are installed. ■ **File properties**: More detailed information about the software, such as version and manufacturer. See "About methods for gathering software inventory" on page 92.

Table 1-1 Inventory types *(continued)*

Type	Description
Custom inventory.	The additional data that you can gather beyond the predefined data classes in Inventory Solution. You can create the additional data classes that may be unique to your environment. You then run the custom scripts that collect the custom inventory data classes. See "About gathering custom inventory" on page 75.
Application metering inventory. (Windows only)	The data that you can gather about the usage of applications. You can monitor the following information: ■ The start, stop, and deny events for the application that are sent to the CMDB. ■ Summary data of monitored applications. This data helps you track how often an application is used, not only if it is installed. This data can help you manage your application licenses. See "About metering and denying applications" on page 106. Inventory Solution provides a software-based usage tracking option to help you easily meter application usage and track and manage software licenses. The software-based usage tracking option associates file information that application metering records to a metered software component. Then it associates the software component to a predefined software product. Due to these associations the usage tracking option helps you track software usage at the product level instead of the file level. See "Metering and tracking usage of the managed software products in the enhanced Symantec Management Console Software view" on page 122. For more information, see the topics about managing software licenses in the *Asset Management Suite User Guide*.
Baseline inventory. (Windows only)	The data that you can gather about the files and registry settings on a computer. You can detect how a computer's files and registry settings change over time. You can also detect the differences between a computer and a reference computer. See "About baseline inventory" on page 133.
Server applications inventory (requires Inventory Pack for Servers).	The data that you can gather about server-class software that is installed on servers. See "About Inventory Pack for Servers" on page 14.

You can gather additional types of inventory using other Symantec products.

For more information on product details and availability of Symantec products, see www.symantec.com

See “About supported Inventory Solution platforms” on page 17.

About supported Inventory Solution platforms

Inventory Solution works on a wide range of supported platforms enabling you to easily gather data in a heterogeneous environment. You can gather inventory on Windows, UNIX, Linux, and Mac computers. To gather inventory, you must have Inventory Plug-in installed on your client computers. Preconfigured policies can automatically and remotely install the plug-in on each computer.

See “Preparing managed computers for inventory and metering” on page 37.

When you configure inventory policies, you select the computers that you want to inventory. You can also customize policies based on the settings that are available for each platform.

For a complete list of supported platforms and versions, see the *Inventory Solution Release Notes* at the following URL:

http://www.symantec.com/business/support/overview.jsp?pid=55266

See “Where to get more information” on page 29.

Additional Symantec products are available to collect inventory data on additional platforms.

You can use the following products:

- Inventory Pack for Servers
  Gathers the inventory from server-based software components.
  For more information on product details and availability of this and other potential products, see www.symantec.com
  See “About Inventory Pack for Servers” on page 14.

What's new in Inventory Solution 7.1 SP2

In the 7.1 SP2 release of Inventory Solution, the following new features are introduced:

Table 1-2 List of new features

Feature	Description
Support for new platforms.	The Inventory Solution 7.1 SP2 release lets you gather inventory on the target servers that run the following platforms: ■ SUSE Linux Enterprise Desktop 11 SP1 ■ SUSE Linux Enterprise Server 11 SP1 ■ Red Hat Enterprise Linux 6.0 ■ Red Hat Enterprise Linux 6.1 ■ Mac OS X 10.7 ■ Solaris 10 9/10 (Update 9)
Support for Solaris Zones.	The Inventory Solution 7.1 SP2 release lets you gather inventory on the global zone that is created on your target Solaris platform.
Support for IBM AIX LPARs.	The Inventory Solution 7.1 SP2 release lets you gather inventory on the logical partitions (LPARs) that run on your target IBM AIX servers.
Stand-alone software inventory.	The Inventory Solution 7.1 SP2 release adds the functionality of Software Management Framework Agent to stand-alone inventory and lets you gather more detailed software inventory on the unmanaged computers.
Software Catalog Data Provider includes approximately 400 predefined software products.	In the Inventory Solution 7.1 SP2 release, the newly discovered software components are automatically matched against the list of approximately 400 predefined software products and correlated to the appropriate products from this list.
Automatic association of key program files with metered software components.	The Inventory Solution 7.1 SP2 release lets you automatically meter newly discovered key program files together with software components and software products. You do not have to manually associate program files to metered software components.

Table 1-2 List of new features *(continued)*

Feature	Description
New filters for Symantec enterprise products.	The Inventory Solution 7.1 SP2 release provides new filters for Symantec enterprise products. For example, filters for the following products are available: ■ Symantec™ Endpoint Protection ■ Symantec™ System Recovery (formerly Symantec Backup Exec™ System Recovery) ■ Symantec™ Data Loss Prevention ■ Veritas Storage Foundation™ from Symantec ■ Symantec pcAnywhere™ ■ PGP™ Whole Disk Encryption from Symantec™ You can view all the product filters in the **Symantec Management Console**, at **Manage > Filters > Software Filters > Agent and Plug-in Filters > Software Products and metering/track usage configuration for the products Filter**.

See "About Inventory Solution" on page 11.

About components of Inventory Solution

Inventory Solution provides many components and tools to help you perform inventory tasks.

Table 1-3 Components of Inventory Solution

Component	Description
Inventory policies and tasks.	Using policies, inventory data can be automatically and remotely collected from managed client computers at scheduled intervals. Inventory collection policies are easily created and managed from the Symantec Management Console. This process eliminates the need for costly physical inventory processes. In most cases you should use inventory policies. You should limit inventory tasks to automated tasks and workflows. See "About methods for gathering inventory" on page 22.

Table 1-3 Components of Inventory Solution *(continued)*

Component	Description
Stand-alone inventory executables (Windows only).	You can collect inventory on the client computers that are not managed through the Symantec Management Platform. You can create and run the executables that gather inventory data and report it to the CMDB. These executables can be delivered through login scripts, USB keys, network shares, and so on. See "About gathering inventory using stand-alone packages" on page 63.
Custom inventory.	Inventory data is gathered for hundreds of predefined data classes. You can expand and customize the type of data you want to collect. For example, you can add specific registry data or a unique hardware component. See "About gathering custom inventory" on page 75.
Software inventory.	You can gather inventory about the software applications that are installed in your environment. You can use the following software inventory methods: ■ Basic application file inventory. ■ Add or Remove Programs list and UNIX/Linux/Mac software packages. ■ Targeted software inventory on Windows computers and software inventory using the `filescan.rule` file on UNIX, Linux, and Mac computers. ■ Validating gathered software inventory data with the Software Catalog Data Provider. See "About gathering software inventory" on page 91.
Application metering. (Windows only).	In addition to knowing what applications are installed, you can identify the usage of installed applications. You can also restrict applications from being run. See "About metering and denying applications" on page 106. Inventory Solution provides a software-based usage tracking option to help you easily meter application usage and track and manage software licenses. The software-based usage tracking option associates file information that application metering records to a metered software component. Then it associates the software component to a predefined software product. Due to these associations the usage tracking option helps you track software usage at the product level instead of the file level. See "Metering and tracking usage of the managed software products in the enhanced Symantec Management Console Software view" on page 122. For more information, see the topics about managing software licenses in the *Asset Management Suite User Guide*.

Table 1-3 Components of Inventory Solution *(continued)*

Component	Description
Baseline inventory. (Windows only).	You can determine how a client computer's inventory data changes compared to a baseline. You can detect how a computer's inventory has changed over time, or the differences between a computer and a reference computer. See "About baseline inventory" on page 133.
Inventory reports.	A portal and many predefined reports let you easily view and analyze your inventory data. You can also create your own custom reports. See "About viewing inventory data" on page 155.

What you can do with Inventory Solution

The Symantec Management Platform gathers basic inventory from managed computers. Inventory Solution adds the ability to gather substantially more data as well as other tools to help you gather and use your inventory data.

You can use the inventory data to do the following:

- Obtain an up-to-date inventory of the computers in your network and their operating system platforms.
- Identify the computers that do not meet minimum security requirements, such as antivirus software, application updates, management agents, and so on.
- Help prepare for a software license audit by providing the number of installed instances of an application.
- Help determine which computers need to be replaced according to age or capabilities.
- Identify the types and amounts of personal data that is stored on computers, such as MP3 files, MPG files, and so on.
- Prepare for operating system migrations by doing the following:
  - Identify the number of different operating systems that are installed.
  - Identify the computers that do and do not meet minimum hardware requirements for a new operating system.
  - Identify the users of computers to be migrated.
  - Determine which applications need to be re-deployed after the migration.
- Compare the files or registry settings of client computers against a baseline.

- Help manage your application licenses by tracking how often an application is used, not only if it is installed.

  For more information, see the topics about managing software licenses in the *Asset Management Suite User Guide*.
- Deny unauthorized applications from running on managed computers.

See "About Inventory Solution" on page 11.

About methods for gathering inventory

You can use different methods for gathering inventory data. Each method has some advantages and possible disadvantages.

Table 1-4 Inventory methods

Method	Description
Basic inventory.	This method is performed automatically when the Symantec Management Agent is installed on managed computers. This feature is a core function of the Symantec Management Platform and does not require any additional inventory components. See "About inventory types" on page 15. Basic inventory gathers information such as the computer's name, domain, installed operating system, MAC and IP address, primary user account, and so on. This information is updated on a regular basis as long as the Symantec Management Agent is running on the computer. The advantages are as follows: ■ Inventory data is automatically collected when the Symantec Management Agent is installed on the client computer - no other components or steps are needed. ■ Inventory data is updated at regular intervals. ■ Can be used on a different platform. The disadvantages are as follows: ■ Inventory data is limited in scope. ■ The computer must be managed using the Symantec Management Agent. For more information, see the topics about the Symantec Management Agent in the *Symantec Management Platform User Guide*.

Table 1-4 Inventory methods *(continued)*

Method	Description
Agent-based inventory on managed computers (computers with the Symantec Management Agent).	You can use this method by installing the Inventory Plug-in on your managed computers and running inventory policies. The Inventory Plug-in works with the Symantec Management Agent and uses scheduled policies to collect more detailed information than basic inventory. You can collect detailed information about the hardware, operating system, local users and groups, software, and virtual software layers. Using the Inventory Plug-in on managed computers, all inventory policies are remotely managed from the Symantec Management Console. Inventory policies can be scheduled to run at the configurable intervals that provide up-to-date data. They can also run at the times that do not affect your network's performance. You can use the Inventory Plug-in on Windows, Linux, UNIX, and Mac platforms. The advantages are as follows: ■ You can gather a broad range of inventory data. ■ Inventory data is automatically collected and updated using scheduled tasks. ■ You can configure policies to report only changed data from the previous inventory. ■ Can be easily used on multiple platforms. The disadvantages are as follows: ■ The target computer must be managed using the Symantec Management Agent. ■ Maintaining current inventory data can be difficult on the computers that are not regularly connected to the network. See "About gathering inventory on managed computers" on page 43.

Table 1-4 Inventory methods *(continued)*

Method	Description
Stand-alone Inventory (for computers without the Symantec Management Agent or connection to a Notification Server). (Windows only)	You can use this method by creating the stand-alone programs that can be run on target computers. These programs can be run on the computers that do not have the Inventory Plug-in. These programs are created using configuration pages in the Symantec Management Console. The programs can be distributed using email, network shares, login scripts , and so on. The advantages are as follows: ■ Does not require the computer to be managed using the Symantec Management Agent or connected to a Notification Server. The disadvantages are as follows: ■ External delivery of inventory package is required. ■ The inventory schedule is not centrally managed. ■ Inventory data may not be current. ■ If the target computer is not connected to a Notification Server, the data must be posted manually. ■ Only Windows-based computers are supported. See Table 1-1 on page 15. See "About gathering inventory using stand-alone packages" on page 63.
Custom inventory.	You can use this method by creating and running the scripts that expand the types of inventory that you gather. The advantages are as follows: ■ By default, inventory data is gathered through more than 100 predefined data classes. You can create the additional data classes that may be unique to your environment. The disadvantages are as follows: ■ You must create custom data classes and include the data classes in the custom scripts. ■ You must create and run the scripts that collect the custom inventory data classes. See Table 1-1 on page 15. See "About gathering custom inventory" on page 75.

Table 1-4 Inventory methods *(continued)*

Method	Description
Application metering. (Windows only)	You can use this method by installing the Application Metering Plug-in on your managed computers. You can meter application usage and track and manage software licenses. See "Metering and tracking usage of the managed software products in the enhanced Symantec Management Console Software view" on page 122. For more information, see the topics about managing software licenses in the *Asset Management Suite User Guide*. The advantages are as follows: ■ You can track how often an application is used, not only if it is installed. This feature can help you manage your application licenses. ■ You can benefit from the usage tracking option that helps you track software usage at the product level instead of the file level. The disadvantages are as follows: ■ The target computer must be managed using the Symantec Management Agent. ■ Only Windows-based computers are supported. See Table 1-1 on page 15. See "About metering and denying applications" on page 106.
Baseline inventory. (Windows only)	You can use this method by generating a baseline that identifies the files or registry settings of a standard configuration computer. You can later run the compliance scans on your client computers to compare their current files or registry keys with those in the baseline. The differences between the baseline scan and compliance scan are reported to the Configuration Management Database (CMDB). See "About baseline inventory" on page 133. The advantages are as follows: ■ You can track the files and registries that deviate from the corporate standards. ■ You can verify the accuracy of rollouts and upgrades. ■ System administrators or the help desk can get automatic notifications when a computer is non-compliant. ■ You can view a compliance level summary of the computer and reports of the changes in file. The disadvantages are as follows: ■ The target computer must be managed using the Symantec Management Agent. ■ Only Windows-based computers are supported.

About inventory performance tuning

Inventory Solution lets you gather inventory data about computers, users, operating systems, and installed software applications in your environment. You can use predefined inventory policies to collect different types of inventory. You can also modify the predefined policies or you can create new inventory policies and tasks.

See "About Inventory Solution" on page 11.

Before you set up policies and tasks to collect inventory in your environment, you need to consider the following questions:

- How much inventory data do you need to gather?
- How often do you need to run the inventory?

These questions help you determine how inventory collection affects performance in your environment. You need to find the balance between collecting a sufficient amount of inventory data and using your resources appropriately.

The features of Symantec Management Platform and Inventory Solution offer you the following ways of tuning the inventory performance:

Using different schedules.

You can gather the following major types of inventory: hardware, software, and file properties. All of these types of inventory do not have to run at the same time.

Symantec recommends that you use unique policies and schedules for different kinds of inventory.

For example, you can run different types of inventory on the following schedule:

- Full hardware inventory every four months, every first Monday
- Delta hardware inventory every two months, every second Monday
- Full software inventory every month, every first Tuesday
- Delta software inventory every week, every Wednesday
- File scan every six months, every second Friday

Using delta inventory.

Delta inventory reports only the data that has changed since the last full inventory scan. Running delta inventory reduces the network load and increases the performance.

However, you must keep in mind that the data in the Configuration Management Database (CMDB) can get outdated and a delta is not adequate anymore. For example, if the full inventory gets purged and deltas continue to come in, only the deltas remain in the database.

Symantec recommends that you also run the full inventory on a recurring basis. You can set up a schedule that serves your requirements but does not affect the performance.

Using compression.

Using compression lets you compress the data files that client computers send to Notification Server. You can specify the minimum file size that is compressed when it is sent over the network. When you plan to use compression, you need to find the balance between client and server load, and the network utilization.

If you set the compression threshold at a lower file size, it increases the workload on both the client computer and the Notification Sever. The client computer has to compress the file and the server has to decompress it. However, this setting decreases the network load.

If you set the compression threshold to a higher value, it lowers the workload on the client computer and the server. However, the network load increases due to the larger files that are sent over the network.

Symantec recommends that you use compression with smaller files only when you have very low bandwidth. When you have a Notification Server that serves a site with very high bandwidth, you do not need to use compression.

Compression is a feature of the Symantec Management Platform that is automatically enabled for all solutions. To use compression, you configure the targeted agent settings that are the general parameters that control the Symantec Management Agent.

For more information, see the topics about configuring the targeted agent settings in the *Symantec Management Platform User Guide*.

Throttling inventory reporting.

Throttling lets you specify the amount of the time that client computers can spend sending inventory data to Notification Server.

Symantec recommends that you use the throttling in larger environments, if inventory makes a significant affect on network bandwidth and Notification Server resources.

For example, you can set the reporting period to 24 hours. At the scheduled time all systems run the inventory, but wait a random amount of time between now and 24 hours, to send the collected inventory to Notification Server. The network and the Notification Server have time to process inventory over time.

See "Inventory advanced options" on page 55.

Note: This feature is currently available for Windows only

Using **System resource usage** settings on a client computer.	The **System resource usage** option lets you define the inventory process priority and thus modify the usage of the client computer's processor and disk during an inventory scan. To determine its value, consider how fast you want the inventory to be gathered and how the inventory process affects performance on the client computer. On the Windows platform, if you decrease the priority, the process of gathering inventory requires less system resources on the client computer, but the inventory scan takes longer. If you increase the priority, the inventory scan finishes faster, but also consumes more resources and can affect the performance of the client computer. On UNIX, Linux, and Mac platforms, computers dedicate more CPU cycles for high priority processes and less CPU cycles for low priority processes. If the computer is in an idle state and runs only the inventory scan, then low priority process may take the available resources. CPU usage reduces as soon as another process with a higher priority begins to run. See "Inventory advanced options" on page 55. **Note:** On the Windows platform, this option is only applicable to file scans. On UNIX, Linux, and Mac platforms, this option is applicable to the entire inventory scan process.

Adhering to the following recommendations lets you effectively tune the inventory performance:

- Use policies for recurring inventory tasks.
  Inventory policies rely on tasks and have more options to work around the systems that may be turned off at the scheduled time.
- Review all inventory tasks before you enable them.
  Inventory tasks have some options enabled by default. Enabling all of them can result in significant database growth. In some cases, the per client database footprint can increase to over 10-20 MB.
- Avoid enabling the **Access network file systems (UNIX/Linux/Mac)** setting if not necessary.
  Scanning remote volumes is disabled by default to prevent numerous computers from reporting redundant inventory data.
- Configure the **Files Properties Scan Settings**.

Drives	Avoid to include the drive that is not necessary to be scanned. By default, all local drives are scanned.
Folders	Include only those directories that you really want to scan.
Files	Use the **Report size/file count only** setting to improve performance if you do not need to collect full information about files.

- Avoid over scheduling of inventory gathering activities.

  Increasing the frequency of an inventory task in an attempt to hit an "online window" causes redundant data to be sent to Notification Server. The workload on Notification Server increases as the duplicate data must still be processed and then discarded. Schedule inventory tasks to occur at the desired data refresh rate, so that the Symantec Management Agent can locally manage the inventory collection process.

- Prevent over usage of the **Collect Full Inventory** policy and its associated inventory task.

  The perceived need to run a full inventory on a frequent basis is a common misconception. Run full inventory only when the Inventory Plug-in reports that Notification Server has more information about a computer than the Notification Server database stores.

  Run full inventory on a monthly basis but use the **System resource usage** and **Throttle inventory reporting evenly over a period of X hours** options to define how fast or when inventory data is reported.

- Use the Software Management Framework components in multiple cloned inventory policies in large environments.

  These components separate inventory policies by geographical, departmental, or other categories. Use these components to spread the timing and receipt of inventory on Notification Server. Then, large groups of computers continue to simultaneously post their inventory data to Notification Server. But Notification Server is busy for a few minutes as opposed to several hours. SQL deadlock warnings in Notification Server log reduce. You achieve a reduction in network traffic because the Inventory Plug-in does not receive the IIS "Server too busy" message and re-post inventory data.

Where to get more information

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

Table 1-5 Documentation resources

Document	Description	Location
Release Notes	Information about new features and important issues.	The **Supported Products A-Z** page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Release Notes**.

Table 1-5 Documentation resources *(continued)*

Document	Description	Location
User Guide	Information about how to use this product, including detailed technical information and instructions for performing common tasks.	■ The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. ■ The **Supported Products A-Z** page, which is available at the following URL: http://www.symantec.com/business/support/index?page=products Open your product's support page, and then under **Common Topics**, click **Documentation**.
Help	Information about how to use this product, including detailed technical information and instructions for performing common tasks. Help is available at the solution level and at the suite level. This information is available in HTML help format.	The Documentation Library, which is available in the Symantec Management Console on the **Help** menu. Context-sensitive help is available for most screens in the Symantec Management Console. You can open context-sensitive help in the following ways: ■ The F1 key when the page is active. ■ The Context command, which is available in the Symantec Management Console on the **Help** menu.

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

Table 1-6 Symantec product information resources

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

Installing Inventory Solution

This chapter includes the following topics:

System requirements for Inventory Solution

The Inventory Solution 7.1 SP2 release has the following system requirement:

- Symantec Management Platform 7.1 SP2

When you install or upgrade Inventory Solution through the Symantec Installation Manager, Symantec Management Platform is installed automatically.

For more information about Symantec Management Platform implementation, see the *Altiris™ IT Management Suite 7.1 SP2 from Symantec™ Planning and Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC4827

See “About Inventory Solution” on page 11.

About installing or upgrading Inventory Solution

You install or upgrade Inventory Solution by using the 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 *Altiris™ IT Management Suite 7.1 SP2 from Symantec™ Planning and Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC4827

You perform the product migration from version 6.x to 7.1 SP2 and from version 7.0 to 7.1 SP2 according to the migration scenario for the *IT Management Suite*.

For more information about migrating from 6.x and 7.0 to 7.1 SP2, see the following documentation resources:

- *IT Management Suite Migration Guide version 6.x to 7.1 SP2* at http://www.symantec.com/docs/DOC4742
- *IT Management Suite Migration Guide version 7.0 to 7.1 SP2* at http://www.symantec.com/docs/DOC4743

See "About Inventory Solution" on page 11.

About licensing Inventory Solution

Each Symantec product includes a trial license that is installed by default. You can register and obtain an extended trial license through the Symantec Web site at the following URL:

http://www.symantec.com/business/products/activating/

You can also purchase a full product license.

Use the Symantec Installation Manager to install licenses.

For more information about applying licenses to a solution, see the *Altiris™ IT Management Suite 7.1 SP2 from Symantec™ Planning and Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC4827

Altiris™ Inventory for Network Devices from Symantec™ is a part of Inventory Solution and shares licenses with Inventory Solution if you install the solutions within any of the following suites:

- Altiris™ Client Management Suite from Symantec™
- Altiris™ Server Management Suite from Symantec™
- Altiris™ IT Management Suite from Symantec™

For more information, see the *Inventory for Network Devices User Guide*.

Altiris™ Inventory Pack for Servers from Symantec™ is a separate product. You need to purchase a separate license for it.

