IT Management Suite 8.1
Data Migration
IT Management Suite 8.1 Data Migration

Legal Notice

Copyright © 2017 Symantec Corporation. All rights reserved.

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

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

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

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

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, et seq. "Commercial Computer Software and Commercial Computer Software Documentation," as applicable, and any successor regulations, whether delivered by Symantec as on premises or hosted services. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.
Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com
Technical Support

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

Symantec’s support offerings include the following:

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

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

support.symantec.com

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

Contacting Technical Support

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

support.symantec.com

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

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

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

**Licensing and registration**

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

www.symantec.com/business/support/

**Customer service**

Customer service information is available at the following URL:

www.symantec.com/business/support/

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

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

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

<table>
<thead>
<tr>
<th>Region</th>
<th>Email</th>
</tr>
</thead>
<tbody>
<tr>
<td>Asia-Pacific and Japan</td>
<td><a href="mailto:customercare_apj@symantec.com">customercare_apj@symantec.com</a></td>
</tr>
<tr>
<td>Europe, Middle-East, and Africa</td>
<td><a href="mailto:semea@symantec.com">semea@symantec.com</a></td>
</tr>
<tr>
<td>North America and Latin America</td>
<td><a href="mailto:supportsolutions@symantec.com">supportsolutions@symantec.com</a></td>
</tr>
</tbody>
</table>
Migrating Patch Management Solution data using standalone replication .................................................. 52
Migrating Patch Management Solution data using manual export and import ................................................ 54
Migrating Software Management Solution data .......................................................... 56
About migrating software components .............................................................................. 60
Migrating physical packages using Symantec Notification Server Migration Wizard .............................................. 62
Migrating software components using the Software Resource Replicator utility .................................................. 65
Migrating ITMS Management Views Data ........................................................................ 66
Migrating Real-Time System Management Data ........................................................... 67
Migrating IT Analytics Server and content pack Data .................................................. 67
Migrating Server Management Suite component data .................................................. 68
Migrating Monitor Solution data ................................................................. 68
Migrating Virtual Machine Management data ....................................................................... 69
Migrating Power Scheme Task component data .................................................. 70
Migrating Workflow Solution ................................................................. 71
Introducing data migration

This chapter includes the following topics:

- About data migration

About data migration

This document describes how to migrate data from older version of IT Management Suite to version 8.1 using standalone replication rules and the import and export functionality within the Symantec Management Console.

Starting from IT Management Suite version 8.0 HF4, you can replicate data between the servers that have different versions of IT Management Suite installed. Similarly, you can export and import data between servers with different versions of IT Management Suite.

This enhancement lets you re-use the data objects from previous IT Management Suite implementations without the need to recreate them after an upgrade. For example, if you perform an off-box upgrade and want to start with a clean database, you can move the data that you require to the new database.

Another scenario for using the data migration enhancements is to keep the old Notification Server fully functional while setting up the new server.

Note: Despite the availability of the data migration feature, Symantec recommends performing an on-box upgrade using the existing hardware.

If you decide to perform an off-box upgrade to introduce a new hardware, Symantec recommends to keep using the existing database.

Migrating data is supported from the following IT Management Suite versions:

- IT Management Suite 7.6 HF7
If you need to migrate a large amount of data, Symantec recommends using the standalone replication rules. You also use the standalone replication rules to migrate the data that cannot be exported and imported between Notification Servers.

See "Performing data migration using standalone replication" on page 11.

**Warning:** Before starting the replication, make sure that FIPS is disabled on your destination Notification Server.

For more information about configuring FIPS on Windows computers, see the article at the following URL:

https://support.microsoft.com/en-us/kb/811833

If you want to move individual data objects from one server to another, use the manual export and import or the `ImportExportUtil.exe` tool. One of the advantages of exporting and importing the data is that you can modify the data in the exported XML file before importing it to the destination Notification Server.

See "Performing data migration using export and import" on page 25.

**Warning:** Before performing the export and import, you must move the cryptographic keys from the source Notification Server to the destination Notification Server.

See "Moving the cryptographic keys from source Notification Server to destination Notification Server" on page 26.

To migrate solution-specific data, refer to the solution-specific content in Chapter 4 of this document.
Migrating data using standalone replication

This chapter includes the following topics:

- Performing data migration using standalone replication
- Limitations of standalone replication in Symantec Management Platform

Performing data migration using standalone replication

Standalone replication lets you reliably move a large amount of data from one Notification Server to another.

Alternatively, you can use the manual export and import to move data between the Notification Servers with different versions.

See “Performing data migration using export and import” on page 25.

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Install the required pointfix on the 7.6 HF7 source Notification Server.</td>
<td>To migrate data successfully, you must install the following pointfix on your 7.6 HF7 source Notification Server: <a href="http://www.symantec.com/docs/INFO3459">http://www.symantec.com/docs/INFO3459</a></td>
</tr>
</tbody>
</table>
Table 2-1  Process for performing data migration using standalone replication  

(continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
</table>
| Step 2  | Configure and run the standalone replication rules. | On the source Notification Server, configure the standalone replication rules to replicate the data to the destination Notification Server.  
**Warning:** Before starting the replication, make sure that FIPS is disabled on your destination Notification Server.  
For more information about configuring FIPS on Windows computers, see the article at the following URL:  
https://support.microsoft.com/en-us/kb/811833  
See “Configuring and running standalone Item Replication Rule” on page 14.  
Note that migrating data using the standalone replication rules has some limitations.  
For more information about replicating solution-specific data, refer to the solution-specific content in Chapter 4 of this document. |
| Step 3  | (Optional) Monitor the progress of the replication. | On the source Notification Server, on the Jobs Management page, you can monitor the progress of the replication.  
This page is available in the Symantec Management Console, at Settings > Notification Server > Hierarchy and Replication > Jobs Management. |
| Step 4  | (Optional) View the reports of the replication. | On the source Notification Server, on the Server Replication report page, you can view the replication statistics.  
This report is available in the Symantec Management Console, at Reports > Notification Server Management > Server > Replication > Server Replication.  
To see the details of each replication, double-click the required row to open the Objects Replicated report. |
Configuring and running standalone Event Replication Rule

Standalone Event Replication Rule replicates selected resources with the selected Event Data Classes. Note that regardless of whether the same resources are in the database on destination Notification Server or not, Event Replication Rule replicates the selected resources along with the selected Event Data Classes for them.

For more information about replicating solution-specific data, refer to the solution-specific content in Chapter 4 of this document.

This task is a step in the process for performing data migration using standalone replication.

See "Performing data migration using standalone replication" on page 11.

To configure and run standalone Event Replication Rule

1. In the Symantec Management Console, on the Settings menu, click Notification Server > Hierarchy.

2. In the left pane, expand Replication folder, right-click the Events folder, and then click New > Event Replication Rule.

