Altiris™ IT Management Suite from Symantec™ Migration Guide version 7.0 to 7.1

Symantec™

Altiris™ IT Management Suite from Symantec™ Migration Guide version 7.0 to 7.1

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Printed in the United States of America.

10 9 8 7 6 5 4 3 2 1

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 or manuals

Support agreement resources

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

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

Contents

Chapter 1

Introducing IT Management Suite

This chapter includes the following topics:

About IT Management Suite

IT Management Suite combines client and server configuration management with IT asset and service management. It promotes effective service delivery and helps reduce the cost and complexity of managing corporate IT assets. These assets may include desktops, laptops, thin clients, and servers in heterogeneous environments running Windows, Linux, UNIX, and Mac. You can manage all of the features of the suite through a central console on a common platform: the Symantec Management Platform. This common platform integrates management functions to accelerate automation for better service, value, and IT efficiency.

IT Management Suite is comprised of the following management capabilities:

- Server management
  The server management capabilities support not only the Windows operating system, but also the UNIX and the Linux operating systems. In addition, the same management disciplines are applied to both physical systems and virtual systems, including both Microsoft Hyper-V and VMware.

- Client management
  The client management capabilities support Windows and a growing number of other platforms, including Mac OS and Linux operating systems.
- IT asset management
  IT asset management builds upon solid inventory foundations for configuration management. It helps you accurately value both your discoverable and non-discoverable assets, and track your assets and your asset-related information. You can manage contracts, software license compliance, and procurement processes as well as the configuration items that are associated with your assets.
- Service management
  IT Management Suite includes fully featured service management capabilities. It provides the necessary components for any ITIL-based service management initiative and covers key functions. These functions include incident and problem management, change management, self service options, and a service catalog.

What's new in IT Management Suite

In addition to full server-side 64-bit support, IT Management Suite includes many new features. The new workflow engine lets you automate human and system interactions to help you complete the sequential tasks that are required for efficient service management. Imaging, deployment, and remote control features are now integrated. The central catalog, the software library, and the new user views deliver a deeper functional integration. New IT Analytics capabilities and the central Software Catalog provide greater intelligence.

The following are some of the key new features in IT Management Suite:

- Intuitive management interface
  IT Management Suite 7.1 introduces an improved management interface that gets you where you want to be faster. The page load times are shorter and are more responsive. Common concepts such as managing computers, delivering software, and managing licenses and deployment are consolidated into an integrated experience. When you click on a computer, resource management details are immediately visible. Powerful search features help you drill down and build filters in a short period of time. You can quickly save the searches for future use. Drag-and-drop functionality lets you select tasks and drag them to one or more selected computers.
- Streamlined software management
  The Software Catalog interface is streamlined and redesigned. Any software that is found is stored in the newly discovered list. From this list you can

quickly determine whether you want to make the identified software a managed product. If not, you can assign it to unmanaged software. After you identify software as a managed software product, you can manage all elements of it in a single interface. Inventory, metering, delivery, and license tracking are all presented in a single interface.

In addition to improvements in the Managed Delivery interface, the Managed Delivery feature is more robust. The Managed Delivery feature now separates the schedule for delivery and the schedule for execution. You can first stage packages in advance, and then later schedule the execution.

- Simplified license management

  License management and asset management and usage are tightly integrated. Within the software display is an at-a-glance view of the current deployments and cost details. These details are based on the current installations and the purchasing details. A graphic can help you to determine if a software product is over-deployed or under-deployed, and evaluate its current usage. It gives visibility into the financial effect of a product. You can see the potential savings from harvesting licenses, and you can see the cost effect when a product is over-deployed.

- Advanced reporting and IT Analytics

  The executive dashboard and trend analysis give you a representative view of your IT assets. Key performance indicators let you measure critical success factors for your organization and quickly assess trends of how these measures change over time. You can use ad-hoc data mining to construct pivot table reports. The reports are based on predefined measures and dimensions. The functionality allows for easy manipulation of the data so you do not have to be a SQL expert to access the information you need. Multidimensional analysis and robust graphical reporting are incorporated to help you arrive at your answers with very little customization and without waiting.

  The MultiCMDB feature provides global IT Analytics reporting across multiple CMDBs without the need to replicate large amounts of data.

- Optimized scalability and performance

  This release increases the overall scalability of the Symantec Management Platform. Each Notification Server computer now scales to support more endpoints than the previous versions supported. The overall goal is to streamline your implementations by using less hardware. In addition to numerous improvements in overall performance, the two key changes are to user interaction and to reporting. With the new management interface, page loads are significantly improved. The advanced IT Analytics features let you gain the efficiency of OLAP cubes. The features create faster reporting times by off-loading report data from the operational database.

- Microsoft Windows 7 application compatibility challenges addressed

A key challenge to moving to Windows 7 is that many legacy Web applications depend on Internet Explorer 6. Symantec Workspace Virtualization includes a new update that solves this challenge. You can virtualize Internet Explorer 6 directly in Windows 7. This ability lets you concurrently run Internet Explorer 6, 7, and 8. You can also run multiple Java versions on the native operating system to achieve normal visibility.

This approach enables side-by-side usage, and offers a secure implementation that is invisible to the user. You can determine which applications should have access to that specific browser. Users are never prompted to choose a browser. The correct version automatically opens for them based on policy. This option helps you move faster and more efficiently to Microsoft Windows 7. Browser plug-ins such as Acrobat and Flash can be installed into the base or into a virtual layer. Multiple Java versions can be installed in the base, or in a layer, and used by a virtual Internet Explorer. Workspace Virtualization automatically supports any group policy objects that your enterprise may have in place for Internet Explorer.

- Built-in process automation

  Workflow capabilities are now included so you can automate the processes that are core to your IT business. In addition to form builders and drag-and-drop process designer capabilities, you can use the full component generator capability for access to third-party technologies. These technologies include HR or finance systems, and the Workflow portal. The Workflow portal lets you track the overall process as a workflow moves through the various stages.

- Migration and deployment enhancements

  Deployment Solution is now natively integrated with the Symantec Management Platform. Consequently, you work with Deployment Solution and Symantec Management Platform through a single console, database, and agent. IT Management Suite 7.1 provides many enhancements to the Deployment Solution console.

  The DeployAnywhere capability supports all plug-and-play driver types for hardware-independent imaging. This addition complements the support for hardware abstraction layers (HAL), network interface cards, and mass-storage-controller drivers to provide a complete hardware-independent imaging solution. Management for the driver database is now available through the console. You can consolidate driver management because both imaging and scripted operating system installations consume the drivers in the DeployAnywhere database.

  Ghost imaging supports the familiar style of RapiDeploy multicasting. PC transplant supports Microsoft Office 2010 (32-bit and 64-bit).

  Enhanced Virtual Machine Management capabilities streamline configuration and extend the virtual machine creation wizard. The wizard can execute any

Deployment Solution job as part of the virtual machine creation process. This ability lets you leverage existing server provisioning jobs and apply them to virtual server provisioning.

Solutions of IT Management Suite

IT Management Suite includes many solutions and components.

Table 1-1 IT Management Suite 7.1 solutions and components

Suite/Platform	Solution/Component
Symantec Management Platform 7.1	Includes the components such as Network Discovery, Notification Server, Symantec Management Console, and Symantec Management Agent ■ Symantec Workflow Solution 7.1 ■ IT Analytics 7.1
Asset Management Suite 7.1	■ Asset Management Solution 7.1 ■ Barcode Solution 7.1 ■ CMDB Solution 7.1
Client Management Suite 7.1	■ Deployment Solution 7.1 SP1 with a license for 6.9 SP5 ■ Inventory Solution 7.1 ■ IT Analytics Client and Server Pack 7.1 ■ IT Analytics SEP Pack 7.1 ■ Out-of-Band Management Component 7.1 ■ Patch Management Solution 7.1 ■ pcAnywhere Solution 12.6 ■ Real-Time System Manager 7.1 ■ Software Management Solution 7.1 ■ Symantec Endpoint Protection Integration Component 7.1 ■ Wise Connector 7.1 ■ Workspace Virtualization 7.1 ■ Wise Connector 7.1

Table 1-1 IT Management Suite 7.1 solutions and components *(continued)*

Suite/Platform	Solution/Component
Server Management Suite 7.1	■ Deployment Solution 7.1 SP1 with a license for 6.9 SP5 ■ Inventory Solution 7.1 ■ Inventory Pack for Servers ■ IT Analytics Client and Server Pack 7.1 ■ IT Analytics SEP Pack 7.1 ■ Monitor Pack for Servers 7.1 ■ Monitor Solution 7.1 ■ Patch Management Solution 7.1 ■ Real-Time System Manager 7.1 ■ Software Management Solution 7.1 ■ Symantec Endpoint Protection Integration Component 7.1 ■ Virtual Machine Management 7.1 ■ Wise Connector 7.1
Other	■ Symantec ServiceDesk 7.1 ■ IT Analytics ServiceDesk Pack 7.1

See "About IT Management Suite" on page 13.

Components of the Symantec Management Platform

The Symantec Management Platform includes the following core components:

- Notification Server
  The Symantec Management Platform service that processes events, facilitates communications with managed computers, and coordinates the work of the other Symantec Management Platform services.
- Symantec Management Console
  A Web-based user interface that lets you monitor and manage Notification Server and its solutions.
- Configuration Management Database (CMDB)
  The database that stores all of the information about managed computers.
- Site servers
  The Symantec Management Platform can host several types of middleware components, such as package servers and task servers. The official name for a middleware component is "site service." Any component that hosts a site service is known as a site server.

- Symantec Management Agent
  The software that is installed on a computer to enable Notification Server to monitor and manage it. After the Symantec Management Agent is installed, that computer becomes a managed computer.
- Software Management Framework
  An interface that lets you create and manage the software resources that are in the Software Catalog. It also lets you manage the packages that are in the Software Library. The Software Catalog page provides a central location for initiating the software-related tasks that are performed in your organization.
- Reports
  A way to gather automated information. You can view reports for any managed computer from the Symantec Management Console.

Where to get more information

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

See "About IT Management Suite" on page 13.

Table 1-2 Documentation resources

Document	Description	Location
Release Notes	Information about new features and important issues.	The **Product Support** page, which is available at the following URL: http://www.symantec.com/business/support/all_products.jsp When you open your product's support page, look for the **Documentation** link on the right side of the page.
User guides	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 **Product Support** page, which is available at the following URL: http://www.symantec.com/business/support/all_products.jsp When you open your product's support page, look for the **Documentation** link on the right side of the page.

Table 1-2 Documentation resources *(continued)*

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

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

Table 1-3 Symantec product information resources

Resource	Description	Location
Best practices Support Knowledgebase	Compilation of "how to" and best practice articles for IT Management Suite.	http://www.symantec.com/docs/HOWTO32608
SymWISE Support Knowledgebase	Articles, incidents, and issues about Symantec products.	http://www.symantec.com/business/theme.jsp?themeid=support-knowledgebase
Symantec Connect	An online resource that contains forums, articles, blogs, downloads, events, videos, groups, and ideas for users of Symantec products.	http://www.symantec.com/connect/endpoint-management

Chapter 2

Overview of migrating to IT Management Suite

This chapter includes the following topics:

About this migration guide

This guide is intended to help you upgrade and migrate your infrastructure to version 7.1.

The guide includes information about the following categories of information:

- Migration wizard instructions
  This release includes a tool that is called the migration wizard. Migration wizard is designed to automate the gathering of data from your previous system so you can bring it into your new system. When you run the wizard, it gathers this data and stores it in a file. After you install version 7.1 you can use the wizard to import the data in this file into your new system.
  See "About data migration" on page 52.
- Manual data migration instructions
  Some data is not stored in your current installed database. The data migration wizard is unable to locate and migrate this data. You must manually copy this data from its previous location to its new equivalent location. After the data

has been moved there may be additional steps you must take to make that data function in your new environment.
See "About the 7.0 data that you must manually migrate to Symantec Management Platform 7.1" on page 62.

Note: Notification Server was renamed Symantec Management Platform (SMP) on December 03, 2010. All previously categorized articles and references that are listed as Notification Server are now found under Symantec Management Platform. This document lists all Notification Server references for 7.1 as Symantec Management Platform. It lists version 6.0 of the comparable architectural objects by their previous names (Notification Server 6.0, etc.)

See "How to use this guide" on page 22.

See "Recommended reading" on page 22.

How to use this guide

This guide is intended to create a plan to migrate your infrastructure to version 7.1. This guide covers specific migration functions you need to follow for migrating data from older version of Altiris products.

In addition to this guide, you can use the following guides to help you migrate to IT Management Suite 7.1:

- *IT Management Suite Planning and Implementation Guide 7.1*
- *Symantec Management Platform 7.1 MP1 User Guide*
- Solution-specific user guides

See "Where to get more information" on page 19.

Each of the guides plays an important role in the migration process, and this guide references them and is a complement to them.

Many of the topics in the listed guides are not duplicated in this migration guide.

See "Recommended reading" on page 22.

Recommended reading

Before you start the migration process it is important to create a plan to migrate your infrastructure to version 7.1.

The *IT Management Suite Planning and Implementation Guide v7.1* contains migration information about prerequisites, infrastructure architecture, performance tuning, and the installation:

- Prerequisites

  As you develop your migration plan and before you attempt a migration, you should understand migration concepts. For example, you use the Symantec Installation Manager to access the migration wizard tool. This tool is made available to you when you complete a new installation of IT Management Suite. You can then copy the tool to your previous server to use it to harvest previous data.

  This process works well if you use new hardware to host your new environment. However, if you attempt to reuse previous hardware, then you must access the migration wizard tool before you install IT Management Suite. At actual installation time, your previous Notification Server no longer exists because it was reconfigured with a 64-bit operating system.

- Infrastructure architecture

  You must determine the best means to upgrade your specific infrastructure. Infrastructure components can include items such as agents, sub-agents, package servers, and task servers. The decisions you make for upgrading infrastructure components are dependent on your specific scenario. The means that you employ may also depend on the limitations of your IT policies or limitations of your network infrastructure.

  For example, if your organization has many managed computers, you may not want to immediately enable many management settings during a large agent migration. By not enabling the settings, you reduce the initial load on your Notification Server when the agents initially check in and begin the upgrade. However, after the agents have been successfully migrated, you can then increase the amount of management operations according to your migration plan.

- Installation

  You must complete a new IT Management Suite installation regardless of the migration path that you choose. IT Management Suite 7.1 requires a 64-bit operating system, but its previous versions did not run on a 64-bit operating system. There is no automated way to upgrade your existing IT Management Suite 32-bit installation. For example, if you intend to reuse existing 64-bit capable Notification Server hardware, you must install the 64-bit operating system first. The *IT Management Suite Planning and Implementation Guide 7.1* contains the steps to install IT Management Suite.

You must make similar considerations when you upgrade agents.

See "About this migration guide" on page 21.

See "How to use this guide" on page 22.

About migrating to Symantec Management Platform 7.1

Symantec Management Platform 7.1 requires the Microsoft Windows Server 2008 R2 (64-bit) operating system to host Notification Server. Because Symantec Management Platform 7.0 used a different operating system than Windows Server 2008 R2, you cannot do an automated, on-box upgrade to 7.1.

For more information, see topics on system requirements in the IT Management Suite Planning and Implementation Guide.

Note: If you have Symantec Management Platform 7.0 installed on a 64-bit server, you can install the Symantec Management Platform 7.1 products on that computer. However, before you install the Windows 2008 R2 operating system, you must complete specific migration steps. Because some of these migration steps might not complete successfully, Symantec discourages the reuse of the current server. For more information about installing the Symantec Management Platform 7.1 products on your current sever, see HOWTO32427.

The migration of data from Symantec Management Platform 7.0 to Symantec Management Platform 7.1 requires two steps. In the first step, you connect to a restored instance of the 7.0 Configuration Management Database (CMDB). You connect to the 7.0 CMDB in Symantec Installation Manager on the **Database Configuration** page when you install the Symantec Management Platform products. Symantec Installation Manager upgrades the existing 7.0 CMDB to the 7.1 schema. This step migrates all of the data in the 7.0 CMDB. In the second step, you use the migration wizard to migrate the data that is not in the CMDB. This data includes KMS keys, packages, security settings, and general Symantec Management Platform settings.

See "About data migration when migrating from Symantec Management Platform 7.0" on page 53.

For more information, see the documents at https://www-secure.symantec.com/connect/articles/altiris-endpoint-management-migrations-and-upgrades-71.

Note: Symantec Management Platform 7.1 does not support a mixed mode of Notification Servers. A 7.0 Notification Server cannot communicate with a 7.1 Notification Server.

The migration process consists of the following phases:

- Prepare
  To minimize downtime and ensure success, use the documentation to create a migration plan for your specific environment. Back up your existing data and create a test environment for evaluating and validating the entire installation and migration process. Symantec recommends that you maintain the test environment for ongoing validation and testing of updates, maintenance packs, and service packs.
- Install and migrate
  During this phase, you install Symantec Management Platform 7.1 on a computer running the Windows 2008 R2 operating system. You also migrate existing Symantec Management Platform 7.0 data from your previous environment to Symantec Management Platform 7.1. You may also manually move some solution-specific data to Symantec Management Platform 7.1.
- Validate
  During the validation phase you confirm that you have set up and configured the new Symantec Management Platform and solutions according to your requirements. The migration wizard verifies the success of the data it imports. However, you should browse to the migrated data such as policies, reports, and packages and verify their state. After you validate the success of the installation and data migration, you redirect groups of managed computers to report to the new 7.1 Notification Server. Once the managed computers report to the 7.1 server, you use an agent upgrade policy to upgrade their agents.

See "Migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1" on page 32.

About testing IT Management Suite

A test server is recommended when you prepare for upgrades or migrations with IT Management Suite 7.1 and future versions.

Symantec recommends that you test the migration process, and then familiarize yourself with the new features of 7.1. Ensure that business functional parity is met on the 7.1 configuration. Many of the features have changed with 7.1, but the business functions the tools provide are much greater than with 6.x.

When the migration process is complete, Symantec recommends that you continue to maintain the test server to test each update, service pack, or maintenance release that you intend to use in production.

See "About post migration configuration" on page 26.

See "About validating a migration" on page 26.

About post migration configuration

After you have migrated your data, browse through the product and ensure that the data is where it is expected to be. Data that gets migrated is available for different actions, and in some cases for review only.

Take some time to familiarize yourself with the data, and ensure that the product is configured to get the data that is not migrated.

See "About validating a migration" on page 26.

See "About testing IT Management Suite" on page 25.

About validating a migration

Much of the effort you make to migrate data is in itself a validation. However, tools are also available to help validate data migration. For example, the migration wizard has a validation process.

Other types of data need to be validated manually by browsing through the content in the console.

Many of the migration steps in the solution sections of this document enable both the configuration and validation of the data. Because validation is often performed as part of the migration process, this document does not include validation-only procedures.

See "About post migration configuration" on page 26.

See "About testing IT Management Suite" on page 25.

About reusing existing hardware to migrate

Symantec recommends that you use a new server to migrate to IT Management Suite 7.1.

By using a new server, you reduce the downtime that results from re-provisioning the operating system of the Notification Server computer.

Before you turn off or re-provision your old server, be sure that the new server meets your business need; otherwise, you may lose data.

Keep the old server running so that you can capture any data on it that was not migrated. Also, by keeping the old server running, you can use it for reporting and configuration reference.

If you must migrate using the existing hardware that currently houses Notification Server, you must take the following actions:

- Thoroughly test the migration process using a test computer to ensure that you capture the data properly before re-provisioning.
- Ensure that your business functional needs and requirements are not offline for lengths of time outside of SLAs
- Develop a reliable agent re-direct process. You must know the new server name before you re-provision Notification Server.