You start to consume a license after Notification Server receives the first standard, custom, application metering, baseline, or server inventory data from a managed computer.

See "About inventory types" on page 15.

A license is not consumed in the following situations:

- When the Inventory plug-in exists on a managed computer but does not collect and report to Notification Server any Inventory Solution data.
- When the Symantec Management Agent collects basic inventory.

  For more information about the basic inventory and the Symantec Management Agent, see the *Symantec Management Platform User Guide*.

After you exceed your client license limit, you continue to receive inventory data from licensed assets. Incoming inventory data from unlicensed assets is discarded.

Expiration of the trial or other temporary licenses results in the following events:

- Inventory plug-in rollouts continue to function without any problems.
- All new incoming inventory data is discarded.
- Inventory reports display a license error.

After AUP expiration, all functions continue to work normally. However, if you install newer versions of the solution, their functionality is not maintained.

If you use Inventory Solution 7.1 SP2, the following actions release a license:

- Setting an asset to the retired state or any other state except active

  Note: Inventory Solution data and all associations with this resource inventory data are purged for retired, returned to lessor, and disposed assets.

  The asset history of retired assets is maintained for reporting and auditing purposes.

- Deletion of the computer resource record

Table 2-1 Asset status change influence on licensing and other behavior of Inventory Solution 7.1 SP2

Asset status	Is an Inventory license released when you change the asset status from Active to this status?	Does Notification Server delete the Inventory Solution data that is already in the database?	Does Notification Server respond to a configuration request?	Does Notification Server change the status to active upon receiving a basic inventory?	Does Notification Server change the status to active upon receiving Inventory Solution data?
Disposed	Yes	Yes	No	No	Yes
In Stock	Yes	No	No	No	No
Missing	Yes	No	No	No	No
On Order	Yes	No	No	No	No
Retired	Yes	Yes	No	No	Yes
Returned to Lessor	Yes	Yes	No	No	Yes
RMA	Yes	No	No	No	No
Any custom status	Yes	No	No	No	No
The computer resource record is deleted	Yes	Yes	Yes A basic inventory is sent as a part of the configuration request. A new resource with **Active** status is created.	Yes A new resource with **Active** status is created as a result of a basic inventory.	Yes Inventory Solution sends basic inventory data. A new resource with **Active** status is created.

See “About Inventory Solution” on page 11.

About uninstalling Inventory Solution

You uninstall Inventory Solution by using the Symantec Installation Manager.

For more information, see the *Altiris™ IT Management Suite 7.1 SP2 from Symantec™ Planning and Implementation Guide* at the following URL:

http://www.symantec.com/docs/DOC4827

See “About Inventory Solution” on page 11.

Preparing managed computers for inventory

This chapter includes the following topics:

Preparing managed computers for inventory and metering

Inventory and application metering policies and tasks require that target computers be managed. Managed computers are the computers that have the Symantec Management Agent installed on them.

See "About methods for gathering inventory" on page 22.

See "About gathering inventory on managed computers" on page 43.

See "About metering and denying applications" on page 106.

Note: Application metering is a Windows-only feature.

Table 3-1 Process for preparing managed computers for inventory and metering

Step	Action	Description
Step 1	Discover the computers that you want to manage.	You can discover the computers that are not yet managed by the Symantec Management Agent. When computers are discovered, resource objects are created for them in the Configuration Management Database (CMDB). You may have discovered computers when you installed the Symantec Management Platform or when you added new computers to the network. For more information, see the topics about the resource discovery in the *Symantec Management Platform User Guide*.
Step 2	Manage the computers by installing the Symantec Management Agent.	You may have performed this task when you installed the Symantec Management Platform or when you added new computers to the network. For more information, see the topic about methods for installing the Symantec Management Agent for Windows, UNIX, Linux, and Mac computers in the *Symantec Management Platform User Guide*.
Step 3	Prepare managed computers by installing or upgrading plug-ins.	To inventory or meter managed computers, you must install or upgrade the following plug-ins on target computers: ■ Inventory Plug-in. You install this plug-in for Windows, UNIX, Linux, and Mac computers. ■ Application Metering Plug-in for Windows. You install this plug-in for Windows client computers only. ■ Inventory Pack for Servers Plug-in. If you have Inventory Pack for Servers, you install this plug-in for Windows, UNIX, Linux, and Mac computers. See "Installing the Inventory and Application Metering Plug-ins" on page 39. See "Upgrading the Inventory and Application Metering Plug-ins" on page 40.

About the Inventory and Application Metering Plug-ins

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

Note: Application metering is a Windows-only feature and is supported on Windows XP and above client computers only. Symantec recommends that you do not install Application Metering Plug-in on Windows servers.

See "Preparing managed computers for inventory and metering" on page 37.

See "About supported Inventory Solution platforms" on page 17.

See "Installing the Inventory and Application Metering Plug-ins" on page 39.

You can use the following plug-ins:

- Inventory Plug-in.
- Application Metering Plug-in for Windows.

If you have Inventory Pack for Servers, you can also use the following plug-in:

- Inventory Pack for Servers Plug-in.

To install a plug-in, you configure a policy that installs the plug-in on target computers. You select 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 a policy is turned on, any new computer that is a member of the target group automatically has the plug-in installed on it.

By default, no plug-in installation policies are enabled. You must manually enable policies.

See "Upgrading the Inventory and Application Metering Plug-ins" on page 40.

See "About uninstalling Inventory Solution" on page 34.

Installing the Inventory and Application Metering Plug-ins

To gather inventory data on managed computers, you must install the Inventory Plug-in on target computers. To meter applications on managed computers, you must install the Application Metering Plug-in on target computers. To install a plug-in, you configure a policy that installs the plug-in on target computers.

See "About the Inventory and Application Metering Plug-ins" on page 38.

Note: Application metering is a Windows-only feature and is supported on Windows XP and above client computers only. Symantec recommends that you do not install Application Metering Plug-in on Windows servers.

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

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

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

See "Preparing managed computers for inventory and metering" on page 37.

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, expand **Discovery and Inventory > Windows/UNIX/Linux/Mac**, and then click the policy for the plug-in that you want to install.
3. 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**.
4. To select the computers to install the plug-in on, click **Apply to** and configure the target computers.
5. Schedule the policy.
6. Click **Save changes**.

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 managed computers.

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

See "About the Inventory and Application Metering Plug-ins" on page 38.

See "Installing the Inventory and Application Metering Plug-ins" on page 39.

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

See "Preparing managed computers for inventory and metering" on page 37.

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.

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 To select the computers to upgrade the plug-in on, click **Apply to** and configure the target computers.

5 Schedule the policy.

6 Click **Save changes**.

Uninstalling the Inventory and Application Metering Plug-ins

If you do not perform inventory or application metering tasks on computers over an extended period of time, you can uninstall the plug-ins. Uninstalling unused plug-ins helps to eliminate unnecessary network traffic.

Note: Before you uninstall the Inventory or Application Metering Plug-in, make sure that you turn off the install policy of the corresponding plug-in.

See "About the Inventory and Application Metering Plug-ins" on page 38.

See "Installing the Inventory and Application Metering Plug-ins" on page 39.

To uninstall 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 uninstall.

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

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

4 To select the computers to uninstall the plug-in from, click **Apply to** and configure the target computers.

5 Schedule the policy.

6 Click **Save changes**.

Chapter 4

Gathering inventory on managed computers

This chapter includes the following topics:

About gathering inventory on managed computers

You can gather inventory data by running automated policies and tasks on managed computers. This method requires the Symantec Management Agent and an Inventory Plug-in that you install on target computers. The inventory policies and tasks use the Inventory Plug-in to perform the inventory scan on the target computer. The inventory data is sent to the CMDB.

See “Preparing managed computers for inventory and metering” on page 37.

See “About methods for gathering inventory” on page 22.

See “About methods for gathering software inventory” on page 92.

You can also use Inventory Pack for Servers, which is a separate product, to gather inventory data from servers. If you have Inventory Pack for Servers installed, it uses the same type of inventory policies.

See “About Inventory Pack for Servers” on page 14.

Inventory policies let you gather inventory on a recurring schedule. Inventory Solution includes the predefined inventory policies that you can use, or you can create your own. You can use unique policies and schedules for different kinds of inventory. For example, you can have one policy collect hardware inventory daily and another policy collect software inventory weekly.

See “About inventory policies and tasks ” on page 44.

You can use predefined inventory policies to gather inventory with little effort.

See “About predefined inventory policies” on page 45.

See “Using predefined inventory policies” on page 49.

Before you gather inventory on managed computers, you must install the Inventory Plug-in on target computers.

See “Gathering inventory on managed computers” on page 48.

See “About the Inventory and Application Metering Plug-ins” on page 38.

About inventory policies and tasks

When you want to run an inventory, you use policies or tasks to configure the inventory configuration options that you want run on target computers. You can choose to gather inventory immediately or you can schedule it. When you want to gather inventory on a recurring schedule, you use inventory policies.

When you schedule an inventory policy, it runs on the schedule irrespective of whether any maintenance window is open. When you schedule an inventory task on a set of computers and do not select the **Override Maintenance Window** option, and the same set of computers has a maintenance window enabled, the task waits for the maintenance window to open.

When you use policies, any new computer that is a member of the target group automatically has the policy run on it.

See “About predefined inventory policies” on page 45.

See “Using predefined inventory policies” on page 49.

See “About running predefined and custom inventory policies as soon as possible” on page 47.

To use inventory policies or tasks, you must install the Inventory Plug-in on target computers.

See “Preparing managed computers for inventory and metering” on page 37.

You can use policies and tasks in the following ways.

Use predefined policies	A few predefined policies are provided to help simplify inventory gathering. You can use predefined policies as they are or modify them to fit your needs. If you want to modify a predefined policy, Symantec recommends that you clone the original policy and then modify the copy. See “About predefined inventory policies” on page 45. See “Using predefined inventory policies” on page 49.
Clone and modify existing policies	You can clone (copy) existing policies and then modify them to meet your needs. See “Using predefined inventory policies” on page 49. See “Inventory policy options” on page 54.
Create your own policies	You can create your own policies and configure them to meet your needs. See “Manually creating and modifying inventory policies and tasks” on page 50.
Create your own tasks	Even though you usually use policies, you can create and use Inventory tasks. However, in most cases, you want to limit them to the automated tasks that are used in a workflow. See “Manually creating and modifying inventory policies and tasks” on page 50.

About predefined inventory policies

You can use predefined inventory policies to quickly start gathering inventory data. You can use the predefined policies as they are or modify them. If you want to modify a predefined policy, Symantec recommends that you clone the original policy and then modify the copy.

See "Using predefined inventory policies" on page 49.

See "About inventory policies and tasks " on page 44.

See "About running predefined and custom inventory policies as soon as possible" on page 47.

To use inventory policies or tasks, you must install the Inventory Plug-in on target computers.

See "Preparing managed computers for inventory and metering" on page 37.

Table 4-1 Predefined inventory policies and tasks

Policy	Enabled by default?	Default schedule	Default target	Notes
Collect Full Inventory	Yes	Weekly, every Monday at 18:00 (6:00 P.M.)	All computers with the Inventory Plug-in installed	This policy collects a full inventory. By default it collects hardware and operating system, software, and file properties inventory data. You can use this default to gather an initial inventory, and then again weekly. Even though this policy is enabled by default, you must install the Inventory Plug-in on target computers before inventory data is gathered. See "Preparing managed computers for inventory and metering" on page 37.
Collect Delta Hardware Inventory	No	Monthly, every first Monday at 18:00 (6:00 P.M.)	All computers with the Inventory Plug-in installed	By default, this policy collects only the hardware inventory data and the operating system inventory data that has changed since the last full hardware inventory. See "Inventory advanced options: Run Options tab" on page 60.
Collect Delta Software Inventory	No	Weekly, every Monday at 18:00 (6:00 P.M.)	All computers with the Inventory Plug-in installed	By default, this policy collects only the software inventory data that has changed since the last full software inventory. See "Inventory advanced options: Run Options tab" on page 60.

Table 4-1 Predefined inventory policies and tasks *(continued)*

Policy	Enabled by default?	Default schedule	Default target	Notes
Collect Full Server Inventory (Inventory Pack for Servers required)	Yes	Weekly, every Monday at 18:00 (6:00 P.M.)	All computers with the Inventory Pack for Servers Plug-in installed	This task only exists if the Inventory Pack for Servers product is installed. See "About Inventory Pack for Servers" on page 14. Even though this policy is enabled by default, you must install the Inventory Plug-in on target computers before inventory data is gathered. See "Preparing managed computers for inventory and metering" on page 37.
Collect Delta Server Inventory (Inventory Pack for Servers required)	No	Weekly, every Monday at 18:00 (6:00 P.M.)	All computers with the Inventory Pack for Servers Plug-in installed	By default, this policy collects only the server applications inventory data that has changed since the last full server inventory. See "Inventory advanced options: Run Options tab" on page 60.

About running predefined and custom inventory policies as soon as possible

The predefined inventory policies are generally scheduled to run at 6:00 P.M. on Mondays. However, administrators do not have to wait for Monday to get all the computers to report their inventory to the Configuration Management Database (CMDB). Inventory policies are configured to run as soon as possible (ASAP) for the first time apart from the configured schedule.

The ASAP behavior is implemented in the following way:

- The enabled predefined inventory policies:
  - Run ASAP after the first time installation.
  - Run ASAP on any new computer that joins the target collection.
  - Run on the defined schedule.
- The custom inventory policies that are enabled and scheduled to run daily, weekly, or monthly:
  - Run ASAP after the schedule is created.

  - Run ASAP on any new computer that joins the target collection.
  - Run on the defined schedule: Daily at 6:00 P.M., weekly on every Monday at 6:00 P.M., or monthly on every first Monday at 6:00 P.M.
- The enabled custom inventory policies with the custom schedule set according to your needs:
  - Do not run automatically ASAP after the schedule is created.
  - Do not run automatically ASAP on any new computer that joins the target collection.
  - Run on the recurring schedule that you define.

  See "Scheduling custom inventory policies to run immediately once and on a recurring schedule later" on page 52.

Inventory policies are not pushed from Notification Server, but pulled by Symantec Management Agent. Thus the run ASAP behavior depends on the following settings:

- **Update configuration interval** - the default interval is one hour.
  This time is the default time when Symantec Management Agent checks with Notification Server, if Notification Server has any new policies for it to run.
- **Symantec Management Agent basic inventory interval** - the default interval is one day.
  Notification Server allows Symantec Management Agent to pull inventory policies only if Notification Server knows that the target computer has the Inventory Plug-in installed.

In the scenario where the target computer does not have the Inventory Plug-in installed and an administrator installs the Inventory Plug-in on that computer, the computer does not receive the inventory policy ASAP until the computer updates its basic inventory information on Notification Server.

See "About inventory policies and tasks " on page 44.

Gathering inventory on managed computers

You can gather inventory data by running automated policies and tasks on managed computers. This method requires that you install the Symantec Management Agent and the Inventory Plug-in on target computers. The inventory policies and tasks use the Inventory Plug-in to perform the inventory scan on the target computer. The inventory data is sent to the CMDB.

See "About gathering inventory on managed computers" on page 43.

Table 4-2 Process for gathering inventory on managed computers

Step	Action	Description
Step 1	Prepare managed computers for inventory.	Target computers must be managed and have the Inventory Plug-in installed. See "Preparing managed computers for inventory and metering" on page 37.
Step 2	Enable an inventory policy or create an inventory policy.	You need to enable and configure a policy or task to collect inventory. You can use an existing policy or create your own. You can also create a task. See "About inventory policies and tasks " on page 44. See "About predefined inventory policies" on page 45. See "Using predefined inventory policies" on page 49. See "Manually creating and modifying inventory policies and tasks" on page 50.
Step 3	(Optional) Modify policy settings or schedules.	You can modify the settings and schedule of a policy to collect inventory. See "Inventory policy options" on page 54.
Step 4	View inventory results.	You can view the gathered inventory data by viewing reports and data in the Resource Manager. See "About viewing inventory data" on page 155. See "Viewing inventory data in reports" on page 156. See "Viewing inventory data in the Resource Manager" on page 158. See "Viewing inventory data in the enhanced Symantec Management Console views" on page 159.

Using predefined inventory policies

You can use predefined inventory polices to quickly start gathering inventory data. You can use the predefined policies as they are or modify them. If you want to modify a predefined policy, Symantec recommends that you clone the original policy and then modify the copy.

See "About predefined inventory policies" on page 45.

See "Manually creating and modifying inventory policies and tasks" on page 50.

To use inventory policies or tasks, you must install the Inventory Plug-in on target computers.

See "Preparing managed computers for inventory and metering" on page 37.

This topic is a step in the process for gathering inventory on managed computers.

See "Gathering inventory on managed computers" on page 48.

To view 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 a policy.

  See "Inventory policy options" on page 54.

To clone (copy) an existing inventory policy

1 In the Symantec Management Console, browse to the item you want to clone.

2 Right-click the item, and click **Clone**.

3 Give the cloned item a unique name, and click **OK**.

To use inventory policies

1 On the inventory policy page, turn on the policy.

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

  See "Inventory policy options" on page 54.

2 Click **Save changes**.

Manually creating and modifying inventory policies and tasks

You can manually create inventory policies or tasks. To manually create an inventory task, you use the Task Management Portal. You can create new policies and tasks or use or modify existing ones.

See "Using predefined inventory policies" on page 49.

See "About gathering inventory on managed computers" on page 43.

Before you can use inventory policies or tasks, you must install the Inventory Plug-in on target computers.

See "Preparing managed computers for inventory and metering" on page 37.

This topic is a step in the process for gathering inventory on managed computers.

See "Gathering inventory on managed computers" on page 48.

To manually create inventory policies

1. In the Symantec Management Console, on the **Home** menu, click **Discovery and Inventory > Inventory**.
2. In the **Inventory Policy status** Web part, click **New**.
3. Configure the policy.

   See "Inventory policy options" on page 54.
4. Click **Save changes**.

To manually create inventory tasks

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, navigate to the folder where you want to create an inventory task, right-click the folder, and then click **New > Task**.

   For example, to create an inventory task in the **Jobs and Tasks** folder, right-click **Jobs and Tasks**, and then click **New > Task**.

   To create an inventory task in the **Inventory** folder, expand **Jobs and Tasks > System Jobs and Tasks > Discovery and Inventory**, right-click **Inventory**, and then click **New > Task**.
3. In the **Create New Task** dialog box, in the left pane, under **Discovery and Inventory**, click **Gather Inventory**.
4. In the right pane, specify the task's details.
5. (Optional) Click **Advanced** to configure the data classes, task run options, or the software inventory rules.

   See "About inventory types" on page 15.

   See "Inventory advanced options" on page 55.
6. Click **OK** to save the task.
7. On the task page, schedule the task.

   See "Selecting computers and scheduling inventory tasks" on page 52.
8. Click **Save changes**.

To modify inventory tasks

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, open the folder that contains the task you want to modify.
3. In the right pane, double-click a task.

4 Modify the settings or schedule of the task.

See "Inventory advanced options" on page 55.

See "Selecting computers and scheduling inventory tasks" on page 52.

5 Click **Save changes**.

Selecting computers and scheduling inventory tasks

Inventory tasks use the task management component of Notification Server that provides flexibility in targeting computers and scheduling tasks. For example, when you select computers you can build and re-use predefined collections of computers. When you schedule tasks, you can configure multiple schedules for an individual task, use maintenance windows, or use shared schedules.

For more information, see the topics about Task Management in the *Symantec Management Platform User Guide*.

See "Manually creating and modifying inventory policies and tasks" on page 50.

See "Inventory policy options" on page 54.

To select computers and schedule inventory tasks

1 In an inventory task, click the **New Schedule** symbol.

2 Select an option:

- **Now**
- **Schedule**

3 Select the computers to run the task on.

4 Click **Schedule**.

5 (Optional) To create multiple schedules and computer lists for this task, click **New Schedule** and create a new schedule instance.

6 Click **Save changes**.

Scheduling custom inventory policies to run immediately once and on a recurring schedule later

You can create a custom inventory policy with the custom schedule set according to your needs. The custom inventory policy does not run automatically as soon as possible (ASAP) after the custom schedule is created. The policy does not run automatically ASAP on any new computer that joins the target collection.

However, you can manually specify the two custom schedules that behave as follows:

- The first schedule runs the policy once at the nearest time after the schedule is created on the current set of targeted computers and on any new computer that joins the target collection later.
- The second schedule reruns the policy later at the predefined time.

See "About running predefined and custom inventory policies as soon as possible" on page 47.

To schedule custom inventory policies to run immediately once and on a recurring schedule later

1. In the **Symantec Management Console**, on the **Manage** menu, click **Policies**.
2. In the left pane, click **Discovery and Inventory > Inventory**, and then, in the right pane, select the inventory policy that you want to schedule.
3. Under **Ensure my inventory is current**, click **Custom schedule**.
4. In the **Edit Policy Schedule** dialog box, select **Use agent time** for the time zone.
5. To specify the schedule that runs the policy once immediately on the current set of targeted computers and on any new computer that joins the target later, perform the following steps in order:
   - Click **Add schedule > Scheduled time**, and then specify the schedule that expires in the next few minutes.
     For example, if the current time is 7:50 A.M., set the schedule to 8:00 A.M.
   - Click **No repeat**, in the **Repeat schedule** dialog box, click **No repeat**, and then click **OK**.
6. To specify the schedule that reruns the policy later at the predefined time, perform the following steps in order:
   - Click **Add schedule > Scheduled time**, and then specify the schedule
   - Click **No repeat**, in the **Repeat schedule** dialog box, specify the appropriate frequency, and then click **OK**.
7. In the **Edit Policy Schedule** dialog box, click **OK**.
8. Under **Applies To/Compliance**, define the set of targeted computers to which you want to apply the policy.
9. On the inventory policy page, turn on the policy.

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

Inventory policy options

An inventory policy page lets you configure an inventory policy. You can configure existing policies or the new policies that you create. If you want to modify a predefined policy, Symantec recommends that you clone the original policy and then modify the copy.

See “About predefined inventory policies” on page 45.

See “Using predefined inventory policies” on page 49.

See “Manually creating and modifying inventory policies and tasks” on page 50.