3. On the New replication rule page, configure the settings as follows:

   - Specify the Resource types or Resource targets that you want to replicate.
   - To specify the Resource types, do the following:
     1. At Resource types, click None selected.
     2. In the Select Resource Types dialog box, under Available items, select the resource types that you want to replicate, and then click OK.

   - To specify the Resource targets, do the following:
     1. At Resource targets, click None selected.
     2. In the Select Resource Targets dialog box, under Available targets, select the resource targets that you want to replicate, and then click OK.

   - Specify the Event Classes that you want to replicate.
   - 1. At Event Classes, click None selected.
   - 2. In the Event Classes dialog box, under Available items, in the Group drop-down list, select the events that you want to replicate for selected resources, and then click OK.
### Configuring and running standalone Item Replication Rule

Replicate **Policies, Tasks, Reports, Filters, Resource Targets, Organizational Views and Groups, custom Data Classes, Microsoft Active Directory Import**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>At <strong>Destination</strong>, click <strong>Specified Notification Servers</strong>.</td>
</tr>
<tr>
<td>2</td>
<td>In the <strong>Notification Servers</strong> dialog box, under <strong>Available Notification Servers</strong>, select the destination Notification Server from the list.</td>
</tr>
</tbody>
</table>
| 3    | (Optional) To add a new Notification Server, click **Add Notification Server** icon on the toolbar. In the **Add a Notification Server by name or browse the network** dialog box, type the host name or FQDN of the destination Notification Server, specify the **Notification Server Web Site**, and then click **Add**. If you want to use a non-default port for replication, you must specify the HTTP or HTTPS port as follows:  
  
  **Notification Server Name**: domain-name.com  
  **Notification Server Web Site**: https://domain-name.com:777/Altiris/NS/ |
| 4    | Click **OK**. |
| 5    | To run the replication rule, right-click the replication rule name in the left pane, and then click **Run**. Alternatively, you can schedule the replication rule to run at a specified time. |

**Specify the Destination Notification Server.**

**Specify the Credentials for accessing the target Notification Server.**

**Maximum rows** Specifies the maximum number of table rows to replicate.
rules, Data Connector sources and rules, etc. using the standalone Item Replication Rule with Replicate All (All selected items are replicated whether they have changed or not.) option selected to sync-up items and their permission settings for replicated Roles on destination Notification Server.

Using the standalone Item Replication Rule, you can replicate the following Symantec Management Platform items:

- Default and custom Automation Policies with custom tasks and shared schedules assigned
- Cleanup Task Data settings
- Cleanup Version Data settings
- Custom Client Tasks, Client Jobs, and Server Jobs with default or custom credentials and with default or custom schedules assigned
- Default and custom Cloud-enabled Management settings policies with default or custom resource targets
- Connector Purge Policy settings
- Custom Data Classes and Virtual Data Classes in default or custom folders with default or custom shared schedules assigned
- Custom Data Connectors sources and rules in default or custom folders
- Default and custom Filters in custom folders
- Global Agent Settings - Tickle Power Management, ACC, Remote Troubleshooting, Events
  Note that Remote troubleshooting password does not migrate.
- Default and custom Maintenance Policies in default or custom folders with default or custom resource targets
- Custom Symantec Management Console menus
- Default and custom Microsoft Active Directory Import rules with custom credentials and custom shared schedules assigned
- Notification Server Settings - Logs, Email, Proxy, Distribution Point Credentials
  Note that Application Identity does not migrate.
- Default and custom Organizational Views with Organizational Groups
- Default Package Server Settings policy with custom settings
- Purging Maintenance settings
- Default and custom Registration Policies in default or custom folders
- Stand-alone replication rules
- Default and custom **Reports** in custom folders
- **Resource History** settings
- Custom **Resource Targets** in default or custom folders
- Custom **Right-click Menu Actions** in default or custom folders
- Default and custom **Shared Schedules**
- Default and custom **Targeted Agent Settings** with default or custom resource targets
- **Task Agent Settings** policy with default or custom resource target assigned
- Default and custom **Task Server Settings** policies with default or custom resource targets
- Default and custom **Task Server Tokens**

Note that for some items, the **Item Replication Rule** automatically replicates all the dependencies of the replicated item. For example, if you replicate a Client Job that contains Client Tasks, and it has custom Schedule and custom Resource Target assigned, this Client Job gets replicated together with its Client Tasks and their credentials, custom Schedule, custom Resource Target, and Filters with Organizational Views and Groups which are in this Resource Target.

Similarly, the following Symantec Management Platform items are replicated with all of their dependencies:

- **Data Connector** sources and rules with custom schedule, filter, resource target, or report assigned
- **Microsoft Active Directory Import Rule** with custom credentials and schedule assigned
- **Policy** with a default or custom resource target assigned
- **Virtual Data Class** with custom schedule assigned

For more information about replicating solution-specific data, refer to the solution-specific content in Chapter 4 of this document.

This task is a step in the process for performing data migration using standalone replication.

See “Performing data migration using standalone replication” on page 11.
To configure and run standalone Item Replication Rule

1. In the Symantec Management Console, on the Settings menu, click Notification Server > Hierarchy.

2. In the left pane, expand Replication folder, right-click the Items folder, and then click New > Item Replication Rule.

3. On the New replication rule page, configure the settings as follows:

   **Item Replication Rule** settings

   **Specify the Items that you want to replicate.**

   1. At Items, click None selected.
   2. In the Select Items dialog box, under Available items, in the Group drop-down list, select the folder or the items that you want to replicate, and then click OK.

      Note that if you select a root folder, all items within the sub-folders are displayed. You can then select the items that you want to replicate.

   **Specify the Destination Notification Server.**

   1. At Destination, click Specified Notification Servers.
   2. In the Notification Servers dialog box, under Available Notification Servers, select the destination Notification Server from the list.
   3. (Optional) To add a new Notification Server, click Add Notification Server icon on the toolbar.

      In the Add a Notification Server by name or browse the network dialog box, type the host name or FQDN of the destination Notification Server, specify the Notification Server Web Site, and then click Add.

      If you want to use a non-default port for replication, you must specify the HTTP or HTTPS port as follows:

      Notification Server Name: domain-name.com
      Notification Server Web Site: https://domain-name.com:777/Altiris/NS/

   4. Click OK.

---

Performing data migration using standalone replication

17Migrating data using standalone replication
Specify the **Credentials** for accessing the target Notification Server.

1. At **Credentials**, click **Specified Credentials**.
   
2. In the **Credentials** dialog box, specify the credentials for source and target Notification Servers.

   Note that if you select **Use these credentials**, you must enter the credentials of a user with **Symantec Administrators** role on source and destination Notification Server.

3. Click **OK**.

Specify the replication options.

The replication options are as follows:

- **Replicate All**
  
  Lets you replicate all items, roles, or privileges regardless whether they have changed or not since previous replication. Every time your standalone replication rule runs, the selected items, roles, or privileges are unconditionally replicated to the destination Notification Servers that you specify.