Chapter 3

Migrating Symantec Management Platform

This chapter includes the following topics:

Best practices for migrating to Symantec Management Platform 7.1

Before you begin the migration process, you should develop a migration plan. As you develop your migration plan, you should consider these best practices.

See "About migrating to Symantec Management Platform 7.1" on page 24.

Table 3-1 Best practices for migrating to Symantec Management Platform 7.1

Best practice	Description
Use a test environment.	Before you install Symantec Management Platform 7.1 in a production environment, create a test environment for evaluating and validating the entire installation and migration process. Symantec recommends that you maintain the test environment for ongoing validation and testing of updates, maintenance packs , and service packs.

Table 3-1 Best practices for migrating to Symantec Management Platform 7.1 *(continued)*

Best practice	Description
Use a pilot test group.	Use a small group of managed computers as a pilot group to test the migration to Symantec Management Platform 7.1. During this pilot test, leave the remaining managed computers supported by the previous version of Notification Server.
Redirect managed computers in stages.	You can redirect 5,000 computers to a single Notification Server at the same time. After you have successfully redirected a group of computers, upgrade the Symantec Management Agent and agent plug-ins for that group. To upgrade an agent or an agent plug-in, you enable the upgrade policy for the agent or the agent plug-in. **Note:** If you redirect more than 5,000 computers at a time, disable any policies and tasks that communicate frequently with the Symantec Management Agent. For example, disable the inventory, software delivery, and patch policies. Disabling the policies and tasks prevents the console and Notification Server from being very slow. See "About redirecting sites and agents to Notification Server 7.1" on page 43. See "About the Symantec Management Agent upgrade policies" on page 45.
Keep your previous Notification Server.	Maintain your previous Notification Server computers as a record for historical data, policy configuration details, and other settings and data. The following are some examples of when you might remove the old server: ■ After the business functional uses on the old server are matched on the new server. ■ After the data saturation on the new server has the needed depth. ■ When the data in the new Configuration Management Database (CMDB) qualifies against your regulatory standards.
Migrate using a new computer.	You must install the Symantec Management Platform 7.1 products on a computer that is running the Windows Server 2008 R2 operating system. Because this operating system is different from what was required for 7.0, Symantec recommends that you install the 7.1 products on a new computer. **Note:** If you have Symantec Management Platform installed on a 64-bit server, you can install the Symantec Management Platform 7.1 products on that computer. However, before you install the Windows 2008 R2 operating system, you must complete specific migration steps. Because some of these migration steps might not complete successfully, Symantec discourages the reuse of the current server. For more information about installing the Symantec Management Platform 7.1 products on your current server, see HOWTO32427.

Important things to know when migrating from Symantec Management Platform 7.0

A migration from Symantec Management Platform 7.0 involves many steps. You should be careful to complete these steps in the recommended order.

See "Migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1" on page 32.

In addition to completing the migration steps in the recommended order, you should also pay particular attention to the following items to avoid major problems:

- Database and server backup
  Before you begin the migration, you need to back up the 7.0 Configuration Management Database (CMDB) and the Symantec Management Platform 7.0 server. If you encounter problems during the migration process, you can then revert to these backups. Back up the CMDB to a secure storage location. Making backups before major migration steps can provide more granular recovery from any issues or unplanned outages that might occur during the process.
  See "Backing up the Configuration Management Database" on page 40.
- Product parity
  When you install the 7.1 products, you must install the same products on the 7.1 server that you installed on the 7.0 server. Failure to have product parity can result in the corruption of the database and the operating system when you connect to the 7.0 database. Before you begin the migration, create a list of the 7.0 products that you currently have installed. You can view a list of the installed products on the **Installed Products** page in Symantec Installation Manager. Symantec recommends that you install any new products after you complete the migration of your 7.0 products.
- SQL collation
  When you restore the CMDB, use the same collation that was used for Symantec Management Platform 7.1. You can restore the database to a new instance with the same name or to the same instance with a new name. You restore the database so that you can connect to it with Symantec Installation Manager during the installation. When you connect to the database, all of its data is migrated.
  See "Restoring the Configuration Management Database" on page 41.
- Server name and IP address
  Symantec recommends that you give the 7.1 server a name and an IP address that is different from the name and IP address of the 7.0 server. You can then run both your old and new server at the same time and reduce functional downtimes.

- Installation path of Symantec Installation Manager
  When you install Symantec Installation Manager on the 7.1 server, you need to use the same installation path that you used on the 7.0 server. If you change the installation path, you cannot upgrade the Symantec Management Agent and the agent plug-ins.
- Mixed mode
  Symantec Management Platform 7.1 does not support mixed mode. A Symantec Management Platform 7.0 server cannot communicate with a Symantec Management Platform 7.1 server.

Migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1

You must install the Symantec Management Platform 7.1 products on a computer that is running the Windows Server 2008 R2 operating system. Because this operating system is different from what was required for 7.0, Symantec recommends that you install the 7.1 products on a new computer.

For more information, see topics on system requirements in the IT Management Suite Planning and Implementation Guide.

Note: If you have Symantec Management Platform 7.0 installed on a 64-bit server, you can install the Symantec Management Platform 7.1 products on that computer. However, before you install the Windows 2008 R2 operating system, you must complete specific migration steps. Because some of these migration steps might not complete successfully, Symantec discourages the reuse of the current server. For more information about installing the Symantec Management Platform 7.1 products on your current sever, see HOWTO32427.

The migration of data from Symantec Management Platform 7.0 to Symantec Management Platform 7.1 requires two steps. In the first step, you connect to a restored instance of the 7.0 Configuration Management Database (CMDB). You connect to the 7.0 CMDB in Symantec Installation Manager on the **Database Configuration** page when you install the Symantec Management Platform products. Symantec Installation Manager upgrades the existing 7.0 CMDB to the 7.1 schema. This step migrates all of the data in the 7.0 CMDB. In the second step, you use the migration wizard to migrate the data that is not in the CMDB. This data includes KMS keys, packages, security settings, and general Symantec Management Platform settings.

See "Important things to know when migrating from Symantec Management Platform 7.0" on page 31.

See "About data migration when migrating from Symantec Management Platform 7.0" on page 53.

See "About the data that the migration wizard migrates from Symantec Management Platform 7.0" on page 54.

Note: Symantec Management Platform 7.1 does not support a mixed mode of Notification Servers. 7.0 Notification Servers cannot communicate with a 7.1 Notification Server.

Table 3-2 Process for migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1

Step	Action	Description
Step 1	Back up the 7.0 Configuration Management Database (CMDB) and the Symantec Management Platform 7.0 server.	You must back up the 7.0 CMDB before you begin the migration process. You should also back up the Symantec Management Platform 7.0 server. If you encounter problems during the migration process you can then revert to these backups. Back up the CMDB to a secure storage location. **Warning:** Before proceeding verify that the CMDB and the Symantec Management Platform 7.0 server have been successfully backed up. See "Backing up the Configuration Management Database" on page 40.

Table 3-2 Process for migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1 *(continued)*

Step	Action	Description
Step 2	Prepare for the migration.	On the Symantec Management Platform 7.0 server, complete the following tasks in order: ■ Verify the completion of all outstanding tasks, policies, package imports, and hierarchy replication schedules. ■ If you use hierarchy, document the hierarchy setup and then remove all hierarchy relationships. The hierarchy setup does not migrate and must be recreated on the 7.1 server. Because Symantec Management Platform 7.1 can manage more endpoints than Symantec Management Platform 7.0, you may be able to reduce or eliminate your hierarchy. For more information, see the IT Management Suite Planning and Implementation Guide. See "Migrating Notification Server computers in a hierarchy" on page 47. ■ Document the Windows Server user accounts you have set up on the 7.0 server. You must recreate these accounts manually on the 7.1 server. ■ Create a backup of your software package files. ■ Create a list of the products that you currently have installed. You must install at least the same products on the 7.1 server that you installed on the 7.0 server. You can install additional products later. You can view a list of the installed products on the **Installed Products** page in Symantec Installation Manager. **Warning:** Failure to have exact product parity can result in the corruption of the database and the operating system when you connect to the 7.0 database. ■ Copy your product licenses to a location that is accessible from the 7.1 server. You must reapply the licenses because they do not migrate. If your licenses are not downloaded or available, you can download them from the Symantec Licensing Portal. For more information about licenses and using the licensing portal, see the Customer Care Information Center. See "About migrating licenses to Symantec Management Platform 7.1" on page 51. ■ Back up the 7.0 database again to capture the most recent data.

Table 3-2 Process for migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1 *(continued)*

Step	Action	Description
Step 3	Restore the backed up 7.0 database.	You can use SQL Server Management Studio to restore the database. You can restore the database to a new instance with the same name or to the same instance with a new name. When you restore the database, use the same collation that was used on the Symantec Management Platform 7.0 server. See "Restoring the Configuration Management Database" on page 41. If you host Microsoft SQL Server on-box, install it on the 7.1 server and copy the backed-up database to the 7.1 server and restore it. If you host Microsoft SQL Server off-box, you can use the same SQL Server or set up a new SQL Server. If you use the same SQL Server, restore the database with a new name to retain the 7.0 database in working order until the migration is successful.
Step 4	Prepare the 7.1 server for the installation.	The 7.1 server must be running the Microsoft Windows 2008 R2 operating system. Symantec recommends that you give the 7.1 server a different name and IP address from the name and IP address of the 7.0 server. Because the Windows server user accounts are not migrated during the migration process, you must recreate them on the 7.1 server. If you use the same user names, they get aligned with the security roles during the migration process. You should also install the following items: ■ SSL and certificates if you use them. ■ Third-party plug-ins that the products you install require. These plug-ins include Microsoft Silverlight 4.0, Adobe Flash Player 10, and Sun Java Runtime 6.

Table 3-2 Process for migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1 *(continued)*

Step	Action	Description
Step 5	Install Symantec Installation Manager on the 7.1 server.	You use Symantec Installation Manager to install the Symantec Management Platform 7.1 products. For more information, see topics on installing Symantec Installation Manager in the IT Management Suite Planning and Implementation Guide. When you install Symantec Installation Manager on the 7.1 server, use the same installation path that you used on the 7.0 server. For example, if the installation path is C:\Program Files on the 7.0 server, then use C:\Program Files on the 7.1 server. If the installation path is D:\Program Files on the 7.0 server, then use D:\Program Files on the 7.1 server. **Warning:** If you change the installation path for Symantec Installation Manager from 7.0 to 7.1, you cannot migrate the Symantec Management Agent and the agent plug-ins.

Table 3-2 Process for migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1 *(continued)*

Step	Action	Description
Step 6	Install the Symantec Management Platform 7.1 products.	You install the Symantec Management Platform 7.1 products with Symantec Installation Manager. When you select the products to install, be sure to install all of the products that are installed on the 7.0 server. Symantec recommends that you install any new products after you complete the migration of your 7.0 products. **Warning:** Failure to install all of the 7.0 products may result in the corruption of the database and the operating system when you connect to the restored 7.0 database. During the installation process, Symantec Installation Manager displays a **Database Configuration** page. Symantec recommends that you connect to your restored 7.0 CMDB from this page. After you connect to the restored 7.0 CMDB, it is upgraded. When you install the Symantec Management Platform products, you should also install the migration wizard components. The migration wizard is used in the next step. During the installation process an **Optional Installations** page appears where you have the option to install the migration wizard components. You can also install the migration wizard components at any time with Symantec Installation Manager. At the end of the installation process, Symantec Installation Manager prompts you to apply licenses to the solutions you installed. You can also run Symantec Installation Manager at a later time to apply the licenses. For more information, see topics on installing the Symantec Management Platform products in the IT Management Suite Implementation Guide.

Table 3-2 Process for migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1 *(continued)*

Step	Action	Description
Step 7	Migrate Symantec Management Platform 7.0 data to the 7.1 server with the migration wizard.	You use the migration wizard to migrate 7.0 data that is not in the restored database. This data includes KMS keys, packages, security settings, and general Symantec Management Platform settings. See "Migrating data to Symantec Management Platform 7.1 with the migration wizard" on page 56. See "About the data that the migration wizard migrates from Symantec Management Platform 7.0" on page 54. The migration wizard process consists of the following steps: ■ Install the migration wizard on the Symantec Management Platform 7.0 server. See "About installing the Symantec Notification Server Migration Wizard" on page 55. ■ Export 7.0 data from the Symantec Management 7.0 server to a data store file. See "Exporting Symantec Management Platform 7.0 data to a data store file " on page 58. ■ Copy the data store file from the 7.0 server to the 7.1 server or to a location that the 7.1 server can access. If a **PackageFiles** folder is in the same directory as the data store file, copy it to the same directory as the data store file. ■ Import 7.0 data from the data store file to the Symantec Management Platform 7.1 server. See "Importing Symantec Management Platform 7.0 data from a data store file" on page 60.
Step 8	Verify that the 7.0 data was successfully migrated.	The migration wizard verifies the success of the data it imports. However, you should browse to the migrated data such as policies, reports, and packages and verify their state. This confirmation should include the data that was in the restored 7.0 database and the 7.0 data that you migrated with the migration wizard.
Step 9	Move solution-specific items from the 7.0 server to the 7.1 server.	Some solution-specific items are not migrated with the CMDB or with the migration wizard. You must manually move these items from the 7.0 server to the 7.1 server. See "About the 7.0 data that you must manually migrate to Symantec Management Platform 7.1" on page 62.

Table 3-2 Process for migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1 *(continued)*

Step	Action	Description
Step 10	Configure site servers.	Before you configure your site servers, you should determine how many site servers you need. If you had 7.0 site servers, you must redirect them to the 7.1 Notification Server and upgrade their Symantec Management Agents. The site servers are then upgraded automatically because their upgrade policies are enabled by default. For new site servers, you must first create the sites and then configure the site servers. See "About upgrading site servers" on page 50. For recommendations on the number of site servers to use, see the IT Management Suite Planning and Implementation Guide. For more information, see topics on site servers in the *Symantec Management Platform User Guide.*
Step 11	Verify that sites, subnets, and connection profiles are intact.	You should go to the **Site Server Settings** page, the **Credentials Management** page, and the **Account Management** page to verify that everything has migrated successfully. For more information, see topics on managing sites and subnets and creating connection profiles in the *Symantec Managment Platform User Guide.*
Step 12	Redirect the Symantec Management Agents to the new server.	The Symantec Management Agents that previously reported to the 7.0 Notification Server need to be redirected to the 7.1 Notification Server. Redirect the managed computers in groups. See "Redirecting managed computers to Notification Server 7.1" on page 44.

Table 3-2 Process for migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1 *(continued)*

Step	Action	Description
Step 13	Upgrade the Symantec Management Agent and the agent plug-ins.	After you have successfully redirected a group of computers, upgrade the Symantec Management Agent and agent plug-ins for the clients in the group. Upgrade the Symantec Management Agent before you upgrade the plug-ins. To upgrade an agent or an agent plug-in, you enable the upgrade policy for the agent or plug-in. See "Upgrading the Symantec Management Agent and the agent plug-ins" on page 49. See "About the Symantec Management Agent upgrade policies" on page 45. For more information, see topics on Symantec Management Agent settings and configuring the agent upgrade in the *Symantec Management Platform User Guide*.
Step 14	Re-establish hierarchical relationships and enable replication.	If you had hierarchical relationships with Symantec Management Platform 7.0 and still need them, re-establish those relationships in Symantec Management Platform 7.1. Because Symantec Management Platform 7.1 can manage more endpoints than Symantec Management Platform 7.0, you may be able to reduce or eliminate your hierarchy. Before you re-establish a hierarchical relationship, you must migrate the Notification Servers that are going to be in the hierarchy to Symantec Management Platform 7.1. You can then enable hierarchy replication and peer-based replication. See "Migrating Notification Server computers in a hierarchy" on page 47. For more information, see topics on configuring hierarchy and replication in the *Symantec Management Platform User Guide*.

Backing up the Configuration Management Database

Backing up the Configuration Management Database (CMDB) is the most important fail-safe measure that you can take during the migration process. After you back up the database, you can restore a new instance of the database with the same name or restore the same instance of the database with a new name. You can connect to the restored database when you install Symantec Management Platform

7.1.You also can use the backup to restore your database to a known good state if anything should happen to compromise your database.

See "Restoring the Configuration Management Database" on page 41.

See "Migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1" on page 32.

To back up the Configuration Management Database

1. Open Microsoft SQL Manager Studio.
2. In the left pane, expand the **Databases** folder.
3. In the left pane, under **Databases**, right-click the name of your database.
4. In the right-click menu, click **Tasks > Back Up**.
5. In the **Back up Database** dialog box, in the **Backup type** drop-down list, click **Full**.
6. In the **Backup set** section, enter a name for your backup.
7. In the **Destination** section, add the location where you want your backup file to be stored.

   This location should be a secure storage location, and should not be on the local computer.
8. Click **OK**.

Restoring the Configuration Management Database

When you migrate from Symantec Management Platform 7.0, you can migrate all of the data in the Configuration Management Database (CMDB). To migrate the data in the CMDB, you first restore the database. You can restore the database to a new instance with the same database name or to an existing instance with a new database name. If you host SQL Server on-box, you must copy the backed up database to the 7.1 server before you restore it. After you restore the database, you can connect to it when you install the Symantec Management Platform products.

See "Backing up the Configuration Management Database" on page 40.

See "Migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1" on page 32.

After you restore the database on a new server, you must also set the appropriate permissions to the SQL database.

See "Setting the appropriate permissions to the SQL database" on page 42.

To restore the Configuration Management Database

1. Open Microsoft SQL Manager Studio.
2. In the left pane, on the right-click menu of the **Databases** folder, click **Restore Database**.
3. In the **Restore Database** dialog box, click **From device**.
4. Click the ellipsis option that is associated with the **From device** option that lets you select the database.
5. In the **Specify Backup** dialog box, click **Add**.
6. In the **Locate Backup File** dialog box, select the CMDB that you backed up on the Symantec Management Platform 7.0 server, and click **OK**.
7. In the **Specify Backup** dialog box, click **OK**.
8. In the **Restore Database** dialog box, in **To database**, enter a name for the database, select the database in the **Select the backup sets to restore** section, and click **OK**.
9. After the database is restored, click **OK** in the dialog box that appears.

Setting the appropriate permissions to the SQL database

When you restore the Configuration Management Database (CMDB) on a new server, you must set the appropriate permissions to the SQL database. If you use application permissions to access SQL in Symantec Installation Manager, you must give the application account database ownership (DBO). If you use a specific SQL account to access SQL in Symantec Installation Manager, you must give that account DBO.

See "Restoring the Configuration Management Database" on page 41.

To set the appropriate permissions to the SQL database

1. Open Microsoft SQL Manager Studio.
2. In the left pane, under the **Databases** folder, on the right-click menu of the CMDB, click **Properties**.
3. In the **Database Properties** dialog box, in the **Select a page** section, click **Files**.
4. In the right pane of the **Database Properties** dialog box, click the ellipsis option that is associated with the **Owner** option.
5. In the **Select Database Owner** dialog box, click **Browse**.
6. In the **Browse for Objects** dialog box, select the appropriate account and click **OK**.

7 In the **Select Database Owner** dialog box, click **OK**.

8 In the **Database Properties** dialog box, click **OK**.

About redirecting sites and agents to Notification Server 7.1

Before you redirect sites and agents to the new Notification Server computer, you should develop a redirection plan. Use the guidelines and information in this topic to help you develop that plan.

See "Redirecting managed computers to Notification Server 7.1" on page 44.