Table 4-3 Inventory policy options

Option	Description
Policy menu.	In the upper left of an inventory policy page, you can click the clipboard icon to open the policy menu. From the menu, you can perform the following operations on the policy: open, clone, rename, move, export, and so on.
Policy name.	The name of the policy. You can click the name and edit it. For a new policy, the default name is **New Inventory Policy**.
Policy description.	The description of the policy. You can click the description and edit it. For a new policy, the default description is **Add description**.
Policy status.	Whether the policy is turned on or off. If the policy clipboard icon is gray, and the colored circle is red, the policy is off. If the policy clipboard icon and the colored circle are green, the policy is on. To turn on the policy , at the upper right of the page, click the colored circle, click **On**, and then click **Save changes**.
Ensure my inventory is current .	The frequency of inventory gathering. You can select to have inventory gathered on the following schedules: ■ Daily at 18:00 (6:00 P.M., Agent time) ■ Weekly, every Monday at 18:00 (6:00 P.M., Agent time) ■ Monthly, every first Monday at 18:00 (6:00 P.M., Agent time) ■ On a custom schedule

Table 4-3 Inventory policy options *(continued)*

Option	Description
Select the types of inventory to gather .	The kind of inventory you gather. See "About inventory types" on page 15. You can click **Advanced** and specify which inventory data classes to collect. See "Inventory advanced options: Data Classes tab" on page 56.
Advanced.	Opens a dialog for advanced settings. See "Inventory advanced options" on page 55.
Applies To/Compliance.	The targets that the policy is applied to and the summary of policy runs. For more information, see the topics about specifying the targets of a policy and specifying filtering rules in the *Symantec Management Platform User Guide*.

Inventory advanced options

The **Advanced Options** dialog box on an inventory policy or task page lets you configure the advanced options of an inventory task.

See "Manually creating and modifying inventory policies and tasks" on page 50.

See "Inventory policy options" on page 54.

Table 4-4 Tabs in the **Advanced Options** dialog box

Tab	Description
Data Classes	The data classes are the specific items of inventory that you can gather. You can select a whole category of data classes or expand it and select a more detailed set of data. See "About inventory types" on page 15. Data classes of a predefined policy are pre-selected based on the policy. See "Inventory advanced options: Data Classes tab" on page 56.

Table 4-4 Tabs in the **Advanced Options** dialog box *(continued)*

Tab	Description
File Properties Scan Settings	(This tab is available only if **File properties - manufacturer, version, size, internal name, etc.** is selected on an inventory policy or task page.) See "Inventory policy options" on page 54. Software rules let you filter drives, folders, and files when you perform a software inventory scan. See "Inventory advanced options: Files Properties Scan Settings tab" on page 56.
Run Options	Run options let you configure inventory and logging options, processor priority, and user context. See "Inventory advanced options: Run Options tab" on page 60.

Inventory advanced options: Data Classes tab

On an inventory policy or task page, at **Advanced Options > Data Classes**, you can select the types of inventory data that you want to gather. You can select a whole category or expand it and select a more detailed set of data.

See "About inventory types" on page 15.

Data classes of a predefined policy are pre-selected based on the policy.

If you use the name of the computer instead of localhost to access the **Symantec Management Console**, for example `http://SouthernWingNS/Altiris/Console/`, you may get the error message `Data could not be loaded` when you select or unselect a data class. You may also get the error message `Permission denied`.

To eliminate the errors, you need to add the link to the **Symantec Management Console** at **Internet Explorer > Tools > Internet Options > Security > Trusted sites > Sites**. Then you should close all the instances of Internet Explorer and reopen the **Symantec Management Console**.

See "Inventory advanced options" on page 55.

Inventory advanced options: Files Properties Scan Settings tab

On an inventory policy or task page, at **Advanced Options > Files Properties Scan Settings**, you can filter drives, folders, and files when you perform a software inventory scan.

See “Manually creating and modifying inventory policies and tasks” on page 50.

By default, all local drives and all folders on those drives are scanned. When you select a folder, all subfolders are included by default. You can add, edit, or delete items in the list.

See “Inventory advanced options” on page 55.

Table 4-5 Options on the **Files Properties Scan Settings** tab

Option	Description
Drives tab	On Windows and Mac computers, you can select the drives that you want to include or exclude during the software inventory scan. By default, all local drives are scanned. On UNIX and Linux computers, you can select the file system types that you want to include or exclude during the software inventory scan.
Folders tab	Lets you select the folders that you want to include or exclude during the software inventory scan. When adding a folder to the list, you can either browse to a folder name or enter the name in the text box. The text box accepts environment variables, such as `%windir%` For UNIX and Linux folders, you can configure software scan to limit the maximum number of subfolder levels. You can also ignore a folder where the count of the files exceeds the given number.
Files tab	Lets you set a rule to include or exclude files for a software inventory scan. You can also edit, delete, or clone a file from the **File Rules** list. Cloning lets you select a rule, create another copy of a rule in the **Software Rules** query builder, and adjust the rule. For UNIX and Linux platforms, the following properties can be specified in the file rules: **File type**, **File Size**, **LastModifiedDate**, and **Permissions**. For the Mac platform, the following properties can be specified in the file rules: **File type**, **File Size**, **LastModifiedDate**, **Permissions**, **File Content** (bundle or file), **Product Name**, **Product Version**, and **Manufacturer**.

The following table explains how to use includes and excludes:

Table 4-6 Software rules includes and excludes

Option	Description
Drives > Include drive	Includes the drive in the scope of software scan.
Drives > Exclude drive	Ignores the drive from software scan.
Drives > Include file system type	For the target computers that are running UNIX and Linux, includes the file system of the given type in the scope of software scan.
Drives > Exclude file system type	For the target computers that are running UNIX and Linux, excludes the file systems of the given type from software scan.
Folders > Include folder	Includes the folder in the scope of software scan.
Folders > Exclude folder	Ignores the folder from software scan. Starting with Inventory Solution 7.0 SP1, new folders have been added to the list of excludes to reduce redundant data. You may want to review these settings to make sure that important applications are not excluded.
Folders > Include folder limits	For the target computers that are running UNIX and Linux. This setting tells the software scan to limit maximum number of subfolder levels or to ignore a folder where the count of files exceeds the given number.
File > Include Rule	Scans the files that match the given rules. Reports the size and the file count information if you have selected “Report size or file count information only” option on the **Include file rules** dialog. Otherwise reports file information (name, path, size, last modified date, manufacturer and so on).
File > Exclude Rule	Does not report the information about the files matching these rules to the CMDB.

The following table explains how the Inventory Plug-in behaves on different platforms:

Table 4-7 Software inventory behavior on different platforms

Possible settings on the Files Properties Scan Settings tab	Behavior of the software scan agent on Windows	Behavior of the software scan agent on UNIX/Linux	Behavior of the software scan agent on Mac
Does not include or exclude any drives or file system types and folders.	UI shows message "Please include at least one Drive or Folder for the Windows scan."	UI shows message "Please include at least one Drive or Folder for the UNIX/Linux scan."	UI shows message "Please include at least one Drive or Folder for the Mac scan."
Includes only drives and does not exclude any drive. Does not include or exclude any folders.	Scans the included drives.	N/A	Scans the included drives.
Includes only the file system type and does not exclude any file system. Does not include or exclude any folders.	N/A	Does not scan anything	N/A
Includes only the folders and does not exclude any folder. Does not include or exclude any drives or file system types.	Scans only the included folders.	Scans only the included folders.	Scans only the included folders.
Excludes a parent folder, but includes the child folder of it.	Does not scan the child folder.	Scans the included child folder.	Scans the included child folder.
Includes a parent folder, but excludes the child folder of it.	Scans the parent folder, but ignores the child folder.	Scans the parent folder, but ignores the child folder.	Scans the parent folder, but ignores the child folder.
Excludes a parent drive, but includes a folder on it.	Scans only the included folder.	N/A	Scans only the included folder.
Excludes the file system type, but includes a folder with this file system type.	N/A	Does not scan the included folder.	N/A
Includes a parent drive, but excludes a folder on it.	Scans the entire drive but ignores the excluded folder.	N/A	Scans the entire drive but ignores the excluded folder.
Includes the file system type, but excludes a folder with this file system type.	N/A	Does not scan anything	N/A

Table 4-7 Software inventory behavior on different platforms *(continued)*

Possible settings on the Files Properties Scan Settings tab	Behavior of the software scan agent on Windows	Behavior of the software scan agent on UNIX/Linux	Behavior of the software scan agent on Mac
Does not include any files.	Does or does not exclude files.	Does not scan any files.	Does not scan any files.
Includes a few files. Does not exclude files.	The included files are scanned in the scope that drives and folders define.	The included files are scanned in the scope that the file system types and folders define.	The included files are scanned in the scope that the drives and folders define.
Includes a few files and also exclude files.	Scans the files matching include file's criteria. Out of these, those matching the exclude criteria are excluded from reporting to the CMDB.	Files not matching the exclude file's criteria and matching include file's criteria are reported to the CMDB.	Files not matching the exclude file's criteria and matching include file's criteria are reported to the CMDB.

Inventory advanced options: Run Options tab

On an inventory policy or task page, at **Advanced Options > Run Options**, you can configure the run options of an inventory scan.

See "Manually creating and modifying inventory policies and tasks" on page 50.

Table 4-8 Options on the **Run Options** tab

Option	Description
Send inventory changes (deltas) only	(This option is not available for stand-alone inventory packages.) You can select this option to send only the changes since the previous inventory. This way, less inventory data is sent across the network to the CMDB. You might want to resend a complete inventory in the following conditions: ■ You reset or cleaned-up your CMDB data. ■ You purged the inventory data. ■ For troubleshooting purposes, you might want a complete inventory of a computer or application folder.

Table 4-8 Options on the **Run Options** tab *(continued)*

Option	Description
Enable verbose client logging	(This option is not available for stand-alone inventory packages.) You can select this option to include additional trace information in the client log. Generally, you would use this option to troubleshoot a problem. For example, the inventory task runs on the computer, but the data is not reported in the database. For Windows computers, the location of the log file is stored in the registry on the Notification Server computer. HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\eXpress\Event Logging\Log File Key Name: Filepath For UNIX, Linux, and Mac computers, when you enable this option, a separate log file with detailed logging is created for every task. The files are created in <agent install dir>/inventory/var/log/ directory (by default, `/opt/altiris/notification/inventory/var/log/`).
Access network file systems (UNIX/Linux/Mac)	(This option is not available for stand-alone inventory packages.) You can select this option to scan the network file systems. Select this option to allow the Inventory Plug-in to scan remote volumes for software and report remote volumes' hardware information. Scanning remote volumes is disabled by default to prevent numerous computers from reporting redundant inventory data. This option takes precedence over UNIX and Linux file system types and Mac drive settings. See "Inventory advanced options: Files Properties Scan Settings tab" on page 56. If you uncheck this check box, remote volumes are not scanned, regardless of whether their file system types are included in the scan.

Table 4-8 Options on the **Run Options** tab *(continued)*

Option	Description
System resource usage	(This option is not available for stand-alone inventory packages.) You can define the inventory process priority and thus modify the usage of the target computer's processor and disk during an inventory scan. The actual resource utilization during an inventory scan depends on the target computer's processor type and hard disk speed. During a file scan for software inventory, the number of files on the hard drive also affects resource utilization. On the Windows platform, if you decrease the priority, the process of gathering inventory requires less system resources on the client computer, but the inventory scan takes longer. If you increase the priority, the inventory scan finishes faster, but also consumes more resources and can affect the performance of the client computer. On UNIX, Linux, and Mac platforms, computers dedicate more CPU cycles for high priority processes and less CPU cycles for low priority processes. If the computer is in an idle state and runs only the inventory scan, then low priority process may take the available resources. CPU usage reduces as soon as another process with a higher priority begins to run. You may want to create multiple separate inventory policies and target similar types of target computers. For example, you can create a policy with servers as targets. You can set the priority to lower than normal to decrease the resource utilization and not adversely affect the performance of the server. You may also want to lower the resource utilization for the other types of computers that generally have slower hard disks and processors. For example, you can lower the resource usage for notebook computers.
Throttle inventory reporting evenly over a period of (Windows only)	(This option is not available for stand-alone inventory packages.) You should enable this option, if inventory makes a significant affect on the network bandwidth and Notification Server resources. For example, you can set the reporting period to 24 hours. At the scheduled time all systems run the inventory, but wait a random amount of time between now and 24 hours, to send the collected Inventory to Notification Server. This option gives the network and Notification Server time to process inventory over time.
Run Inventory as	(This option is not available for stand-alone inventory packages.) You can specify the user account that the task runs in, based on the platform the target computer is running.
MySQL	You can specify, edit, or delete MySQL credentials such as user name, password, and connection parameters.
Oracle	You can specify, edit, or delete Oracle credentials such as user name, password, and Oracle System ID (SID).

Chapter 5

Gathering inventory using stand-alone packages

This chapter includes the following topics:

About gathering inventory using stand-alone packages

(Windows only)

One method of gathering inventory data is using stand-alone inventory packages. A stand-alone inventory package is an executable file that you create from the Symantec Management Console. You run the package on target computers and gather the inventory data of that computer. This method lets you gather inventory on the target computers that are not managed through the Symantec Management Agent.

This method does not apply to the following cases:

- Older or same version of Symantec Management Agent is installed on a computer.
- Symantec Management Agent is installed on a computer but not connected to the Notification Server computer.
- Symantec Management Agent is installed but broken or not functioning on a computer.
- Symantec Management Agent is installed but disabled on a computer.

Note: Stand-alone inventory packages can only run on Windows-based computers. To gather inventory on the computers that run on other platforms, you must use different methods.

See “About methods for gathering inventory” on page 22.

If you use stand-alone packages, you must be able to report the inventory data back to the Notification Server computer. You can use different options of reporting data depending on the configuration of your network. You can create multiple packages with different options based on your needs.

See “Gathering inventory using stand-alone packages” on page 66.

To run a stand-alone package and gather the inventory correctly, the logged on user must be a local administrator.

See “About gathering stand-alone software inventory” on page 64.

About gathering stand-alone software inventory

(Windows only)

Starting from the SP2 release of Inventory Solution 7.1, stand-alone inventory lets you benefit from the Software Management Framework Agent functionality when you gather software inventory on the unmanaged computers. Stand-alone inventory packages perform **Software Discovery** scan and gather inventory data of the installed software with Software Management Framework Agent API (application programming interface). You can gather more detailed and accurate software inventory data from unmanaged computers. The new type of gathered data is not limited to Add/Remove Program information from the scans of the **Uninstall** registry key entries.

For more information, see the topics about Software Management Framework Agent and the **Software Discovery** scan in the *Symantec Management Platform User Guide*.

On managed computers, Software Management Framework Agent is installed along with Symantec Management Agent. During stand-alone inventory on unmanaged computers, Software Management Framework Agent does not depend on Symantec Management Agent. When you create a stand-alone inventory package, Software Management Framework Agent is picked up from the following location on your Notification Server computer:

`%InstallDir%\Altiris\Altiris Agent\Agents\SoftwareManagement`

When the stand-alone inventory package runs, Software Management Framework Agent stores the software discovery information in files with an NSE extension at the location that you specified for the package.

See "Gathering inventory using stand-alone packages" on page 66.

With the enhanced stand-alone software inventory that scans the **Uninstall** registry key entries, MSI cache, and other locations on the unmanaged computer, you can gather the following inventory data:

- Add/Remove Program information
- Installed software information
- MSI information

Note: Stand-alone software inventory with Software Management Framework Agent invokes **Software Discovery** scan and can take more resources and more time (up to 30 minutes) than the scan of registry key entries. However, this inventory method lets you gather more detailed and reliable inventory data of the software that is installed in your environment.

You can view the results of stand-alone software inventory in the following reports:

Newly Discovered Software report

A list of software applications that have been discovered using software inventory and have not matched the list of known applications and predefined software products.

To view the report, in the **Symantec Management Console**, on the **Manage** menu, click **Software**, and then in the left pane, under **Installed Software**, click **Newly Discovered Software**.

Installed Software report	A list of the software that is marked as installed, its version, count, and company name. To view the report, in the **Symantec Management Console**, on the **Reports** menu, click **All Reports > Discovery and Inventory > Inventory > Cross-platform > Software/Applications > Software**. To view additional details such as the computers on which the software is installed, right-click the software and click **View Details**.

See “About viewing inventory data” on page 155.

Note: To gather complete software inventory with stand-alone inventory packages from the Inventory Solution versions that are earlier than 7.1 SP2, you have to recreate and redistribute the packages. You recreate the stand-alone inventory packages by editing them and saving the changes.

See “Creating, editing, or cloning stand-alone inventory packages” on page 67.

Stand-alone software inventory helps you track the count of installed software but does not provide the count of computers that use the installed software. Thus you cannot harvest unused software licenses for unmanaged computers. For license harvesting, you need to install the Application Metering plug-in that runs within Symantec Management Agent only on managed computers.

See “About metering and denying applications” on page 106.

Gathering inventory using stand-alone packages

(Windows only)

Stand-alone packages let you gather inventory on the target computers that are not managed through the Symantec Management Agent.

See “About gathering inventory using stand-alone packages” on page 63.

See “About gathering stand-alone software inventory” on page 64.

Table 5-1 Process for gathering inventory using stand-alone packages

Step	Action	Description
Step 1	Create a stand-alone inventory package.	You create stand-alone inventory packages from the Symantec Management Console. See "Creating, editing, or cloning stand-alone inventory packages" on page 67.
Step 2	Run the stand-alone inventory package on the target computers.	You run the stand-alone packages on the target computers that gather the inventory data. See "Running stand-alone inventory packages on target computers" on page 71.
Step 3	If you need to, manually copy inventory data to the Notification Server computer.	If the target computer cannot communicate directly to the Notification Server computer, you must manually report the inventory data. See "Manually reporting stand-alone inventory data" on page 74.

Creating, editing, or cloning stand-alone inventory packages

(Windows only)

You can create, edit or clone a stand-alone inventory package. When you configure a package, you select how the data is reported to the Notification Server computer. The inventory data is stored in files with an NSE extension.

By default, your stand-alone inventory packages are located on your Notification Server computer in the following location:

```
%InstallDir%\Altiris\Notification
Server\NSCap\bin\Win32\X86\Inventory\StandalonePackages
```

This topic is a step in the process for gathering inventory using stand-alone packages.

See "Gathering inventory using stand-alone packages" on page 66.

To create, edit, or clone a stand-alone inventory package

1. In the **Symantec Management Console**, on the **Settings** menu, click **All Settings**.
2. In the left pane, under **Settings**, expand **Discovery and Inventory > Inventory Solution**, and then click **Stand-alone Inventory Packages**.
3. In the right pane, do one of the following:
   - To create a new package, click **New package**.
   - To edit a package, select an existing package and click the edit symbol.
   - To create an identical copy of a package, select a package and click **Clone package**.
     On the **Cloning the package** page, name the package, and then click **OK**.
4. Name and describe the package.
5. Configure the package options.

   See "Stand-alone inventory package options" on page 68.
6. Click **OK**.
7. You can view the properties of the package from the **Stand-alone Inventory Packages** page.

   The properties include the path of the package file as well as the configuration settings of the package.

Stand-alone inventory package options

(Windows only)

When you create or edit a stand-alone inventory package, you can configure the its options. You define the type of inventory gathered, where to store the data, and other options. You can view the properties of a package from the main **Stand-alone Inventory Packages** page.

When configuring where to store the inventory data, you select an option based on what access target computers have to the Notification Server computer.

See "Gathering inventory using stand-alone packages" on page 66.

See "Creating, editing, or cloning stand-alone inventory packages" on page 67.

See "Running stand-alone inventory packages on target computers" on page 71.

Note: When the package is run, you can override some of these settings with a command-line switch.

See "Stand-alone inventory package command-line switches" on page 73.

Table 5-2 Stand-alone inventory package options

Setting	Description
Select the types of inventory to gather	You can select the type of inventory data to gather. To select a detailed set of data, click **Advanced**. See "Inventory advanced options" on page 55. See "About inventory types" on page 15.
When running on the target computer	The option **Show progress** causes a dialog box to open on the computer that is running the package. The dialog displays the data classes that are gathered and then where the data is posted after the inventory is completed.
After running on the target computer	The option **Keep the inventory cached for future comparisons** keeps the inventory data cached so that you can compare the inventory data in the future. Inventory data comparisons are performed using command-line switches. See "Running stand-alone inventory packages on target computers" on page 71.

Table 5-2 Stand-alone inventory package options *(continued)*

Setting	Description
Send inventory data to	This option lets you configure where the inventory data is stored after it is gathered. You can choose from the following options: ■ **Notification Server** If target computers can communicate with the Notification Server computer using HTTP (port 80 open) or HTTPS (port 443 open), you can use this option. When the package is run, the inventory data is automatically sent to the Notification Server computer. The URL that is used is displayed on the page. ■ **Folder** You can store the data on the local computer, on a share, or on the Notification Server computer. When the package is run, the inventory data is automatically saved on that share. Inventory data files are stored with an NSE extension. If target computers can access a shared folder on the Notification Server computer, you can store it directly to a share on the server. The Notification Server computer share to use with this option is: \\notification_server_name\NSCap\EvtInbox If the target computer cannot access the Notification Server computer, you can store the inventory data on the local computer. You can also store it on another computer that is not the Notification Server computer. You must then manually copy the files to the Notification Server computer. You may have to use this option for the following situations: ■ Computers that are not regularly attached to the network ■ Computers that are outside the intranet that the Notification Server computer is on. You can specify a share or a path on the local computer. If you specify a local path, that folder is created on each target computer. For example, C:\Inventory_Data Inventory data files are stored with an NSE extension. You can also use environment variables when specifying the path to folder. For example: \\IntermediateShare\\`%computername%` If stand-alone inventory fails to post the NSEs to the specified target (an HTTP or HTTPS location or a folder), it deletes the NSE, NSI, and BAK files from the folders *`%programfiles%`*`\Altiris\NSI` and *`%programfiles%`*`\Altiris\Inventory\Outbox`. When the stand-alone inventory runs next time, it recreates the inventory. The **NSI** and **Outbox** folders are removed if they are empty. This procedure is done to make sure stand-alone inventory reports correct inventory to the Notification Server computer even if users are running stand-alone inventory packages with the `/SendChangedInventory` command-line switch.

Table 5-2 Stand-alone inventory package options *(continued)*

Setting	Description
Advanced	You can configure advanced settings for running a stand-alone inventory package. See "Inventory advanced options" on page 55.

Running stand-alone inventory packages on target computers

(Windows only)

After you create stand-alone inventory packages on Notification Server, you run the packages on target computers to gather inventory data. Stand-alone inventory packages are EXE files.

See "Creating, editing, or cloning stand-alone inventory packages" on page 67.

To run a stand-alone package and gather the inventory correctly, the logged on user must be a local administrator.

This topic is a step in the process for gathering inventory using stand-alone packages.

See "Gathering inventory using stand-alone packages" on page 66.

To run stand-alone inventory packages on target computers

1. Make the stand-alone inventory package available to the target computers.

   See "About methods for making stand-alone inventory packages available to target computers" on page 72.

2. (Optional) Use command-line switches to modify the default behavior of the package.

   See "Stand-alone inventory package command-line switches" on page 73.