- **Replicate If Changed**
  
  Lets you minimize the overhead of successive replications and skip the items, roles, or privileges that have not changed since previous replication.

- **Replicate Security Only**
  
  Applies to item replication rules only. Lets you only replicate security information (permissions) for selected items.

4. Click **Save changes**.

5. To run the replication rule, right-click the replication rule name in the left pane, and then click **Run**.

   Alternatively, you can schedule the replication rule to run at a specified time.

**Configuring and running standalone Resource Replication Rule**

Replicate the **Computers, Devices, Users, Sites, Subnets**, etc. along with their **Inventory Data Classes** data using the standalone **Resource Replication Rule**.

Note that **Resource Replication Rule** does not replicate Event Data Classes data for the selected resources.

For more information about replicating solution-specific data, refer to the solution-specific content in Chapter 4 of this document.
This task is a step in the process for performing data migration using standalone replication.

See “Performing data migration using standalone replication” on page 11.

To configure and run standalone Resource Replication Rules

1. In the Symantec Management Console, on the Settings menu, click Notification Server > Hierarchy.

2. In the left pane, expand Replication folder, right-click the Resources folder, and then click New > Resource Replication Rule.

3. On the New replication rule page, configure the settings as follows:

   **Resource Replication Rule settings**

   Specify the **Resource types** or **Resource targets** that you want to replicate.

   To specify the **Resource types**, do the following:
   1. At Resource types, click None selected.
   2. In the Select Resource Types dialog box, under Available items, in the Group drop-down list, select the resource types that you want to replicate, and then click OK.

   To specify the **Resource targets**, do the following:
   1. At Resource targets, click None selected.
   2. In the Select Resource Targets dialog box, under Available targets, in the Folder drop-down list, select the resource targets that you want to replicate, and then click OK.

   Specify the **Data Classes** that you want to replicate.

   1. At Data Classes, click None selected.
   2. In the Inventory Data Classes dialog box, under Available items, in the Group drop-down list, select the data classes that you want to replicate for selected resources, and then click OK.
Specify the **Destination Notification Server**.

1. At Destination, click **Specified Notification Servers**.

2. In the Notification Servers dialog box, under **Available Notification Servers**, select the destination Notification Server from the list.

3. (Optional) To add a new Notification Server, click **Add Notification Server** icon on the toolbar.

   In the **Add a Notification Server by name or browse the network** dialog box, type the host name or FQDN of the destination Notification Server, specify the **Notification Server Web Site**, and then click **Add**.

   If you want to use a non-default port for replication, you must specify the HTTP or HTTPS port as follows:

   - **Notification Server Name**: domain-name.com
   - **Notification Server Web Site**: https://domain-name.com:777/Altiris/NS/

4. Click **OK**.

Specify the **Credentials** for accessing the target Notification Server.

1. At **Credentials**, click **Specified Credentials**.

2. In the **Credentials** dialog box, specify the credentials for source and target Notification Servers.

   Note that if you select **Use these credentials**, you must enter the credentials of a user with **Symantec Administrators** role on source and destination Notification Server.

3. Click **OK**.

Configure **Data verification**.

   The **Maximum percent of data to verify during each replication** lets you reduce the load that is imposed on the server and can verify small amounts of resource data on every replication. You can specify a verification percentage in the replication rule. For example, if you verify 10% of the data for each replication, that ensures that all data has been verified after 10 replications.

   Symantec recommends using this option if a destination server has recently purged its event classes or if you have experienced network problems between the servers.
4 Click **Save changes**.

5 To run the replication rule, right-click the replication rule name in the left pane, and then click **Run**.

Alternatively, you can schedule the replication rule to run at a specified time.

### Configuring and running standalone Security Replication Rule

Replicate the **Roles** and **Accounts** using the standalone **Role Replication Rule**. The **Role Replication Rule** automatically replicates all accounts that are assigned to the replicated role as well as all roles that are members of the replicated role.

Note that you must replicate **Roles** before replicating the **Privileges**.

Replicate the **Privileges** using the standalone **Privileges Replication Rule**. After the replication, the privileges are automatically applied to the replicated roles. Each role gets the privileges that it has on the source Notification Server.

If you replicate a privilege of a product that does not exist on the destination Notification Server, the following warning message appears in the log of the destination Notification Server during the replication:


For more information about replicating solution-specific data, refer to the solution-specific content in Chapter 4 of this document.

This task is a step in the process for performing data migration using standalone replication.

See “Performing data migration using standalone replication” on page 11.

### To configure and run standalone Security Replication Rule

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

2 In the left pane, expand **Replication** folder, right-click **Security** folder, and then, depending on your requirement, click **New > Role Replication Rule** or **New > Privilege Replication Rule**.

3 On the **New replication rule** page, configure the settings as follows:
Specify the **Roles** or **Privileges** that you want to replicate.

To specify the **Roles**, do the following:

1. At **Roles**, click **None selected**.
2. In the **Select Roles** dialog box, under **Available items**, select the items that you want to replicate, and then click **OK**.

To specify the **Privileges**, do the following:

1. At **Privileges**, click **None selected**.
2. In the **Select Privileges** dialog box, under **Available items**, select the items that you want to replicate, and then click **OK**.

Specify the **Destination** Notification Server.

1. At **Destination**, click **Specified Notification Servers**.
2. In the **Notification Servers** dialog box, under **Available Notification Servers**, select the destination Notification Server from the list.
3. (Optional) To add a new Notification Server, click **Add Notification Server** icon on the toolbar.

In the **Add a Notification Server by name or browse the network** dialog box, type the host name or FQDN of the destination Notification Server, specify the **Notification Server Web Site**, and then click **Add**.

If you want to use a non-default port for replication, you must specify the HTTP or HTTPS port as follows:

- **Notification Server Name**: domain-name.com
- **Notification Server Web Site**: https://domain-name.com:777/Altiris/NS/

4. Click **OK**.

Specify the **Credentials** for accessing the target Notification Server.

1. At **Credentials**, click **Specified Credentials**.
2. In the **Credentials** dialog box, specify the credentials for source and target Notification Servers.

Note that if you select **Use these credentials**, you must enter the credentials of a user with **Symantec Administrators** role on source and destination Notification Server.

3. Click **OK**.
Specify the replication options. The replication options are as follows:

- **Replicate All**
  Lets you replicate all items, roles, or privileges regardless whether they have changed or not since previous replication. Every time your standalone replication rule runs, the selected items, roles, or privileges are unconditionally replicated to the destination Notification Servers that you specify.

- **Replicate If Changed**
  Lets you minimize the overhead of successive replications and skip the items, roles, or privileges that have not changed since previous replication.

4. Click **Save changes**.
5. To run the replication rule, right-click the replication rule name in the left pane, and then click **Run**.

Alternatively, you can schedule the replication rule to run at a specified time.