Symantec recommends that you keep the Symantec Management Platform 7.0 server and the Symantec Management Platform 7.1 server running at the same time. Over time you incrementally move groups of client computers to the Symantec Management Platform 7.1 server. By maintaining your Symantec Management Platform 7.0 server, you preserve a historical record of your settings and data. You also have more control over what client computers you move and when you move them.

Use the following guidelines when you redirect sites and their site servers to the 7.1 Notification Server:

- When you redirect a site, Symantec recommends that you redirect and upgrade its site server before you redirect any other agents within the site. If there is more than one site server for a location or logical group, migrate the sites servers with their clients in proportional groups. You redirect and upgrade the site servers first so that they are available in the new environment when the agents in the site are redirected.
- After a site server is redirected to the 7.1 Notification Server, you must remove the site server from the 7.0 Notification Server as soon as possible.
  You remove a site server from the 7.0 Notification Server to prevent the agents that are still in the 7.0 environment from communicating with it.
- After you redirect a site server to the 7.1 Notification Server, upgrade the site server immediately.
  To upgrade a site server, upgrade the Symantec Management Agent. You use upgrade policies on the Symantec Management Platform 7.1 server to upgrade the agent. After the Symantec Management Agent is upgraded, the site services are upgraded automatically because the upgrade policies are enabled by default.
  See "About upgrading site servers" on page 50.
  See "About the Symantec Management Agent upgrade policies" on page 45.
  See "Upgrading the Symantec Management Agent and the agent plug-ins" on page 49.
- Redirect task servers before you redirect package servers.

How you redirect sites and agents depends on whether you have sites defined and the number of agents in your environment as follows:

No sites are defined.	■ If the number of agents is less than 5,000, any site servers should be redirected to the new Notification Server and then the Symantec Management Agents in the site. ■ If the number of agents is more than 5,000, Symantec recommends that you first define sites in Symantec Management Platform 7.0. Each site should have at least one site server and no site should have more than 5,000 agents. After you define the sites, redirect each site to the new Notification Server. When you redirect a site, redirect the site servers and then the agents within the site.
Sites are defined.	■ If a site has less than 5,000 agents, redirect each site server to the new Notification Server. When you redirect a site, redirect the site servers and then the agents within the site. ■ If a site has more than 5,000 agents, Symantec recommends that you divide the site into smaller sites. ■ If multiple sites share a site server and the sites have a total of less than 5,000 agents, redirect the site servers and sites together. ■ If multiple sites share a site server and the sites have a total of more than 5,000 agents, temporarily remove the site server from the 7.0 system. After you redirect all the sites to the new Notification Server, recreate the shared site server.

Redirecting managed computers to Notification Server 7.1

The Symantec Management Agents that previously reported to the 7.0 Notification Server need to be redirected to the 7.1 Notification Server. When you redirect a group of computers, create a filter for the first group of computers that you want to move. You then target the filter with the targeted agent settings policy and exclude it from the targets of other policies. You can then expand the membership of the filter as needed until it includes all computers.

See "About redirecting sites and agents to Notification Server 7.1" on page 43.

Although 20,000 computers can be managed with a single Notification Server, Symantec recommends that you redirect no more than 5,000 computers at the same time. However, it is possible to redirect up to 15,000 computers to a single Notification Server at the same time.

Note: If you redirect more than 5,000 computers at a time, disable any policies and tasks that communicate frequently with the Symantec Management Agent. Disabling the policies and tasks prevents the console and Notification Server from being very slow.

See "Best practices for migrating to Symantec Management Platform 7.1" on page 29.

For more information, see topics on the **Targeted Agent Settings** page in the *Symantec Management Platform User Guide*.

To redirect computers to Symantec Management Platform 7.1

1. In the 7.1 environment, install a package service and a task service on a site server to handle clients as they are redirected.

   By default, a task service is installed on the Symantec Management Platform server. However, Symantec recommends that you always set up at least one task server to service the client computers.

   Your environment might require multiple site servers. You might elect to redirect a package server and then the clients that use that package server to ensure that packages are available regionally. You can also use virtual machines to serve as temporary site servers during the redirection process. After all the agents for those sites have upgraded, you should then remove the virtual machines.
2. On the **Settings** menu, click **Agents/Plug-ins > Targeted Agent Settings**.
3. On the **Targeted Agent Settings** page, select the policy that contains the agents that you want to redirect to 7.1, and click the **Advanced** tab.
4. In the **Alternate URL for accessing NS** section, specify the URL for the 7.1 Notification Server as follows:
   - **Server Name**
     Symantec recommends that you use the fully qualified domain name.
   - **Server Web**
     The Server Web address should be in the following format:
     https://<NS_FQDN>:<port>/Altiris/
5. Click **Save changes**.

About the Symantec Management Agent upgrade policies

You use a Symantec Management Agent upgrade policy to upgrade the 7.0 Symantec Management Agent on your managed computers. To perform the

upgrade, you select and enable the appropriate policy and apply it to a set of computers. Upgrade the Symantec Management Agent before you upgrade the agent plug-ins.

See "Upgrading the Symantec Management Agent and the agent plug-ins" on page 49.

The Symantec Management Agent has a set of site server upgrade policies and a set of upgrade policies for all other computers. Both sets have two policies for upgrading 64-bit computers and another policy for upgrading 32-bit computers. One 64-bit upgrade policy upgrades a 64-bit computer with a 64-bit agent, while the other policy upgrades a 64-bit computer with a 32-bit agent.

The upgrade polices for the Symantec Management Agent are in a **Non Site Server** folder and a **Site Server** folder. To access these folders, on the **Settings** menu, click **Agents/Plug-ins > Symantec Management Agent** and expand the **Windows** folder.

Note: The upgrade policy for the Symantec Management Agent for UNIX/Linux/Mac is in the **UNIX/Linux/Mac** folder.

When you install a 64-bit agent on a computer, 64-bit sub-agents or plug-ins are installed when they are available. If a 64-bit plug-in is not available, a 32-bit plug-in is installed, and it runs in a surrogate service that was created for this scenario. When you install a 32-bit agent on a 64-bit computer, 32-bit sub-agents or plug-ins are installed.

Warning: If you install the 32-bit agent on a 64-bit computer, the agent may have trouble returning some inventory data because it is runs in the WOW64 memory space. Applications that run in the WOW64 memory space do not see the actual registry and file system on a 64-bit computer.

For more information, see topics on file system redirector and registry redirector in the Microsoft MSDN library.

Note: When you install the Symantec Management Agent with a scheduled push install on a 64-bit computer, the 64-bit agent is installed by default. However, if you check the **Force installation of 32-bit Symantec Management Agent on 64-bit systems** option, the 32-bit agent is installed. The option to force a 32-bit installation is on the **Symantec Management Agent Installation Options** dialog box. You access this dialog box when you click the **Settings** option on the **Symantec Management Agent Install** page.

Migrating Notification Server computers in a hierarchy

The supported method is to migrate the Notification Server computers in the hierarchy from the bottom up. Therefore, you should migrate the lowest child node first and then work up. Ensure that each child Notification Server is migrated to a higher version before its parent.

Because Symantec Management Platform 7.1 can manage more endpoints than Symantec Management Platform 7.0, you may be able to reduce or eliminate your hierarchy. You might also be able to flatten your hierarchy and reduce the replication traffic and processing on each server including the parent server. Evaluate your topology before you reconnect child servers because they may not be needed.

For more information, see topics on hierarchy in the IT Management Suite Planning and Implementation Guide.

Before you begin the migration process, document your hierarchy settings and the replication rules that you use.

Note: Symantec Management Platform 7.1 does not support a mixed mode of Notification Servers. 7.0 Notification Servers cannot communicate with a 7.1 Notification Server.

You need to ensure that there are no replication jobs currently running at the time that you choose to migrate each Notification Server computer. To check, you can run the Current Replication Activity report for the Notification Server computer that you are migrating. The report shows results only if a replication job is currently in progress.

See "Disabling hierarchy replication" on page 48.

When you migrate your Notification Servers that are in a hierarchy, use the procedure that best meets your needs. If you safely fall within the performance and scaling numbers to use a single server, then eliminate your hierarchy. If you need to maintain hierarchy, Symantec recommends migrating all the child servers before the parent server. This method lets you carefully account for the performance on the parent and the child servers as you add servers to the hierarchy and run replication.

Migrating the parent server and eliminating the child servers

1. Remove all hierarchy relationships.
2. Redirect all clients to a single Notification Server.

Migrating the parent server after migrating all of the child servers

1. Remove all hierarchy relationships.
2. Migrate all of the child servers to Symantec Management Platform 7.1.
3. Migrate the parent server to Symantec Management Platform 7.1.
4. Reestablish the hierarchy relationships of the migrated child servers and the migrated parent server along with the replication rules.

Migrating the parent server after migrating half of the child servers

1. Remove the hierarchy from a child server and migrate it to Symantec Management Platform 7.1.

   Do not reconnect the child to the parent at this time.
2. Repeat the first step on a second child server.

   Assuming that you have four Notification Servers, half of your child servers are now in a hierarchy and half of them are not.
3. Remove all hierarchy relationships, and migrate the parent server to Symantec Management Platform 7.1.
4. Immediately, reestablish the hierarchy relationships of the migrated child servers and the migrated parent server along with the replication rules.

   Note: If the parent server is performing upgrades, for example to agents and inventories, the server could be busy. Consequently, the server may be slow during the first replication job.
5. Migrate the two remaining child servers to Symantec Management Platform 7.1.
6. Reestablish the hierarchy relationships of the last two migrated child servers and the migrated parent server along with the replication rules.

Disabling hierarchy replication

Symantec recommends that you disable hierarchy replication on each adjacent hierarchy node. This step prevents any replication data from being sent to a Notification Server computer while it is mid-way through a migration. You need to disable replication on the local server that you are about to migrate. You also must disable replication on any parent and any child Notification Server computers (those that are directly before or after the local server). By completing this step, you prevent the local server from carrying out any of its usual replication jobs.

When the Notification Server computer migration has completed, you need to enable hierarchy replication again. Repeat the procedure and select **Enable Replication** from the context menu. Replication resumes as normal.

To disable hierarchy replication on a hierarchy node

1. On the Notification Server computer, open the Symantec Management Console.
2. On the **Settings** menu, click **Notification Server > Hierarchy**.
3. On the **Hierarchy Management** page, on the **Topology** tab, in the Diagram view, right-click on the local server node.
4. On the context menu, click **Disable Replication**.

See "Migrating Notification Server computers in a hierarchy" on page 47.

Upgrading the Symantec Management Agent and the agent plug-ins

After you migrate to Symantec Management Platform 7.1, you need to upgrade the Symantec Management Agent and agent plug-ins on the client computers. Upgrade the Symantec Management Agent before you upgrade the agent plug-ins.

See "About the Symantec Management Agent upgrade policies" on page 45.

See "Migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1" on page 32.

Warning: If you install the 32-bit agent on a 64-bit computer, the agent may have trouble returning some inventory data because it is runs in the WOW64 memory space. Applications that run in the WOW64 memory space do not see the actual registry and file system on a 64-bit computer.

For more information, see topics on file system redirector and registry redirector in the Microsoft MSDN library.

To upgrade the Symantec Management Agent and the agent plug-ins

1. In Symantec Management Platform 7.0, redirect the managed computers to the 7.1 Notification Server.

   See "About redirecting sites and agents to Notification Server 7.1" on page 43.

   See "Redirecting managed computers to Notification Server 7.1" on page 44.
2. In Symantec Management Platform 7.1, use filters and targets to create a test group of clients on which to test the upgrade of the agent and the agent plug-ins.
3. For the test group, enable the Symantec Management Agent upgrade policy.

4. For the test group, enable the upgrade policies for the agent plug-ins that correspond to the plug-ins that were installed on client computers before you migrated to 7.1.
5. For the test group, validate that policies, tasks, and other functionality works correctly.
6. For the rest of your client computers, repeat the preceding steps that you performed on the test group.

   You can broaden the scope a few thousand clients at a time. Symantec recommends that you do not upgrade more than 5,000 clients at the same time. You can upgrade up to 15,000 clients at the same time. However, you should then disable any policies and tasks that communicate frequently with the Symantec Management Agent.
7. For the clients that are not available during the migration, ask your network team to make the following change:

   - Delete the Symantec Management Platform 7.0 DNS A Record.
   - Create DNS Alias (CNAME) to direct the host name for Notification Server 7.0 to Symantec Management Platform 7.1.

   Keep these settings in place until the upgrade of the agent and the agent plug-ins is completed on all of the remaining clients.

About upgrading site servers

You need to upgrade your site servers in a site before you redirect your managed computers in the site to the 7.1 Notification Server. To upgrade a site server, redirect it to the 7.1 Notification Server and upgrade its Symantec Management Agent. Because the policies that upgrade the services on the site are enabled by default, the site server is then automatically upgraded. The Legacy Windows Package Server Agent Upgrade policy upgrades the package servers. The Legacy Task Service Upgrade policy upgrades the task servers.

See "Upgrading the Symantec Management Agent and the agent plug-ins" on page 49.

See "About redirecting sites and agents to Notification Server 7.1" on page 43.

For a lengthy migration, Symantec recommends that you set up temporary site servers or move your site servers in proportional groups along with their clients. For example, suppose you have 10,000 clients pointing to a Notification Server and four site servers. You do not want to leave either your old or new Notification Server with no site servers. You should either add temporary site servers or move 1/4 of your site servers with 1/4 of your clients.

When you set up package servers, you prepare the network topology for the agent packages that are available from regional package servers. If you have remote sites with a slow connection, you should upgrade their package servers before you upgrade the agents on the clients. By upgrading the package servers, you reduce the load of the package traffic.

Warning: Do not upgrade package servers before their client base is targeted to be upgraded.

If you upgrade the agent on a package server to a 64-bit agent, its 32-bit assemblies are removed and 64-bit assemblies are installed. The existing registry and folder structure for packages remains intact. If you upgrade the agent on a package server to a 32-bit agent, the package server is also upgraded to 32-bit.

After a package server is upgraded, it downloads any new 7.1 system-based packages that the 7.1 Notification Server hosts. These packages include all solution plug-ins. Any package that has not changed is not re-downloaded.

To access the package server agent upgrade policy, on the **Settings** menu, click **All Settings**. You then navigate to **Settings > Notification Server > Site Server Settings > Package Service > Advanced > Windows > Legacy Windows Package Server Agent Upgrade**.

To access the 64-bit task server agent upgrade policy, on the **Settings** menu, click **All Settings**. You then navigate to **Settings > Notification Server > Site Server Settings > Task Service > Advanced > Legacy Task Service Upgrade (x64)**.

To access the 32-bit task server agent upgrade policy, on the **Settings** menu, click **All Settings**. You then navigate to **Settings > Notification Server > Site Server Settings > Task Service > Advanced > Legacy Task Service Upgrade (x86)**.

About migrating licenses to Symantec Management Platform 7.1

When you migrate from Symantec Management Platform 7.0 to Symantec Management Platform 7.1, the licenses for your products are not migrated. You must copy the 7.0 licenses to a location where you can access them on the Symantec Management Platform 7.1 server.

See "Migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1" on page 32.

After you migrate the licenses, you must apply them. You can apply the licenses when you install a product or at a later time. You apply the licenses on the **Product Licensing** page in Symantec Installation Manager.

For more information, see topics on applying licenses in the IT Management Suite Planning and Implementation Guide.

If your licenses are not available, you can download them from the Symantec Licensing Portal. If you cannot apply your old licenses in Symantec Installation Manager, then you must also download new licenses from the licensing portal.

For more information about licenses and using the licensing portal, see the Customer Care Information Center.

About data migration

When you migrate to Symantec Management Platform 7.1, you can also migrate the Symantec Management Platform 7.0 data to Symantec Management Platform 7.1.

See "About data migration when migrating from Symantec Management Platform 7.0" on page 53.

Symantec provides the following tools to assist in the process of migrating data to Symantec Management Platform 7.1:

- Symantec Installation Manager
  You use the Symantec Installation Manager to install the migration wizard components. The migration wizard components give you access to the Symantec Notification Server Migration Wizard.
  You also use the Symantec Installation Manager to connect to a restored 7.0 Configuration Management Database (CMDB). When you connect to the 7.0 database, all of its data is migrated.
  See "About installing the Symantec Notification Server Migration Wizard" on page 55.
- Symantec Notification Server Migration Wizard
  You use the Symantec Notification Server Migration Wizard to migrate Symantec Management Platform 7.0 data to Symantec Management Platform 7.1. The migration wizard migrates data that is not in the CMDB.
  See "About the Symantec Notification Server Migration Wizard" on page 54.
  See "About the data that the migration wizard migrates from Symantec Management Platform 7.0" on page 54.

For more information, see the documents at https://www-secure.symantec.com/connect/articles/altiris-endpoint-management-migrations-and-upgrades-71.

About data migration when migrating from Symantec Management Platform 7.0

When you migrate from Symantec Management Platform 7.0, you can migrate all of the data in the 7.0 Configuration Management Database (CMDB). Because the 7.0 database is compatible with Symantec Management Platform 7.1, you can connect to a restored instance of the database to migrate the data. Symantec recommends that you use Symantec Installation Manager to connect to the restored 7.0 database.

See "About data migration" on page 52.

See "Migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1" on page 32.

See "Important things to know when migrating from Symantec Management Platform 7.0" on page 31.

However, the following Symantec Management Platform 7.0 data is not stored in the database and must be migrated separately:

- Symantec Management Platform security settings and some general settings
  You can migrate these settings with the Symantec Notification Server Migration Wizard.
  See "About the Symantec Notification Server Migration Wizard" on page 54.
  See "About the data that the migration wizard migrates from Symantec Management Platform 7.0" on page 54.
- Windows Server user accounts
  You must recreate the user accounts on the new computer.
- Some solution-specific files and settings
  You must manually move some solution-specific files and settings.
  See "About the 7.0 data that you must manually migrate to Symantec Management Platform 7.1" on page 62.
- Hierarchical relationships
  If you used hierarchical relationships and still need them, you must recreate them and enable replication. Because Symantec Management Platform 7.1 can manage more endpoints than Symantec Management Platform 7.0, you may be able to reduce or eliminate your hierarchy.
  For more information, see topics on hierarchy in the IT Management Suite Planning and Implementation Guide.
- Product licenses
  You must copy the product licenses to a location that is accessible from the 7.1 server.

See "About migrating licenses to Symantec Management Platform 7.1" on page 51.

For more information, see the documents at https://www-secure.symantec.com/connect/articles/altiris-endpoint-management-migrations-and-upgrades-71.

About the data that the migration wizard migrates from Symantec Management Platform 7.0

When you migrate from Symantec Management Platform 7.0, you use the Symantec Notification Server Migration Wizard to migrate Symantec Management Platform 7.0 data. The migration wizard migrates data that is not in the Configuration Management Database (CMDB). You migrate the data in the 7.0 database when you connect to a restored instance of the 7.0 CMDB. You connect to the 7.0 CMDB in Symantec Installation Manager on the **Database Configuration** page when you install the Symantec Management Platform products.

See "About data migration" on page 52.

See "About the Symantec Notification Server Migration Wizard" on page 54.

You can migrate the following Symantec Management Platform data with the migration wizard:

- KMS keys
- Credential manager keys
- Selected core settings
- Email settings
- Security roles
- Some event log registry keys

If you store your software packages locally, the migration wizard can also migrate them. When you import the packages, they are imported to the same location they had on the 7.0 server unless you specify an alternate location. The migration wizard can also migrate all patch packages regardless of where they are stored and import them into the default location.