3. Run the stand-alone inventory package.

4. (Optional) If you distribute the stand-alone inventory packages manually, you must also manually copy the inventory data files to the Notification Server computer after you run the package.

   See "Manually reporting stand-alone inventory data" on page 74.

About methods for making stand-alone inventory packages available to target computers

(Windows only)

Before you can run stand-alone inventory package, you must make it available to the target computers.

See "Running stand-alone inventory packages on target computers" on page 71.

You can use multiple methods to make the packages available to target computers. The method that you use affects how the inventory data is reported back to Notification Server.

Table 5-3 Methods for making the stand-alone inventory packages available to target computers

Method	Description
Packages are made available on the Notification Server computer.	If target computers can communicate with the Notification Server computer, you can make the stand-alone inventory packages available on the Notification Server computer. Client computers can access the packages in following ways: ■ From a Notification Server URL (port 80 open for HTTP and port 443 open for HTTPS) ■ From a Notification Server share See "Stand-alone inventory package options" on page 68. When you create a package, you can view the paths for the package on the **Standalone Inventory Packages** page.
Packages are distributed manually.	If the target computer cannot access the Notification Server computer using a URL or share, you can manually distribute the package. For example, you can email the package or place it on a different server's share or URL. If you use this method, you must manually copy the inventory data files to the Notification Server computer after you run the package. See "Manually reporting stand-alone inventory data" on page 74.

Stand-alone inventory package command-line switches

(Windows only)

When you run a stand-alone inventory package, the package uses the options that are selected when the package was created. When you run a package, you can use command-line switches to modify default behavior.

See "Stand-alone inventory package options" on page 68.

See "Running stand-alone inventory packages on target computers" on page 71.

These switches are not case-sensitive.

Table 5-4 Stand-alone inventory package command-line switches

Command-line switch	Description
`/EnableVerboseLog`	By default, all the errors are logged. If you specify `/EnableVerboseLog` at the command line, it enables verbose logging. If verbose logging is enabled, the trace messages are also logged. The log is stored on the local computers at the following locations: ■ `*InstallDir*\Altiris\Altiris Agent\Logs` folder as `Agent*.log` on managed computers ■ `*%ProgramFiles%*\Altiris\Altiris Agent\Logs` folder as `a*.log` on unmanaged computers.
`/SendChangedInventory`	By default, a stand-alone inventory package reports all the gathered inventory. If you use this switch, the package reports only the inventory data that has changed since the last scan. To gather only changed data, the package compares the previously collected data, if the previous data was cached. To cache inventory data, check **Keep the inventory cached for future comparisons** in the package configuration page. See "Creating, editing, or cloning stand-alone inventory packages" on page 67. If no previous inventory data is present, all gathered inventory is reported. If you have multiple Notification Servers, do not use this option if you report data to a server that does not have the previous data stored on it.

Table 5-4 Stand-alone inventory package command-line switches *(continued)*

Command-line switch	Description
`/SendInventoryTo` *destination*	Use this switch to override the value for the **Send inventory data to** option that is specified in the stand-alone package. The destination can be either an http(s) link to the Notification Server computer or a folder path. For example, you can store the NSE on a USB drive. You can use environment variables when specifying the destination. For example, you can use the following command: `package_name.exe /SendInventoryTo \\server_name\Inventory\%COMPUTERNAME%.` This command creates a separate folder for each computer at `\server_name\Inventory` and stores the NSEs in that folder. The folder is the same as the target computer's name.

Manually reporting stand-alone inventory data

(Windows only)

When the stand-alone inventory package runs, its options or a command-line switch determine where the inventory data is stored. If the stand-alone inventory package saves the inventory data to a location other than the Notification Server computer, you must manually copy the inventory data.

See "Running stand-alone inventory packages on target computers" on page 71.

The inventory data is stored in files with an NSE extension. The NSE files must be copied to a Notification Server computer by a user who has rights to the server. Generally, any user on a managed computer has sufficient rights.

This topic is a step in the process for gathering inventory using stand-alone packages.

See "Gathering inventory using stand-alone packages" on page 66.

Manually reporting stand-alone inventory data

◆ Copy the inventory files to the following folder:

```
\\notification_server_name\NSCap\EvtInbox
```

When the files are copied, the inventory data is stored in the Configuration Management Database (CMDB).

Gathering custom inventory

This chapter includes the following topics:

About gathering custom inventory

Custom inventory helps you extend the type of inventory you gather by adding the new data classes that are not included by default.

Custom inventory also lets you extend the use of a predefined data class by customizing it. For example, the attributes of the **Processor Extension** data class are **Device ID**, **L2 Cache Size**, and **L2 Cache Speed**. You can customize this data class by adding or removing attributes.

See "Gathering custom inventory" on page 76.

See "Creating and customizing a data class" on page 78.

If a custom data class is saved in the Configuration Management Database (CMDB) and is empty, you can modify it in the following ways:

- You can add nullable, non-nullable, key, and non-key attributes to it.

- You can delete its attributes.
- You can change the properties of its attributes.

If the custom data class contains data, you cannot modify it.

After you customize a data class, you create a task with scripting logic and schedule it to run on the target computers.

See "Creating a custom inventory script task" on page 80.

Warning: Use caution if you gather inventory using the custom data class and the same data class is also part of the standard inventory. When a standard inventory follows a custom inventory, the data that the standard inventory gathers overwrites the data that the custom inventory gathers. To prevent the custom inventory data from being overwritten, you must perform the custom inventory after the standard inventory.

Gathering custom inventory

Custom inventory lets you customize the set of inventory data that is gathered and reported to the Configuration Management Database (CMDB).

See "About gathering custom inventory" on page 75.

Table 6-1 Process for gathering custom inventory

Step	Action	Description
Step 1	Create a custom data class.	Create a custom data class from the data class manager user interface. After you create a custom data class, you can add, edit, and delete its attributes. See "Creating and customizing a data class" on page 78.

Table 6-1 Process for gathering custom inventory *(continued)*

Step	Action	Description
Step 2	Create a task with scripting logic and schedule it to run on the target computers.	You can create a new task or clone an existing sample task. To gather the inventory you want, you can use the script that is included in the sample task or you can create your own logic. Depending on the platform, you can write the logic in JavaScript, shell script, or other scripting languages. See "Creating a custom inventory script task" on page 80.
Step 3	View the gathered inventory.	Use the Resource Manager to view the custom inventory data that is gathered. See "Viewing gathered custom inventory data" on page 88.

About custom inventory data classes

Custom inventory data classes store the custom inventory data. A data class is a table in the Configuration Management Database (CMDB). For example, the **Processor_Ex** data class is the **Inv_Processor_Ex** table in the CMDB. Each data class has a set of attributes that define its properties.

Table 6-2 Example of attributes of the **Processor Extension** data class

Attribute	Description
Device ID	Specifies the unique index that is used to identify the device.
L2 Cache Size	Specifies the size of the Level 2 processor cache in kilobytes.
L2 Cache Speed	Specifies the clock speed of the Level 2 processor cache in megahertz.

You can create a data class, and then customize it by adding, editing, and deleting its attributes. A data class that is customized is referred to as a custom data class.

See "Creating and customizing a data class" on page 78.

After you customize a data class, you can create a task, customize the task script, and roll it out to the target computers.

See "Creating a custom inventory script task" on page 80.

The custom inventory script task that runs on the client computers generates a Notification Server Event (NSE) that contains inventory for a data class. A unique GUID identifies each data class. The inventory in the NSE is coupled with the GUID of a data class. The NSE loads the inventory in the data class that has the same GUID associated with it.

Note: The script that gathers inventory on Windows computers contains a reference to the GUID of a custom data class. Every time you create or edit an existing custom data class, the data class is assigned with a new GUID. You must manually update the script with the new GUID, if it refers to the older GUID for the same custom data class.

Creating and customizing a data class

From the Symantec Management Console, you can create a custom data class. You can add, edit, and delete attributes of the data class and you can change the position of the attribute. You can also find the GUID and view the data in the data class.

Be aware that every time you modify an attribute and you save the changes, the data class is assigned a new GUID.

See "About custom inventory data classes" on page 77.

See "About gathering custom inventory" on page 75.

This topic is a step in the process for gathering custom inventory.

See "Gathering custom inventory" on page 76.

To create and customize a data class

1. In the **Symantec Management Console**, on the **Settings** menu, click **All Settings**.
2. In the left pane, under **Settings**, expand **Discovery and Inventory > Inventory Solution**, and then click **Manage Custom Data classes**.
3. To create a data class, do the following:
   - On the **Manage Custom Data Classes** page, click **New data class**.
   - On the **New Data Class** page, enter a name and a description for the data class and click **OK**.
     The name of the new data class must be unique.

4 To customize a data class, on the **Manage Custom Data Classes** page, in the data classes list, click the data class.

You customize the data class by adding, editing, and deleting its attributes.

5 (Optional) To add an attribute to the data class, do the following:

- Click **Add attribute**.
- In the **Data Class Attributes** dialog box, specify the details of the attribute.
  To add an attribute that uniquely defines a row in the data class, in the **Key** drop-down list, click **Yes**. You enforce that the attribute always has a unique value that is other than NULL.
  To add an attribute that should never be empty or blank, in the **Data required** drop-down list, click **Yes**.
  If in the **Key** drop-down list, you click **Yes**, the **Data required** option is automatically set to **Yes**. You cannot change it unless in the **Key** drop-down list, you click **No**.
- Click **OK**.

6 (Optional) To edit or delete the attributes, select the attribute, and then click the **Edit** or **Delete** symbols.

7 (Optional) To let the data class store inventory of multiple objects, on the **Manage Custom Data Classes** page, check **Allow multiple rows from a single computer resource**. The data class can store the inventory of services, user accounts, files, network cards, and other objects.

8 (Optional) To specify the sequence of the attributes, on the **Manage Custom Data Classes** page, click the attribute, whose position you want to change, and then click the up arrow or down arrow.

When you report inventory values for the columns in a Notification Server Event (NSE), the attributes are identified by the column ID and not by the column name. As a result, the order of attributes in a data class must be correct.

9 Click **Save changes**.

Warning: The final step of saving changes is very important. When you create any data class or add any attributes, all the information is stored in memory. Nothing is created in the database and on details page, no GUID is yet assigned. As a result, a 00000000-0000-0000-0000-000000000000 GUID is displayed in the property of the data class. Only after you click **Save changes** on the **Manage Custom Data Classes** page, the data class is saved in the database, and the GUID is generated. Note that the GUID changes every time you make changes to the definition of the data class and save it.

Creating a custom inventory script task

After you have created the custom inventory data class, you create a custom inventory script task that gathers the custom inventory. The script task is configured with the script to gather the custom inventory and the schedule of the task.

See "Creating and customizing a data class" on page 78.

To create a custom inventory script task, you can clone a sample script task and modify it with the custom data classes that you created. You can also create and confgure a custom inventory script task on the **Jobs and Tasks** portal page.

When you customize your custom inventory script, you can benefit from different options that let you easily insert a token to the script and create or edit tokens for use in the script.

For more information, see the topics about the **Run script task** page and the **Tokens** page in the *Symantec Management Platform User Guide*.

Note: The process of creating a custom inventory script task is the same across all platforms: Windows, UNIX, Linux, and Mac. However, the scripting language and the logic that is used in the scripts are different.

For more information, see the topics about running a task and about task advanced options in the *Symantec Management Platform User Guide*.

See "About gathering custom inventory" on page 75.

This topic is a step in the process for gathering custom inventory.

See "Gathering custom inventory" on page 76.

To clone a sample custom inventory script task

1. In the **Symantec Management Console**, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, under **Jobs and Tasks**, expand **Samples > Discovery and Inventory > Inventory samples > Custom**.
3. Right-click the sample custom inventory script task and click **Clone**.
4. In the **Clone** dialog box, give the cloned script a descriptive name and click **OK**.

5 (Optional) Customize the sample script, and then click **Save changes**.

Depending on the selected script type, you have different options to customize the sample script.

See "Customizing the custom inventory sample script for Windows" on page 82.

See "Customizing the custom inventory sample script for UNIX, Linux, and Mac" on page 86.

6 Under **Task Status**, do one of the following:

- To schedule the task to run on client computers, click **New Schedule**.
- To perform a quick run of the task on client computers, click **Quick Run**.

7 Click **Save changes**.

To create a custom inventory script task

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

2 In the left pane, navigate to the folder where you want to create a custom inventory script task, right-click the folder, and then click **New > Task**.

For example, to create the task in the **Jobs and Tasks** folder, right-click **Jobs and Tasks**, and then click **New > Task**.

To create the task in the **Inventory** folder, expand **Jobs and Tasks > System Jobs and Tasks > Discovery and Inventory**, right-click **Inventory**, and then click **New > Task**.

3 In the **Create New Task** dialog box, in the left pane, click **Run Script**.

4 In the right pane, enter a descriptive name for the task.

5 In the **Script type** drop-down list, select the script type.

6 Enter your own script or copy a sample custom inventory script to the script editor.

To easily insert a token to your custom inventory script, do the following:

- In the **Insert token** drop-down list, select the token that you want to insert.
- Click **Insert**.

To access a sample custom inventory script, do the following:

- In the **Symantec Management Console**, on the **Manage** menu, click **Jobs and Tasks**.
- In the left pane, under **Jobs and Tasks**, expand **Samples > Discovery and Inventory > Inventory samples > Custom**.

7 (Optional) In the **Create New Task** dialog box, in the script editor, customize the copied sample script or your own script.

Depending on the selected script type, you have different options to customize the script.

See "Customizing the custom inventory sample script for Windows" on page 82.

See "Customizing the custom inventory sample script for UNIX, Linux, and Mac" on page 86.

8 (Optional) To configure the advanced options for running the custom inventory script task, do the following:

- Click **Advanced**, and on the **Script** tab, specify the user account that the task runs in and other script options.
- In the **Task options** tab, specify the settings for running the script task simultaneously with other tasks and the maximum possible length of the script task.
- Click **OK**.

9 In the **Create New Task** dialog box, click **OK**.

10 On the **Run Script** page, under **Task Status**, do one of the following:

- To schedule the task to run on client computers, click **New Schedule**.
- To perform a quick run of the task on client computers, click **Quick Run**.

11 Click **Save changes**.

Customizing the custom inventory sample script for Windows

(Windows only)

The easiest way to create a new custom inventory script task is to clone the existing sample and customize it according to your needs. The sample script for Windows already contains the required code for a WMI query. You only need to add your own logic to gather the data that you want and to populate the attribute variables in the script.

Note: Every time you create or edit an existing custom data class, the data class is assigned a new GUID. You must manually update the script with the new GUID, if it refers to the older GUID for the same custom data class.

See “Creating a custom inventory script task” on page 80.

See “Gathering custom inventory” on page 76.

To customize the custom inventory sample script for Windows

1 Clone or open an existing sample of the custom inventory script task.

2 Specify the values that you want to gather.

   Example:

   ```
   strComputer = "."

   Set objWMIService = GetObject("winmgmts:" &

   "{impersonationLevel=impersonate}!\\" & strComputer &
   "\root\cimv2")

   'Fire WMI Query

   Set objCIMObj = objWMIService.ExecQuery("select * from
   CIM_processor")
   ```

3 Replace the GUID with the GUID of the data class that you created.

   Example:

   ```
   set objDCInstance = nse.AddDataClass ("{e8220123-4987-4b5e-bc39-
   ec6eaea312ef}")
   ```

   To access the GUID of the data class that you created, do the following:

   - In the **Symantec Management Console**, on the **Settings** menu, click **All Settings**.
   - In the left pane, under **Settings**, expand **Discovery and Inventory > Inventory Solution**, and then click **Manage Custom Data classes**.
   - On the **Manage Custom Data Classes** page, select the data class and click the **Details** symbol.

4 Update attributes of the data class.

Example:

```
For each objInfo in objCIMObj

'Add a new row

dim objDataRow

set objDataRow = objDataClass.AddRow

'Set columns

objDataRow.SetField 0, objInfo.DeviceID

objDataRow.SetField 1, objInfo.L2CacheSize

objDataRow.SetField 2, objInfo.L2CacheSpeed

Next
```

5 Click **Save changes**.

Custom inventory sample script for Windows

(Windows only)

The sample inventory script for Windows does the following:

- Creates a WMI object, runs a WMI query, and stores the result set.
- Creates a Notification Server event (NSE) object.
- Creates an Inventory data block and associates it with a specific custom data class.
- Loops through each row in the result set and populates each row of the result set into a row in the data block.
- Processes and sends the NSE to Notification Server.

See "Customizing the custom inventory sample script for Windows" on page 82.

The following is a sample script:

```
'The following is a sample custom inventory script gathering
information about the processor of a computer and posting data to
the server using Altiris NSE Component

'===================================================================

' On Error Resume Next

'Create instance of Wbem service object and connect to namespace
```

```
strComputer = "."

Set objWMIService = GetObject("winmgmts:" &

"{impersonationLevel=impersonate}!\\" & strComputer & "\root\cimv2")

'Fire WMI Query

Set objCIMObj = objWMIService.ExecQuery("select * from CIM_processor")

'======================================================================

'Create instance of Altiris NSE component

dim nse

set nse = WScript.CreateObject ("Altiris.AeXNSEvent")

' Set the header data of the NSE

' Please don't modify this GUID

nse.To = "{1592B913-72F3-4C36-91D2-D4EDA21D2F96}"

nse.Priority = 1

'Create Inventory data block. Here assumption is that the data class
with

below guid is already configured on server

dim objDCInstance

set objDCInstance = nse.AddDataClass ("{e8220123-4987-4b5e-bc39-

ec6eaea312ef}")

dim objDataClass

set objDataClass = nse.AddDataBlock (objDCInstance)

For each objInfo in objCIMObj

'Add a new row

dim objDataRow

set objDataRow = objDataClass.AddRow

'Set columns

objDataRow.SetField 0, objInfo.DeviceID

objDataRow.SetField 1, objInfo.L2CacheSize

objDataRow.SetField 2, objInfo.L2CacheSpeed
```

```
Next
```

```
nse.SendQueued
```

Customizing the custom inventory sample script for UNIX, Linux, and Mac

(UNIX, Linux, and Mac only)

The custom inventory script for UNIX, Linux, and Mac generates a text output that contains the collected inventory data in a specified format. This data is used to create the NSE and is posted into the Configuration Management Database (CMDB). The logic of creating the NSE and posting the data is hidden from the user.

When you customize the sample script, you can modify the output that the script generates.

See “Creating a custom inventory script task” on page 80.

See “Gathering custom inventory” on page 76.

To customize the custom inventory sample script for UNIX, Linux, and Mac

1. Clone or open an existing sample of the custom inventory script task.

   Note that the first lines of the script should not be changed. Changes should be made after the `# SCRIPT_BEGINS_HERE` label.

2. Specify the data class.

   Example:

   ```
   echo UNIX_PS_List
   ```

3. Specify the delimiters.

   Example:

   ```
   echo "Delimiters=\" \" "
   ```

4. Specify the data type and the length of each column.

   Example:

   ```
   echo string20 string20 string20 string256
   ```

5. Specify the column names.

   Example:

   ```
   echo PID Terminal Time Command
   ```

   Note that the column names are not used in 7.x custom inventory. The column names are left for backward compatibility with 6.x Inventory Solution. You can leave this line empty in 7.x but keep the `echo` command intact.

   Example:

   ```
   echo
   ```

6. Specify commands to retrieve data from system.

   Example:

   ```
   ps -e
   ```

7. Click **Save changes**.

Custom inventory sample script for UNIX, Linux, and Mac

(UNIX, Linux, and Mac only)

The sample inventory script for UNIX, Linux, and Mac does the following:

- Includes a helper script that implements the logic of creating NSE and posting it to Configuration Management Database (CMDB).
- Specifies the data class.
- Specifies delimiters for use in parsing the data that is returned from the command that runs.
- Specifies the data type and length of each column.
- Specifies the column names. The column names are only required when the command that runs does not already include column headings.
- Runs the desired command. In this case, appropriate platform-specific commands run.

See "Customizing the custom inventory sample script for UNIX, Linux, and Mac" on page 86.

The following is a sample script:

```
. `aex-helper info path -s INVENTORY`/lib/helpers/custominv_inc.sh

#

# Sample script for custom inventory
```

```
# The first line of code should be always included at the begin of
the script

# Actual script for collecting inventory data begins after the
following label:

# SCRIPT_BEGINS_HERE

#!/bin/sh

echo UNIX_PS_List

echo "Delimiters=\" \" "

echo string20 string20 string20 string256

echo PID Terminal Time Command

if [ "`uname -s`" = "Darwin" ] ; then

ps -ax | sed -e "1d" | awk '{print $1 " " $2 " " $4 " " $5 " " }'

else

ps -e | sed -e "1d" | awk '{print $1 " " $2 " " $3 " " $4 " " }'

fi
```

Viewing gathered custom inventory data

When the inventory data is gathered, it is stored in the Configuration Management Database (CMDB). You can use the Resource Manager to view the custom inventory data that is gathered from a computer.

For more information, see the topics about using the Resource Manager in the *Symantec Management Platform User Guide*.

See "About viewing inventory data in the Resource Manager" on page 157.

This topic is a step in the process for gathering custom inventory.

See "Gathering custom inventory" on page 76.

To view gathered custom inventory data

1. In the Symantec Management Console, on the **Manage** menu, click **Filters**.
2. On the left pane, click **Computer Filters > All Computers**.
3. On the right pane, under **Filter Membership**, right-click a computer, and then click **Resource Manager**.

4 On the **Resource Manager** page, click **View > Inventory**.

5 To view the data, double-click a data class.

Chapter 7

Gathering software inventory

This chapter includes the following topics:

About gathering software inventory

Software inventory collects information about the applications that are installed on your client computers and helps you analyze different aspects of your resources.

For example, you can identify the computers that do not meet minimum security requirements: you collect information about the computers that do not have antivirus software or application updates installed. You can also prepare for a software license audit by finding out the number of installed instances of an application. Or you can quickly check whether a specific software is installed on your managed computers.

Software inventory tasks or policies scan the target computers for the available software applications and report the collected information to Notification Server.

You can collect information about both standard applications and custom software applications that are installed on your client computers.

The installed software that you can identify and inventory on your client computers is defined as a software component. You can have software components automatically associated with the predefined software products that Inventory Solution provides. Thus Inventory Solution lets you manage and track software usage at the product level instead of the file level. For example, you can manage Microsoft Office 2008 as a software product, and see it in reports as Microsoft Office 2008, not as `winword.exe`.

For more information, see the topics about managing software in the *Altiris™ IT Management Suite 7.1 from Symantec™ Enhanced Console Views Getting Started Guide* at the following URL:

http://www.symantec.com/docs/DOC3563

See "About targeted software inventory" on page 94.