**Limitations of standalone replication in Symantec Management Platform**

Migrating Symantec Management Platform data using standalone replication has the following limitations:

- If you replicate **Cloud-enabled Management Settings** policy to the destination Notification Server where the **Cloud-enabled Management Agent IIS Website** is not created yet, the replicated **Cloud-enabled Management Settings** policy will be disabled and the following error message appears in the destination Notification Server logs:

  "Agent Site is not configured. Policy cannot be enabled: 'Windows 2008 clients - Cloud-enabled Management Settings' (4595932f-aecc-408a-9cc9-4e7f688e3df2\", "ClientInternetBasedManagementConfiguration", "Altiris.NS.StandardItems.dll", "53", "Warnings"

  To avoid this issue, create the **Cloud-enabled Management Agent IIS Website** on destination Notification Server before replicating the **Cloud-enabled Management Settings** policy.

- If you replicate custom Organizational Views with Organizational Groups that have Resources (Computers or Users) assigned but these Resources are not replicated to destination Notification Server, the association between custom
Organizational Views with Organizational Groups and the Resources breaks on the destination Notification Servers.
To avoid this issue, replicate the required Resources (Computers, Users, etc.) using the standalone **Resource Replication Rule** before replicating the Organizational Views with Organizational Groups using the standalone **Items Replication Rule**.

- Avoid migrating the following items using the standalone replication:
  - Default Data Classes
  - Default Filters
  - Default Reports
  - Default Resources
  - Default Resource Targets
  - Default Rollout Policies

- Migrating data using the standalone replication rules is supported from the following IT Management Suite versions only:
  - IT Management Suite 7.6 HF7
  - IT Management Suite 8.0 HF6

For more information about solution-specific limitation of standalone replication, refer to the solution-specific content in Chapter 4 of this document.
Migrating data using export and import

This chapter includes the following topics:

- Performing data migration using export and import
- Limitations of export and import in Symantec Management Platform

Performing data migration using export and import

You can migrate data using the manual export and import if you want to move individual items from one server to another.

If you need to move a large amount of data from one Notification Server to another, Symantec recommends using the standalone replication.

See “Performing data migration using standalone replication” on page 11.

Table 3-1 Process for performing data migration using export and import

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Install the required pointfix on the 7.6 HF7 source Notification Server.</td>
<td>To migrate data successfully, you must install the following pointfix on your 7.6 HF7 source Notification Server: <a href="http://www.symantec.com/docs/INFO3459">http://www.symantec.com/docs/INFO3459</a></td>
</tr>
<tr>
<td>Step 2</td>
<td>Synchronize the encryption keys.</td>
<td><strong>Warning:</strong> Before performing the export and import, you must move the encryption keys from the source Notification Server to the destination Notification Server. See “Moving the cryptographic keys from source Notification Server to destination Notification Server” on page 26.</td>
</tr>
</tbody>
</table>
### Table 3-1 Process for performing data migration using export and import (continued)

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 3</td>
<td>Export and import the required items manually.</td>
<td>You can migrate items and folders using manual export and import. See “Migrating data using manual export and import” on page 27. Note that migrating data using the export and import has some limitations. See “Limitations of export and import in Symantec Management Platform” on page 29. For more information about exporting and importing solution-specific data, refer to the solution-specific content in Chapter 4 of this document.</td>
</tr>
<tr>
<td>Step 4</td>
<td>(Optional) Use the ImportExportUtil.exe tool to export and import.</td>
<td>Alternatively, you can export and import the items and folders using the ImportExportUtil.exe tool. See “Migrating data using the ImportExportUtil.exe tool” on page 28.</td>
</tr>
</tbody>
</table>

### Moving the cryptographic keys from source Notification Server to destination Notification Server

You can back up the Notification Server cryptographic keys in Symantec Installation Manager, during the first-time installation of the Symantec products or after the installation.

In the Symantec Management Console of the destination Notification Server, you import the cryptographic keys.

This task is a step in the process for performing data migration using export and import.

See “Performing data migration using export and import” on page 25.

**To back up the cryptographic keys of source Notification Server**

1. On source Notification Server, in Symantec Installation Manager, on the Installed Products page, click **Back up Notification Server Cryptographic Keys**.

2. On the Back up or Restore Notification Server Cryptographic Keys page, do the following:
   - Select **Perform backup**.
   - Browse and select the location where you want the backup file to be stored.
   - Provide a password for the cryptographic keys backup file.
To import the cryptographic keys to destination Notification Server

1. In the Symantec Management Console of the destination Notification Server, on the Settings menu, click All Settings.

2. In the left pane, under Settings folder, expand Notification Server, and then click Notification Server Settings.

3. On the Notification Server Settings page, on the Encryption Keys Management tab, click Import, choose the backup file to import, type the encryption password, click OK, and then click Save changes.

Migrating data using manual export and import

You can migrate single items and folders using manual export and import. If you export and import a folder, all its subfolders are also exported and imported.

You can manually export and import the following Symantec Management Platform items:

- Automation Policies
- Cleanup Task Data policy
- Cleanup Version Data policy
- Cloud-enabled Management Settings policies
- Communication Profiles
- Editable Data Classes
- Virtual Data Classes
- Data Connector sources and rules
- Filters
- Folders
- Maintenance Window policies
- Organizational Views and Organizational Groups
- Registration policies
- Reports
- Resource Lookup Keys
- Resource Targets
- Custom Right-click Actions
Server and Client Jobs
Server and Client Tasks
Task Agent Settings policy
Task Service Settings policies

For more information about exporting and importing solution-specific data, refer to the solution-specific content in Chapter 4 of this document.

This task is a step in the process for performing data migration using export and import.

See “Performing data migration using export and import” on page 25.

To migrate data using manual export and import

1. On the source Notification Server, in the Symantec Management Console, navigate to the item that you want to export.
2. In the left pane, right-click the item that you want to export, and then click Export.
3. Click Save.
   To change the default location of the exported file, click Save As, select the required location, and then click Save.
4. In the Symantec Management Console of the destination Notification Server, navigate to the location where you want to place the imported item.
5. In the left pane, right-click the location, and then click Import.
6. In the Import Item dialog box, choose the XML file to import, and then click OK.

Migrating data using the ImportExportUtil.exe tool

You can use the ImportExportUtil.exe tool to migrate single items or folders. If you export and import a folder, all its subfolders with their items are also exported and imported.

For more information about exporting and importing solution-specific data, refer to the solution-specific content in Chapter 4 of this document.

This task is an optional step in the process for performing data migration using export and import.

See “Performing data migration using export and import” on page 25.
To migrate data using `ImportExportUtil.exe` tool

1. On the source Notification Server, navigate to the item that you want to export, and to the following:
   - Right-click the item, and then click **Properties**.
   - In the **Properties** dialog box, copy the **Guid** of the item.

2. On the source Notification Server, at the command prompt, go to the following location:
   ```
   %InstallDir%\Notification Server\Bin\Tools\
   ```

3. Use the following command to perform the export:
   ```
   /export <Item OR Folder GUID to export> <Path to export destination folder>
   ```
   Use the `/?` command to see the `ImportExportUtil.exe` help.