About the Symantec Notification Server Migration Wizard

When you migrate to Symantec Management Platform 7.1, you use the Symantec Notification Server Migration Wizard to migrate 7.0 data that is not in the database. This data includes KMS keys, packages, security settings, and general Symantec Management Platform settings.

See "About the data that the migration wizard migrates from Symantec Management Platform 7.0" on page 54.

See "About data migration" on page 52.

Migrating data with the migration wizard involves the following steps:

- Export the data to a data store file with the migration wizard.
- Copy the data store file to a location that the Symantec Management Platform 7.1 server can access.
  If a **PackageFiles** folder is in the same directory as the data store file, copy it to the same directory as the data store file.
- Import the data from data store file with the migration wizard.

See "About the data store file" on page 63.

To migrate data with the migration wizard, you must install the migration wizard on your 7.0 server and on the 7.1 server. How you install the migration wizard varies depending on where you install it.

See "About installing the Symantec Notification Server Migration Wizard" on page 55.

The migration wizard uses exporters to export data and a corresponding set of importers to import data. Each product that has data to migrate has its own set of exporters and importers. By default, the migration wizard exports and imports all of the data. Symantec recommends that you use the default setting to export and import all of the data.

The EXE for the migration wizard is `NSUUpgradeWizard.exe`, and it is in the C:\Program Files\Altiris\Upgrade directory by default. To run the migration wizard, you must be a member of the local administrators group.

About installing the Symantec Notification Server Migration Wizard

You use the Symantec Notification Server Migration Wizard to migrate data from Symantec Management Platform 7.0 to Symantec Management Platform 7.1. To migrate data with the migration wizard, you must install the migration wizard on your 7.0 server and on the 7.1 server. How you install the migration wizard varies depending on where you install it.

See "About data migration" on page 52.

See "About the Symantec Notification Server Migration Wizard" on page 54.

Note: To run the migration wizard, you must be a member of the local administrators group.

Table 3-3 About installing the Symantec Notification Server Migration Wizard

Where the migration wizard is installed	How to install the migration wizard
Symantec Management Platform 7.1 server	Use Symantec Installation Manager on the computer to install the migration wizard components. After you select the products to install, Symantec Installation Manager displays an **Optional Installations** page that includes the **Install Migration Wizard Components** option. If you check this option, the migration wizard components are installed with the selected products. You can also access the **Optional Installations** page at a later time to install the migration wizard components.
Current Notification Server	Copy the migration wizard installation package from the Symantec Management Platform 7.1 server. The migration wizard installation package has a 32-bit and a 64-bit version. Copy the 32-bit version. You then run the installation package to install the migration wizard. The migration wizard installation package is only available on the 7.1 server if you have installed the optional migration wizard components on that computer. By default, the migration wizard installation package is installed at C:\Program Files\Altiris\Symantec Installation Manager\MigrationPackage. **Note:** The **MigrationPackage** folder contains four files. Two of the files include the word "silent" in their name. Use the migration package files that do not contain the word "silent" to install the migration wizard. **Note:** You can install Symantec Installation Manager on another computer and install only the migration wizard components on that computer. You can then copy the migration wizard installation package to your current Notification Server and migrate its data. You might install just the migration wizard if you need to install the Symantec Management Platform 7.1 products on your current server. However, Symantec discourages the reuse of the current server. For more information about installing the Symantec Management Platform 7.1 products on your current server, see HOWTO32427.

Migrating data to Symantec Management Platform 7.1 with the migration wizard

You use the Symantec Notification Server Migration Wizard to migrate Symantec Management Platform 7.0 data to Symantec Management Platform 7.1. This topic provides an overview of the process of migrating data with the migration wizard.

See "About the Symantec Notification Server Migration Wizard" on page 54.

See "About the data that the migration wizard migrates from Symantec Management Platform 7.0" on page 54.

Table 3-4 Process for migrating data to Symantec Management Platform 7.1 with the migration wizard

Step	Action	Description
Step 1	Install the migration wizard on the Symantec Management Platform 7.0 server.	Before you can migrate data with the migration wizard, you must first install it. You use Symantec Installation Manager to install the migration wizard components on the 7.1 server. You then copy the migration wizard installation package to your current Notification Server and install it. See "About installing the Symantec Notification Server Migration Wizard" on page 55.
Step 2	Export 7.0 data to a data store file.	After the migration wizard is installed on the Symantec Management Platform 7.0 server, it starts in export mode. The migration wizard lets you export 7.0 data to a data store file. You can also manually run the migration wizard and export data multiple times. See "Exporting Symantec Management Platform 7.0 data to a data store file " on page 58. See "About the data store file" on page 63.
Step 3	(Optional) View the data in the data store file.	After you export data to a data store file, you can use Store Browser to view the data that was exported. See "Viewing the data in a data store file" on page 64.
Step 4	(Optional) Compare two data store files.	If you export 7.0 data multiple times, you can use StoreDiff to compare two data store files. StoreDiff creates a data store file that contains the differences between the two data store files. You can then use Store Browser to view these differences. See "Comparing two data store files" on page 66.
Step 5	Copy the migration data to the Symantec Management Platform 7.1 server.	You need to copy the migration data to a location that is accessible to the Symantec Management Platform 7.1 server. By default, a data store file is created in the Altiris\Upgrade\Data directory. If package files are exported, this directory also contains a **PackageFiles** folder. You must put the **PackageFiles** in the same directory where you put the data store file. You may also want to copy this data to a neutral location to back up the data.

Table 3-4 Process for migrating data to Symantec Management Platform 7.1 with the migration wizard *(continued)*

Step	Action	Description
Step 6	Import the 7.0 data to Symantec Management Platform 7.1.	On the Symantec Management Platform 7.1 server, use the migration wizard to import the 7.0 data. If the migration wizard is not installed on this computer, you must first install it. See "About installing the Symantec Notification Server Migration Wizard" on page 55. See "Importing Symantec Management Platform 7.0 data from a data store file" on page 60.

Exporting Symantec Management Platform 7.0 data to a data store file

When you migrate to Symantec Management Platform 7.1, you use the Symantec Notification Server Migration Wizard to migrate Symantec Management Platform 7.0 data. When you use the migration wizard, one step in the migration process is to export the 7.0 data to a data store file. By default, the data store file is saved in the C:\Program Files\Altiris\Upgrade\Data directory.

See "Migrating data to Symantec Management Platform 7.1 with the migration wizard" on page 56.

See "About data migration" on page 52.

See "About the data store file" on page 63.

When the migration wizard runs in export mode, it uses exporters to export data. Each product that has data to migrate has its own set of exporters. By default, the migration wizard exports all of the data. Symantec recommends that you use the default setting to export all of the data.

When you export data, additional data migration files may be created and saved in this same directory. For example, when you export locally saved software package files, a **PackageFiles** folder is created that contains folders for all of the package files.

To export Symantec Management Platform 7.0 data to a data store file

1. Install and run the migration wizard on the Symantec Management Platform 7.0 server.

   After the migration wizard is installed on the Symantec Management Platform 7.0 server, it starts in export mode. You can also manually run NSUpgradewizard.exe to start the migration wizard manually. The migration wizard EXE is in the C:\Program Files\Altiris\Upgrade directory by default.

   See "About installing the Symantec Notification Server Migration Wizard" on page 55.

   See "About the Symantec Notification Server Migration Wizard" on page 54.

2. If the **Welcome** page of the migration wizard appears, click **Next**.

3. On the **Export / Import Task Selection** page, specify a name and location for the data store file, and click **Next.**

   The default name has three parts: the word Store, the date, and the time. The data store extension must be .adb.

4. On the **Password Protection** page, if you want to encrypt the data, enter a password.

   You must then use this password when you import the data on the Symantec Management Platform 7.1 server.

5. On the **Exporter Configuration** page, select the data to export, and click **Next**.

   Symantec recommends that you select all of the available data.

   See "Exporter Configuration or Importer Configuration page" on page 61.

6. On the **Product Readiness Check** page, review the messages, and click **Next**.

   This page displays each product that has data that is not included in the export. To view an explanation of why the data is not included, click in the **Message** column.

7. If the product readiness warning message appears, click **Yes**.

   This message indicates that not all products meet the product readiness check. To view the explanations for any product readiness warnings, click **No**, and then click **Back**.

8. On the **Task Summary** page, verify that the migration wizard is about to perform the correct tasks, and click **Next**.

9. When the message that the data export has completed successfully appears, click **OK**.

   If the data is not exported successfully, a message with instructions appears.

10 (Optional) To display details about each action, check **Show Details**.

11 Click **Finish**.

Importing Symantec Management Platform 7.0 data from a data store file

You use the Symantec Notification Server Migration Wizard to migrate Symantec Management Platform 7.0 data to Symantec Management Platform 7.1. When you use the migration wizard, one step in the migration process is to import the 7.0 data from a data store file.

See "Migrating data to Symantec Management Platform 7.1 with the migration wizard" on page 56.

See "About the data store file" on page 63.

See "About the Symantec Notification Server Migration Wizard" on page 54.

When the migration wizard runs in import mode, it uses importers to import data. Each product that has data to migrate has its own set of importers. By default, the migration wizard imports all of the data.

You can import all of the data at one time or perform multiple imports and import the data in stages. For example, you can perform an import for each product and then check the data after each import. If you do not import all of the data initially, you must manually run the migration wizard for subsequent imports. If you import the same data twice, the last import overwrites any previous import.

To import Symantec Management Platform 7.0 data from a data store file

1 Do one of the following to start the migration wizard in the import mode:

- Install the migration wizard on the Symantec Management Platform 7.1 server with Symantec Installation Manager. By default, the migration wizard starts after it is installed.
  See "About installing the Symantec Notification Server Migration Wizard" on page 55.
  See "About the Symantec Notification Server Migration Wizard" on page 54.
- Run the migration wizard EXE manually.
  When you install the optional migration wizard components, the migration wizard EXE is installed. The EXE for the migration wizard is `NSUpgradeWizard.exe`, and by default it is in the C:\Program Files\Altiris\Upgrade directory.

2 If the **Welcome** page appears, click **Next**.

3 On the **Export / Import Task Selection** page, select the data store file you created when you exported the 7.0 data, and click **Next**.

4 On the **Password Protection** page, if a password was used when the data was exported, enter that password.

5 On the **Importer Configuration** page, select the data to import, and click **Next**.

See "Exporter Configuration or Importer Configuration page" on page 61.

6 On the **Product Readiness Check** page, review the messages, and click **Next**.

This page displays each product that has data that is not included in the import. To view an explanation of why the data is not included, click in the **Message** column.

7 On the **Task Summary** page, verify the migration tasks the wizard is about to perform, and click **Next**.

8 When the message that the data import has completed successfully appears, click **OK**.

If the data is not imported successfully, a message with instructions appears.

9 (Optional) To display each action's sub-actions, check **Show Details**.

10 Click **Finish**.

Exporter Configuration or Importer Configuration page

These configuration pages let you select the products whose data you want to migrate. For each product, you can select the exporters or importers to use. These exporters or importers define what data is migrated. For each exporter or importer, you can filter the data to export or import. To access these configuration pages, run Symantec Notification Server Migration Wizard. The Exporter Configuration page appears when the migration wizard runs in export mode. The Importers Configuration page appears when the migration wizard runs in import mode.

See "About data migration" on page 52.

See "About the Symantec Notification Server Migration Wizard" on page 54.

Table 3-5 Options on the configuration pages

Option	Description
Products	Displays the products whose data you can migrate. Data is exported or imported only for the products that are checked.

Table 3-5 Options on the configuration pages *(continued)*

Option	Description
Importers or **Exporters**	Displays the exporters or importers for the product that is selected in the **Products** section. Data is exported or imported only for the exporters or importers that are checked in the **Enabled** column.
Filters	Displays a dialog box that lets you filter the data that an exporter or importer migrates as follows: ■ You can uncheck any item that you do not want to migrate. ■ The **Details** option lets you display the **Filter Details** dialog box. You can sometimes change a value on the **Filter Details** dialog box. For example, when you import a locally stored package file, you can sometimes change the drive to which it is migrated.

About the 7.0 data that you must manually migrate to Symantec Management Platform 7.1

When you migrate from Symantec Management Platform 7.0 to Symantec Management Platform 7.1, not all of the data is migrated with the migration wizard. You must manually migrate some data from the 7.0 server to the 7.1 server. For some of the migrated data, you must also complete additional manual steps to make the data fully functional.

The following products have some 7.0 data that you must manually migrate to Symantec Management Platform 7.1:

- Inventory Solution
  See "About manually migrating to Inventory Solution 7.1" on page 71.
- Software Management Solution
  See "Migrating Software Management Solution from 7.0 to 7.1" on page 97.
- Barcode Solution
  See "Manually migrating your Barcode Solution files and settings" on page 136.
- Out-of-band Management Solution
  See "Manually migrating Out of Band Management Component to version 7.1" on page 126.
- Real-Time System Management Solution

See "About manually migrating Real-Time System Manager Solution files and settings" on page 114.

- Real-Time Console Infrastructure Solution
  See "About manually migrating Real-Time Console Infrastructure files and settings" on page 118.

You must also copy the licenses of your Symantec Management Platform 7.0 products to a location that is accessible from the 7.1 server.

About the data store file

A data store file stores Symantec Management Platform data. When you migrate Symantec Management Platform 7.0 data to Symantec Management Platform 7.1 with the migration wizard, you use a data store file. First, you export the 7.0 data to a data store file. You then import the data from the data store file into Symantec Management Platform 7.1.

See "About the Symantec Notification Server Migration Wizard" on page 54.

By default, the data store file is saved in the C:\Program Files\Altiris\Upgrade\Data directory. It has an .adb extension, is easy to copy and back up, and is not dependent on SQL.

You can view the data in a data store file with the Store Browser. If you perform multiple imports, you can view the data to determine which data to import next. The data store file organizes all the data except key data by product. The data for each product is stored in tables. The name of each table is *ProductName.TableName*.

See "Viewing the data in a data store file" on page 64.

About the Store Browser

The Store Browser lets you do the following with data store files:

- Analyze the data before you import it.
  The Store Browser lets you view each table and the data in each row of a table before you import the data. If you perform multiple imports, you can view the data to determine what data to import next.
- Export specific data to create a smaller data store file.
  If you encounter errors when you import data, you may need to send a data store file that contains the data to Symantec Technical Support. The Store Browser lets you export specific data to create a smaller data store file that is more portable.
  See "Exporting data from a data store file" on page 65.

- View differences between two data store files.
  If you have two similar data store files, you can use the StoreDiff utility to create a data store file that highlights their differences. The Store Browser lets you open this data store file and view the differences.
  See "Comparing two data store files" on page 66.

See "About the data store file" on page 63.

See "Viewing the data in a data store file" on page 64.

By default, the EXE for the Store Browser is installed at C:\Program Files\Altiris\Upgrade. It is installed whenever the migration wizard is installed.

Viewing the data in a data store file

You use Symantec Notification Server Migration Wizard to migrate Symantec Management Platform 7.0 data to Symantec Management Platform 7.1. When you migrate data with the migration wizard, you export the data to a data store file and then import the data from the data store file. After you create a data store file, you can use the Store Browser to view the data in the data store file.

See "About data migration" on page 52.

See "About the data store file" on page 63.

See "About the Store Browser" on page 63.

To view the data in a data store file

1. Start the Store Browser.

   By default, this file is installed at C:\Program Files\Altiris\Upgrade.

2. In the **Store Browser**, on the **File** menu, click **Open** and select the data store file.

3. In the **Table Name** column, select a table.

   The rows of the table appear in the right pane.

4 To search for specific data in a table, use the following options at the bottom of the right pane:

Starting index	Type a number of a table row, and click **Refresh**. The table row becomes the first row in the right pane.
Find	Type the search criteria, and select the columns of the table in which to perform the search. All rows in the table that match the search criteria are highlighted. To use regular expressions for the search criteria, check **Regex**.
Inverse	Check this option to highlight the text that does match the search criteria.
Regex	Check this option to perform a search with regular expressions. You then type the regular expression in **Find**.
Refresh	Click this option to complete the search.
Find Next	Click this option to move to the next row that matches the search criteria.

5 If a table row has an **Xml** column, do the following to view the XML:

- Double-click the row.
- In the **Data View for table** dialog box, on the first **Column** drop-down list, click the XML entry.
  The XML appears in the **Value** pane.
- On the second **Column** drop-down list, click **View as XML**.

Exporting data from a data store file

If you encounter errors when you import data from a data store file, you may need to send the file to Symantec Technical Support. For a large file, you can use Store Browser to create a data store that is a subset of the original data store file. You can export the data that causes the errors and then send this smaller file to support so that they can help resolve the problem.

See "About the Store Browser" on page 63.

See "About the data store file" on page 63.

When you export data with the Store Browser, you can select the data tables to export and the specific rows in the data tables. You can specify the rows to export with row numbers, row ranges, or a data string.

To export data from a data store file

1. Double-click `StoreBrowser.exe`.

   By default, this file is installed at C:\Program Files\Altiris\Upgrade. It is installed whenever the migration wizard is installed.

2. In the **Store Browser**, on the **File** menu, click **Open**, and select the data store file that contains the data.
3. On the **File** menu, click **Export Data**.
4. In the **Export Data Form** dialog box, in the **Export** column, check the tables whose data you want to export.

   The NSCore.ExporterVersionInfo table is always exported. It contains the data that the migration wizard needs to import the data from the data store file.

5. To export the data for specific rows of a table, click in the **Rows to Export** column and specify the rows as follows:
   - In the **Export Options Form** dialog box, click **Specified Rows**.
   - To specify rows by row number, check **Row Ranges**, and list the rows.
   - To specify the rows that contain a data string, check **Containing String**, and define the string.
   - Click **OK**.
6. In the **Export Data Form** dialog box, in **Destination Store**, specify the name and location for the new data store file.
7. Click **Export**.

Comparing two data store files

You can export the same type of 7.0 data to a data store file multiple times. If the data on the 7.0 server changes between exports, then subsequent data store files contain differences. You can use the StoreDiff utility to compare two data store files.

When you compare two data store files that are different, a data store file is created that contains the differences. You then use Store Browser to view this data store file and see the differences. You can use this information to determine the data to import. The data store file that StoreDiff creates cannot be used to import data into Symantec Management Platform 7.1.

See "About the data store file" on page 63.

See "About the Store Browser" on page 63.

To compare two data store files

1. Start the StoreDiff utility.

   By default, the EXE for the StoreDiff utility is installed in the C:\Program Files\Altiris\Upgrade directory. It is installed whenever the migration wizard is installed.

2. On the **Compare Data Stores** dialog box, click **Browse** to select each of the data store files.

3. In **Diff Store**, specify the name and location for the new data store file.

   This data store file highlights the differences between the two data stores.

4. Click **Generate Diff**.

5. On the message that appears, click **OK**.

   The message either states that the two data store files are identical or that a new data store file is generated. If a new data store file is generated, the **Store Browser** opens.

6. In the **Store Browser**, on the **File** menu, click **Open**, and select the new data store file.

7. On the **Diff Store Summary** dialog box, click **OK**.

   This dialog box lists the data store files that are compared in this new data store file.

   This dialog box also has the following color key for the differences between the two data store files:

Green	New data that exists only in the second data store.
Yellow	Deleted data that exists only in the first data store.
Salmon	Data that exists in both data stores but is different.

8. In the left pane of the **Store Browser**, select a table that is shaded with one of the three colors.

   Only the tables that have differences between the two data store files are shaded.

9. In the right pane, view the rows that have differences between the two data store files.

10. If a table row has an **Xml** column, do the following to view the XML:

    - Double-click the row.