See "About how Inventory Solution works with the Software Catalog Data Provider" on page 100.

See "About viewing inventory data" on page 155.

About methods for gathering software inventory

You can gather inventory about the software applications that are installed in your environment. For example, you can gather information about the application version, build number, and manufacturer.

Note: If a manufacturer does not provide the version of its software, a version is not populated for the relevant software component.

When you perform a software inventory, you can use different methods to gather different types of data.

See "About viewing inventory data" on page 155.

Table 7-1 Methods for gathering software inventory

Method	Description
Basic application file inventory.	This method scans the file system on target computers and reports software inventory based on the application EXE files that are found. For example, it reports file name, size, path, and so on. You can perform this inventory by selecting the **File Properties - manufacturer, version, size, internal name, etc.** option in the Inventory policies or tasks.
Add or Remove Programs list and UNIX/Linux/Mac software packages.	To perform this inventory, select the **Software – Windows Add/Remove Programs and UNIX/Linux/Mac software packages** option in the Inventory policies or tasks. This option is enabled by default. See "Inventory policy options" on page 54. This option uses the Software Discovery task to collect the information about the installed applications. For more information, see the topics about Software Discovery in the *Symantec Management Platform User Guide*. On Windows computers, you can gather information about the applications that are in the **Add or Remove Programs** list on target computers (MSI cache). Note that when Inventory Solution is installed, it turns off any schedules for the Software Discovery task. Instead, it uses the schedules of the Inventory policies that use it. On Windows computers, you can gather software inventory even if the target computers are not managed through the Symantec Management Agent. Stand-alone inventory packages let you gather inventory data of the installed software on the unmanaged Windows computers. See "About gathering stand-alone software inventory" on page 64. On UNIX, Linux, and Mac computers, you can gather information about the software packages on target computers.

Table 7-1 Methods for gathering software inventory *(continued)*

Method	Description
Targeted software inventory on Windows computers. Targeted software inventory using the `filescan.rule` file on UNIX, Linux, and Mac computers.	On Windows computers, this method lets you use rules to identify specific software applications. You can perform this inventory by running the **Targeted Software Inventory** policy. See "About targeted software inventory" on page 94. On UNIX, Linux, and Mac computers, this method lets you collect information about the installed applications using the `filescan.rule` file. The software inventory agent compares a list of applications in the `filescan.rule` file with the actual file system data to determine which applications are installed. See "About software inventory using the `filescan.rule` file" on page 97.
Gather software information and validate it using the Software Catalog Data Provider. (Windows only)	The Software Catalog Data Provider is a component that can be used to import software inventory data into the Software Catalog. The Software Catalog Data Provider is installed with Inventory Solution. The Software Catalog Data Provider provides a list of known applications and predefined software products that is imported in the Configuration Management Database (CMDB). When you perform a software inventory, the gathered data about applications can be compared to the list of known applications and predefined software products. If the application data matches, it helps ensure that your software inventory data is accurate and lets you manage installed software at the product level. See "About using Inventory Solution with the Software Catalog Data Provider" on page 99.

See "About gathering software inventory" on page 91.

About targeted software inventory

(Windows only)

Targeted software inventory feature determines whether a specific software is installed on managed computers. To find the software, it uses the software resource and detection rule information that is defined in the Software Catalog. This feature works with Windows computers only.

See “About methods for gathering software inventory” on page 92.

See “Running a targeted software inventory” on page 96.

To find the software, targeted software inventory feature uses the following information that is defined in the Software Catalog:

- Software resource.
  A software resource consists of the metadata that describes a specific instance of a software application. A software resource is associated with the physical package file that installs the software. On the **Targeted Software Inventory** policy page, you specify the software that you want to inventory. The policy then reports the computers that contain the software.
- The detection rule of a software resource.
  The detection rule that is associated with a software resource can be used to create a policy to determine if that software resource is installed on a given computer.
- The file associations of a software resource.
  The files that are associated with a software resource can be used to analyze the Inventory Solution file scan data to determine what software is installed on a given computer.

You can use the software information that is defined in the Software Catalog to determine whether a specific software is installed on one or more managed computers.

The **Targeted Software Inventory** policy populates the inventory cache on each client computer with the currently installed software data. That data is communicated to the Notification Server computer.

The software that you inventory must be defined as a software resource in the Software Catalog. It must also have at least one detection rule. If the software resource is not defined, contact an administrator who can edit the Software Catalog.

You can see the results of the Targeted Software Inventory in the **Installed Software** report. This report lists the software that is marked as installed, its version, and company name. To view additional details such as the computers on which the software is installed, right-click the software and click **View Details**. You can access the **Installed Software** report from the **Reports** menu, at **All Reports > Discovery and Inventory > Inventory > Cross-platform > Software/Applications > Software**.

See “About viewing inventory data” on page 155.

See “About how Inventory Solution works with the Software Catalog Data Provider” on page 100.

See "About gathering software inventory" on page 91.

Running a targeted software inventory

(Windows only)

Targeted software inventory determines whether specific software is installed on managed computers. To find the software, it uses the software resource and detection rule information that is defined in the Software Catalog.

See "About targeted software inventory" on page 94.

To run a targeted software inventory

1. In the **Symantec Management Console**, on the **Manage** menu, click **Policies**.
2. In the left pane, expand **Discovery and Inventory**.
3. Right-click **Targeted Software Inventory**, and then click **New > Targeted Software Inventory**.
4. In the upper left of the right pane, click and type the following text:

New Targeted Software Inventory	Type a name for this policy. Because the description does not always appear, make the name descriptive enough for other administrators to easily identify this policy.
Add description	Type a description to further identify this policy.

5. In the right pane, expand the **Software to inventory** section, and click **Select Software**.
6. In the **Select Software** dialog box, from the **Available software** list, select one or more software resources, add them to the **Selected software** list, and then click **OK**.
7. To edit the detection rule for a software resource, under the **Software to inventory** section, select the software resource, and click **Edit Rule**.

   For more information, see the topics about creating or editing inventory rules in the *Symantec Management Platform User Guide*.
8. On the policy page, expand the **Schedule** section, and define the schedule on which to check the client computers.

   See "Selecting computers and scheduling inventory tasks" on page 52.

9 On the policy page, expand the **Applied to** section, and select the client computers to check for the specified software resource.

See “Selecting computers and scheduling inventory tasks” on page 52.

10 On the policy page, turn on the policy.

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

11 On the policy page, click **Save changes**.

About software inventory using the `filescan.rule` file

(UNIX, Linux, and Mac only)

Software inventory using the `filescan.rule` file lets you collect information about the installed applications on your UNIX, Linux, and Mac computers.

A file scan agent that is included in software inventory uses the `filescan.rule` file to detect the applications that are installed on your client computers. The `filescan.rule` file contains the data sets that represent information regarding different applications. The file scan agent compares each data set to the actual file system data to find out whether an application is installed.

See “Running software inventory using the `filescan.rule` file” on page 98.

Each data set in the `filescan.rule` file consists of two lines of data. The first line is the application description data, and the second line is the matching criteria data. The application description data consists of the product name, the manufacturer, the version, and the description of the application. The matching criteria data includes a file name or the absolute path to the file that is part of the application, file size, and cyclic redundancy check (CRC). When the file scan agent finds this file in the specified directories, the associated product is reported as part of the inventory on that system.

A data set that represents information about an application in the `filescan.rule` file looks as follows:

```
product name = "Watcher" manufacturer = "Company" version = "3.24"
description = ""

file = "/opt/secret/eys/watcher" size = "45698" CRC = ""
```

A default `filescan.rule` file is included in the Inventory Plug-in installation package for each platform. It contains an example list of some common applications.

Symantec recommends that you customize the default `filescan.rule` file to include the additional applications that the software inventory should report. You can also add entries for the applications that are developed in-house.

After you customize the `filescan.rule` file, you can create a Quick Delivery task to redistribute it to all UNIX, Linux, and Mac client computers.

For more information, see the topics about creating a **Quick Delivery** task in the *Software Management Solution User Guide*.

See "About gathering software inventory" on page 91.

Running software inventory using the `filescan.rule` file

(UNIX, Linux, and Mac only)

To run the software inventory using the `filescan.rule` file, you must have the Symantec Management Agent and the Inventory Plug-in installed on your UNIX, Linux, and Mac client computers. The Inventory Plug-in installation package includes a default `filescan.rule` file that contains an example list of some common applications.

You can customize the default `filescan.rule` file and add the applications that you want to be reported. You can also use the aex-filesurveyor utility to scan your UNIX, Linux, and Mac systems for executables. The output of the scan is formatted for use as a `filescan.rule` file. After you create or customize a `filescan.rule` file, you can distribute it to the client computers.

The file scan agent uses the settings of the Inventory task or policy to scan the directories. If you want to change the set of the directories that are scanned, you must edit the advanced settings of the Inventory task or policy. When no directories are specified, then all local drives are scanned.

See "About software inventory using the `filescan.rule` file" on page 97.

To run software inventory using filescan.rule file

1. (Optional) Copy the default `filescan.rule` file from the client computer to the Notification Server computer and customize it.
2. (Optional) To distribute the customized `filescan.rule` file to the client computers, create a **Quick Delivery** task in the **Symantec Management Console**.

   The `filescan.rule` file should be copied to the following folder:

   ```
   /opt/altiris/notification/inventory/etc/
   ```

   You can use the following universal path with custom installation directories:

   ```
   `aex-helper info path -s INVENTORY`/etc/
   ```

   For more information, see the topics about creating a **Quick Delivery** task in the *Software Management Solution User Guide*.
3. For the Inventory policy that gathers software inventory, ensure that the option **File properties - manufacturer, version, size, internal name, etc.** is checked.

About using Inventory Solution with the Software Catalog Data Provider

(Windows only)

The Software Catalog Data Provider (SCDP) is a component that can be used to import software inventory data into the Software Catalog. The SCDP is installed with Inventory Solution. It provides a list of known applications and predefined software products that is imported into the Configuration Management Database (CMDB).

See "About how Inventory Solution works with the Software Catalog Data Provider" on page 100.

You need the SCDP to identify software in the following instances:

- The information that identifies the software cannot be gathered from Add/Remove Programs.
- The software is identified as a suite, and you need to identify a specific product in the suite.
- The software is identified as a product, and you need to identify the suite.
- You need to identify the edition of a software product such as standard, professional, or enterprise.

The data about the applications that software inventory gathers can be compared to the list of known applications and predefined software products. If the application inventory data matches the list of known applications, it helps ensure that your software inventory data is accurate. You can also have the matched application inventory data imported into the Software Catalog. This process runs automatically with the default inventory policy settings. You can view the list of the applications that are in the Software Catalog.

If the application inventory data matches the predefined software product data, the software component automatically becomes a managed software product and appears in the Software Catalog, in the **Managed software products** list.

For more information, see the topics about managing software in the *Altiris™ IT Management Suite 7.1 from Symantec™ Enhanced Console Views Getting Started Guide* at the following URL:

http://www.symantec.com/docs/DOC3563

About how Inventory Solution works with the Software Catalog Data Provider

(Windows only)

Several components work together to identify the detected software and to create a software resource for that software in the Software Catalog . By default, most of the Software Catalog Data Provider (SCDP) components perform automatically.

To have Inventory Solution work with the SCDP, in the inventory policy or task, ensure that the following checkboxes are checked:

- **Software – Windows Add/Remove Programs and UNIX/Linux/Mac software packages**
- **File properties - manufacturer, version, size, internal name, etc.**

See "About using Inventory Solution with the Software Catalog Data Provider" on page 99.

Table 7-2 Software Catalog Data Provider components

Component	Description
Software Catalog Data Provider component.	This component is installed with Inventory Solution. It contains a data file with a list of known applications and predefined software products such as Microsoft, Adobe, and Symantec products. This data file is updated regularly to include new applications, versions of applications, and predefined software products.

Table 7-2 Software Catalog Data Provider components *(continued)*

Component	Description
Software Catalog Data Provider task.	When the database of known applications and predefined software products is installed, this task automatically imports the list of known applications and predefined software products into the CMDB. To view this read-only task, in the **Symantec Management Console**, on the **Settings** menu, click **All Settings > Software > Data Provider > Providers > Software Catalog Data Provider**.
Data provider summary.	This summary is the list of known applications that has been automatically imported into the CMDB. To view this list, in the **Symantec Management Console**, on the **Settings** menu, click **Console > Views**, and then in the left pane, click **Software > Data Provider Summary**. For more information, see the topics about the **Data Provider Summary** page and about gathering available software resources in the *Symantec Management Platform User Guide*.
Predefined software products.	Software products are collections of one or many software components that administrators and users intend to purchase, license, inventory, and manage. SCDP provides software product definitions that let you distinguish which software components on your client computers can be defined as a software product. The list of predefined software products includes the programs about which companies are most concerned in terms of managing software licenses and being prepared for software audits. For example, the list includes Microsoft, Adobe, and Symantec products. Predefined software products have the product name, the product version, and the associated application files. Predefined software products let you easily perform the following actions at the product level: ■ Meter application usage ■ Track and manage software licenses See "Metering and tracking usage of the managed software products in the enhanced Symantec Management Console Software view" on page 122. For more information, see the topics about managing software licenses in the *Asset Management Suite User Guide*. You can view the predefined software products that are installed and discovered in your environment in the Software Catalog, in the **Managed software products** list or in the **Unmanaged software** list.

Table 7-2 Software Catalog Data Provider components *(continued)*

Component	Description
Inventory policy or task.	Run an inventory policy or task with the following checkboxes checked: ■ **Software – Windows Add/Remove Programs and UNIX/Linux/Mac software packages**. ■ **File properties - manufacturer, version, size, internal name, etc.** By default, the **Collect Full Inventory** policy runs every Monday at 18.00 (6:00 P.M., agent time). The software inventory data is gathered and entered into the CMDB.
Software Catalog Data Provider Inventory task.	This task compares the gathered software inventory to the list of known applications (software resources) in the CMDB. By default, this task runs every Wednesday. You can also schedule a new task. For more information, see the topics about schedules in the *Symantec Management Platform User Guide*. To view the task, in the **Symantec Management Console**, on the **Settings** menu, click **All Settings > Software > Data Provider > Software Catalog Data Provider Inventory**. If the data matches, the application data is automatically imported into the Software Catalog. The software resource is created with the minimum metadata that consists of company (vendor) name, software name, and version. If the software resource is already in the Software Catalog, precedence settings determine if it can update the data. For more information, see the topics about precedence settings in the *Symantec Management Platform User Guide*.

Table 7-2 Software Catalog Data Provider components *(continued)*

Component	Description
Dynamic real-time association event.	A predefined event that automatically runs on Notification Server every time a new software component is discovered and imported into the CMDB. This event compares the software components that software inventory discovers with the predefined software products. If there is a match, the event associates the discovered software components with the relevant predefined software product and moves the product to the Software Catalog, to the **Managed software products** list. The discovered software components become a managed software product. **Note:** If a manufacturer does not provide the version of its software, a version is not populated for the relevant software component. As a result, the software component does not get dynamically associated with a proper predefined software product. See "About the predefined nightly task NS.Nightly schedule to associate Software component to software product" on page 121. For more information, see the topics about managing software in the *Altiris™ IT Management Suite 7.1 from Symantec™ Enhanced Console Views Getting Started Guide* at the following URL: http://www.symantec.com/docs/DOC3563
Newly Discovered Software report.	A list of software applications that have been discovered using software inventory and have not matched the list of known applications and predefined software products. To view the list, in the **Symantec Management Console**, on the **Manage** menu, click **Software**, and then in the left pane, under **Installed Software**, click **Newly Discovered Software**.

Chapter 8

Metering and denying applications

This chapter includes the following topics:

- About application summary data
- About how application metering summary is sent
- Configuring application metering data
- Viewing application metering reports
- Viewing usage tracking reports in the enhanced Symantec Management Console Software view

About metering and denying applications

(Windows only)

Application metering lets you perform following tasks on your managed computers:

- Control the availability of applications
- Monitor the use of applications

This feature requires the Symantec Management Agent and an Application Metering Plug-in be installed on target computers.

Note: Application metering is a Windows-only feature and is supported on Windows XP and above client computers only. Symantec recommends that you do not install Application Metering Plug-in on Windows servers.

See "Preparing managed computers for inventory and metering" on page 37.

Table 8-1 Application metering functions

Function	Description
Monitoring applications.	You can monitor and record the usage of applications. The data is recorded in the CMDB and is viewable through reports. Application metering reports let you view the following information: ■ Which metered applications were used ■ Application resource usage statistics See "About application metering start, stop, and denial events" on page 124. See "About metering and tracking usage of the managed software products in the enhanced Symantec Management Console Software view" on page 119. See "About application summary data" on page 126. See "Viewing application metering reports" on page 130. See "About viewing inventory data" on page 155.
Denying applications.	You can control the availability of an application with the following options: ■ Allow an application to run at all times ■ Deny an application from running at all times ■ Deny an application from running at specified times or on specified days If a user tries to run a denied application, it is stopped immediately. A prompt can be shown to the user for the application that was denied. You can also configure deny events to be sent to Notification Server when a user tries to run a denied application. These events can then be used to trigger sending an email to an administrator. You can also view the reports that list the denied applications that were attempted to run. See "Metering and denying applications" on page 113. You can deny one or more applications using a single policy. You can also deny several applications using the Blacklisted Applications policy. See "About blacklisting applications" on page 109.

When you meter applications, you define the applications you want to monitor or deny by creating application definitions.

See "About defining applications to meter or deny" on page 109.

Notification Server polices control the rules for metering applications. The Application Metering Plug-in that runs with the Symantec Management Agent on the target computer enforces the properties of the policies.

See "About how application metering works" on page 108.

See "Metering and denying applications" on page 113.

You can meter a variety of types of applications.

Table 8-2 Application types that you can meter

Operating system	Win64 Applications	Win32 Applications	Win16 Applications
Windows NT / 2000 / XP / Vista / 7	Yes	Yes	No
Windows 9x / ME	No	No	No

Warning: When you use application metering policies, it is possible for multiple policies to monitor the same application. This situation might cause erroneous data in reports or trigger duplicate notification policy actions.

About how application metering works

(Windows only)

The rules for metering applications are controlled through Notification Server polices. The Application Metering Plug-in, which runs with the Symantec Management Agent on the target computer, enforces the properties of the policy. An application metering policy can meter one or more applications.

See "About metering and denying applications" on page 106.

When an application starts on a managed computer, the Application Metering Plug-in checks for an enabled policy monitoring the application.

If the plug-in finds an enabled policy, it does the following functions:

- Records the application summary data locally and sends this data to the Configuration Management Database (CMDB) at the end of the application monitoring period.

- Sends the event notifications to the CMDB as specified in the monitoring policy. It can send application start, stop, or denial events. It sends this information in batches at a specified interval.
- Denies the use of the application if the monitoring policy so specifies.

About blacklisting applications

(Windows only)

Blacklisting is an application metering feature that lets you deny multiple applications from running on client computers.

See “About metering and denying applications” on page 106.

Blacklisting is performed by configuring the Blacklisted Applications policy. This policy is a predefined policy. You can add as many applications to this policy as you want. The other way to add applications to the Blacklisted Applications policy is to right-click an application in the Software Catalog, and then click **Actions > Blacklist Application**.

When you blacklist any software component, the software component is scanned looking for an .exe file. If that software component contains any .exe file, it is blacklisted. A separate rule is created for every .exe file.

If the software component is successfully blacklisted, the following message is displayed in a dialog:

“The following software has been successfully marked as blacklisted.”

Otherwise it displays “The following software cannot be blacklisted because it is not associated with any executable files.”

See “Creating and configuring application metering policies” on page 115.

About defining applications to meter or deny

(Windows only)

When you configure an application metering policy, you define the applications you want to meter by creating application definitions. You can use broad or specific product definitions. For example, you can use one definition to meter all Microsoft applications or you can use a specific definition to meter Word version 12. The metering options for each policy apply to all the applications you have added in the list for that policy.

See “About metering and denying applications” on page 106.

Several predefined application metering policies are included.

Each application that you define has a set of definition details about the application. The details include the product name, file name, product version, product company, and so on. Application metering policies use these details to identify the applications to meter on target computers. You can specify as many or as few of these details as needed.

You add definitions by populating fields in the **Application Definition Details** dialog box. The definition details correspond to the properties of an EXE file. You can see the properties of an EXE by right-clicking the file, then clicking **Properties** then the **Version** tab. You can populate these fields manually or import them from a known application.

See “About application definition details” on page 111.

After you add an application definition to a policy, it appears in the list on the **Software** tab of the application metering policy page. You can also edit application definitions.

See “Defining applications to meter or deny” on page 110.

Defining applications to meter or deny

(Windows only)

When you configure an application metering policy, you define the applications you want to meter by creating application definitions. You specify a list of application definitions for every application metering policy. When you define application definitions, you specify a set of definition details about the application.

For each metering policy, you can have one or more applications defined.

See “About defining applications to meter or deny” on page 109.

To define applications to meter or deny

1. Open an application metering policy.

   See “Creating and configuring application metering policies” on page 115.

2. On the application metering policy page, on the **Software** tab, click the **Add** drop-down list.

3. Select one of the following methods that let you enter definition details for an application and create a list of applications in a single policy:

   - Click **Software**, and in the **Select Software** dialog box, click the application that you want to meter or deny; then click **OK**.
     On the **Software** tab, you can choose applications from a list of known software programs that are defined in the Software Catalog. The list generally contains the software that is already installed on computers on

your network. The list may contain multiple versions of the same application.

This method is useful to quickly include a known software application without manually configuring application definition details. However, the known application definition details may be too specific. For example, it is important to note that application definitions may be version-specific, especially those using known software application details. If you use a known application from the **Software** drop-down menu, you may want to edit application definition details to meet your needs.

See "About defining applications to meter or deny" on page 109.

- Click **Rule**, and in the **Application Definition Details** dialog box, enter the application definition details; then click **OK**.

  On the **Rule** tab, you can manually create your own application definitions. The application definition detail fields are case-sensitive.

  This method is useful for defining the software applications that are not already installed on computers on your network. For example, you can deny applications such as games or P2P file-sharing programs before they are ever used.

  See "About application definition details" on page 111.

4. (Optional) To edit application definition details, perform the following steps:
   - On the **Software** tab, click the application detail that you want to edit, and then click the **Edit** symbol.
   - In the **Application Definition Details** dialog box, edit the application definition details, and then click **OK**.
5. Add all of the application definitions that you want to meter using this policy.
6. To configure the application metering options for the selected applications, on the application metering policy page, click the **Options** tab.

   See "Application metering policy options" on page 116.
7. Click **Save changes**.