4. On the destination Notification Server, at the command prompt, go to the following location:
   ```
   %InstallDir%\Notification Server\Bin\Tools\
   ```

5. Use the following command to perform the import:
   ```
   /import <Import path to either item.xml file OR directory>
   ```

**Limitations of export and import in Symantec Management Platform**

The following Symantec Management Platform items cannot be exported and imported between Notification Servers:

- Domain Membership/WINS
- Global Agent Settings
- Microsoft Active Directory Import rules
- Notification Server Settings
- Package Server Settings
- Purging Maintenance
- Resource History
- Resource Membership Update
- Shared Schedules
Symantec Management Console menus

Tokens

Avoid migrating the following items using the export and import:

- Default Data Classes
- Default Filters
- Default Reports
- Default Resources
- Default Resource Targets
- Default Rollout Policies

When you export and import the items below, you must consider the following limitations:

- Before you import an Automation Policy, you must import the tasks and the reports that are used in this Automation Policy.
- After you import a task with custom credentials, you must manually re-enter the credentials of this imported task.
- You must import the Roles and Accounts one by one. You cannot import several Roles or Accounts at once.
- If you import Cloud-enabled Management policy to Notification Server that has no Cloud-enabled Management Web Site created yet, the Cloud-enabled Management policy will be disabled.
- Before you import Resource Targets, you must import all dependent Filters, Organizational Views, and Organizational Groups.
- Import all required Resource Targets before importing the policies. If you import the policies before importing the Resource Targets, they will be without these resource targets.
- Manual export does not automatically detect referenced Items of exported Items. For example, if you manually export a report that has a drill-down report, the drill-down report does not get exported. Also, if you manually export a Filter that has other referenced Filters, the referenced other Filters do not get exported.
- The default value of maxRequestLength is 10240 in the Web.config file, If you import an XML file that is larger than 10 MB, you get the following error in the Symantec Management Console and in the Notification Server logs:

HTTP Request failed:
/Altiris/NS/Admin/Menu Items/ImportItem.aspx?ParentGuid=...
Maximum request length exceeded.
To work around this issue, increase the default value of `maxRequestLength` to required size in the `Web.config` file, and save the changes. The file is located at: `<Install Dir>\Altiris\Notification Server\Web\`

Manual export and import of Item security settings have the following limitations:

- For each manually imported Item, the `<ownerNSGuid>` of destination Notification Server is automatically set.
- Manually exported and imported Items lose the security permission settings on destination Notification Server and only `Symantec Administrators` role will automatically have all security permissions for them.
- Manually imported Roles will lose their privileges and permissions, so you must manually configure the privileges and permissions settings for each imported Role on destination Notification Server.

For more information about solution-specific limitations of export and import, refer to the solution-specific content in Chapter 4 of this document.
Migrating data of IT Management Suite solutions and components

This chapter includes the following topics:

- Migrating Asset Management Solution Data
- Migrating Deployment Solution data using manual export and import and replication methods
- Migrating Inventory Solution data using standalone replication
- Migrating Inventory Solution data using manual export and import
- Migrating Patch Management Solution data using standalone replication
- Migrating Patch Management Solution data using manual export and import
- Migrating Software Management Solution data
- About migrating software components
- Migrating physical packages using Symantec Notification Server Migration Wizard
- Migrating software components using the Software Resource Replicator utility
- Migrating ITMS Management Views Data
- Migrating Real-Time System Management Data
- Migrating IT Analytics Server and content pack Data
- Migrating Server Management Suite component data
Migrating Monitor Solution data

Migrating Virtual Machine Management data

Migrating Power Scheme Task component data

Migrating Workflow Solution

Migrating Asset Management Solution Data

Data migration using the standalone replication rules is not supported for Asset Management Solution data.

You can migrate data using the manual export and import method.

See "Migrating data using manual export and import" on page 27.

When you export/import the items below, consider the following limitations:

- You cannot export a folder with several items. You must export Asset items one by one using the right-click menu option.
- After you export Software License, the default Software License Rule is not assigned.
  To assign a license rule, click Click to select… next to License Rule in the Software License Details dialog box.

Migrating Deployment Solution data using manual export and import and replication methods

From IT Management Suite 8.0 HF4 release onwards you can migrate data from Deployment Solution 7.6 HF7 and 7.5 SP1 latest updates. For more information, refer to the following articles:

http://www.symantec.com/docs/TECH227363
http://www.symantec.com/docs/TECH234364

Deployment Solution supports the export/import and replication method to migrate the settings, packages, and tasks.

Prerequisites to migrate Deployment Solution data

- Migrate the encryption keys.
  See "Moving the cryptographic keys from source Notification Server to destination Notification Server" on page 26.
Navigate to `Altiris\Notification Server\Bin\Tools\NSConfigurator` tool on the destination Notification Server and enable core settings `ReplicationOverwriteSourceNS`.

### Table 4-1: Process for migrating Deployment Solution data using manual Export/Import and Replication

<table>
<thead>
<tr>
<th>Step</th>
<th>Action</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Migrate Deployment Solution Settings</td>
<td>Migrating settings includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Global Settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- See &quot;Migrating Global Settings&quot; on page 34.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- OS Licenses</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- See &quot;Migrating OS Licenses&quot; on page 35.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Predefined Computers</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- See &quot;Migrating Predefined Computers&quot; on page 35.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- System Configuration</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- See &quot;Migrating System Configuration&quot; on page 35.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- OS Files Settings</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- See &quot;Migrating OS Files Settings&quot; on page 36.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Image Multicasting</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- See &quot;Migrating Image Multicasting&quot; on page 37.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Preboot Configurations</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- See &quot;Migrating Preboot Configurations &quot; on page 37.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Migrate Deployment Solution Packages</td>
<td>Migrating Deployment Solution Packages includes:</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Image Packages</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- See &quot;Migrating Image Packages&quot; on page 38.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- Copy File resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- See &quot;Migrating Copy File Resources&quot; on page 39.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- PCT resources</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- See &quot;Migrating PCT resources&quot; on page 39.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Migrate Tasks and Jobs</td>
<td>Migrate the tasks and jobs that you want using the export/import procedure.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>- See &quot;Migrating data using manual export and import&quot; on page 27.</td>
</tr>
</tbody>
</table>

**Migrating Settings**

**Migrating Global Settings**

1. In the Symantec Management Console of the source Notification Server, navigate to **Settings > Deployment > Global Settings**.
2. Right-click on **Global Settings** and select **Export**.
3. Save and copy the XML on the destination computer.
Navigate to **Settings > All Settings** of the destination computer and right-click on the **Deployment** node and select import.

In the **Import Item** dialog box, browse and select the XML file to import.