- In the **Data View for table** dialog box, on the first **Column** drop-down list, click the XML entry.
  The XML appears in the **Value** pane.
- On the second **Column** drop-down list, click **View as XML**.

Chapter 4

Migrating Inventory Solution

This chapter includes the following topics:

Before you migrate to Inventory Solution 7.1

To successfully migrate to Inventory Solution 7.1, perform the following preliminary actions:

- Check which items are not migrated with Symantec Notification Server Migration Wizard, and then back up the items.
  See "About migrating to Inventory Solution 7.1 with Symantec Notification Server Migration Wizard" on page 70.
  See "About manually migrating to Inventory Solution 7.1" on page 71.

About migrating to Inventory Solution 7.1 with Symantec Notification Server Migration Wizard

To successfully migrate Inventory Solution, you perform the following types of product migration:

- Migration to Symantec Management Platform 7.1 with the Symantec Notification Server Migration Wizard.
  See "Before you migrate to Inventory Solution 7.1" on page 69.
  See "Migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1" on page 32.
  See "About data migration" on page 52.
  See "About the Symantec Notification Server Migration Wizard" on page 54.
- Manual migration.
  See "About manually migrating to Inventory Solution 7.1" on page 71.

The following items are automatically migrated during the upgrade from Symantec Management Platform 7.0 to Symantec Management Platform 7.1:

- Inventory Solution 7.0 configuration settings are preserved after the upgrade.
- Predefined and custom 7.0 inventory policies and tasks are upgraded to the equivalent 7.1 task-based policies.
- Predefined and custom 7.0 application metering policies.
- Predefined and custom 7.0 inventory reports.
- Predefined and custom 7.0 inventory data classes.
- 7.0 inventory data from 7.0 inventory data classes.
- 7.0 custom inventory script files for Windows and for UNIX, Linux, and Mac.
  7.0 custom inventory script files that are configured within the **Jobs and Tasks** are included into 7.0 inventory tasks. Such script files are migrated with the Symantec Notification Server Migration Wizard and do not require any manual migration steps.
- Legacy 6.x custom inventory script files for UNIX, Linux, and Mac created by users on local disk or in shared location.
- Predefined and custom 7.0 application metering reports, data classes, and data.

The following items are not migrated with the Symantec Notification Server Migration Wizard to the 7.1 database due to extensive changes in the database structure:

- Stand-alone inventory packages.

See "Process for manually migrating your stand-alone inventory packages " on page 89.

- Legacy 6.x custom inventory script files for Windows created by users on local disk or in shared location.
  See "Process for manually migrating your custom inventory script files" on page 72.
- Inventory baseline configuration and snapshot files.
  See "Process for manually migrating your Inventory Solution baseline configuration files" on page 86.

About manually migrating to Inventory Solution 7.1

When you use the Symantec Notification Server Migration Wizard to migrate to 7.1, some of your Inventory Solution files and settings do not migrate. This situation occurs because of the extensive changes in the database structure. To preserve these files and settings, you must manually migrate them from your previous Notification Server computer to your Notification Server 7.1 computer. After you move these files to your new environment, you must complete configuration steps to make them operate correctly.

See "Before you migrate to Inventory Solution 7.1" on page 69.

See the following for information about manually migrating Inventory Solution items:

- Legacy 6.x custom inventory script files for Windows created by users on a local disk or in a shared location.
  If you have created legacy 6.x custom inventory script files for Windows in your 7.0 environment, you can manually migrate them to the 7.1 environment. However, you must perform custom configuration steps to make them operate correctly in the 7.1 environment.
  See "Process for manually migrating your custom inventory script files" on page 72.
- Inventory baseline configuration and snapshot files.
  You can manually migrate your baseline configuration and snapshot files. However, you must perform custom configuration steps to make them operate correctly in the 7.1 environment.
  See "Process for manually migrating your Inventory Solution baseline configuration files" on page 86.
- Stand-alone inventory packages.
  You can manually migrate your 7.0 stand-alone packages. However, you should be aware of certain limitations before you choose to do so. To make your 7.0

stand-alone packages operate correctly in the 7.1 environment, you must perform custom configuration steps.
Depending on the specific requirements of your organization, it may be preferable to create new version 7.1 stand-alone packages.
See "Process for manually migrating your stand-alone inventory packages " on page 89.

Process for manually migrating your custom inventory script files

If you have created legacy 6.x custom inventory script files for Windows in your 7.0 environment, you can manually migrate them to the 7.1 environment. However, you must perform custom configuration steps to make them operate correctly in the 7.1 environment.

Table 4-1 Process for manually migrating your custom inventory script files for Windows from 7.0 to 7.1

Step	Action	Description
Step 1	Create a backup of your custom inventory script files.	Before you migrate your custom inventory files, create a backup copy of them in a neutral storage location. See "Backing up your custom inventory script files" on page 74.
Step 2	Perform the migration to Inventory Solution 7.1 with the Symantec Notification Server Migration Wizard.	Migration to Inventory Solution 7.1 with the Symantec Notification Server Migration Wizard lets you automatically migrate a number of Inventory Solution items. See "About migrating to Inventory Solution 7.1 with Symantec Notification Server Migration Wizard" on page 70.

Table 4-1 Process for manually migrating your custom inventory script files for Windows from 7.0 to 7.1 *(continued)*

Step	Action	Description
Step 3	Copy your custom inventory script files for Windows to your Notification Server 7.1 computer.	Copy your custom inventory script files to your Notification Server 7.1 computer. When you install or upgrade to Symantec Management Platform 7.1 on Windows computers, it automatically creates a package directory for storing your custom inventory. See "Copying your custom inventory script files to your Notification Server 7.1 computer" on page 75.
step 4	Meet the prerequisites to create a custom inventory software resource package.	Before setting up the software resource package, you must ensure that the certain prerequisites are met on your Notification Server 7.1 computer. See "Prerequisites for creating a custom inventory software resource package" on page 76.
Step 5	Create a software resource with a package and a command line.	You need to create a software resource with a package and a command line before performing **Quick Delivery** tasks. A software resource contains the package definition that includes the path to the package, and the program definition that includes the desired command line. See "Creating a software resource with a package and a command line for custom inventory script files" on page 77.

Table 4-1 Process for manually migrating your custom inventory script files for Windows from 7.0 to 7.1 *(continued)*

Step	Action	Description
Step 6	Create a **Quick Delivery** task for a custom inventory script file.	To successfully use your manually migrated custom inventory script files in the 7.1 environment, you need Software Management Solution to create and perform **Quick Delivery** tasks. See "Creating a Quick Delivery task for a custom inventory script file" on page 78.
Step 7	Create a custom data class.	Create a custom data class for a custom inventory script task. When you create the custom data class, ensure that you enter the name and the description for the data class from your manually migrated custom inventory script file. See "Creating and customizing a data class" on page 79.
Step 8	Create a custom inventory script task.	Create a custom inventory script task that gathers the custom inventory. See "Creating a custom inventory script task" on page 80. When you customize the custom inventory script task, ensure that you add the logic to gather the data and populate the attribute variables in the script according to the data in your manually migrated custom inventory script file. See "Customizing the custom inventory sample script for Windows" on page 82.

Backing up your custom inventory script files

This task is a part of the process for manually migrating your custom inventory script files.

See "Process for manually migrating your custom inventory script files" on page 72.

Before you migrate your custom inventory files, create a backup copy of them in a neutral storage location.

To back up your custom inventory script files for Windows

- On your previous Notification Server computer, copy all of your custom inventory script files (.CIT, .XML, etc.) to a neutral storage location.

  By default, your custom inventory script files are located on your previous Notification Server computer in the following location:

  - `C:\Program Files\Altiris\Notification Server\NSCap\bin\Win32\X86\Inventory\Custom Inventory 6.1`

  The default location may not include other locations where you have placed your custom inventory script files. Ensure that you also back up the custom inventory script files that you have created outside of the default location.

Copying your custom inventory script files to your Notification Server 7.1 computer

(Windows only)

This task is a part of the process for manually migrating your custom inventory script files.

See "Process for manually migrating your custom inventory script files" on page 72.

When you install or upgrade to Symantec Management Platform 7.1 on Windows computers, it automatically creates a package directory for storing your custom inventory.

By default, the path to the custom inventory directory for Windows is `C:\Program Files\Altiris\Notification Server\NSCap\bin\Win32\X86\Inventory\Custom Inventory 6.1`.

The package directory for Windows contains the following files:

- `AeXInvSoln.exe`

  This file is the same as the file in 6.1 SP2. This file launches `AeXCustInv.exe` and `AeXNSInvCollector.exe` as specified in `AeXInvSoln.ini`.

- `AeXCustInv.exe`

  This file differs from the file in 6.1 SP2. This file has bug fixes.

- `AeXNSInvCollector.exe`

This file differs from the file in 6.1 SP2. This file behaves in a similar way to the 6.1 SP2 file. However, this file generates Notification Server events (NSEs) in the new format that is required to store inventory to your Notification Server 7.1 computer.

- `AeXNSEvent.dll`

  This file is new. `AeXNSInvCollector.exe` uses this file for generating NSEs in the new format.

- `AeXInvSoln.ini`

  This file specifies an example of how to launch the `AeXCustInv.exe` and `AeXNSInvCollector.exe` files.

- `AeXCustInvStd.cit`

  This file is a sample custom inventory script from version 6.1 SP2.

To copy your custom inventory files to a Notification Server 7.1 computer

- Copy all of your custom inventory script files for Windows (.CIT, .XML, etc.) to `C:\Program Files\Altiris\Notification Server\NSCap\bin\Win32\X86\Inventory\Custom Inventory 6.1`.

Prerequisites for creating a custom inventory software resource package

(Windows only)

The task of meeting the prerequisites is a part of the process for manually migrating your custom inventory script files.

See "Process for manually migrating your custom inventory script files" on page 72.

Before setting up the software resource package, you must ensure that the following prerequisites have been met on your Notification Server 7.1 computer:

- Java 2 JRE 1.6 is required for some Symantec Management Console screens.
- The appropriate interpreters for Perl, Python, VBScript, etc. must be installed.
- The Symantec Management Agent and Software Management Solution plug-in must be installed on each client computer.
- The 7.1 version of `aexinvcollector.exe` must exist on the 7.1 Notification Server computer. This file is installed by default as part of the installation.
- Ensure that the 7.0 custom inventory data classes are migrated. Create new custom inventory data classes if needed.

Creating a software resource with a package and a command line for custom inventory script files

(Windows only)

This task is a part of the process for manually migrating your custom inventory script files.

See "Process for manually migrating your custom inventory script files" on page 72.

A software resource contains the package definition that includes the path to the package, and the program definition that includes the desired command line.

To create a software resource for custom inventory script files

1. In the **Symantec Management Console**, on the **Manage** menu, click **Software Catalog**.
2. On the **Manage Software Catalog** page, click **Import**.
3. On the **Import Software: Specify Software** page, perform the following steps:

Software type	Select **Software Release**.
Package source	In the **Source** field, select **Access Package from an existing UNC**. In the **Location** field, browse to: *\\local_NS7_servername*\nscap\bin\win32\x86\Inventory\Custom Inventory 6.1
Package contents	Click **Display Location** and select `AeXInvSoln.exe`. Click **Set Installation File**. Click **Next**.

4. Select **Create a new software resource** and enter a name for the package.
5. Make sure that **Open software resource for editing when finished** is checked.
6. Click **OK**.
7. On the **Software Resource** editing page, click the **Package** tab.
8. In the **Command Lines** section, click **Add command**. `aexinvsoln.exe` should be the command line.
9. Click **Edit**.

10 On the **Add or Edit Command Line** page, perform the following steps:

Name	Enter *Custinv - Win32_UserAccount - CommandLine*
Command line requires a package	Select this option.
Package	Select the name that you entered when you created the software resource package.
Installation File Type	Select **EXE Software Installation File**.
Command Type	Select **Custom**.
Command Line	Enter `AeXInvSoln.exe /s win32_useraccount`

11 Click **OK**.

12 Click **Save Changes**.

Creating a Quick Delivery task for a custom inventory script file

(Windows only)

This task is a part of the process for manually migrating your custom inventory script files.

See "Process for manually migrating your custom inventory script files" on page 72.

To successfully use your manually migrated custom inventory script files, you need Software Management Solution to perform **Quick Delivery** tasks.

For more information, see the topics about managed software delivery in the *Software Management Solution Help*.

To create a Quick Delivery task for a custom inventory script file

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

2 In the left pane, expand **System Jobs and Tasks > Software**.

3 Right-click the **Quick Delivery** folder under which you want to create a task, and then click **New > Task**.

4 In the **Create New Task** dialog box, in the left pane, under **Software**, click **Quick Delivery**.

5 Change the **Name** of the task.

6 Under **Software**, select a custom inventory software resource package to deliver.

7 Under **Command line**, select a command line.

8 Under **Package**, select an installation package.

9 Click **OK**.

10 (Optional) To run the task immediately, click **Quick Run**.

Alternatively, you can click **New Schedule** to schedule the task.

Creating and customizing a data class

This task is a part of the process for manually migrating your custom inventory script files.

See "Process for manually migrating your custom inventory script files" on page 72.

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.

For more information, see the topics about custom inventory data classes and about gathering custom inventory in the *Inventory Solution Help*.

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**.
- 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.

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

- Click **Add attribute**.

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

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. On the **Manage Custom Data Classes** page, you can also specify the sequence of the attributes.

8 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

This task is a part of the process for manually migrating your custom inventory script files.

See "Process for manually migrating your custom inventory script files" on page 72.

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 79.

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 an inventory script task on the **Jobs and Tasks Portal** page.

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 gathering custom inventory in the *Inventory Solution Help*.

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 Item** dialog box, give the cloned script a descriptive name and click **OK**.
5. (Optional) Customize the sample script and click **Save changes**.

   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.
6. Under **Task Status**, schedule the task to run on client computers.

   For more information, see the topics about running a task in the *Symantec Management Platform Help*.

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, right-click **Jobs and Tasks**, 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 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) Customize the sample script and click **OK**.

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.

8 Under **Task Status**, schedule the task to run on client computers.

For more information, see the topics about running a task in the *Symantec Management Platform Help*.

Customizing the custom inventory sample script for Windows

(Windows only)

This task is a part of the process for manually migrating your custom inventory script files.

See "Process for manually migrating your custom inventory script files" on page 72.

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 that 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.

For more information, see the topics about gathering custom inventory in the *Inventory Solution Help*.

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

The sample inventory script for Windows does the following:

- Creates a WMI object, runs a WMI query, and stores the result set.
- Creates an 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
```

Process for manually migrating your Inventory Solution baseline configuration files

You can manually migrate your baseline configuration and snapshot files. However, you must perform custom configuration steps to make them operate correctly in the 7.1 environment.

Table 4-2 Process for manually migrating your Inventory Solution baseline configuration files

Step	Action	Description
Step 1	Create a backup of your baseline configuration files.	Before you decommission your previous Notification Server computer, back up your baseline configuration files to a neutral storage location. See "Backing up your Inventory Solution baseline configuration files" on page 87.
Step 2	Perform the migration to Inventory Solution 7.1 with the Symantec Notification Server Migration Wizard.	Migration to Inventory Solution 7.1 with the Symantec Notification Server Migration Wizard lets you automatically migrate a number of Inventory Solution items. See "About migrating to Inventory Solution 7.1 with Symantec Notification Server Migration Wizard" on page 70.
Step 3	Restore your baseline configuration files on the 7.1 Notification Server computer.	After you install the Symantec Management Platform, restore your baseline configuration files on your Notification Server 7.1 computer. See "Restoring your Inventory Solution baseline configuration files" on page 87.

Table 4-2 Process for manually migrating your Inventory Solution baseline configuration files *(continued)*

Step	Action	Description
Step 4	Create a **File baseline** task and **Registry baseline** task.	After you restore your baseline configuration files on your Notification Server 7.1 computer, you must create a **File Baseline** task and a **Registry Baseline** task to make them function in the new 7.1 environment. See "Creating a File Baseline task and a Registry Baseline task" on page 88.

Backing up your Inventory Solution baseline configuration files

This task is a part of the process for manually migrating your Inventory Solution baseline configuration files.

See "Process for manually migrating your Inventory Solution baseline configuration files" on page 86.

Before you decommission your previous Notification Server computer, back up your baseline configuration files to a neutral storage location.

To back up your Inventory Solution baseline configuration files

- On your previous Notification Server computer, copy all of your baseline configuration files in the folders **FileBaselinePackage** and **RegBaselinePackage** to a neutral storage location.

  By default, your baseline configuration files are located on your previous Notification Server computer in the following location:

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

  The default location may not include other locations where you have placed your baseline configuration files. Ensure that you also back up the baseline configuration files that you have created outside of the default location.

Restoring your Inventory Solution baseline configuration files

This task is a part of the process for manually migrating your Inventory Solution baseline configuration files.

See "Process for manually migrating your Inventory Solution baseline configuration files" on page 86.

After you install the Symantec Management Platform, restore your baseline configuration files on your Notification Server 7.1 computer.

See "Backing up your Inventory Solution baseline configuration files" on page 87.

To restore your Inventory Solution baseline configuration files

1. Copy your baseline configuration files and snapshot files from your neutral storage location.
2. On your Notification Server 7.1 computer, paste your baseline configuration and snapshot files to the following location:

```
C:\Program Files\Altiris\Notification
Server\NSCap\bin\Win32\X86\Inventory\Application Management
```

Creating a File Baseline task and a Registry Baseline task

This task is a part of the process for manually migrating your Inventory Solution baseline configuration files.

See "Process for manually migrating your Inventory Solution baseline configuration files" on page 86.

After you restore your baseline configuration files on your Notification Server 7.1 computer, you must create a **File Baseline** task and a **Registry Baseline** task to make them function in the new 7.1 environment.

See "Restoring your Inventory Solution baseline configuration files" on page 87.

To create a File Baseline task

1. In the **Symantec Management Console**, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, right-click **Jobs and Tasks**, and then click **New > Task**.
3. In the **Create New Task** dialog box, in the left pane, click **File Baseline**.
4. On the **File Baseline** task page, configure the task and click **OK**.

To create a Registry Baseline task

1. In the **Symantec Management Console**, on the **Manage** menu, click **Jobs and Tasks**.
2. In the left pane, right-click **Jobs and Tasks**, and then click **New > Task**.

   In the **Create New Task** dialog box, in the left pane, click **Registry Baseline**.
3. On the **Registry Baseline** task page, configure the task and click **OK**.

Process for manually migrating your stand-alone inventory packages

You can manually migrate your 7.0 stand-alone packages . However, you must perform custom configuration steps to make them operate correctly in the 7.1 environment.

Table 4-3 Process for manually migrating your stand-alone inventory packages

Step	Action	Description
Step 1	Create a backup of your stand-alone inventory packages .	Before you decommission your previous Notification Server computer, back up your stand-alone inventory packages to a neutral storage location. See "Backing up your stand-alone inventory packages" on page 89.
Step 2	Perform the migration to Inventory Solution 7.1 with the Symantec Notification Server Migration Wizard.	Migration to Inventory Solution 7.1 with the Symantec Notification Server Migration Wizard lets you automatically migrate a number of Inventory Solution items. See "About migrating to Inventory Solution 7.1 with Symantec Notification Server Migration Wizard" on page 70.
Step 3	Restore your stand-alone inventory packages on your Notification Server 7.1 computer.	After you install the Symantec Management Platform 7.1, restore your stand-alone inventory packages on your Notification Server 7.1 computer. See "Restoring your stand-alone inventory packages" on page 90.

Backing up your stand-alone inventory packages

This task is a part of the process for manually migrating your stand-alone inventory packages.

See "Process for manually migrating your stand-alone inventory packages " on page 89.

Before you decommission your previous Notification Server computer, back up your stand-alone inventory packages to a neutral storage location.

See "Restoring your stand-alone inventory packages" on page 90.

To back up your stand-alone inventory packages

- On your previous Notification Server computer, copy all of your stand-alone inventory packages to a neutral storage location.

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

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

  The default location may not include other locations where you have placed your stand-alone inventory packages. Ensure that you also back up the stand-alone inventory packages that you have created outside of the default location.

Restoring your stand-alone inventory packages

This task is a part of the process for manually migrating your stand-alone inventory packages.

See "Process for manually migrating your stand-alone inventory packages " on page 89.

After you install the Symantec Management Platform 7.1, restore your stand-alone inventory packages on your Notification Server 7.1 computer.

See "Backing up your stand-alone inventory packages" on page 89.

To restore your stand-alone inventory packages

1. Copy your stand-alone inventory packages from your neutral storage location.
2. On your Notification Server 7.1 computer, paste your stand-alone inventory packages to the following location:

   ```
   C:\Program Files\Altiris\Notification
   Server\NSCap\Bin\Win32\X86\Inventory\StandalonePackages
   ```

Data migration to Inventory for Network Devices 7.1

You perform the product migration from 7.0 to 7.1 according to the migration scenario for Inventory Solution and IT Management Suite.

See "Before you migrate to Inventory Solution 7.1" on page 69.

See "Migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1" on page 32.

See "About data migration" on page 52.

See "About the Symantec Notification Server Migration Wizard" on page 54.

Chapter 5

Migrating Patch Management Solution

This chapter includes the following topics:

About migrating Patch Management Solution data

The solution-specific data is migrated when you migrate the product data according to the process that is defined in the Migrating Symantec Management Platform chapter.

You should verify and validate that the solution data and settings have been migrated correctly.

See "About migrating software update package files" on page 93.

See "Data that is not migrated from 7.0 to 7.1" on page 94.

See "SQL tables that are deleted or renamed" on page 94.

About migrating software update package files

In 7.1, the migration wizard lets you export the downloaded software update package files from the 7.0 server and store them in the same location as the .adb file. You can then use the migration wizard to import the files to the new 7.1 server.

Migration wizard will import the exported packages to the location that is specified on the **Core Settings** page. This setting can be migrated from the 7.0 server. In case the migrated path is not available on the new server, the default location will be used, which is `C:\Program Files\Altiris\Patch Management\Packages\Updates`.

Note: Currently, migration wizard can migrate packages only if the Symantec Management Platform is installed at the default location. If you installed Symantec Management Platform to a custom location, you must manually move the software update package files from migration folder to the desired location.

When you run the **Import Patch Data** task, the packages will be recreated (but not redownloaded), and then appear in the Symantec Management Console.

Data that is not migrated from 7.0 to 7.1

The following table lists the items that are not migrated from 7.0 to 7.1.

Table 5-1 Data that is not migrated from 7.0 to 7.1

Item	Description
Patch Management Solution for Linux subscribed channels list	Because of architectural changes, the subscribed channels list is not migrated from 7.0 to 7.1. After you upgrade to 7.1, you must import the software channels list (both Red Hat and Novell) and select the channels for which you want to download updates. You can select the channels on the **Manage > Jobs and Tasks > System Jobs and Tasks > Software > Patch Management > Import Patch Data for Novell/Red Hat** page.

SQL tables that are deleted or renamed

When you migrate data from 7.0 Patch Management Soluton to 7.1, some of the SQL tables are removed and data is transferred.

The following tables are deleted during the upgrade:

- Inv_Installed_Red_Hat_Software_Update
- Inv_Applicable_Red_Hat_Software_Update
- Inv_Patchable_Red_Hat_Software_Update
- Inv_Installed_Novell _Software_Update

- Inv_Applicable_Novell_Software_Update
- Inv_Patchable_Novell_Software_Update

Table 5-2 shows the data that is moved to the new tables.

Table 5-2 SQL data that is transferred

Table name in 7.0	Table name in 7.1
Inv_Installed_Red_Hat_Software_Update	Inv_InstalledSoftware
Inv_Patchable_Red_Hat_Software_Update	Inv_Patchable_Linux_Software_Update
Inv_Installed_Novell_Software_Update	Inv_InstalledSoftware
Inv_Patchable_Novell_Software_Update	Inv_Patchable_Linux_Software_Update

Chapter 6

Migrating Software Management Solution

This chapter includes the following topics:

Migrating Software Management Solution from 7.0 to 7.1

Most solution-specific data is migrated when you migrate the product data according to the process that is defined in the Migrating Symantec Management Platform chapter.

You should verify and validate that the solution data and settings have been migrated correctly.

The following are things to consider if you want to migrate Software Management Solution 7.0 to 7.1:

- For 7.1, you do not conduct an actual in-place upgrade. You export supported data from the old database. Then you use a migration wizard to put that data into the new structure after 7.1 is installed. This process is called an off-box upgrade.

  Because you perform an off-box upgrade, take the following into consideration:

  - If the software library was located on the Notification Server computer, you must manually move the physical files to the new 7.1 server. The migration wizard does not move these files.
  - If you used a custom local path for the software resources on the 7.0 Notification Server computer, you must recreate the same file structure on the new 7.1 server.

For example, if the software resources were located on disk F, then disk F must also be on the new 7.1 computer; otherwise, Software Management Solution does not work.

- If a path that is used in a software resource is longer than 248 characters, the physical files cannot be migrated.
  For example, Microsoft SQL Server 2008 folder structure can exceed 248 symbols. You can recreate the folder structure and migrate such files manually.

- The packages on the client computers are not kept and are re-downloaded.

Chapter 7

Migrating Deployment Solution

This chapter includes the following topics:

About migrating from Deployment Solution 6.9

Deployment Solution 6.9 is a standalone product and is not designed to be integrated with Symantec Management Platform. Deployment Solution 7.1 SP1 offers the core imaging and deployment capabilities of Deployment Solution 6.9 that are natively integrated on the Symantec Management Platform. Hence, Deployment Solution 7.1 SP1 does not require its own agent, console, or database infrastructure separate from what is already provided with Symantec Management Platform. Instead, Deployment Solution 7.1 SP1 plugs in and extends the capabilities natively offered by Symantec Management Platform.

Though Deployment Solution 7.1 SP1 supports most of the functionalities of Deployment Solution 6.9, you cannot migrate jobs and tasks from version 6.9. You have to manually recreate the supported functionalities. The process for recreating these tasks is exceptionally valuable since many of the attributes of these items can be made broadly consumable by many tasks.

You can only migrate Ghost and RapiDeploy images. If you want to migrate your existing images, you must create a backup copy of them on a neutral storage

location before you upgrade. After you upgrade to version 7.1 SP1, you can then restore them to their correct location.

Before you begin

Before you start migrating Deployment Solution 7.0 to 7.1 SP1, ensure that the following tasks are completed:

- Verify and complete all outstanding tasks, policies, package copies, and hierarchy replication schedules, if they are in use.
- Disable all hierarchy and peer-based replication schedules, if they are in use.
- Run the Migration wizard ("%altirisInstallFolder%\Symantec Installation Manager\MigrationPackage\") to export solution-specific items to a folder, such as the Upgrade folder.
- Take a backup of the Deployment Solution 7.0 CMDB.
- Store all IT Management Suite licenses in a safe location.
- Create a backup copy of the following Deployment Solution items on a neutral storage location:

Deployment .CAB files.	These files are stored by default at: `C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\Sysprep\Deploy_Cab`
Image packages.	These files are stored by default at: `C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\image`
PCT packages.	These files are stored by default at: `C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\PCTPackages`
SOI packages.	These files are stored by default at: `C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\SOI`
Custom answer files.	These files are stored by default at: `C:\Program Files\Altiris\Notification Server\NSCap\bin\Win32\X86\Deployment\Custom`

Copy File packages.	These files are stored by default at: `C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\CopyFile`
Any drivers that you added to the drivers database.	These files are stored by default at: `C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\DriversDB`
Any drivers that you added for bootwiz.	These files are stored by default at: `C:\Program Files\Altiris\Altiris Agent\Agents\Deployment\Task Handler\bootwiz\Platforms` Operating system-specific drivers are stored in an applicable operating system folder under the `Platforms` folder.
Any .PBT files that you added to the NSCap folder.	These files are stored by default at: `C:\Program Files\Altiris\Notification Server\NSCap\bin\Win32\X86\Deployment\PCT`
Any HTTP locations that you created for imaging.	You must create a backup of the images in their existing HTTP location. You must recreate the same HTTP location on your new server and move the backup of your images to the new server computer.
Any UNC locations that you created for the **Copy File** task.	You must create a backup of the UNC location and folder structure. You must recreate the same location and folder structure on your new server computer.

- Before disconnecting Notification Server of IT Management Suite 7.0 from the network, ensure that all backup data is copied to a different location. Also ensure that the backup data is accessible to IT Management Suite 7.1.

See "Migrating from Deployment Solution 7.1 to 7.1 SP1" on page 101.

Migrating from Deployment Solution 7.1 to 7.1 SP1

Ensure that you have performed the required steps before you start migrating to IT Management Suite 7.1 and upgrade to Deployment Solution 7.1 SP1.

See "Before you begin" on page 100.

To migrate from Deployment Solution 7.1 to 7.1 SP1

1. Prepare a new computer with Windows Server 2008 R2 x64 as IT Management Suite 7.1.

   Configure this server to use the IP address and name of the previous Notification Server (IT Management Suite 7.0).

2. Install the latest IT Management Suite 7.1 on Windows Server 2008 R2 computer.

3. Copy the files from the neutral storage location to the same structure on the new 7.1 server computer.

   See "Before you begin" on page 100.

4. In the Symantec Management Console on the **Settings** menu, select **Symantec Management Platform > Database Settings**.

5. Select the restored database and click **Save**.

6. Copy the upgrade folder containing the data exported by migration wizard from the IT Management Suite 7.0 computer to the IT Management Suite 7.1 computer.

7. Run the **Migration** wizard from the **Upgrade** folder to import the data that has been exported from IT Management Suite 7.0.

8. Enable the following Symantec Management Platform upgrade policies:

Symantec Management Agent	Enable the upgrade policy from **Symantec Management Console > Settings > Agent\Plug-ins > Symantec Management Agent > Windows**. Verify the upgraded Symantec Management Agent versions from **Symantec Management Platform Agent > About Symantec Management Agent**.
Task Service	Enable the upgrade policy from **Symantec Management Console > Settings > Notification Server > Site Server settings > Task Service > Advanced**. Verify the upgraded Task Service by checking the version of **Altiris Client Task Server Agent** in **Symantec Management Platform Agent**.
Windows package server agent	Enable the upgrade policy from **Symantec Management Console > Settings > Notification Server > Site Server Settings > Package Server > Advanced > Windows**. Verify the upgraded Windows package server agent by checking the version of package servers in **Symantec Management Platform Agent**.

9 Enable the following Deployment Solution upgrade policies:

See "Upgrading Deployment Solution components" on page 104.

Upgrade your deployment site servers.	Enable the Deployment site server upgrade policy from **Symantec Management Console > Settings > Agents/Plug-ins > Deployment and Migration > Windows**. Verify that the Deployment site server component is upgraded. To do this step, check the version of Deployment Task Server Handlers in Symantec Management Agent on the site server computer.
Upgrade the deployment plug-in for Windows.	Enable the Deployment Plug-in upgrade policy from **Symantec Management Console > Settings > Agents/Plug-ins > Deployment and Migration > Windows**. Make sure that the Deployment Plug-ins are upgraded by checking the version of Deployment Solution Plug-in from the Symantec Management Agent.
Install the automation folder on managed computers with the deployment plug-in for Windows.	Enable the automation folder upgrade policy from **Symantec Management Console > Settings > Agents/Plug-ins > Deployment and Migration > Windows**. Select **Deployment Automation Folder for Windows (x86) - Install**. Assign and schedule the policy on the filter **Computers with latest Deployment Plug-in installed on Windows**. To upgrade the automation folder from x86 to x64 on a Windows client computer, you must first uninstall the automation folder for Windows x86. Then, reinstall the automation folder for Windows x64.

10 If you have cloned policies in Deployment Solution 7.1 MR1, MR2, and MR3 versions, then after migration you must clone the policy again. You also have to configure the settings and target collection according to the previous clone policy.

See " Checklist for verifying a successful migration from 7.1" on page 104.

Upgrading Deployment Solution components

You can upgrade the Deployment Plug-in, Automation Folder, and Deployment site server components to the latest version by using the upgrade policy. By default, this policy is turned off. The Deployment Plug-in upgrade is not supported in the Linux operating system.

The upgrade policy uses filters to determine if an upgrade is necessary. You can access the filters that are used from the **Manage > Filters > Software Filters > Agent and Plug-in Filters** menu.

To upgrade Deployment Solution components

1. In the Symantec Management Console, on the **Settings** menu, click **Agent/Plug-ins > All Agents/Plug-ins**.
2. In the left pane, expand the **Agents/Plug-ins > Deployment and Migration** folders.
3. Click the relevant upgrade policy.
4. In the right pane, in the **Program name** box, ensure that the correct policy is selected.
5. Under **Applied to**, select the computers that you want to upgrade the plug-in on.
6. (Optional) Under **Schedule**, select when you want to upgrade the plug-in.
7. (Optional) Click **Advanced** to check if the computers you selected are available at the exact time that you scheduled.
8. Under **Extra schedule options**, select the options that you want.
9. Ensure that the policy is enabled.

   A green **On** symbol shows in the top right corner.
10. Click **Save changes**.

Checklist for verifying a successful migration from 7.1

After you have completed the process of migrating to 7.1 SP1, you can perform the following checks to verify the success of migration.

- Deployment Solution files and folders use the latest version.
- Default Automation packages are created for x86 as well as x64.
- x86 and x64 components, tools, and MSI are available.

- Installation and registry go to the native path and not to WOW Directory or registry for x64 client computers.
- Manually migrated items are copied without any errors.
- After the upgrade of preboot policy, the old preboot images are recreated without any error.
- Installation log and Altiris log contain no error.
- Deployment Solution-specific data that is related to tasks, policies, and settings are preserved when existing database is used.
- All new policies that are related to x64-bit components are present.
- Both x64 and x86 policies point to the correct set of collection.
- All policies are executed successfully and they should install the latest version.
- All new features are available.
- Previously and newly created tasks are available and execute successfully.

See "Migrating from Deployment Solution 7.1 to 7.1 SP1" on page 101.

Chapter 8

Migrating Monitor Solution

This chapter includes the following topics:

About Monitor Solution migration

You perform the product migration to version 7.1 according to the migration scenario for IT Management Suite. The majority of the solution-specific data is migrated when you migrate according to the process that is defined in the Migrating Symantec Management Platform chapter.

See "Migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1" on page 32.

See "About data migration" on page 52.

Only the custom or the cloned policies that are enabled before migration remain enabled after you migrate. All default policies are switched off after migration.

After migration the agentless resources are available from the new local Remote Monitor Server (RMS) installed on Symantec Management Platform 7.1. The old RMS is uninstalled during migration. If you want to monitor agentless resources from off-box RMS, you need to install the RMS using the site server settings.

Since Monitor Solution 7.1 supports multiple RMS, you may monitor agentless resources from different locations. As a consequence, you do not need to uninstall an RMS before you install another one.

Agent-based resources are not available after migration. To make agent-based resources available, you need to first upgrade the Symantec Management Agent with the Monitor Plug-in. To upgrade you need to redirect the needed resources to the Symantec Management Platform 7.1 from the old platform. For more information, see topics on Symantec Management Agent in the *Symantec Management Platform User Guide*. You then need to enable the applicable upgrade policy for the Monitor Plug-in.

See "About Monitor Pack for Servers migration" on page 108.

About Monitor Pack for Servers migration

When you upgrade the Monitor Pack for Servers component from 7.0 SP2 to 7.1, the **Windows 2000** monitor pack is migrated. However, Monitor Pack for Servers 7.1 does not support the **Windows 2000** monitor pack. Note, that the **Windows 2000**monitor pack is not included in a clean installation of Monitor Pack for Servers 7.1.

Any default rule or metric settings are reset to their default values after migration. If you modified a default monitor pack policy to include your custom metrics, the rules and metrics are not migrated. Instead these settings are lost. Only monitor pack cloned policy settings, cloned rule settings, and cloned metric settings are migrated. To work around this issue you can create clones of these policies. Your new custom monitor policies can then be migrated.

Policies that have been updated as part of the 7.1 release are reset unless they were cloned.

See "Manually cloning your changed default monitor pack policies, metrics, and rules" on page 108.

See "About Monitor Solution migration" on page 107.

Manually cloning your changed default monitor pack policies, metrics, and rules

If you want to migrate changes you have made to a monitor pack default policy, you should clone them. When you migrate a cloned policy, you also need to clone the rules and metrics that you want to migrate. These cloned rules and metrics then need to be added to the cloned policy. If a cloned policy contains default rules

or metrics and you change their settings, the default settings are restored after the migration.

See "About Monitor Pack for Servers migration" on page 108.

Table 8-1 Process for manually cloning your changed default monitor pack policies, metrics, and rules

Step	Action	Description
Step 1	Clone a changed default policy.	If you want to migrate changes you have made to a monitor pack default policy you should clone them. See "Cloning a changed default policy for migration" on page 109.
Step 2	Clone a changed default rule.	When you migrate a cloned policy, you also need to clone the rules that you want to migrate. See "Cloning a changed default rule for migration" on page 110.
Step 3	Clone a changed default metric.	When you migrate a cloned policy, you also need to clone the metrics that you want to migrate. See "Cloning a changed default metric for migration" on page 110.

Cloning a changed default policy for migration

If you want to migrate changes you have made to a monitor pack default policy, you should clone them.

See "Manually cloning your changed default monitor pack policies, metrics, and rules" on page 108.

To clone a changed default policy for migration

1. In the Symantec Management Console, on the **Home** menu, click **Monitoring and Alerting**.