About application definition details

(Windows only)

When you configure an application metering policy, you can add new or edit the existing definition details for an application. Any application that you want to meter must have definition details specified. The **Application Definition Details** dialog box lets you specify the details of applications that the policy meters. You can populate these fields manually or import them from a known application.

See "About metering and denying applications" on page 106.

See "Creating and configuring application metering policies" on page 115.

See "Defining applications to meter or deny" on page 110.

The application definition details correspond to the properties of an executable file. On Windows NT/2000/XP, you can see the properties when you right-click an executable file, click **Properties**, and then click the **Version** tab. On Windows Vista/7, you can see the properties when you right-click an executable file, click **Properties**, and then click the **Details** tab.

See Table 8-6 on page 125.

Table 8-3 Guidelines for specifying application definition details

Item	Description
All fields must be met.	For an application to be monitored, it must meet the criteria of all the fields. For example, if you specify the File name and File version, only the applications that meet both of these criteria are monitored. Unspecified fields are ignored. You can use the * wildcard in these fields to represent any number of characters.
Internal file properties.	Symantec recommends that you specify internal file properties rather than depend on the file name. The internal file properties are compiled into the file and are not editable by a user. The internal file properties are internal name, file version, company name, product name, and product version. If you monitor the file name and the user renames the file, your monitor policy will no longer work for that user.
Details are case-sensitive.	The definition detail fields are case-sensitive.
Specify a definition name.	Definition name is used in the definition list. Each definition must have a definition name.

Table 8-3 Guidelines for specifying application definition details *(continued)*

Item	Description
File and product versions.	When you specify application definitions, it is important to note that they may be version-specific. You can have a definition with a specific version or you cannot use a version at all. If you do not specify a version, all versions of the application are metered. The following examples illustrate when you may or may not want to use versions: ■ You want to monitor the general use an application and want to track the usage of any and all versions. For example, you want to track the use of all versions of Adobe Acrobat Reader. You create a rule for Acrobat, enter AcroRd32.exe, or its internal name, in the file name field, and leave the version fields blank. ■ You want to monitor the use of each version of an application. For example, you want to track the usage of each version of an antivirus application. This option lets you determine how many users use the version. You create a separate definition for each version of the application you want to meter and enter the specific version in each rule. ■ You want to allow one version of an application to run but deny other versions. This option lets you enforce the use of a certain version of an application. For example, you can allow the version of an application that has a security fix while blocking the use of other versions. You create two application metering policies. In one policy, you create a rule for the approved version and set the policy to allow it to run. In the other policy, you create a definition for each version that you want to deny and set the policy to deny the applications.
Wildcards.	When specifying application definitions, you can use wildcards to broaden the scope of a definition. You use wildcards by placing an * before and after a string. For example, if you want to deny certain games from running, you can use a wildcard to deny all applications from a game software company. Create a rule, and in the Company name field, enter **company_name*.
Command line.	The **Command line** field contains the command line that the application must use to be monitored. Include an * before and after the command-line text to ensure that the entire command line is included.

Metering and denying applications

(Windows only)

You can use the application metering feature to do the following:

- Monitor the use of applications on managed computers
- Control the availability of applications on managed computers

This task requires the Symantec Management Agent and an Application Metering Plug-in be installed on target computers.

See "About metering and denying applications" on page 106.

See "Preparing managed computers for inventory and metering" on page 37.

Table 8-4 Process for metering and denying applications

Step	Action	Description
Step 1	Prepare computers for metering.	Target computers must be managed and have the Application Metering Plug-in installed. See "Preparing managed computers for inventory and metering" on page 37.
Step 2	Configure global metering options.	You can configure data purging options and software inventory integration. See "Configuring application metering data" on page 129. You must also configure global email settings. For more information see the topic about email server and address settings in the *Symantec Management Platform User Guide*.
Step 3	Create and configure metering policies.	You can create and configure the policies that run metering functions on target computers and gather the data that you want to collect. See "Creating and configuring application metering policies" on page 115. You can meter and track usage of the managed software at the product level instead of the file level. See "About metering and tracking usage of the managed software products in the enhanced Symantec Management Console Software view" on page 119.

Table 8-4 Process for metering and denying applications *(continued)*

Step	Action	Description
Step 4	View metering data.	You can view the metering data by viewing reports. See "Viewing application metering reports" on page 130. See "Viewing usage tracking reports in the enhanced Symantec Management Console Software view" on page 130.

Creating and configuring application metering policies

(Windows only)

You can meter applications on Windows computers by monitoring the use of software or denying software from running. To meter applications, you configure the policies that run metering functions on target computers.

See "About metering and denying applications" on page 106.

For application metering policies to work, you must have the Application Metering Plug-in installed on target computers.

Several predefined policies exist for the common applications that you may want to monitor. For example, there are policies for Microsoft Office products, instant messaging software, and software games. You can also create new polices from scratch or clone and modify existing policies. You can define one or more applications in one policy.

If you want to deny several applications, you can add them to the Blacklisted Applications policy. This policy is a predefined policy that denies applications from running.

See "About blacklisting applications" on page 109.

This topic is a step in the process for metering and denying applications.

See "Metering and denying applications" on page 113.

To access predefined application metering policies

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

2 In the left pane, expand **Software > Application Metering**.

   You can use an existing policy or clone an existing policy to create a new one.

To create application metering policies

1. In the **Symantec Management Console**, on the **Manage** menu, click **Policies**.
2. In the left pane, expand **Software > Application metering**.
3. Right-click the **Application metering** folder and click **New > Application metering policy**.

   You can also edit an existing policy or clone and existing policy to create a new one.

To configure application metering policies

1. On the policy page, click the name and edit it to give it a unique name.
2. Add a description.
3. Turn on the policy.

   At the upper right of the page, click the colored circle, and then click **On**.
4. On the **Software** tab, select the applications you want to meter or deny.

   To add to the list of applications, click the **Add** drop-down list.

   You can also edit application definitions or delete applications from the list.

   See "Defining applications to meter or deny" on page 110.
5. On the **Options** tab, configure metering and denying options.

   See "Application metering policy options" on page 116.
6. Click **Apply to**, and select the resources to which you want to apply the policy.

   For more information, see the topics about using policies in the *Symantec Management Platform User Guide*.
7. Click **Save changes**.

Application metering policy options

(Windows only)

When you configure an application metering policy, on the **Options** tab, you specify the metering options for applications to be monitored or denied. The options apply to all the applications that are defined in the policy.

See "About metering and denying applications" on page 106.

See "Creating and configuring application metering policies" on page 115.

See "Defining applications to meter or deny" on page 110.

Table 8-5 Application metering policy options

Option	Description
Metering options	You can configure if and when the applications in this policy can run. You can select the following options: ■ The **Allow** option lets the application run at any time. ■ The **Only deny running** option lets you deny applications on certain days or during certain times. For example, you can deny an application from running during business hours. ■ The **Deny from running** option prevents the application from running at all times.

Table 8-5 Application metering policy options *(continued)*

Option	Description
Record usage events	You can enable application event tracking. This option lets you track the usage events of the applications that are defined in the policy. When a selected event occurs, a record of the event is sent to the Configuration Management Database (CMDB). You can view the events using reports. See "Viewing application metering reports" on page 130. For allowed applications you can record the following events: ■ Start events ■ Start and Stop events For scheduled denied applications you can record the following events: ■ Start events ■ Deny events ■ Start and deny events This option generates start events during the allowed time and deny events during the denial time. For denied applications you can record the following events: ■ Deny events You can also specify the following intervals when the events are sent to the CMDB: ■ Daily ■ Weekly All the application events that are generated for the metered applications are saved in a local queue file on the managed computer. Depending on the schedule selected, the batch of saved events is sent to the CMDB from the queue file. The data is sent at a random time each day or each week. See "About application metering start, stop, and denial events" on page 124. To track software usage at the product level instead of the file level, you can also enable the software-based usage tracking option in the enhanced Symantec Management Console **Software** view. See "About metering and tracking usage of the managed software products in the enhanced Symantec Management Console Software view" on page 119.

Table 8-5 Application metering policy options *(continued)*

Option	Description
If run attempted during deny hours	You can define the actions to be taken when a denied application attempts to run. You can select from the following actions to occur when a denied application attempts to run: ■ **No action**. ■ **Send an e-mail**. When a user attempts to start a denied application, you can send an email that reports the denied application event. In the **Mail Settings** dialog box, enter the recipient's email address in the **E-mail ID** field, enter a subject and text for the email, and click **OK**. ■ **Inform user**. In addition to the other options, when a user attempts to start a denied application, you can prompt the user with a message. To prompt the user with a message, check **Inform user** and enter the text of the message.
Add computer, group of computers or user.	You can select the target computers to which you want to apply this application metering policy. For more information, see the topics about using policies in the *Symantec Management Platform User Guide*.

About metering and tracking usage of the managed software products in the enhanced Symantec Management Console Software view

(Windows only)

Inventory Solution provides the software-based usage tracking option to help you easily meter application usage on the product level and track and manage software licenses.

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

You see the enhanced views in Symantec Management Console if you install Symantec Management Platform 7.1 SP2 and any of the following full suites:

- IT Management Suite
- Server Management Suite

- Client Management Suite

Note: The enhanced views do not appear if you install Inventory Solution individually without installing the full suite first, or you disable Deployment Solution in the suite.

For more information, see the topics about the enhanced views in the *Altiris™ IT Management Suite 7.1 from Symantec™ Enhanced Console Views Getting Started Guide* at the following URL:

http://www.symantec.com/docs/DOC3563

By using the enhanced **Software** view to meter and track usage of the managed software products, you can track the following events:

- License deployment

  For more information, see the topics about managing software licenses in the *Asset Management Suite User Guide*.
- The usage of the software product
- Last usage time
- Installation date

See "Creating and configuring application metering policies" on page 115.

See "Application metering policy options" on page 116.

The software-based usage tracking option lets you associate the key program file information that application metering records to a metered software component. The software component is associated to a managed software product. Due to these associations the option helps you track software usage at the product level instead of the file level. For example, you can track Microsoft Office 2008 as a separate software product. You can see it in usage tracking reports as Microsoft Office 2008, not as `winword.exe`.

See "Metering and tracking usage of the managed software products in the enhanced Symantec Management Console Software view" on page 122.

See "Viewing usage tracking reports in the enhanced Symantec Management Console Software view" on page 130.

The program files that you want to meter get updated or patched regularly, and their names and versions can change. When you run software inventory, such files are reported as new program files. Inventory Solution lets you automatically meter the new key program files together with the metered software components and software products. The predefined nightly task **NS.Nightly schedule to**

associate Software component to software product automatically associates the new program files with software components.

See "About the predefined nightly task NS.Nightly schedule to associate Software component to software product" on page 121.

Note: Currently, only the program files that are installed with an MSI-based installer can be automatically associated with software components. You have to create associations manually for the program files that are installed with other installers.

The **Metered software without a file association** report helps you define to which software components you need to manually associate new key program files. The report lists the managed and metered software products that have the software components with no associations to any program files. You can view the **Metered software without a file association** report in the application metering reports.

See "Viewing application metering reports" on page 130.

About the predefined nightly task NS.Nightly schedule to associate Software component to software product

Inventory Solution provides the predefined nightly task **NS.Nightly schedule to associate Software component to software product** that helps you perform the following important software management steps:

- Associate new software components with the relevant predefined software product and populate the Software Catalog.
  The **NS.Nightly schedule to associate Software component to software product** task compares the software components that software inventory discovers with the predefined software products. If there is a match, the task associates the discovered software components with the relevant predefined software product and moves the product to the Software Catalog, to **Managed software products**.
  See "About how Inventory Solution works with the Software Catalog Data Provider" on page 100.
- Assign the **Newly Discovered Software** status to the software components that are associated with a deleted managed software product.
  In the enhanced Symantec Management Console **Software** view, under **Installed Products**, you may right-click and delete a managed software product. The **NS.Nightly schedule to associate Software component to software product** task assigns the **Newly Discovered Software** status to the software components that are associated with the deleted managed software product. Only then can

you view the software components in the **Newly Discovered Software** pane or in the Software Catalog, under **Newly discovered/undefined software**.

- Automatically meter new key program files together with the metered software components and software products.

  The **NS.Nightly schedule to associate Software component to software product** task compares the program files that software inventory discovers with the key program files that are already associated with a software component. You can see the associated key program files of the software component when you view the relevant metered software product in the **Software Product** dialog box, on the **Meter / track usage** tab. If there is a match and the relevant software component is associated with a metered software product, the task associates the discovered program files with the software component.

  Note: Currently, the nightly task can automatically associate with software components only the program files that are installed with an MSI-based installer. You have to create associations manually for the program files that are installed with other installers.

  See "About metering and tracking usage of the managed software products in the enhanced Symantec Management Console Software view" on page 119.

The task **NS.Nightly schedule to associate Software component to software product** runs automatically on the Notification Server computer every night at 12:30 A.M. The task manages the software components and program files that are discovered and imported into the Configuration Management Database (CMDB). To immediately get the results, you can run the task manually from **Task Scheduler Library**.

See "Manually running the task NS.Nightly schedule to associate Software component to software product" on page 124.

Metering and tracking usage of the managed software products in the enhanced Symantec Management Console Software view

(Windows only)

Inventory Solution provides the software-based usage tracking option to help you easily meter application usage and track and manage software licenses.

See “About metering and tracking usage of the managed software products in the enhanced Symantec Management Console Software view” on page 119.

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

For more information, see the topics about the enhanced views in the *Altiris™ IT Management Suite 7.1 from Symantec™ Enhanced Console Views Getting Started Guide* at the following URL:

http://www.symantec.com/docs/DOC3563

See “Viewing usage tracking reports in the enhanced Symantec Management Console Software view” on page 130.

This topic is a step in the process for metering and denying applications.

See “Metering and denying applications” on page 113.

To meter and track usage of the managed software products in the enhanced Symantec Management Console Software view

1. In the **Symantec Management Console**, on the **Manage** menu, click **Software**.
2. In the **Software** pane, under **Installed Software**, click **Installed Products**.
3. In the **Installed Products** pane, double-click the software product that you want to meter.
4. In the **Software Product** dialog box, click the **Meter / track usage** tab.
5. On the **Meter / track usage** tab, click **Add Program** next to the software component that you want to meter.
6. In the **Add Program** dialog box, add the program files from the **Available programs** list to the **Associated programs** list, and then click **OK**.
7. On the **Meter / track usage** tab, in the **Count software as used if run in the last ... days** box, type the number of days.
8. On the **Meter / track usage** tab, ensure that **Turn on metering / usage tracking for this software product** is checked.
9. Click **OK**.

Manually running the task NS.Nightly schedule to associate Software component to software product

The task **NS.Nightly schedule to associate Software component to software product** runs on the Notification Server computer automatically every night at 12:30 A.M. You can run the task manually from **Task Scheduler Library**.

See "About the predefined nightly task NS.Nightly schedule to associate Software component to software product" on page 121.

To manually run the task NS.Nightly schedule to associate Software component to software product

1 On the Notification Server computer, in the taskbar, click **Start > Administrative Tools > Task Scheduler**.

2 On the **Task Scheduler** page, in the left pane, click **Task Scheduler Library**.

3 In the central pane, right-click the task **NS.Nightly schedule to associate Software component to software product.{a48d3b11-5169-464b-9773-6c0f476e7748}**, and then click **Run**.

About application metering start, stop, and denial events

(Windows only)

Inventory Solution provides the application metering policy option **Record usage events**. This option lets you track the usage events of the applications that are defined in the policy.

See "Application metering policy options" on page 116.

When the **Record usage events** option is enabled, and a user of a managed computer starts or stops a monitored application, an event is generated. When a user tries to use an application whose monitoring policy denies its use, a denial event is generated. Every start event has a stop event or becomes a denial event. After the events are sent to the Configuration Management Database (CMDB), you can generate reports to view this data.

See "About metering and denying applications" on page 106.

See "Viewing application metering reports" on page 130.

See "About application summary data" on page 126.

The Application Metering Plug-in sends the events to the CMDB in a batch at a specified interval.

The event data is very small, such as a few thousand bytes. If the Symantec Management Agent cannot connect to the CMDB, the managed computer saves the information locally and sends it later.

If a managed computer terminates abnormally, then the next time it starts, the Application Metering Plug-in does the following functions:

- Determines which applications were running when the computer was terminated
- Generates the appropriate stop events

Application metering records a variety of application events.

When you view an application in the **Resource Manager**, you can view application metering start and stop events data by clicking **View > Events**, and then expanding **Data Classes > Inventory > Application metering**.

Table 8-6 Application metering start events data

Field	Description	Example
FileResourceGUID	Resource guid that is generated by using various attributes of a file. For example, its internal name, manufacturer, version etc.	{018B191B-47AE-4180-9FCD-7F3CEA4F1E12}
UserGuid	Resource guid that is generated for a specific user on a domain.	{493435F7-3B17-4C4C-B07F-C23E7AB7781F}
PID	Process ID of the application.	804
Policy Name	Name of the application metering policy.	Microsoft Word
Start Date	Date and time of the event.	9/03/2004 9:51:18 A.M.
Policy GUID	The GUID of the policy that caused the event to be generated.	{CC1355B1-3993-4519-BB4C-8C41735E3825}
command-line	The command-line options that are used to start the application.	*/n*
Denied	Specifies whether this event is a denial event. 0 = not a denial event 1 = denial event	0
File Path	Path to the application file on the managed computer.	`C:\Program Files\Microsoft Office\Office\WINWORD.EXE`

Table 8-7 Application metering stop events data

Field	Description	Example
PID	Process ID of the application.	804
Policy Name	Name of the application metering policy.	Microsoft Word
Start Date	Date and time of the event.	9/03/2004 9:51:18 A.M.
Total Run Time	Time Total amount of time in seconds that the application was used during the monitoring period . When the application is monitored, this value is updated every 30 seconds.	188714
Peak Memory	Maximum amount of memory in bytes used by the application during the monitoring period. When the application is monitored, this value is updated every 30 seconds.	7921664
Average CPU	Average CPU usage by the application during the monitoring period, where 100 equals 100 percent usage. When the application is monitored, this value is updated every 30 seconds. This information is not available from the managed computers that are running Windows 9x/Me.	0.7652

About application summary data

(Windows only)

Each time a monitored application starts, the Application Metering Plug-in records the application’s summary data. This data is stored on the managed computer and sent to the Configuration Management Database (CMDB) at the end of the application monitoring period. If any data was sent during the monitoring period, it is replaced at the end of the monitoring period.

See “Configuring application metering data” on page 129.

See “About how application metering summary is sent” on page 128.

The application summary data is viewable in the following application metering reports:

- **Concurrent Usage**
- **Executable Usage**
- **Underutilized Software**

See “Viewing application metering reports” on page 130.

Application metering records data for each monitored application in the order in which it is stored in the data file.

Table 8-8 Application summary data

Field	Description	Example
FileResourceGUID	Resource guid that is generated by using various attributes of a file. For example, its internal name, manufacturer, version etc.	{018B191B-47AE-4180-9FCD-7F3CEA4F1E12}
User Guid	Resource guid that is generated for a specific user on a domain.	{493435F7-3B17-4C4C-B07F-C23E7AB7781F}
Last Start	Date the application was last started	11/13/2004 8:38:18 A.M.
Month Year	Month and year of the monitoring period	September 2008
Run Count	Number of times the application was started during the monitoring period.	3
Denial Count	Number of times the use of the application was denied during the monitoring period.	1
Total Run Time	Total amount of time in seconds that the application was used during the monitoring period When the application is monitored, this value is updated every 30 seconds.	188714

Table 8-8 Application summary data *(continued)*

Field	Description	Example
Peak Memory	Maximum amount of memory in bytes used by the application during the monitoring period. When the application is monitored, this value is updated every 30 seconds.	7921664
Average CPU	Average CPU usage by the application during the monitoring period, where 100 equals 100 percent usage. When the application is monitored, this value is updated every 30 seconds. This information is not available from the managed computers that are running Windows 9x/Me.	0.7652
Month End Summary	Specifies whether the current set of application summary data is the final set for the month. 0 = not the final data 1 = the final data	0

About how application metering summary is sent

(Windows only)

The metering summary data is sent to the Configuration Management Database (CMDB) in batches. You can also specify to send event data in batches when you create an application monitor policy.

An application metering usage summary is sent for all application metering policies for which the applications are marked as allowed. The summary is sent daily by default.

See “About application summary data” on page 126.

See “Configuring application metering data” on page 129.

To prevent an overload to the system when this data is sent, the data is not all sent at the same time. The data is randomly sent over an interval of time. A value in the HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Application Metering registry key on each client computer determines the length of the interval. The name of the value is Fuzzy Factor and its default value is 10.

This value specifies the time interval when the data can be sent as a percentage of the total batch creation time. For example, the data is sent to the CMDB every seven days (168 hours) and the Fuzzy Factor value is 10. Then the length of the interval is 10% of seven days or about 17 hours. Half of this interval precedes the specified send time and half of it follows. Thus the time interval in which the data is sent would start after about 159 hours and end after 177 hours.

To change the length of this time interval, you must change the value of this registry key on each client computer. Any registry changes should be done with caution.

Configuring application metering data

(Windows only)

Application metering data is stored on metered computers and then sent to the Configuration Management Database (CMDB). Over time, you may want to archive or delete (purge) application metering data. You can archive summary data or you can purge metering events, reports, and summary data. You can also configure the settings that archive or purge the data at configured time intervals.

You configure how to manage metering data on the **Application Metering Configuration** page.

See “About application summary data” on page 126.

This topic is a step in the process for metering and denying applications.

See “Metering and denying applications” on page 113.

To configure application metering data

1. In the **Symantec Management Console**, on the **Settings** menu, click **All Settings**.
2. In the left pane, under **Settings**, expand **Discovery and Inventory > Inventory Solution**, and then click **Application Metering Configuration**.
3. To archive summary data, click **Archive when older than ... months**, type the number of months, and then click **Archive Data Now**.
4. To purge data, perform one of the following steps:
   - To purge events, check the **Purge events older than ... days** box, type the number of days, and then click **Purge Events Now**.
   - To purge reports, check the **Purge reports older than ... days** box, type the number of days, and then click **Purge Reports Now**.

- To purge summary data, click **Purge when older than ... months**, type the number of months, and then click **Purge Data Now**.
- To purge archives with summary data, check **Purge archives older than ... months** box, type the number of months, and then click **Purge Archive Data Now**.

5 Click **Save changes**.

Viewing application metering reports

(Windows only)

Application metering data is recorded in the Configuration Management Database (CMDB).You can view the data through reports.

Application metering reports let you view the following information:

- The usage of an executable file
- Application denial events
- The usage of an application

You can view an existing report or create a new one.

For more information, see the topics about using reports in the *Symantec Management Platform User Guide*.

See "Application metering policy options" on page 116.