**Migrating OS Licenses**

1. In the Symantec Management Console of the source Notification Server, navigate to **Settings > All Settings**.
2. In the **Settings** pane, navigate to **Notification Server > Hierarchy and Replication > Replication > Items**.
3. Right-click on the **Items** icon and select **New > Item Replication Rule**.
4. In the **New replication rule** page, click the link next to **Items**.
5. In the **Select Items** window, select **Group** as **Settings** from the drop-down menu.
6. Navigate to **Deployment > OS Licenses** and click the > icon to include the OS Licenses in the **Selected items** pane.
7. Click **OK**.
8. In the **New replication rule** page, click the link next to **Destination**.
9. In the **Notification Server** window, click on the add icon and enter the name of the target Notification Server and Notification Server website.
10. In the **New replication rule** page, click the link next to **Credentials**.
11. In the **All Settings** pane, right-click on the New replication rule and select **Run**.

**Migrating Predefined Computers**

1. From the source Notification Server, copy the predefined CSV file to the destination Notification Server computer.
2. Launch the Symantec Management Console on the target Notification Server computer and navigate to **Settings > Deployment > Predefined Computers**.
3. In the **Predefined Computers** window, click **Import Computers** and select the CSV file.

**Migrating System Configuration**

1. In the Symantec Management Console of the source Notification Server, navigate to **Settings > Deployment > System Configurations**.
2. Right-click on **System Configurations** and select **Export**.
3. Save the exported XML file and copy it on the destination Notification Server.
4 On the target Notification Server computer, navigate to Settings > Deployment.

5 Right-click on the Deployment node, click Import and enter the path of the XML.

**Migrating OS Files Settings**

1 In the Symantec Management Console of the source Notification Server, navigate to Settings > All Settings.

---

**Note:** Copy the package from the following path of the source Notification server to the same folder structure of the destination computer:

```
%Altiris Install Dir%\Altiris\Notification Server\NSCap\bin\Deployment\Packages\SOI
```

2 In the Settings pane, navigate to Notification Server > Hierarchy and Replication > Replication > Resources.

3 Right-click on the Resources and select New > Resource Replication Rule.

4 In the New replication rule page, select Resource types and click the link next to it.

5 If you select the ResourceType, in the Select Resource Types window, select Group as Settings from the drop-down menu.

6 Navigate to Deployment > OS Licenses and click the > icon to include the OS Licenses in the Selected items pane.

7 Click OK.

8 In the New replication rule page, click the link next to Data Classes.

9 From Inventory Data Classes, select Data Classes > Software Management > OS File Resource Component.

10 In the Notification Server window, click on the add icon and enter the name of the target Notification Server and the Notification Server Web Site.

11 In the New replication rule page, click the link next to Credentials.

12 In the All Settings pane, right-click on the New replication rule and select Run.

OS Files setting will migrate on the destination computer.

Copy the package from the source to the destination computer with the same folder structure.
Migrating Image Multicasting

1. In the Symantec Management Console of the source Notification Server, navigate to Settings > Deployment > Image Multicasting.
2. Right-click on Image Multicasting, select Export and save the output XML file.
3. Copy the XML on the destination computer.
4. On the target computer, navigate to Settings > Deployment. Right-click on the Deployment and select import. In the window, provide the path of the XML.

Migrating Preboot Configurations

Note: The ADK, that is installed on the destination computer should be same as the ADK that is imported into Deployment Solution and is updated on the NBS site servers.

1. In the Symantec Management Console of the source Notification Server, navigate to Settings > All Settings > Notification Server > Hierarchy and Replication > Replication > Items.
2. Right-click on the Item and select New Item replication rule.
3. In the New replication rule page, click the link next to Items.
4. Select Settings > Deployment from the Group drop down and select Preboot Configurations.
5. In Notification Server window, click the add icon and enter the name of the target Notification Server and Notification Server website.
6. In the New replication rule page, click the link next to Credentials.
7. Select Replicate All option and click Save changes.
8. Right-click on the New Item replication rule and select Run.

Note: PXE images are created on the NBS site server. You must recreate the automation folders on the destination computers.

To migrate NBS General Settings and NBS Global Settings, ensure that Preboot Configurations are replicated on the destination computers.
Migrating NBS General Settings and NBS Global Settings

1. In the Symantec Management Console of the source Notification Server, navigate to Settings > Notification Server > Site Server Settings > Network Boot Service Settings > Settings.

2. Right-click on NBS General Settings and select Export. Save the exported XML. Repeat the steps for NBS Global Settings.

3. Copy the exported XML files on the destination computer.

4. On the destination computer, navigate to Settings > Notification Server > Site Server Settings > Network Boot Service Settings > Settings. Right-click on the Settings and select Import to import the NBS General Settings and NBS Global Settings.

Migrating Deployment Solution packages

Migrating Image Packages

1. From the source Notification Server, copy the various images to the destination Notification Server from the following path:

   %Altiris Install Dir%\Altiris\Notification Server\NSCap\bin\Deployment\Packages\Images

   Images that are stored on a Site Server, can be accessed by pointing the Site Servers to the new Notification Server.

2. Enable the ReplicationOverwriteSourceNS setting on the destination computer. To access the tool navigate to Altiris\Notification Server\Bin\Tools\NSConfigurator tool and select Core settings > Replication Settings > ReplicationOverwriteSourceNS on destination Notification Server and enable it.

3. Run the query to change Replication Mode on the 7.6 HF7 setup or install the v5.1 rollup.

   UPDATE [ResourceTypeDataClassReplication] SET [ReplicationMode] = 1 WHERE [ResourceDataClassGuid] IN ('e32ba902-73ad-480a-94f9-aafa05db5ad5', '81edc8dd-c6fe-4a7b-bf2c-3603ac22d2cf', 'AFCAFF44-7E3E-49ad-9AC8-D6BC3F22ED52')


5. In the ResourceType, select Image Resource.
6 In the **Data class**, select **Image Resource Component** from the **Software Management Component** folder. Provide Notification Server credential for the destination Notification Server and **Run** the replication rule.

7 Connect the Site Servers of the older Notification Server to the new Notification Server. This causes all the Image resources being replicated to destination Notification Server. Navigate to **Settings > Deployment > Disk Images** to validate if the resources are imported.

**Migrating Copy File Resources**

- Copy the image resources from the following location of source Notification Server computer to the destination Notification Server:

  ```
  %Altiris Install Dir%\Altiris\Notification Server\NSCap\bin\Deployment\Packages\CopyFile
  ```

The Copy File resources that are on the Site Server, can be accessed by pointing the Site Servers to the new Notification Server.

Export the file at **Settings > Deployment > Copy File Contents**.

Change all the paths by replacing the source Notification Server name by the destination Notification Server name by opening each software resource and saving it.

**Migrating PCT resources**

1 Copy the PCT packages from the following location from source Notification Server to the destination Notification Server:

  ```
  %Altiris Install Dir%\Altiris\Notification Server\NSCap\bin\Deployment\Packages\PCT
  ```

PCT packages that are stored on a Site Server, can be accessed by pointing the Site Servers to the new Notification Server.