2. In the left pane, click **Monitoring and Alerting > Monitor > Policies > Monitor Policies**.
3. Expand the **Monitor Policies** folders to reach the monitor policy you want to clone.

4 Right-click the policy you want to clone, and click **Clone**.

A clone of the policy is created in the library with **Copy of** prepended to the original name.

5 Select the newly created policy and edit it as needed.

Cloning a changed default rule for migration

When you migrate a cloned policy, you also need to clone the rules that you want to migrate.

See "Manually cloning your changed default monitor pack policies, metrics, and rules" on page 108.

To clone a changed default rule for migration

1 In the Symantec Management Console, on the **Home** menu, click **Monitoring and Alerting**.

2 In the left pane, click **Monitoring and Alerting > Monitor > Policies > Rule Library**.

3 In either the **Agent-based** rules table or in the **Agentless** rules table, select the rule to clone.

4 In the toolbar, click the **Clone** symbol.

A clone of the rule is created in the library with **Copy of** prepended to the original name.

5 Select the newly created rule and edit it as needed.

6 Use this cloned rule in a cloned or a new policy to save rule settings after migration.

Cloning a changed default metric for migration

When you migrate a cloned policy, you also need to clone the metrics that you want to migrate.

See "Manually cloning your changed default monitor pack policies, metrics, and rules" on page 108.

To clone a changed default metric for migration

1 In the Symantec Management Console, on the **Home** menu, click **Monitoring and Alerting**.

2 In the left pane, click **Monitoring and Alerting > Monitor > Policies > Metric Library**.

3 In either the **Agent-based** rules table or in the **Agentless** metrics table, select the metric to clone.

4 In the toolbar, click the **Clone** symbol.

A clone of the metric is created in the library with **Copy of** prepended to the original name.

5 Select the newly created metric and edit it as needed.

6 Use this new metric in a cloned rule to save metric settings after migration.

Chapter 9

Migrating Real-Time System Manager Solution

This chapter includes the following topics:

About Real-Time System Manager Solution migration to version 7.1

You can migrate from Real-Time System Manager Solution 7.0 to Real-Time System Manager Solution 7.1. In addition to using the migration wizard to migrate, you must complete some manual steps. You need to manually move and store some .XML files on the 7.1 computer.

See "Manually migrating Real-Time System Manager Solution to version 7.1" on page 113.

Manually migrating Real-Time System Manager Solution to version 7.1

You can use the Symantec Notification Server Wizard to help you migrate Real-Time System Manager Solution to version 7.1.

Table 9-1 Process for manually migrating Real-Time System Manager Solution to version 7.1

Step	Action	Description
Step 1	Export the data from the previous Notification Server computer.	When you migrate to Symantec Management Platform 7.1, you use the Symantec Notification Server Wizard to migrate the previous Notification Server data. When you use the migration wizard, you must export Notification Server data to a data store file. See "Exporting Symantec Management Platform 7.0 data to a data store file " on page 58.
Step 2	Import the exported data from the previous Notification Server computer to the Symantec Management Platform 7.1.	You use the Symantec Notification Server Migration Wizard to migrate the previous Notification Server data to Symantec Management Platform 7.1. When you use the migration wizard, you must import the data from a data store file. See "Importing Symantec Management Platform 7.0 data from a data store file" on page 60.
Step 3	Move and store Real-Time System Manager Solution files and settings.	You need to move and store some XML files from the old Notification Server computer to the Symantec Management Platfrom 7.1 computer. See "About manually migrating Real-Time System Manager Solution files and settings" on page 114.

About manually migrating Real-Time System Manager Solution files and settings

The Real-Time System Manager Solution Migration Wizard contains the following exporter and importer objects:

- Boot Redirection task

- Network Filtering task
- Password Management task
- Process Management task
- Service Management task
- Network Filtering task

The majority of your Real-Time System Manager Solution data is migrated using the migration wizard. However, to have full predefined functionality, you must move some files. You need to manually move and store these files from the old Notification Server computer to the new 7.1 computer.

By default, the files that need to be moved are located on your previous Notification Server in specific locations.

Table 9-2 Real-Time System Manager Solution files path

Notification Server path	Symantec Management Platform 7.1 path
`C:\Program Files\Altiris\RTSM\Web\Bin\WebTerminal.config`	Same location on the new 7.1 Symantec Management Platform.
`C:\Program Files\Altiris\RTSM\Web\UIData\PingFilter.xml`	Same location on the new 7.1 Symantec Management Platform.
`C:\Program Files\Altiris\RTSM\Web\UIData\CBFilters.xml`	Same location on the new 7.1 Symantec Management Platform.

How to validate Real-Time System Manager Solution after the migration

After you finish the migration process, it is necessary to validate the migrated items. In fact, you need to make sure that these items have been correctly migrated to your new 7.1 Symantec Management Platform environment. They still should have the same predefined functionality. You need to check the following items:

- Connection settings and credential profiles
  If you have used a security certificate in your connection settings, you need to make sure that it has a correct server name and location.
  For more information, see the topics about connection profiles in the *Symantec Management Platform Help*.
- Network filters

For more information, see the topics about filtering network traffic on multiple computers in the *Real-Time System Manager User Guide*.

- Boot Redirection
  You need to manually move and store your redirection images from your old Notification Server to your new 7.1 Symantec Management Platform environment.
  For more information, see the topics about booting multiple computers from another device in the *Real-Time System Manager User Guide*.
- Network Filtering
  You need to manually move and store your predefined custom network filters from your old Notification Server to your new 7.1 Symantec Management Platform environment.
  For more information, see the topics about filtering network traffic on multiple computers in the *Real-Time System Manager User Guide*.
- Password Management
  For more information, see the topics about resetting a local user password on multiple computers in the *Real-Time System Manager User Guide*.
- Process Management
  For more information, see the topics about running or stopping a process on multiple computers in the *Real-Time System Manager User Guide*.
- Service Management
  For more information, see the topics about running or stopping a service on multiple computers in the *Real-Time System Manager User Guide*.

Chapter 10

Migrating Real-Time Console Infrastructure

This chapter includes the following topics:

About Real-Time Console Infrastructure migration to version 7.1

You can migrate from Real-Time Console Infrastructure 7.0 to Real-Time Console Infrastructure 7.1. In addition to using the migration wizard to migrate, you must complete some manual steps. You need to manually move and store some .XML files on the 7.1 computer.

See "Manually migrating Real-Time Console Infrastructure to version 7.1" on page 117.

Manually migrating Real-Time Console Infrastructure to version 7.1

You can use the Symantec Notification Server Migration Wizard to help you migrate Real-Time Console Infrastructure to version 7.1.

Table 10-1 Process for manually migrating Real-Time Console Infrastructure to version 7.1

Step	Action	Description
Step 1	Export data from the previous Notification Server. computer	When you migrate to Symantec Management Platform 7.1, you use the Symantec Notification Server Migration Wizard to migrate the previous Notification Server data. When you use the migration wizard, you must export Notification Server data to a data store file. See "Exporting Symantec Management Platform 7.0 data to a data store file " on page 58.
Step 2	Import the exported data from the previous Notification Server computer to the Symantec Management Platform 7.1.	You use the Symantec Notification Server Migration Wizard to migrate the previous Notification Server data to Symantec Management Platform 7.1. When you use the migration wizard, you must import the old data from a data store file. See "Importing Symantec Management Platform 7.0 data from a data store file" on page 60.
Step 3	Move and store Real-Time Console Infrastructure files and settings.	You need to move and store some XML files from the old Notification Server computer to the Symantec Management Platfrom 7.1 computer. See "About manually migrating Real-Time Console Infrastructure files and settings" on page 118.

About manually migrating Real-Time Console Infrastructure files and settings

The majority of your Real-Time Console Infrastructure Solution data is migrated when you migrate your Real-Time Console Infrastructure to your new 7.1 Symantec Management Platform. However, you must manually migrate some files. To migrate these files, you use your previous Notification Server computer files and move them to your new 7.1 Symantec Management Platform environment.

Table 10-2 Real-Time Console Infrastructure files path

Old Notification Server path	Symantec Management Platform 7.1 path
C:\Program Files\Altiris\RTCI\Web\UIData\BIOSAttributes.xml	Same location on the new 7.1 Symantec Management Platform.
C:\Program Files\Altiris\RTCI\Web\UIData\EventFilter_AMT.xml	Same location on the new 7.1 Symantec Management Platform.
C:\Program Files\Altiris\RTCI\Web\UIData\EventFilter_DASH.xml	Same location on the new 7.1 Symantec Management Platform.
C:\Program Files\Altiris\RTCI\Web\UIData\PortCheck.xml	Same location on the new 7.1 Symantec Management Platform.

How to validate Real-Time Console Infrastructure after the migration

You need to check if your previous settings and options have been correctly migrated. In addition, if you had any scheduled tasks on your old Notification Server computer, check that those predefined tasks have been correctly migrated.

Predefined tasks may consist of the predefined time schedule, computer profiles, connection profiles, and credential profiles as follows:

- Connection and credential profiles
  If you have used a security certificate in your connection settings, you need to make sure that it has a correct server name and location.
  For more information, see the topics about connection profiles in the *Symantec Management Platform Help*.
- Get out-of-band inventory
  For more information, see the topics about collecting and viewing Intel AMT and DASH inventory in the *Real-Time Console Infrastructure User Guide*.
- Power management
  For more information, see the topics about managing the power state of computers remotely in the *Real-Time Console Infrastructure User Guide*.
- Update Intel AMT credentials
  For more information, see the topics about updating Intel AMT credentials in the *Real-Time Console Infrastructure User Guide*.
- Update Intel AMT settings

For more information, see the topics about updating Intel AMT settings and configuring Intel AMT in the *Real-Time Console Infrastructure User Guide*.

- Update out-of-band alert settings
  You need to make sure that you have a correct **SNMP server** for Intel AMT and ASF and also correct **Destination URL** for DASH.
  For more information, see the topics about updating Intel AMT and DASH alert settings in the *Real-Time Console Infrastructure User Guide*.

Chapter 11

Migrating pcAnywhere Solution

This chapter includes the following topics:

Before you begin the migration from 7.0 to 7.1 with pcAnywhere

Before you begin the upgrade from 7.0 to 7.1, ensure that the following tasks are completed:

- Back up your current 7.0 server and databases before starting any migration work.
- Verify and complete all outstanding tasks, policies, package copies, and hierarchy replication schedules, if they are in use.
- Disable all hierarchy and peer-based replication schedules, if they are in use.
- Review the data available in the pcAnywhere reports and verify if the data is correctly displayed.
- Back up the current database to capture the most recent one.
- Shut down the 7.0 Notification Server computer.

See "Migrating from 7.0 to 7.1 with pcAnywhere" on page 122.

Migrating from 7.0 to 7.1 with pcAnywhere

Ensure that you have performed the required steps before you start migrating to IT Management Suite 7.1 and upgrade to pcAnywhere Solution 7.1 SP1.

See "Before you begin the migration from 7.0 to 7.1 with pcAnywhere" on page 121.

To migrate from 7.0 to 7.1 with pcAnywhere

1. Prepare the target server for the installation of IT Management Suite 7.1.

   IT Management Suite 7.1 requires and is currently supported on Microsoft Windows 2008 R2 x64. If you are using SSL and other certificates, make sure that they are in place on the 7.1 target server before you install Symantec Installation Manager or solutions.

2. Install IT Management Suite 7.1 or pcAnywhere 12.6.65 onto the target server (with migration components within the optional components).

   Ensure that the Symantec database name is not the default name.

3. Use the migration wizard to export 7.x data from the source 7.0 server.

4. Copy the x86 migration package from your IT Management Suite 7.1 server.

   The package is located at `Program Files\Symantec Installation Manager \Migration Package\`

   Multiple migration packages are launched and installed for pcAnywhere.

5. From the `program files\ upgrade` directory on the 7.0 server, run the migration wizard (NSUpgradeWizard.exe).

   The migration wizard exports KMS and CM keys into a data store file (*.adb).

6. Back up the data store file (*adb).

7. Restore the backed up Symantec database from Notification Server 7.0 to 7.1.

8. Restore the backed up registry key and XML file.

9. Reconfigure the backed up database from the Symantec Management Platform Console and save the changes.

10. Run the x64 migration wizard and import the backed up .adb file.

11. Redirect package servers first to prepare the topology for regionally available agent packages.

    Alternatively, package servers can be temporarily added to the topology during the migration process and removed after 7.0 package servers have completed their upgrades.

12 Redirect all the agents that were previously reporting to the 7.0 server to the new 7.1 server.

   You can use the Notification Server 7.0 agent settings to do this.

13 Enable upgrade policies for the Symantec Management Agent and the pcAnywhere plug-ins.

   Re-establish hierarchy relationships

   Re-enable hierarchy and peer-based replication

Chapter 12

Migrating Out of Band Management Component

This chapter includes the following topics:

About Out of Band Management Component migration to version 7.1

This chapter provides details of migration from Out-of-Band Management Component 7.0 to Out-of-Band Management Component 7.1. In addition to using the migration wizard to migrate, you must complete some manual steps. You need to manually move and store some databases on the 7.1 computer.

See "Manually migrating Out of Band Management Component to version 7.1" on page 126.

Manually migrating Out of Band Management Component to version 7.1

Table 12-1 Process for manually migrating Out of Band Management Component 7.0 to version 7.1

Step	Action	Description
Step 1	Export data from the previous Notification Server 7.0.	When you migrate to Symantec Management Platform 7.1, you use the Symantec Notification Server Migration Wizard to migrate Notification Server 7.0 data. When you use the migration wizard, you must export Notification Server data to a data store file. See "Exporting Symantec Management Platform 7.0 data to a data store file " on page 58.
Step 2	Redirect the Altiris Agent from Notification Server 7.0 to Symantec Management Platform 7.1.	You need to redirect the existing clients pointing to 7.0 Notification Server to the new Symantec Management Platform 7.1. See "Redirecting the Altiris Agent from Notification Server 7.0 to Symantec Management Platform 7.1" on page 128.
Step 3	Detach the *Symantec_CMDB database* from the old Notification Server database.	Before you start the migration process, you must manually move the *Symantec_CMDB database* to the 7.1 computer. Also, after you move it and reconfigure it, you need to redirect the existing clients that point to 7.0 Notification Server to the new 7.1 Symantec Management Platform. See "Moving and restoring Symantec_CMDB database to the 7.1 computer" on page 129.

Table 12-1 Process for manually migrating Out of Band Management Component 7.0 to version 7.1 *(continued)*

Step	Action	Description
Step 4	Attach the *Symantec_CMDB database* to the 7.1 database.	Before you start the migration process, you must manually move the *Symantec_CMDB database* to the 7.1 computer. Also, after you move it and reconfigure it, you need to redirect the existing clients that point to 7.0 Notification Server to the new 7.1 Symantec Management Platform. See "Moving and restoring Symantec_CMDB database to the 7.1 computer" on page 129.
Step 5	Reconfigure the *Symantec_CMDB database* on the Symantec Management Platform 7.1.	After you manually move the *Symantec_CMDB database* to your new environment, you must reconfigure it. See "Reconfiguring Notification Server database (Symantec_CMDB)" on page 129.
Step 6	Detach the *Intel AMT database*.	The *Intel AMT database* is not migrated through the migration process. To preserve it, you must manually migrate it from 7.0 Notification Server to Symantec Management Platform 7.1. See "Migrating the Intel AMT database" on page 130.
Step 7	Attach the *Intel AMT database* to the 7.1 database.	The *Intel AMT database* is not migrated through the migration process. To preserve it, you must manually migrate it from 7.0 Notification Server to Symantec Management Platform 7.1. See "Migrating the Intel AMT database" on page 130.
Step 8	Reconfigure the *Intel AMT database* on the Symantec Management Platform 7.1.	After you move the *Intel AMT database* to your new environment, you must validate it and make sure that it operates correctly. See "Configuring the Intel AMT database" on page 131.

Table 12-1 Process for manually migrating Out of Band Management Component 7.0 to version 7.1 *(continued)*

Step	Action	Description
Step 9	Import the exported data from 7.0 Notification Server to the Symantec Management Platform 7.1.	You use the Symantec Notification Server Migration Wizard to migrate Notification Server 7.0 data to Symantec Management Platform 7.1. When you use the migration wizard, you must import the 7.0 data from a data store file. See "Importing Symantec Management Platform 7.0 data from a data store file" on page 60.
Step 10	Fine-tune Out of Band Management Component 7.1 after the migration.	After you have finished all the migration steps, you can fine-tune Out of Band Management Component 7.1. See "Fine-tuning Out of Band Management Component 7.1 after the migration" on page 132.

Redirecting the Altiris Agent from Notification Server 7.0 to Symantec Management Platform 7.1

You need to redirect the existing clients pointing to 7.0 Notification Server to the new Symantec Management Platform 7.1.

See "About Out of Band Management Component migration to version 7.1" on page 125.

See "Manually migrating Out of Band Management Component to version 7.1" on page 126.

To redirect the Altiris Agent from Notification Server 7.0 to Symantec Management Platform 7.1

1. In the Symantec Management Console, click **Settings > All Settings**.
2. Click **Settings > Agents/Plug-ins > Symantec Management Agent > Settings > Symantec Management Agent Settings - Targeted**.

3 In the right pane, under **All Desktop computers (excluding 'Site Servers')**, click the **Advanced** tab.

4 Under **Alternative URL for accessing NS**, check **Specify an alternative URL for the Symantec Management Agent to use to access the NS** and specify the 7.1 **Server Name** and **Server Web**.

Moving and restoring Symantec_CMDB database to the 7.1 computer

Before you start the migration process, you must manually move the *Symantec_CMDB database* to the 7.1 computer. Also after you move it and reconfigure it, you need to redirect the existing clients that point to 7.0 Notification Server to new 7.1 Symantec Management Platform. You can redirect them by changing the server name and server web address to the new 7.1 Symantec Management Platform.

See "About Out of Band Management Component migration to version 7.1" on page 125.

See "Manually migrating Out of Band Management Component to version 7.1" on page 126.

To move the Symantec_CMDB database

1 On the 7.0 computer, open Microsoft SQL Manager Studio.

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

3 In the left pane, under **Databases**, right-click on the *Symantec_CMDB*.

4 In the right-click menu, click **Tasks > Detach**.

To restore the Symantec_CMDB database

1 On the 7.1 computer, open Microsoft SQL Manager Studio.

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

3 In the left pane, right-click the **Databases**.

4 In the right-click menu, click **Tasks > Attach**.

Reconfiguring Notification Server database (Symantec_CMDB)

After you manually move the *Symantec_CMDB database* to your new environment, you must reconfigure it.

See "Moving and restoring Symantec_CMDB database to the 7.1 computer" on page 129.

See "About Out of Band Management Component migration to version 7.1" on page 125.

See "Manually migrating Out of Band Management Component to version 7.1" on page 126.

To reconfigure Notification Server database (Symantec_CMDB)

1. In the Symantec Management Platform, on the **Settings** menu, click **Notification Server > Database Settings**.
2. On the **General** page, under **Database Name**, select **Use existing database** and assign it to the *Symantec_CMDB_New*.
3. Click **Reconfigure Database**.

After the database is reconfigured, you can import the exported data from 7.0 Notification Server to the Symantec Management Platform 7.1.

See "Importing Symantec Management Platform 7.0 data from a data store file" on page 60.

Migrating the Intel AMT database

The *Intel AMT database* is not migrated through the migration process. To preserve it, you must manually migrate it from the previous Notification Server to Symantec Management Platform 7.1. You must manually move the *Intel AMT database* to your new environment by using Microsoft SQL Management Studio.

See "About Out of Band Management Component migration to version 7.1" on page 125.

See "Manually migrating Out of Band Management Component to version 7.1" on page 126.

To move the Intel AMT database

1. On the old Notification Server computer, open Microsoft SQL Manager Studio.
2. In the left pane, expand the **Databases** folder.
3. In the left pane, under **Databases**, right-click on the *Intel AMT database*.
4. In the right-click menu, click **Tasks > Detach**.

To restore the Intel AMT database

1. On the 7.1 computer, open Microsoft SQL Manager Studio.
2. In the left pane, expand the **Databases** folder.

3 In the left pane, right-click the **Databases**.

4 In the right-click menu, click **Tasks > Attach**.

Configuring the Intel AMT database

After you move the *Intel AMT database* to your new environment, you must validate it and make sure that it operates correctly. In addition, make sure that the correct address of the SQL Server and SQL Login is specified in the Out of Band Management Component settings.

See "Migrating the Intel AMT database" on page 130.

See "About Out of Band Management Component migration to version 7.1" on page 125.

See "Manually migrating Out of Band Management Component to version 7.1" on page 126.

To configure the Intel AMT database

1 In the Symantec Management Console, on the **Home** menu, click **Remote Management > Out of Band Management**.

2 In the left pane, under **Configure Additional OOB Site Server**, click **Configure and Assign OOB Site Server**.

3 Click **Site Management > Settings > OOB Service > OOB Service Settings**.

4 Under **Global OOB site service installation settings**, edit **SQL server**. You must specify the SQL Server name where the *Intel AMT database* is now located.