See "About viewing inventory data" on page 155.

To view application metering reports

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

2 In the left pane, under **Reports**, expand **Software > Application Metering**.

Viewing usage tracking reports in the enhanced Symantec Management Console Software view

(Windows only)

Inventory Solution provides the software-based usage tracking option to help you easily meter application usage and track and manage software licenses.

See "About metering and tracking usage of the managed software products in the enhanced Symantec Management Console Software view" on page 119.

See “Metering and tracking usage of the managed software products in the enhanced Symantec Management Console Software view” on page 122.

You can view usage tracking reports in the enhanced Symantec Management Console **Software** view.

For more information, see the topics about the enhanced views in the *Altiris™ IT Management Suite 7.1 from Symantec™ Enhanced Console Views Getting Started Guide* at the following URL:

http://www.symantec.com/docs/DOC3563

The following gathered usage tracking data is available in the usage tracking reports:

- License deployment.
  For more information, see the topics about managing software licenses in the *Asset Management Suite User Guide*.
- The usage of the software product.
- Last usage time.
- Installation date.

This topic is a step in the process for metering and denying applications.

See “Metering and denying applications” on page 113.

To view usage tracking reports in the enhanced Symantec Management Console Software view

1. In the **Symantec Management Console**, on the **Manage** menu, click **Software**.
2. In the **Software** pane, under **Metered Software**, click **Usage Tracking**.
3. In the **Usage Tracking** pane, click the software product whose reports you want to view.
4. In the right pane, view **Software Product License and Usage**.
5. In the right pane, expand **Computers with software installed**.

Chapter 9

Gathering baseline inventory

This chapter includes the following topics:

About baseline inventory

(Windows only)

Baseline inventory lets you track and compare the changes in files and registry keys for different computers. You generate a baseline that identifies the files or registry settings of a standard configuration computer. You can later run the compliance scans on your client computers to compare their current files or registry keys with those in the baseline. The differences between the baseline scan and compliance scan are reported to the Configuration Management Database (CMDB).

Note: Baseline inventory is a Windows-only feature.

Baseline inventory reports newly added files, missing files, and registry keys. It also reports duplicate files and indicates if the files have the same version or a different version.

You can use the baseline inventory for the following purposes:

- Track the files and registries that deviate from the corporate standards.
- Verify the accuracy of rollouts and upgrades.
- Automatically notify system administrators or the help desk when a computer is non-compliant.
- View a compliance level summary of the computer and reports of the changes in a file.

Baseline inventory uses standard tasks to perform the baseline scan and compliance scan. You view reports to track baseline and compliance scan information.

See “About baseline files” on page 135.

The baseline inventory is the same for file and registry baselines. However, the configuration files, snapshot files, and tasks differ. The baseline configuration file contains the options that determine the files or registry settings to scan. You can use the default configuration file, edit it, or create one or more custom configuration files.

The compliance scan compares the current files or registry keys on one or more computers with the baseline snapshot (BLS) files. The differences between the baseline and the compliance scans are written to an output file on the scanned computer and reported to the CMDB.

The baseline scan captures the current files or registry keys settings on a standard configuration computer. It also compiles a baseline snapshot file which is used during the compliance scan.

The baseline scan and the compliance scan report information about the computers that were scanned and the scan results. You can use notification tasks to automatically notify the system administrator or the help desk when certain events occur. This feature helps you prevent the system failures that might occur when a computer becomes non-compliant.

See “Running a registry baseline scan” on page 148.

See "Running a file baseline scan" on page 136.

About baseline files

(Windows only)

The baseline inventory process uses and creates several baseline files. The baseline configuration file contains options for running the scans. For example, you configure the files or registry keys to be included or excluded, the directories to scan, and so on. You can use the default configuration file, edit it, or create one or more custom configuration files. Configuration files for registry baselines are in INI format. The default registry baseline configuration file is `AexRegScan.ini`. Configuration files for file baselines are in INI format but have the .bls extension. The default file baseline configuration file is r.

The local baseline tasks use the default configuration files.

See "About baseline inventory" on page 133.

The location of the default baseline configuration files and additional sample configuration files is as follows:

InstallDir\Altiris\Notification Server\NSCap\bin\Win32\X86\Inventory\Application Management

A baseline snapshot (BLS) file maintains a record of the files or registry settings on a computer at a given time. This data is gathered during a baseline scan that is based on options in a baseline configuration file. Registry baseline snapshots are saved to a new file on the scanned computer in .RBL format.

File baseline snapshots are appended to the baseline configuration file. The location of the default baseline snapshot files is as follows:

%*ProgramFiles*%\Altiris\eXpress\Baseline

The file compliance scan and the registry compliance scan create output in XML format. This output is stored in Notification Server Events (NSEs) and reported to the Configuration Management Database (CMDB).

The following folders represent the packages for file baseline tasks and registry baseline tasks respectively:

InstallDir\Altiris\Notification Server\NSCap\bin\Win32\X86\Inventory\Application Management\FileBaselinePackage

InstallDir\Altiris\Notification Server\NSCap\bin\Win32\X86\Inventory\Application Management\RegBaselinePackage

You need to make sure that you copy or keep the baseline configurations and baseline snapshots that you want to use for compiling a custom baseline or comparing with a custom baseline when running these tasks. Otherwise, the task fails.

Running a file baseline scan

(Windows only)

The file baseline scan gathers data about the files on a computer at a given time. The data that is gathered during this scan is saved in a baseline snapshot (BLS) file on the scanned computer. The files that are found during subsequent scans of that computer, are compared to the baseline snapshot. Baseline inventory also contains predefined reports to track baseline and compliance information.

You perform a file baseline scan by creating and running a **File Baseline** task. Symantec recommends that you run the file baseline scan once to establish the baseline, and then re-run the file baseline scan only when the standard configuration changes.

You should not run the file baseline scan on a regular basis if the file baseline scan and compliance scan run on the same computer. If you do, then you continually overwrite the file baseline snapshot file.

See "About baseline inventory" on page 133.

See "File Configuration Editor dialog box" on page 139.

See "File Snapshot Editor options" on page 146.

To run a file baseline scan

1. In the Symantec Management Console, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, navigate to the folder where you want to create and run a file baseline scan task, right-click the folder, and then click **New > Task**.

   For example, to create a file baseline scan task in the **Jobs and Tasks** folder, right-click **Jobs and Tasks**, and then click **New > Task**.

   To create a file baseline scan task in the **Inventory** folder, expand **Jobs and Tasks > System Jobs and Tasks > Discovery and Inventory**, right-click **Inventory**, and then click **New > Task**.
3. In the **Create New Task** dialog box, in the left pane, under **Discovery and Inventory**, click **File Baseline**.
4. In the right pane, configure the task.

   See "File Baseline task options" on page 137.

5 Click **OK** to save the task.

6 On the **File Baseline** task page, under **Task Status**, schedule the task and add computers to which you want to apply the schedule.

For more information, see the topic about **New schedule** dialog box in the *Symantec Management Platform User Guide*.

7 Click **Save changes**.

File Baseline task options

(Windows only)

You can create a new task to track the file changes in baseline inventory.

See "About baseline inventory" on page 133.

See "Running a file baseline scan" on page 136.

Table 9-1 **File Baseline** task options

Option	Description
Name	Lets you specify a name for the task that you want to roll out to the target folder. This name helps you identify the task. By default, the task name is **File Baseline**.

Table 9-1 **File Baseline** task options *(continued)*

Option	Description
Compile a baseline snapshot	Lets you capture and set the captured file settings as the file baseline. This option helps you create a new file baseline setup. You can use the following options: ■ **Use local baseline configuration** This option compiles a baseline snapshot using the `local_master.bls` as the baseline configuration. The compiled baseline snapshot, `local_master.bls` is located on the client computers. The default location is as follows: `%`*`Program Files`*`%\Altiris\eXpress\Baseline` ■ **Use custom baseline configuration** This option lets you create a new baseline configuration with the **File Configuration Editor** or use an existing custom baseline configuration. See "File Configuration Editor dialog box" on page 139. The compiled baseline snapshot, *`GivenBaselineConfiguratinName`*`.bls`, is stored on the client computers. The default location is as follows: `%`*`Program Files`*`%\Altiris\eXpress\Baseline` To use the baseline snapshot for a compliance scan, you must copy it to the Notification Server computer in the following path: *`InstallDir`*`\Altiris\Notification Server\NSCap\bin\Win32\X86\Inventory\Application Management\FileBaselinePackage` You can also browse for an existing file.
Compare with a baseline snapshot	Lets you compare the target with the baseline. The differences are reported to the Configuration Management Database (CMDB). You can use the following options: ■ **Compare with local baseline snapshot** Lets you compare the computer's present state with the local baseline snapshot, `local_master.bls` that is on the client computers. ■ **Compare with custom baseline snapshot** Lets you compare the computer's present state with a custom snapshot that you created on the client computers.
Advanced	Lets you configure download and run options of the **File Baseline** task. You can also define when to end the task and whether to allow other tasks to run while running this task.

File Configuration Editor dialog box

(Windows only)

You can edit or create the baseline configuration files. The baseline configuration file contains the options that determine the files to scan. You can use the default configuration file, edit it, or create one or more custom configuration files. You can scan all files on a computer, certain file types, directories, and so on.

See "Running a file baseline scan" on page 136.

You can use the **File Baseline Snapshot Editor** to edit a baseline snapshot (.BLS) file after the baseline snapshot information has been added.

See "File Snapshot Editor options" on page 146.

Table 9-2 Tabs in the **File Baseline Configuration Editor** dialog box

Tab	Description
General	Lets you specify the settings that help you identify the baseline file and track the information in the compliance scan output. See "File Configuration Editor: General tab" on page 141.
Extensions	Lets you specify the file extensions to locate during the baseline scan. See "File Configuration Editor: Extensions tab" on page 141.
Duplicates	Lets you determine how the compliance scan finds and reports duplicate files. The duplicate file names must be the same. The compliance scan output indicates if the duplicate files have the same or a different version. See "File Configuration Editor: Duplicates tab" on page 142.
Directories	Lets you specify the directories to scan for a baseline snapshot. It checks whether the compliance scan uses the same directories as the baseline scan. When you specify directories, you can use environment variables. Enclose the variables in % characters: for example, %TEMP%. See "File Configuration Editor: Directories tab" on page 143.

Table 9-2 Tabs in the **File Baseline Configuration Editor** dialog box *(continued)*

Tab	Description
Known As	Lets you specify an alias that replaces a file's product name in the compliance scan output. During a scan, the **Known As** attribute is initially set to the file's product name. If the configuration file contains an alias for that product, the alias is reported instead of the product name. This information lets you more easily analyze the scan data. See "File Configuration Editor: Known As tab" on page 143.
Manufacturer Known As	Lets you specify an alias that replaces a manufacturer's company name in the compliance scan output. During a scan, the **Manufacturer Known As** attribute is initially set to the file's company property. If the configuration file contains an alias for the variants of that company name, the alias is reported instead of the company property. This information lets you more easily analyze the scan data. When you change or add to the Known As or Manufacturer Known As values, Symantec recommends that you use the Software Management Framework. The **NS.File Baseline INI Creator Task** updates the .BLS files at `InstallDir\Altiris\Notification Server\NSCap\bin\Win32\X86\Inventory\Application Management` for these changes. By default, this task runs daily at 2:10 A.M. See "File Configuration Editor: Manufacturer Known As tab" on page 144.
Exclusion Filters	Lets you specify the files to be excluded from the scan based on the rules that consist of sets of file properties. Any file that meets the criteria is not evaluated for inclusion in the scan. You can copy and paste rules from the **File Snapshot Editor** into the **Exclusion Filters** tab. See "File Configuration Editor: Exclusion Filters tab" on page 144.

Table 9-2 Tabs in the **File Baseline Configuration Editor** dialog box *(continued)*

Tab	Description
Baseline Scan	Lets you specify the file properties that the compliance scan uses to compare files on the computer to files in the baseline snapshot. The properties that do not have a check box are always included. See "File Configuration Editor: Baseline Scan tab" on page 145.
Advanced	Lets you override the default values used to generate data for the output files. You can maintain multiple snapshots on a single system by customizing these settings. See "File Configuration Editor: Advanced tab" on page 145.

File Configuration Editor: General tab

(Windows only)

This tab lets you specify the settings that help you identify the baseline file in the compliance scan output.

See "File Configuration Editor dialog box" on page 139.

Table 9-3 Options on the **General** tab

Option	Description
Baseline Name	Lets you specify the name for the baseline file. The name helps you identify the baseline file.
Comments	Lets you write a description about the baseline file.
Version	Lets you specify the version number of the baseline file. You must update the version number every time you change the file.

File Configuration Editor: Extensions tab

(Windows only)

This tab lets you specify the extensions of the files that you want to include in the scan.

See "File Configuration Editor dialog box" on page 139.

Table 9-4 Options on the **Extensions** tab

Option	Description
Extension	Lets you specify the extension of the files to locate during the baseline scan. You can specify executable files such as EXE, DLL, and OCX files. You can also specify data files such as XLS and DOT. In this field, do not include (.) before the extension.
Report if files with this extension are	Lets you specify the conditions that are required for a file to be reported in the compliance scan output. You can select **Missing**, **Different versions**, **Added**, or any combination. By default, all of these check boxes are selected.
Maximum items reported	Lets you specify the limit of the output rows that are generated in the compliance scan output files.

File Configuration Editor: Duplicates tab

(Windows only)

This tab lets you specify the settings for reporting the duplicate files.

See "File Configuration Editor dialog box" on page 139.

Table 9-5 Options on the **Duplicates** tab

Option	Description
Report duplicate files	Lets you enable the reporting of the duplicate files.
Extension	Lets you specify the extension of the file to locate during the baseline scan. You can specify executable files such as EXE, DLL, and OCX files. You can also specify data files such as XLS and DOT. In this field, do not include (.) before the extension.
Scan	Lets you specify the directories to scan. You can use the following options: ■ **Baseline directories only** Lets you scan for duplicate files in the baseline scan directories. ■ **Scan all local drives** Lets you scan for duplicate files on all the local hard drives.

Table 9-5 Options on the **Duplicates** tab *(continued)*

Option	Description
Maximum items reported	Lets you limit the output rows that are generated in the compliance scan output files.

File Configuration Editor: Directories tab

(Windows only)

This tab lets you specify the directories that you want to scan.

See "File Configuration Editor dialog box" on page 139.

Table 9-6 Options on the **Directories** tab

Option	Description
Scan all local drives	Lets you perform the baseline snapshot scan on all local drives.
Scan only these directories	Lets you specify the directories on which you want to perform the baseline snapshot scan. The scan includes any subdirectories of the specified directories.
When scanning for compliance relative to this baseline	Lets you specify the settings that are used during the compliance scan. You can use the following options: ■ **Scan the same directories as listed** Lets you perform the compliance scan on the same directories that are listed in the baseline scan. ■ **Scan all local drives** Lets you perform the compliance scan on all the local drives, regardless of what the baseline scan checked.
Directory	Lets you specify a drive or a directory that you want to exclude during the File Compliance scan. The scan excludes all the listed directories and also their subdirectories.

File Configuration Editor: Known As tab

(Windows only)

This tab lets you define a name that replaces the file's product name in the compliance scan output.

See “File Configuration Editor dialog box” on page 139.

Table 9-7 Options on the **Known As** tab

Option	Description
Internal name	Lets you enter a product’s name as it appears in the file’s version properties.
Known as	Lets you enter the product’s alias to be used in the compliance scan output. When you change or add to the Known As values, Symantec recommends that you use the Software Management Framework. The**NS.File Baseline INI Creator Task** updates the BLS files at `*InstallDir*\Altiris\Notification Server\NSCap\bin\Win32\X86\Inventory\Application Management` for these changes. By default, this task runs daily at 2:10 A.M.

File Configuration Editor: Manufacturer Known As tab

(Windows only)

This tab lets you define a name that replaces the manufacturer’s company name in the compliance scan output.

See “File Configuration Editor dialog box” on page 139.

Table 9-8 Options on the **Manufacturer Known As** tab

Option	Description
Manufacturer Name	Lets you enter the manufacturer’s name as it appears in the file’s version properties.
Regular Expression	Lets you enter the manufacturer’s name and convert it to a regular expression or enter the regular expression in this field.
Replace with	Lets you enter the manufacturer’s alias to be used in the compliance scan output.

File Configuration Editor: Exclusion Filters tab

(Windows only)

This tab lets you specify the criteria by which the files are excluded from the scan.

See “File Configuration Editor dialog box” on page 139.

Table 9-9 Options on the **Exclusion Filters** tab

Option	Description
Exclusion Filters	Lets you manage the exclusion filters. In the **New Rule** dialog box, you can specify the settings or you can use the **Get Resource Information from File** option to populate the fields. If you specify multiple values, all entered values must match for a file to be excluded. All fields support wildcards.

File Configuration Editor: Baseline Scan tab

(Windows only)

This tab lets you specify the file properties that are used for comparing the files on the disk to the files in the baseline.

See “File Configuration Editor dialog box” on page 139.

Table 9-10 Options on the **Baseline Scan** tab

Option	Description
List of different properties	Lets you select the properties that are used for comparing the files. A property is not included in the scan comparison on following conditions: ■ The file property exists in the snapshot file but the associated check box is cleared. ■ The associated check box is selected but the property does not exist in the snapshot file.

File Configuration Editor: Advanced tab

(Windows only)

This tab lets you override the default values that are used to generate data for the output files.

See “File Configuration Editor dialog box” on page 139.

Table 9-11 Options on the **Advanced** tab

Option	Description
Alternate XML output	Lets you specify a directory path to override the XML output file (NSI). You can also leave this option blank to save the output file (NSI) in the default location. The default location is as follows: `C:\Program Files\Altiris\eXpress\Baseline`
Slow mode delay (in milliseconds)	Lets you specify the number of milliseconds that the compliance scan should wait after it scans each file. This setting helps to slow down the scanning process and reduces the rate of disk I/O on the scanned computer.
Product Exclusion Match	Lets you specify the files to be excluded from the scan. You can use the following options: ■ **Exact** Lets you exclude only the specified files in the **Exclusion Filters** tab from the scanning process. ■ **Substring** Lets you exclude all the files that have the specified substring in the Exclusion Filter.

File Snapshot Editor options

(Windows only)

A baseline snapshot (BLS) file contains a record of the files on a computer at a given time. This data is gathered during an initial baseline scan, which is based on options in a baseline configuration file.

See "Running a file baseline scan" on page 136.

Even if you customize the configuration file before you run the baseline scan, the scan collects the data that you do not want to compare. To remove this data, or to refine the baseline data, you can edit the snapshot file.

Table 9-12 Tabs in the **File Snapshot Editor** dialog box

Tab	Description
Settings	Lets you edit the settings that are reported in the output file that File Snapshot generates. See "File Snapshot Editor: Settings tab" on page 147.

Table 9-12 Tabs in the **File Snapshot Editor** dialog box *(continued)*

Tab	Description
Rules	Lets you define the criteria that File Snapshot uses for detecting deviations from the snapshot. See "File Snapshot Editor: Rules tab" on page 147.

File Snapshot Editor: Settings tab

(Windows only)

This tab lets you edit the settings that are stored in the snapshot file and that are reported in the output file that File Snapshot generates.

See "File Snapshot Editor options" on page 146.

Table 9-13 Options on the **Settings** tab

Option	Description
Reference system	Lets you specify the name of the computer on which the baseline snapshot was created. The file compliance scan includes this information in the snapshot file.
Baseline name	Lets you specify the name for the baseline file. This setting helps you identify the baseline file.
Comments	Lets you specify the description about the baseline file.
Version	Lets you specify the version number of the baseline file. You must update the version number every time you change the file.

File Snapshot Editor: Rules tab

(Windows only)

This tab lets you define the criteria that File Snapshot uses for detecting deviations from the snapshot.

See "File Snapshot Editor options" on page 146.

Table 9-14 Options on the **Rules** tab

Option	Description
Rules	Lets you manage the rules to detect deviations. To add a rule, click **Add**. In the **New Rule Properties** dialog box, you can specify the settings or you can use the **Get Resource Information from File** option to populate the fields.

Running a registry baseline scan

(Windows only)

The registry baseline scan gathers data about the registry settings on a computer at a given time. The data that is gathered during this scan is saved in a registry baseline snapshot file (RBL) on the scanned computer. The registry settings that are found during subsequent scans of that computer, are compared to the baseline snapshot.

You perform a registry baseline scan by creating and running a **Registry Baseline** task. Symantec recommends that you run each registry baseline scan once to establish the baseline, and then re-run the registry baseline scan only when the standard configuration changes.

Generally, you should not run the registry baseline scan on a regular basis if the registry baseline scan and the compliance scan run on the same computer. If you do, then you continually overwrite the baseline snapshot file.

See "About baseline inventory" on page 133.

See "Registry Configuration Editor options" on page 151.

See "Registry Snapshot Editor options" on page 153.

To run a registry baseline scan

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

2 In the left pane, navigate to the folder where you want to create and run a registry baseline scan task, right-click the folder, and then click **New > Task**.

For example, to create a registry baseline scan task in the **Jobs and Tasks** folder, right-click **Jobs and Tasks**, and then click **New > Task**.

To create a registry baseline scan task in the **Inventory** folder, expand **Jobs and Tasks > System Jobs and Tasks > Discovery and Inventory**, right-click **Inventory**, and then click **New > Task**.

3 In the **Create New Task** dialog box, in the left pane, under **Discovery and Inventory**, click **Registry Baseline**.

4 In the right pane, configure the task.

See "Registry Baseline task options" on page 149.

5 Click **OK** to save the task.

6 On the **Registry Baseline** task page, under **Task Status**, schedule the task and add computers to which you want to apply the schedule.

For more information, see the topic about **New schedule** dialog box in the *Symantec Management Platform User Guide*.

7 Click **Save changes**.

Registry Baseline task options

(Windows only)

You can create a new task to track the registry changes in baseline management. Baseline inventory also contains reports to track baseline and compliance information.

See "About baseline inventory" on page 133.

See "Running a registry baseline scan" on page 148.

Table 9-15 Registry Baseline task options

Option	Description
Name	Lets you enter a name for the task that you want to roll out to the target folder. This name helps you identify the task. By default, the task name is **Registry Baseline**.