2 Enable the **ReplicationOverwriteSourceNS** setting on the destination computer. Navigate to **Altiris\Notification Server\Bin\Tools\NSConfigurator tool**. Select the **Core settings > Replication Settings > ReplicationOverwriteSourceNS** on destination Notification Server and enable it.

3 Run the query to change Replication Mode at 7.6 HF7 setup or install the v5.1 roll up. **UPDATE** [ResourceTypeDataClassReplication] **SET**

   ```
   [ReplicationMode] = 1 WHERE [ResourceDataClassGuid] IN ('e32ba902-73ad-480a-94f9-aafa05db5ad5',
   '81edc8dd-c6fe-4a7b-bf2c-3603ac22d2cf',
   'AFCAFF44-7E3E-49ad-9AC8-D6BC3F22ED52')
   ```

**Migrating data of IT Management Suite solutions and components**

**Migrating Deployment Solution data using manual export and import and replication methods**

5 To replicate all the PCT resources to the destination Notification Server, connect the Site Servers connected to older Notification Server to the new Notification Server.

6 To run the tasks, export the Distribute Personality task from the parent Notification Server and import it on destination Notification Server at Deployment folder.

Migrating Inventory Solution data using standalone replication

See “About data migration” on page 9.

See “Performing data migration using standalone replication” on page 11.

The following Inventory Solution components can be migrated using standalone replication:

See Table 4-2 on page 41.

The following Inventory Solution components cannot be migrated using standalone replication:

See Table 4-3 on page 46.
Table 4-2  Migrating Inventory Solution components using standalone replication

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Predefined and custom inventory policies | To migrate predefined and custom inventory policies using the standalone Item Replication Rule, do the following:  
  ■ To configure and run the standalone Item Replication Rule, perform the steps in the following topic:  
    See “Configuring and running standalone Item Replication Rule” on page 14.  
  ■ While you specify the Items that you want to replicate, click Policies > Discovery and Inventory > Inventory, and then select the required inventory policies.  

  **Note:** If you migrate from 7.6 HF7, policy credentials may not be re-encrypted, and the affected policy may become disabled. For example, policy credentials are not re-encrypted if FIPS mode is enabled on your destination Notification Server.  
  ■ If policy credentials are not re-encrypted, the following error message appears on the policy page:  
    At least one of credentials defined in policy have been reset to default values, policy has been disabled. Please review and adjust credentials information before enabling policy.  
  ■ The affected credentials are reset to the following default values:  
    ■ If the password for Specified User fails to be re-encrypted, the Run As option is set to SYSTEM.  
    ■ If the passwords for Oracle and MySQL fail to be re-encrypted, the affected Oracle and MySQL credentials are removed.  

  If policy credentials are not re-encrypted, you need to re-enter the credentials and save changes in the policy.
Table 4-2  Migrating Inventory Solution components using standalone replication (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gather Inventory</td>
<td>To migrate Gather Inventory tasks using the standalone Item Replication Rule, do the following:</td>
</tr>
<tr>
<td></td>
<td>■ To configure and run the standalone Item Replication Rule, perform the steps in the following topic: \</td>
</tr>
<tr>
<td></td>
<td>See “Configuring and running standalone Item Replication Rule” on page 14. \</td>
</tr>
<tr>
<td></td>
<td>■ While you specify the Items that you want to replicate, click Tasks &gt; Jobs and Tasks, and then select the required Gather Inventory tasks. \</td>
</tr>
<tr>
<td>Note: If you migrate from 7.6 HF7, the credentials for a specified user, Oracle, and MySQL databases may not be re-encrypted, and the following events may occur: \</td>
<td></td>
</tr>
<tr>
<td></td>
<td>■ One or both of the following error messages appear in the Notification Server logs: \</td>
</tr>
<tr>
<td></td>
<td>■ 'Run as' credentials defined in task have been reset to default values. Please review and adjust credentials information before task execution: Cannot decrypt context password for task: &lt;task guid&gt; \</td>
</tr>
<tr>
<td></td>
<td>■ Database credentials defined in task have been removed. Please review and adjust credentials information before task execution: Cannot decrypt database password for task: &lt;task guid&gt; \</td>
</tr>
<tr>
<td></td>
<td>■ The affected credentials are reset to the following default values: \</td>
</tr>
<tr>
<td></td>
<td>■ If the password for Specified User fails to be re-encrypted, the Run As option is set to SYSTEM.</td>
</tr>
<tr>
<td></td>
<td>■ If the passwords for Oracle and MySQL fail to be re-encrypted, the affected Oracle and MySQL credentials are removed.</td>
</tr>
<tr>
<td>If the credentials are not re-encrypted, you need to re-enter the credentials and save changes in the task.</td>
<td></td>
</tr>
</tbody>
</table>
### Table 4-2  Migrating Inventory Solution components using standalone replication (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Custom inventory tasks                   | Before the replication of custom inventory tasks, you must replicate the custom inventory data classes that you use in the tasks. To migrate custom inventory data classes using the standalone Item Replication Rule, do the following:  
  - To configure and run the standalone Item Replication Rule, perform the steps in the following topic:  
    See “Configuring and running standalone Item Replication Rule” on page 14.  
  - While you specify the Items that you want to replicate, click Settings > Notification Server > Resource and Data Class Settings > Data Classes > Inventory > Custom, and then select the required custom data classes that you want to replicate.  
  To migrate custom inventory tasks using the standalone Item Replication Rule, do the following:  
  - To configure and run the standalone Item Replication Rule, perform the steps in the following topic:  
    See “Configuring and running standalone Item Replication Rule” on page 14.  
  - While you specify the Items that you want to replicate, select the required inventory tasks in the Tasks folder. |
| Data from predefined inventory data classes | You can use inventory policies or tasks to gather new inventory data on your destination Notification Server computer. If you want to keep old inventory data from your source Notification Server computer, you may migrate old data from predefined inventory data classes.  
  To migrate data from predefined inventory data classes using the standalone Resource Replication Rule, do the following:  
  - To configure and run the standalone Resource Replication Rule, perform the steps in the following topic:  
  - While you specify the Resource types or Resource targets, select Computer or the target that contains only the computers for which you want to migrate the data.  
  - While you specify the Data Classes that contain the data you want to replicate, select the data classes that are located in the Inventory folder. |
| Application metering policies            | To migrate application metering policies using the standalone Item Replication Rule, do the following:  
  - To configure and run the standalone Item Replication Rule, perform the steps in the following topic:  
    See “Configuring and running standalone Item Replication Rule” on page 14.  
  - While you specify the Items that you want to replicate, click Policies, navigate to the application metering policies that you want to replicate, and select the policies. |
Before the replication of targeted software inventory policies, you must migrate the following dependencies:

- Software components that are included into targeted software inventory policies
- Detection rules that are associated to the software components

See "About migrating software components" on page 60.