If you have used the default Intel AMT database name (*NS_Database_Name_AMT*) on your previous Notification Server and transferred it to a 7.1 computer database with the same name, Out of Band Management Component 7.1 automatically accepts the previous database. In some cases, before the installation of out-of-band site servers, you need to modify out-of-band site server settings with your custom database name.

For more information, see the topics about configuring the out-of-band site server installation settings in the *Out of Band Management Component Implementation Guide*.

Fine-tuning Out of Band Management Component 7.1 after the migration

You can start to fine-tune Out of Band Management Component 7.1 after you complete the steps for manual migration.

See "Manually migrating Out of Band Management Component to version 7.1" on page 126.

You might experience the following errors on different pages:

- `Configuration saved but cannot be applied. Please check that currently selected Intel SCS is installed and running in Service Location page`

  After you have configured the Intel AMT database, you can receive this error on the page.

  This message is an expected issue and it means that you do not have an Out of Band Management Component site server installed. It needs to apply the SQL settings to the out-of-band site server. You need to install an out-of-band site server.

  For more information, see the topics about installing an out-of-band site server in the *Out of Band Management Component Implmentation Guide*.

- `One or more of Intel® AMT Setup and Configuration Servers in outdated. You have to upgrade it by turning on the 'Out of Band Service Agent' policy. If you don't want to use this server, you can delete it`

  When you try to view configured Intel AMT computers on the **Intel AMT Computers** page, you may see this error message.

  You can remove all site servers from the current computer. The other workaround is to remove an entry inside the URL from *dbo.Inv_OOB_Site_Server_State* and also *dbo.csto_servers*. It is a common resolution in case your old Notification Server is not functional. You also need to verify the out-of-band site server installation by checking the general settings for the Intel AMT computers.

- **Secure TLS profiles**

  If you previously used Secure TLS profiles, then you need to request a new security certificate for the new 7.1 Symantec Management Platform.

  For more information, see the topics about configuring TLS in the *Out of Band Management Component Implementation Guide*.

Chapter 13

Migrating CMDB Solution

This chapter includes the following topics:

Migrating to CMDB Solution 7.1

You perform the product migration from 7.0 to 7.1 according to the migration scenario for Asset Management Solution and IT Management Suite.

See "About migrating Asset Management Solution" on page 141.

See "Migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1" on page 32.

See "About data migration" on page 52.

See "About the Symantec Notification Server Migration Wizard" on page 54.

Chapter 14

Migrating Barcode Solution

This chapter includes the following topics:

About migrating Barcode Solution

In addition to using the migration wizard to migrate Barcode Solution, you must complete some manual steps.

See "Manually migrating your Barcode Solution files and settings" on page 136.

Before you migrate your data, you need to take the following actions:

- Ensure that handheld devices have uploaded their data to the previous Notification Server computer.
  See "Synchronizing data" on page 137.
- Ensure that all batches in the upload verification section have been processed.
  See "Verifying asset data" on page 138.
- Back up the default synchronization profile.
  See "Backing up the Barcode Solution default synchronization profile" on page 139.

Manually migrating your Barcode Solution files and settings

The majority of your Barcode Solution data is migrated when you migrate your Configuration Management Database (CMDB) using the migration wizard. However you must first manually migrate your default synchronization profile settings. To migrate these settings you use the console to export them into an XML file. You then import this XML file after you install your new Symantec Management Platform. In addition, Symantec recommends that you finish synchronizing all your data from the handheld devices. Also, ensure that you verify your asset data before you load it into the CMDB by processing all batches.

See "About migrating Barcode Solution" on page 135.

Table 14-1 Process for manually migrating your Barcode Solution files and settings

Step	Action	Description
Step 1	Handheld devices have uploaded their data to the previous Notification Server computer.	You must finish synchronizing all your data from the handheld device to the Barcode Solution before you migrate. Failure to do this means you may lose data. You cannot upload the data from the old version of Barcoder to the new version Barcode Solution. You have to upload to the old version of the Barcode Solution first and then migrate the data over again. See "Synchronizing data" on page 137.
Step 2	All batches in the upload verification section have been processed.	All batches in the upload verification section have been processed. If you migrate from 7.0 to 7.1, then any unprocessed batches will be available to process in 7.1. However, Symantec recommends that you still undertake this step as a best practice. See "Verifying asset data" on page 138.

Table 14-1 Process for manually migrating your Barcode Solution files and settings *(continued)*

Step	Action	Description
Step 3	Back up the Barcode Solution default synchronization profile.	Use the Symantec Management Console to export your default synchronization profile settings into an XML file. Store this file on a neutral storage location. See "Backing up the Barcode Solution default synchronization profile" on page 139.
Step 4	Use the Symantec Notification Server Migration Wizard to export and import your data.	Use the Symantec Notification Server Migration Wizard to export and import your data. See "Exporting Symantec Management Platform 7.0 data to a data store file " on page 58. See "Importing Symantec Management Platform 7.0 data from a data store file" on page 60. **Warning:** Since Barcode Solution relies on CMDB Solution, the CMDB data must be imported at the same time or before you import your barcode data. For this reason ensure that you have **CMDB Solution** selected in the **Exporter Configuration** page of the Symantec Notification Server Migration Wizard .
Step 5	Restore the Barcode Solution default synchronization profile file	Use the Symantec Management Console to import your default synchronization profile settings from an XML file. See "Restoring the Barcode Solution default synchronization profile" on page 139.

Synchronizing data

Any data that is specified in the **Synchronization Profiles** page is uploaded to the barcode device in the initial synchronization. It may involve the transfer of

a significant amount of data. Ensure a good connection (either wireless or through a cradle) with the Notification Server computer.

This task is part of the process for manually migrating your Barcode Solution files settings. After you complete this task, you can complete the rest of the process.

See "Manually migrating your Barcode Solution files and settings" on page 136.

To synchronize data

1. Make sure that the barcode device has a connection to the host computer, either wireless or through a synchronization cradle.
2. On the barcode device, click **Start > Programs > Symantec Altiris Barcoder**.
3. Select **Synchronize** from the menu option.
4. Enter your security credentials and click **Login**.

   Your password and user name are cached for an hour on the handheld device. If you do not use it for over an hour, you must reenter your security credentials. Closing the application clears the cached credentials; they need to be reentered on launching the application again.
5. Select the synchronization profile to use, and click **Next**.
6. Choose one of the synchronization options, and click **Sync**.

Verifying asset data

By default, you need to verify your asset data before you load it into the Configuration Management Database. You verify asset data from the **Batch Uploads** page.

This task is part of the process for manually migrating your Barcode Solution files settings. After you complete this task, you can complete the rest of the process.

See "Manually migrating your Barcode Solution files and settings" on page 136.

To verify asset data

1. In the Symantec Management Console, on the **Home** menu, click **Service and Asset Management > Barcode**.
2. In the left pane, click **Barcode Solution > Manage Changes > Batch Uploads**.
3. In the **Batch uploads** page, select the batch of uploaded data that you want to verify.
4. Click **View Batch Details** select a resource and click **Resource Details** to view its changed details.

5 In the **Batch Details** dialog box, select a resource and click **View Resource Details** to view its changed details.

6 Select a resource from the list in the top section and click **Accept** to return to the **Batch Details** dialog box.

7 In the **Batch Details** dialog box, click **Accept Batch** to save your changes to the database.

Backing up the Barcode Solution default synchronization profile

Before you decommission your previous Notification Server computer, back up your Barcode Solution default synchronization profile to a neutral storage location.

Name the clone default profile `Default profile 7.0` or similar. Since the default profile already exists on 7.1, renaming the cloned default profile ensures that it can be identified differently in the 7.1 environment. By being uniquely identifiable, the cloned default profile is not overwritten.

This task is part of the process for manually migrating your Barcode Solution files settings. After you complete this task, you can complete the rest of the process.

See "Manually migrating your Barcode Solution files and settings" on page 136.

To back up the Barcode Solution default synchronization profile:

1 On your previous Notification Server computer, in the **Symantec Management Console**, go to **Home > Service and Asset Management > Barcode**.

2 In the left pane, expand **Barcode Solution > Synchronization Profiles > Default**.

3 Right-click **Default**, and click **Export**.

4 Save the `Default.xml` file to a neutral storage location.

5 Clone the default profile to ensure that it can be identified in the 7.1 environment.

Restoring the Barcode Solution default synchronization profile

After you install Symantec Management Platform and have run the migration wizard, you can restore your Barcode Solution default synchronization profile.

This task is part of the process for manually migrating your Barcode Solution files settings. After you complete this task, you can complete the rest of the process.

See "Manually migrating your Barcode Solution files and settings" on page 136.

To restore the Barcode Solution default synchronization profile:

1. On your new Notification Server computer, in the **Symantec Management Console**, go to **Home > Service and Asset Management > Barcode**.
2. In the left pane, expand **Barcode Solution > Synchronization Profiles > Default**.
3. Right-click the **Synchronization Profiles** folder, and click **Import**.
4. Browse to the default synchronization file.
5. Click **Open**.

Chapter 15

Migrating Asset Management Solution

This chapter includes the following topics:

About migrating Asset Management Solution

You perform the product migration from Asset Management Solution 7.0 to version 7.1 according to the migration scenario for IT Management Suite. No manual solution-specific migration steps are required. The solution-specific data is migrated when you migrate the product data according to the process that is defined in the Migrating Symantec Management Platform chapter.

You should verify and validate that the solution data and settings have been migrated correctly.

See "Migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1" on page 32.

See "About data migration" on page 52.

Chapter 16

Migrating Workflow Solution

This chapter includes the following topics:

About migrating Workflow Solution

You perform the Workflow Solution data migration from 7.0 to 7.1 according to the migration scenario for IT Management Suite.

See "Migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1" on page 32.

See "About data migration" on page 52.

After you migrate your data, you must upgrade your Workflow processes.

See "Upgrading Workflow processes" on page 143.

Upgrading Workflow processes

If you already have a Workflow Server running on a Symantec Management Platform computer, installing Workflow does not upgrade Workflow Server. Upgrading Workflow Server would break running processes. Instead, the Workflow installation adds a message in the Symantec Management Console that the Workflow Server should be upgraded manually.

Symantec recommends that you schedule a service stop, upgrade Workflow Server, test the published processes, and then resume the service.

Warning: You can disrupt currently-running processes by installing Workflow if you do not keep the same persistence settings. Ideally, you should use the same persistence settings for Workflow that you used for the earlier versions of Workflow. During installation you can set the persistence setting for Workflow. If the persistence settings in the earlier versions of Workflow are not supported in the current version of Workflow, version your projects so that you do not overwrite the currently-running processes.

See "Determining a project's persistence settings" on page 145.

See "Versioning a process" on page 147.

Table 16-1 Process for upgrading Workflow processes

Step	Action	Description
Step 1	Back up your projects	Create packages for all your projects, and store these packages on a safe directory. For more information on creating a project package, see the *Symantec Workflow Solution User Guide*.
Step 2	Back up the Ensemble database	Create a backup of your Ensemble database. Store the database backup on a safe directory.
Step 3	Install Workflow on a testing computer	When you install Workflow on your testing computer, make sure that you do the following: ■ Use the same Workflow persistence settings as in your earlier version of Workflow configuration. See "Determining a project's persistence settings" on page 145. If you use the persistence settings that are not supported by Workflow, version your projects. See "Versioning a process" on page 147. ■ Set Workflow to have access to a Symantec Management Platform server (Notification Server).
Step 4	Revise your projects	Open each project and make the necessary changes for it to be compatible with Workflow and the Symantec Management Platform. Change any old Notification Server components and settings. If possible use the same persistence setting for your Workflow projects as you used for your earlier versions of Workflow projects. See "Determining a project's persistence settings" on page 145.

Table 16-1 Process for upgrading Workflow processes *(continued)*

Step	Action	Description
Step 5	Publish revised projects to Workflow testing computer	Publish the revised projects to the Workflow testing computer. For more information on publishing projects, see the *Symantec Workflow Solution User Guide*.
Step 6	Test revised projects	Conduct thorough tests to ensure that your projects work properly in a Workflow and Symantec Management Platform environment. If you encounter any problems, fix the project and republish. **Warning:** Publishing untested processes in a production environment can cause significant problems. Symantec recommends that you test all processes thoroughly, before you publish them to a production environment.
Step 7	Install Workflow on a production computer	When you install Workflow on your production computer, make sure that you use the same persistence settings as in your earlier version of configuration. See "Determining a project's persistence settings" on page 145.
Step 8	Publish revised projects to production computer	Publish all of your revised projects to the Workflow production computer. For more information on publishing projects, see the *Symantec Workflow Solution User Guide*.

Determining a project's persistence settings

Persistence refers to how a running process is stored in memory to improve the performance of Workflow. Persistence is set at the project level, but most projects use the default setting that is set when Workflow is installed (almost always file-based). For the earlier versions of Workflow projects, the persistence settings are configured under the project's **Publishing** data tab in the **Work Queue Service Name** property.

See "Upgrading Workflow processes" on page 143.

Table 16-2 Persistence options

Persistence option	Description
LogicBase.Components.Ensemble.WSWorkQueue	Uses Process Manager SQL database settings. The workflow project uses the Ensemble database for persistence. There is no Workflow equivalent of this setting.

Table 16-2 Persistence options *(continued)*

Persistence option	Description
LogicBase.Components.Default.ExchangeAdapters. LogicBaseExchangeWorkQueue	Uses Exchange for persistence. This is the most common persistence setting. This setting uses either file-based or SQL-based persistence over Exchange. For information on determining whether this setting uses file-based or SQL-based persistence, see the following section: The Workflow equivalent of this is Exchange (file-based) or SQL-based persistence. You can set this when you install Workflow.
LogicBase.Core.Workflow.FileSystemAdapters. FileSystemWorkQueue	Uses direct file-based persistence. There is no Workflow equivalent of this setting.
LogicBase.Core.Models.Workflow.InMemoryWorkQueue	Uses internal Workflow memory. There is no Workflow equivalent of this setting.
LogicBase.Core.Workflow.SQLServerAdapters. SQLServerWorkQueue	Uses direct SQL-based persistence. There is no Workflow equivalent of this setting.

Your projects are probably set to use **LogicBase.Components.Default.ExchangeAdapters.LogicBaseExchangeWorkQueue**. In this case, you can determine whether the exchange is set to file-based or SQL-based persistence in the Configuration and Logging Tool.

If any of your projects use a persistence setting other than **LogicBase.Components.Default.ExchangeAdapters.LogicBaseExchangeWorkQueue**, you should version them to avoid losing process data.

See "Versioning a process" on page 147.

To determine the default persistence setting in the Workflow Explorer

1. Open the Configuration and Logging Tool.

   Click **Start > Programs > Symantec > Workflow Designer > Tools > Workflow Explorer**.

2. Click the **SymQ Configuration** tab.

3 In the left pane, click **SymQ_Local_Defaults**.

4 In the right pane, double-click **local.workflow-**.

If the **Deliver To Queue** property is set to **LBME.Workflow** (with a prefix), the default persistence setting is file-based.

If the **Deliver To Queue** property is set to **workflowsqlexchange** (with a prefix), the default persistence setting is SQL-based.

Versioning a process

If you have an earlier version of Workflow project that uses a persistence setting that is not supported in the current version of Workflow, version the project so that you do not lose any process data (such as tasks). Process versioning is handled in IIS. When you publish a workflow project, a new virtual directory is created in IIS, unless one of the same name already exists. If an identical one exists, the new process overwrites the process that is already published there. You must create a new virtual directory to contain the updated process while the old process runs in its virtual directory. The following steps assume that you have a currently running process that you replace with an updated version.

Versioning works only with the “Publish Application to Server” publishing option. Because the other publishing options do not let you set the virtual directory name, you cannot use versioning with them.

See “Upgrading Workflow processes” on page 143.

See “Determining a project's persistence settings” on page 145.

To version a process

1 In Workflow Designer, when you are ready to publish your updated process, click **File > Deploy Project > Publish Project**.

2 In the **Virtual Directory** field, add the updated version number to the end of the name of the virtual directory.

For example, if the old process is in a virtual directory called “PurchaseOrder”, call the new virtual directory “PurchaseOrder2.0.”

Warning: If you publish without changing the name of the virtual directory, your new process completely replaces the old one and breaks any of its current instances.

---

3 Complete the publishing process as normal.

4. Repoint the invocation links to the virtual directory of the updated process.

   In other words, whatever invoked the old process (such as Process Manager service catalog item or external link) must be repointed to the new virtual directory that contains the process.

5. After the old process has finished all activity, delete its virtual directory.

Chapter 17

Migrating Inventory Pack for Servers Solution

This chapter includes the following topics:

Migrating to Inventory Pack for Servers 7.1

You perform the product migration from 7.0 to 7.1 according to the migration scenario for Inventory Solution and IT Management Suite.

See "Before you migrate to Inventory Solution 7.1" on page 69.

See "Migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1" on page 32.

See "About data migration" on page 52.

See "About the Symantec Notification Server Migration Wizard" on page 54.

Chapter 18

Migrating Power Scheme Solution

This chapter includes the following topics:

About migrating Power Scheme

No manual solution-specific migration steps are required. The solution-specific data is migrated when you migrate the product data according to the process that is defined in the Migrating Symantec Management Platform chapter.

You should verify and validate that the solution data and settings have been migrated correctly.

See "Migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1" on page 32.

See "About data migration" on page 52.

Chapter 19

Migrating Recovery Solution

This chapter includes the following topics:

About migrating Recovery Solution

Recovery Solution is not a part of IT Management Suite 7.1.

Do not upgrade from 7.0 to IT Management Suite 7.1 if you want to keep the Recovery Solutions features.

Until Recovery Solution 7.1 is released, you must run a dual environment if you want to use both IT Management Suite 7.1 and Recovery Solution.

Further information about Recovery Solution

For more information about new versions and upgrades, visit the support page for Recovery Solution.You can also contact the Symantec Business Sales team.

Chapter 20

Migrating Mobile Management Solution

This chapter includes the following topics:

About migrating Mobile Management Solution

Mobile Management Solution is not a part of IT Management Suite 7.1.

Do not upgrade from 7.0 to IT Management Suite 7.1 if you want to keep the Mobile Management Solution features.

Until Mobile Management Solution 7.1 is released, you must run a dual environment to use both IT Management Suite 7.1 and Mobile Management Solution.

Further information about Mobile Management Solution

For more information about new versions and upgrades, visit the support page for Mobile Management Solution.You can also contact the Symantec Business Sales team.

Chapter 21

Migrating Wise Connector Solution

This chapter includes the following topics:

About migrating Wise Connector

You cannot upgrade from a previous version of Wise Connector. Upgrading is not supported. You must install and use a clean installation of Wise Connector.

For more information, see *Wise Connector User Guide*.

Chapter 22

Migrating ServiceDesk Solution

This chapter includes the following topics:

About migrating from ServiceDesk 7.0

You can upgrade any Symantec ServiceDesk 7.0 installation to 7.1. ServiceDesk 7.1 installation updates the SQL database automatically.

For more information, see *ServiceDesk Implementation Guide*.

Chapter 23

Migrating Virtual Machine Management Solution

This chapter includes the following topics:

About migrating Virtual Machine Management data

There are no manual solution-specific migration steps to perform. The solution-specific data is migrated when you migrate the product data according to the process that is defined in the Migrating Symantec Management Platform chapter.

You should verify and validate that the solution data and settings have been migrated correctly.

See "Migrating from Symantec Management Platform 7.0 to Symantec Management Platform 7.1" on page 32.

See "About data migration" on page 52.

Index

E

F

H

I

O

P

R

S

T

U

V

W