Table 9-15 Registry Baseline task options *(continued)*

Option	Description
Compile a baseline snapshot	Lets you capture and set the captured registry settings as the registry baseline. This option helps you create a new registry baseline setup. You can use the following options: ■ **Use local baseline configuration** ■ **Use custom baseline configuration** This option lets you create a new baseline configuration with the **Registry Configuration Editor** or select an existing custom configuration. See "Registry Configuration Editor options" on page 151. To use the baseline snapshot for a compliance scan, you must copy it to the Notification Server computer in the following path: `*InstallDir*\Altiris\Notification Server\NSCap\bin\Win32\X86\Inventory\Application Management\RegBaselinePackage`
Compare with a baseline snapshot	Lets you compare the target with the baseline snapshot. You can use the following options: ■ **Compare with local baseline snapshot** ■ **Compare with custom baseline snapshot** You can browse for an existing baseline configuration file or baseline snapshot file. You can also create a new snapshot using the **Registry Snapshot Editor**. A baseline snapshot file maintains a record of the files or registry settings on a computer at a given time. The data is gathered during a registry baseline scan that is based on options in a baseline configuration file. Registry baseline snapshots are saved on the scanned computer to an RBL file. Registry baseline configuration files are in INI format. The default registry baseline configuration file is `AexRegScan.ini`. See "Registry Snapshot Editor options" on page 153.
Advanced	Lets you configure download and run options of the **Registry Baseline** task. You can also define when to end the task and whether to allow other tasks to run while running this task.

Registry Configuration Editor options

(Windows only)

Registry Configuration Editor lets you create or edit configuration files. The baseline configuration file contains the options that determine the registry settings to scan. You can use the default configuration file, edit it, or create one or more custom configuration files.

See "Running a registry baseline scan" on page 148.

Table 9-16 Tabs in the **Registry Configuration Editor** dialog box

Tab	Description
Include Keys	Lets you specify the registry keys to be included in the scan. The number of registry keys in the original baseline configuration affects the run time of baseline snapshot scans. See "Registry Configuration Editor: Include Keys tab" on page 151.
Exclude Keys	Lets you specify the registry keys to be excluded from the scan. See "Registry Configuration Editor: Exclude Keys tab" on page 152.
Remote Computers	Lets you specify the remote computers to be included in the scan.
Advanced	Lets you override the default values for the compliance scan output. You can maintain multiple snapshots on a single system by customizing these settings. See "Registry Configuration Editor: Advanced tab" on page 152.

Registry Configuration Editor: Include Keys tab

(Windows only)

This tab lets you specify the registry keys that you want to include in the scan.

See "Registry Configuration Editor options" on page 151.

Table 9-17 Options on the **Include Keys** tab

Option	Description
Root	Lets you select the root for the key and enter a key in the field. For example, in the **Root** drop-down list, click **HKEY_CURRENT_CONFIG**. In the box under the drop-down list, type **DATA** and then click **Add Key**. KEY_CURRENT_CONFIG/DATA is added to the **Keys** list.
Launch Registry Editor	Lets you open the registry editor to copy the key name instead of typing it. Either `regedit32.exe` or `regedit.exe` opens.
Report if this key is	Lets you specify the conditions that are required for a registry key to be reported in the compliance scan output. Select **Added**, **Deleted**, **Modified**, or any combination.

Registry Configuration Editor: Exclude Keys tab

(Windows only)

This tab lets you specify the registry keys that you want to exclude from the scan.

See "Registry Configuration Editor options" on page 151.

Table 9-18 Options on the **Exclude Keys** tab

Option	Description
Root	Lets you select the root for the key and enter a key in the field. For example, in the **Root** drop-down list, click **HKEY_CURRENT_CONFIG**. In the box under the drop-down list, type **DATA** and then click **Add Key**. KEY_CURRENT_CONFIG/DATA is added to the **Keys** list.
Launch Registry Editor	Lets you open the registry editor to copy the key name instead of typing it. Either `regedit32.exe` or `regedit.exe` opens.

Registry Configuration Editor: Advanced tab

(Windows only)

This tab lets you override the default values that are used to generate data for the output files.

See "Registry Configuration Editor options" on page 151.

Table 9-19 Options on the **Advanced** tab

Option	Description
Alternate MIF output path	This option is not applicable. Do not use this option.
Alternate XML output path	Lets you specify a directory path to override the XML output file (NSI). You can also leave this option blank to save the output file (NSI) in the default location. The default location is as follows: `C:\Program Files\Altiris\eXpress\Baseline`
When processing	Lets you specify the registry keys that you want to scan. You can use the following options: ■ **Scan only 'Included Keys' keys** Lets you scan only the registry keys that are listed on the **Include Keys** tab. ■ **Scan all registry keys** Lets you scan all the registry keys.
Maximum items to report	Lets you specify a number to limit the output rows of data that are generated in the compliance scan output files.
Defaults for the Results group	This option is not applicable. Do not use this option.
Defaults for the Values group	This option is not applicable. Do not use this option.
Output format	This option is not applicable. Do not use this option.

Registry Snapshot Editor options

(Windows only)

A registry baseline snapshot file (RBL) contains a record of the registry settings on a computer at a given time. This data is gathered during an initial baseline scan, which is based on options in a baseline configuration file.

See "Running a registry baseline scan" on page 148.

Even if you customize the configuration file before you run the baseline scan, the scan might collect the data that you do not want to compare. To remove this data, or to refine the baseline data, you can edit the snapshot file.

Table 9-20 **Registry Snapshot Editor** options

Option	Description
Input filename	Lets you browse for the input file in which you want to create a record of the registry settings on a computer. Registry baseline snapshots are in .RBL format.
Output filename	Lets you browse for the output file to which you want to write the modified file. To overwrite the existing file, you can specify the same file as in the **Input filename**.
Existing keys	Lets you view the registry keys that the baseline scan finds. The check boxes let you specify the registry keys that you want to delete.

Viewing inventory data and reports

This chapter includes the following topics:

About viewing inventory data

When inventory data is gathered, it is stored in the Configuration Management Database (CMDB).

You can use the following functions of the Symantec Management Platform to view the information in the CMDB:

- Inventory and application metering reports
  See "Viewing inventory data in reports" on page 156.
- The Resource Manager
  See "About viewing inventory data in the Resource Manager" on page 157.

You can see inventory data in the enhanced console views if you install Symantec Management Platform 7.1 SP2 and any of the following full suites:

- IT Management Suite
- Server Management Suite

- Client Management Suite

Note: The enhanced views do not appear if you install Inventory Solution individually without installing the full suite first or disable Deployment Solution in the suite.

See "Viewing inventory data in the enhanced Symantec Management Console views" on page 159.

For more information, see the topics about the enhanced views in the *Altiris™ IT Management Suite 7.1 from Symantec™ Enhanced Console Views Getting Started Guide* at the following URL:

http://www.symantec.com/docs/DOC3563

Viewing inventory data in reports

When you use reports, you can use a wide variety of predefined reports or you can create your own.

For more information, see the topics about creating and modifying custom reports in the *Symantec Management Platform User Guide*.

See "About viewing inventory data" on page 155.

Most reports let you filter the information that you view. For example, there is an inventory report that lists computers with their BIOS information. You can view the BIOS manufacturer, version, and release date. You can also filter the report to view computers in a certain domain. You can also filter the list of computers by using wildcards.

For more information, see the topics about using reports in the *Symantec Management Platform User Guide*.

This topic is a step in the process for gathering inventory on managed computers.

See "Gathering inventory on managed computers" on page 48.

To view inventory data in reports

1. In the **Symantec Management Console**, on the **Reports** menu, click **All Reports**.
2. To view inventory reports, in the left pane, under **Reports**, expand **Discovery and Inventory > Inventory**.

   To view application metering reports, in the left pane, under **Reports**, expand **Software > Application Metering**.

   See "Viewing application metering reports" on page 130.
3. Browse the report categories and select the report you want to view.

About viewing inventory data in the Resource Manager

You can use the Resource Manager to view all of the inventory data for a single resource. You can view the basic inventory that is gathered from all managed computers. An example of basic inventory is the computer's IP address. You can also view the more detailed data that the Inventory Solution gathers. For example, you can quickly view which operating system a certain computer is running. You can also view the status of that inventory data, such as when the data was last gathered. You also use the Resource Manager to view custom inventory.

See "About inventory types" on page 15.

For more information, see the topics about using the Resource Manager in the *Symantec Management Platform User Guide*.

You can view the content of the actual data classes or you can view hardware and software summaries.

See "About viewing inventory data" on page 155.

See "Viewing inventory data in the Resource Manager" on page 158.

The hardware summary page includes the following sections:

Table 10-1 Hardware inventory summary page

Section	Description
Agent	This section lists the agents that are installed on the resource, the version number, the date they were first discovered, the date when the last inventory was collected, and so on.

Table 10-1 Hardware inventory summary page *(continued)*

Section	Description
Hardware	This section contains the details of the processor, such as the type, speed, model, sound card, RAM size, and so on.
Drives	This section contains the details of the drives that are available on the resource.
Installed Software	This section displays the installed applications and their details such as the version, the date they were installed, etc.
Users and Groups	This section contains the details such as GUID, users, group, and primary user.

The software summary page includes the following sections:

Table 10-2 Software inventory summary page

Section	Description
Installed Software	This section displays the installed applications and their details such as the version, the date they were installed, and so on.
Add Remove Program	This section lists the programs that are in the Add Remove Programs of the Control Panel of the computer. It lists the name of the programs, their version number, the date they were installed, the manufacture type, estimated size, and so on.
Installed File Details	This section lists all the files that are associated with the software component installed on the computer. It displays details such as the file version, name, size, path, and so on.

Viewing inventory data in the Resource Manager

You can use the Resource Manager to view all of the inventory data for a single resource. You can view the basic inventory that is gathered from all managed computers.

For more information, see the topics about using the Resource Manager in the *Symantec Management Platform User Guide*.

See “About viewing inventory data” on page 155.

See “About viewing inventory data in the Resource Manager” on page 157.

This topic is a step in the process for gathering inventory on managed computers.

See "Gathering inventory on managed computers" on page 48.

To view the inventory data for a computer in the Resource Manager

1. In the Symantec Management Console, on the **Manage** menu, click **Filters**.
2. On the left pane, click **Computer Filters > All Computers**.
3. On the right pane, under **Filter Membership**, right-click a computer, and then click **Resource Manager**.
4. To view the hardware summary, on the **Resource Manager** page, click **Summaries > Hardware Summary**.
5. To view the software summary, on the **Resource Manager** page, click **Summaries > Software Summary**.
6. To view the **Installed Software Report**, on the **Resource Manager** page, in the left pane, click **More actions**, and then click **Installed Software Report**.

To view the inventory data for a data class in the Resource Manager

1. In the Resource Manager, on the **View** menu, click **Inventory**.
2. In the central pane, select the data class on which you want to view inventory data.
3. In the right pane, select the tab that contains the information you want to view.

Viewing inventory data in the enhanced Symantec Management Console views

The enhanced Symantec Management Console views let you quickly and easily view inventory data about computers, users, operating systems, and installed software products in your environment.

See "About viewing inventory data" on page 155.

You see the enhanced views in Symantec Management Console if you install Symantec Management Platform 7.1 SP2 and any of the following full suites:

- IT Management Suite
- Server Management Suite
- Client Management Suite

Note: The enhanced views do not appear if you install Inventory Solution individually without installing the full suite first or disable Deployment Solution in the suite.

For more information, see the topics about the enhanced views in the *Altiris™ IT Management Suite 7.1 from Symantec™ Enhanced Console Views Getting Started Guide* at the following URL:

http://www.symantec.com/docs/DOC3563

This topic is a step in the process for gathering inventory on managed computers.

See “Gathering inventory on managed computers” on page 48.

To view inventory data in the enhanced Symantec Management Console Computers view

1. In the **Symantec Management Console**, on the **Manage** menu, click **Computers**.
2. In the **Computers** pane, under **All Computer Views**, select the organizational view and group you want to view.

   For example, to view virtual machines, expand**All Computers > Virtual Machine**.
3. In the central pane, click the computer whose reports you want to view.
4. In the right pane, in the top section, view a flipbook and perform one of the following actions to change the information that you see:
   - Click the title to select an option from the drop-down list.
   - Click the links on either side of the title to move the flipbook in that direction.
5. In the right pane, expand **Software**.

To view software inventory data in the enhanced Symantec Management Console Software view

1. In the **Symantec Management Console**, on the **Manage** menu, click **Software**.
2. In the **Software** pane, select the subpane and the entry you want to view.

   For example, to view usage tracking reports for Windows computers, expand the **Metered Software** subpane, and then click the **Usage Tracking** entry.

   See “Viewing usage tracking reports in the enhanced Symantec Management Console Software view” on page 130.
3. In the central pane, click the software product you want to view.

4 In the right pane, view the top section.

5 In the right pane, expand **Computers with software installed**.

Altiris Inventory Solution™ 7.1 SP2 from Symantec™ Third-Party Legal Notices

This appendix includes the following topics:

Third-Party Legal Attributions

This Symantec product may contain third party software for which Symantec is required to provide attribution ("Third Party Programs"). Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Software does not alter any rights or obligations you may have under those open source or free software licenses. This appendix contains proprietary notices for the Third Party Programs and the licenses for the Third Party Programs, where applicable.

RegExp

MIT License

This code is licensed under the license terms below, granted by the copyright holder listed above. The term copyright holder” in the license below means the copyright holder listed above.

Copyright (c) <year> <copyright holders>

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Linux PCI ID Repository

Copyright (c) 2007, pciids project All rights reserved.

This code is licensed under the license terms below, granted by the copyright holder listed above. The terms “owner” and “organization” in the license below mean the copyright holder listed above.

Copyright (c) <YEAR>, <OWNER>

All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

- Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
- Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

Linux USB ID Repository

TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Microsoft Windows Server 2008 Redistributables

Microsoft Chart Controls for Microsoft .NET Framework

MICROSOFT SOFTWARE LICENSE TERMS

MICROSOFT WINDOWS SOFTWARE DEVELOPMENT KIT for Windows Server 2008 and .NET Framework 3.5

These license terms are an agreement between Microsoft Corporation (or based on where you live, one of its affiliates) and you. Please read them. They apply to the software named above, which includes the media on which you received it, if any. The terms also apply to any Microsoft

- updates,
- supplements,
- Internet-based services, and
- support services

for this software, unless other terms accompany those items. If so, those terms apply.

BY USING THE SOFTWARE, YOU ACCEPT THESE TERMS. IF YOU DO NOT ACCEPT THEM, DO NOT USE THE SOFTWARE.

If you comply with these license terms, you have the rights below.

1. INSTALLATION AND USE RIGHTS.

a. Installation and Use. One user may install and use any number of copies of the software on your devices to design, develop and test your programs that run on a Microsoft Windows operating system.

b. Included Microsoft Programs. The software contains other Microsoft programs. These license terms apply to your use of those programs.

2. ADDITIONAL LICENSING REQUIREMENTS AND/OR USE RIGHTS.

a. Distributable Code. The software contains code that you are permitted to distribute in programs you develop if you comply with the terms below.

i. Right to Use and Distribute. The code and text files listed below are "Distributable Code."

- REDIST.TXT Files. You may copy and distribute the object code form of code listed in REDIST.TXT files.
- Sample Code. You may modify, copy, and distribute the source and object code form of code marked as "sample."
- Microsoft Merge Modules. You may copy and distribute the unmodified output of Microsoft Merge Modules.
- Third Party Distribution. You may permit distributors of your programs to copy and distribute the Distributable Code as part of those programs.

ii. Distribution Requirements. For any Distributable Code you distribute, you must

- add significant primary functionality to it in your programs;
- for any Distributable Code having a filename extension of .lib, distribute only the results of running such Distributable Code through a linker with your application;
- distribute Distributable Code included in a setup program only as part of that setup program without modification;
- require distributors and external end users to agree to terms that protect it at least as much as this agreement;
- display your valid copyright notice on your programs;
- for Distributable Code from the Windows Media Services SDK portions of the software, include in your program's Help-About box (or in another obvious place if there is no box) the following copyright notice: "Portions utilize Microsoft Windows Media Technologies. Copyright (c) 2006 Microsoft Corporation. All Rights Reserved"; and
- indemnify, defend, and hold harmless Microsoft from any claims, including attorneys' fees, related to the distribution or use of your programs.

iii. Distribution Restrictions. You may not

- alter any copyright, trademark or patent notice in the Distributable Code;
- use Microsoft's trademarks in your programs' names or in a way that suggests your programs come from or are endorsed by Microsoft;
- include Distributable Code in malicious, deceptive or unlawful programs; or
- modify or distribute the source code of any Distributable Code so that any part of it becomes subject to an Excluded License. An Excluded License is one that requires, as a condition of use, modification or distribution, that

- the code be disclosed or distributed in source code form; or
- others have the right to modify it.

b. Additional Functionality. Microsoft may provide additional functionality for the software. Other license terms and fees may apply.

3. INTERNET-BASED SERVICES. Microsoft provides Internet-based services with the software. It may change or cancel them at any time. You may not use this service in any way that could harm it or impair anyone else’s use of it. You may not use the service to try to gain unauthorized access to any service, data, account or network by any means.

4. MICROSOFT .NET BENCHMARK TESTING. The software includes one or more components of the .NET Framework 3.5 (“.NET Components”). You may conduct internal benchmark testing of those components. You may disclose the results of any benchmark test of those components, provided that you comply with the conditions set forth at http://go.microsoft.com/fwlink/?LinkID=66406. Notwithstanding any other agreement you may have with Microsoft, if you disclose such benchmark test results, Microsoft shall have the right to disclose the results of benchmark tests it conducts of your products that compete with the applicable .NET Component, provided it complies with the same conditions set forth at http://go.microsoft.com/fwlink/?LinkID=66406.

5. Scope of License. The software is licensed, not sold. This agreement only gives you some rights to use the software. Microsoft reserves all other rights. Unless applicable law gives you more rights despite this limitation, you may use the software only as expressly permitted in this agreement. In doing so, you must comply with any technical limitations in the software that only allow you to use it in certain ways. For more information, see www.microsoft.com/licensing/userights. You may not

- work around any technical limitations in the software;
- reverse engineer, decompile or disassemble the software, except and only to the extent that applicable law expressly permits, despite this limitation;
- make more copies of the software than specified in this agreement or allowed by applicable law, despite this limitation;
- publish the software for others to copy;
- rent, lease or lend the software; or
- use the software for commercial software hosting services.

6. CODE GENERATION AND OPTIMIZATION TOOLS. You may not use the code generation or optimization tools in the software (such as compilers, linkers, assemblers, runtime code generators, and code generating design and modeling tools) to create programs, object code, libraries, assemblies, or executables to run

on a platform other than Microsoft operating systems, run-time technologies, or application platforms.

7. BACKUP COPY. You may make one backup copy of the software. You may use it only to reinstall the software.

8. DOCUMENTATION. Any person that has valid access to your computer or internal network may copy and use the documentation for your internal, reference purposes.

9. TRANSFER TO A THIRD PARTY. The first user of the software may transfer it, and this agreement, directly to a third party. Before the transfer, that party must agree that this agreement applies to the transfer and use of the software. The first user must uninstall the software before transferring it separately from the device. The first user may not retain any copies.

10. Export Restrictions. The software is subject to United States export laws and regulations. You must comply with all domestic and international export laws and regulations that apply to the software. These laws include restrictions on destinations, end users and end use. For additional information, see www.microsoft.com/exporting.

11. SUPPORT SERVICES. Because this software is “as is,” we may not provide support services for it.

12. Entire Agreement. This agreement, and the terms for supplements, updates, Internet-based services and support services that you use, are the entire agreement for the software and support services.

13. Applicable Law.

a. United States. If you acquired the software in the United States, Washington state law governs the interpretation of this agreement and applies to claims for breach of it, regardless of conflict of laws principles. The laws of the state where you live govern all other claims, including claims under state consumer protection laws, unfair competition laws, and in tort.

b. Outside the United States. If you acquired the software in any other country, the laws of that country apply.

14. Legal Effect. This agreement describes certain legal rights. You may have other rights under the laws of your country. You may also have rights with respect to the party from whom you acquired the software. This agreement does not change your rights under the laws of your country if the laws of your country do not permit it to do so.

15. Disclaimer of Warranty. The software is licensed “as-is.” You bear the risk of using it. Microsoft gives no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this agreement

cannot change. To the extent permitted under your local laws, Microsoft excludes the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

16. Limitation on and Exclusion of Remedies and Damages. You can recover from Microsoft and its suppliers only direct damages up to U.S. $5.00. You cannot recover any other damages, including consequential, lost profits, special, indirect or incidental damages.

This limitation applies to

- anything related to the software, services, content (including code) on third party Internet sites, or third party programs; and
- claims for breach of contract, breach of warranty, guarantee or condition, strict liability, negligence, or other tort to the extent permitted by applicable law.

It also applies even if Microsoft knew or should have known about the possibility of the damages. The above limitation or exclusion may not apply to you because your country may not allow the exclusion or limitation of incidental, consequential or other damages.

Please note: As this software is distributed in Quebec, Canada, some of the clauses in this agreement are provided below in French.

Remarque : Ce logiciel étant distribué au Québec, Canada, certaines des clauses dans ce contrat sont fournies ci-dessous en français.

EXONÉRATION DE GARANTIE. Le logiciel visé par une licence est offert « tel quel ». Toute utilisation de ce logiciel est à votre seule risque et péril. Microsoft n’accorde aucune autre garantie expresse. Vous pouvez bénéficier de droits additionnels en vertu du droit local sur la protection dues consommateurs, que ce contrat ne peut modifier. La ou elles sont permises par le droit locale, les garanties implicites de qualité marchande, d’adéquation à un usage particulier et d’absence de contrefaçon sont exclues.

LIMITATION DES DOMMAGES-INTÉRÊTS ET EXCLUSION DE RESPONSABILITÉ POUR LES DOMMAGES. Vous pouvez obtenir de Microsoft et de ses fournisseurs une indemnisation en cas de dommages directs uniquement à hauteur de 5,00 $ US. Vous ne pouvez prétendre à aucune indemnisation pour les autres dommages, y compris les dommages spéciaux, indirects ou accessoires et pertes de bénéfices.

Cette limitation concerne :

- tout ce qui est relié au logiciel, aux services ou au contenu (y compris le code) figurant sur des sites Internet tiers ou dans des programmes tiers ; et

- les réclamations au titre de violation de contrat ou de garantie, ou au titre de responsabilité stricte, de négligence ou d'une autre faute dans la limite autorisée par la loi en vigueur.

Elle s'applique également, même si Microsoft connaissait ou devrait connaître l'éventualité d'un tel dommage. Si votre pays n'autorise pas l'exclusion ou la limitation de responsabilité pour les dommages indirects, accessoires ou de quelque nature que ce soit, il se peut que la limitation ou l'exclusion ci-dessus ne s'appliquera pas à votre égard.

EFFET JURIDIQUE. Le présent contrat décrit certains droits juridiques. Vous pourriez avoir d'autres droits prévus par les lois de votre pays. Le présent contrat ne modifie pas les droits que vous confèrent les lois de votre pays si celles ci ne le permettent pas.

Index