To migrate targeted software inventory policies using the standalone Item Replication Rule, do the following:

- To configure and run the standalone Item Replication Rule, perform the steps in the following topic:
  See "Configuring and running standalone Item Replication Rule" on page 14.
- While you specify the Items that you want to replicate, click Policies, navigate to the targeted software inventory policies that you want to replicate, and select the policies.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Targeted software inventory policies | Before the replication of targeted software inventory policies, you must migrate the following dependencies:  
  - Software components that are included into targeted software inventory policies  
  - Detection rules that are associated to the software components  
  See "About migrating software components" on page 60.  
  To migrate targeted software inventory policies using the standalone Item Replication Rule, do the following:  
  - To configure and run the standalone Item Replication Rule, perform the steps in the following topic:  
    See "Configuring and running standalone Item Replication Rule" on page 14.  
  - While you specify the Items that you want to replicate, click Policies, navigate to the targeted software inventory policies that you want to replicate, and select the policies. |
<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Software-based usage tracking: software products and usage-tracking data | To migrate the software products that are configured for software-based usage tracking, use the standalone **Resource Replication Rule** as follows:  
- To configure and run the standalone **Resource Replication Rule**, perform the steps in the following topic:  
- While you specify the **Resource types** or **Resource targets**, select **Software Product** or the targets that contain the required software products.  
You can track usage of a migrated software product only if the following requirements are met:  
- The software product has the association with at least one software component that is installed and discovered in your environment.  
- At least one software component in the software product has the association with a key program file.  
You need to run software inventory on managed computers to discover and gather software inventory data. If the software products, software components, and the key program files have the required associations created automatically on the source Notification Server, the same associations are automatically created on destination Notification Server after all the required software inventory data is entered into the Configuration Management Database.  
**Note:** You need to create associations manually for the key program files that have been manually associated to the software components on your source Notification Server.  
For more information, see the topics about tracking usage of the managed software products in the *Inventory Solution User Guide* at the following URL:  
http://www.symantec.com/docs/DOC8636 |
| The installation, upgrade, and uninstall policies for Inventory Plug-in, Application Metering Plug-in, and Inventory Pack for Servers Plug-in | To migrate the policies for Inventory Plug-in, Application Metering Plug-in, and Inventory Pack for Servers Plug-in using the standalone **Item Replication Rule**, do the following:  
- To configure and run the standalone **Item Replication Rule**, perform the steps in the following topic:  
  See “Configuring and running standalone Item Replication Rule” on page 14.  
- While you specify the **Items** that you want to replicate, click **Settings > Agents/Plug-ins > Discovery and Inventory > Windows/UNIX/Linux/Mac**, navigate to the policy that you want to replicate, and select the policy. |
To migrate custom inventory reports using the standalone Item Replication Rule, do the following:

- To configure and run the standalone Item Replication Rule, perform the steps in the following topic:
  See “Configuring and running standalone Item Replication Rule” on page 14.
- While you specify the Items that you want to replicate, click Reports, navigate to the reports that you want to replicate, and select the reports.

**Note:** The migrated inventory reports present the information only after the corresponding data classes get populated with data.

---

### Table 4-3  Inventory Solution components that you cannot migrate using standalone replication

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stand-alone inventory packages</td>
<td>Migration of stand-alone inventory packages is not supported.</td>
</tr>
</tbody>
</table>
| File and registry baseline tasks | You can manually copy configuration and snapshot files from the following locations on your source Notification Server computer:  
\`\`\`\`localhost\NSCap\bin\Win32\X86\Inventory\Application Management\FileBaselinePackage  
\`\`\`\`localhost\NSCap\bin\Win32\X86\Inventory\Application Management\RegBaselinePackage  
Then you can paste the files to same locations on your destination Notification Server computer and use them to re-create your baseline tasks. |
| Agentless inventory tasks | You can export custom SNMP data mapping tables from the **SNMP Data Mapping Tables** page on your source Notification Server computer. Then you can import the tables to your destination Notification Server computer and create new agentless inventory task to collect inventory on required devices. |

---

**Migrating Inventory Solution data using manual export and import**

See “About data migration” on page 9.
The following Inventory Solution components can be migrated using export and import options:

See Table 4-4 on page 47.

The following Inventory Solution components cannot be migrated using export and import options:

See Table 4-5 on page 52.

Table 4-4  Migrating Inventory Solution components using manual export and import

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Predefined and custom inventory policies</td>
<td>Before migrating the policy that uses custom targets, you must migrate the policy targets separately.</td>
</tr>
<tr>
<td></td>
<td>To migrate predefined and custom inventory policies using manual export and import, perform the steps in the following topic:</td>
</tr>
<tr>
<td></td>
<td>See “Migrating data using manual export and import” on page 27.</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: If you migrate from 7.6 HF7, policy credentials may not be re-encrypted, and the affected policy may become disabled. For example, policy credentials are not re-encrypted if FIPS mode is enabled on your destination Notification Server.</td>
</tr>
<tr>
<td></td>
<td>■ If policy credentials are not re-encrypted, the following error message appears on the policy page:</td>
</tr>
<tr>
<td></td>
<td><strong>At least one of credentials defined in policy have been reset to default values, policy has been disabled. Please review and adjust credentials information before enabling policy.</strong></td>
</tr>
<tr>
<td></td>
<td>■ The affected credentials are reset to the following default values:</td>
</tr>
<tr>
<td></td>
<td>■ If the password for <strong>Specified User</strong> fails to be re-encrypted, the <strong>Run As</strong> option is set to <strong>SYSTEM</strong>.</td>
</tr>
<tr>
<td></td>
<td>■ If the passwords for Oracle and MySQL fail to be re-encrypted, the affected Oracle and MySQL credentials are removed.</td>
</tr>
<tr>
<td></td>
<td>If policy credentials are not re-encrypted, you need to re-enter the credentials and save changes in the policy.</td>
</tr>
<tr>
<td>Component</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------</td>
<td>--------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Gather Inventory tasks</td>
<td>To migrate <strong>Gather Inventory</strong> tasks using manual export and import, perform the steps in the following topic: See &quot;Migrating data using manual export and import&quot; on page 27. Note: If you migrate from 7.6 HF7, the credentials for a specified user, Oracle, and MySQL databases may not re-encrypted, and the following events may occur:</td>
</tr>
<tr>
<td></td>
<td>- One or both of the following error messages appear in the Notification Server logs:</td>
</tr>
<tr>
<td></td>
<td>- 'Run as' credentials defined in task have been reset to default values. Please review and adjust credentials information before task execution: Cannot decrypt context password for task: &lt;task guid&gt;</td>
</tr>
<tr>
<td></td>
<td>- Database credentials defined in task have been removed. Please review and adjust credentials information before task execution: Cannot decrypt database password for task: &lt;task guid&gt;</td>
</tr>
<tr>
<td></td>
<td>- The affected credentials are reset to the following default values:</td>
</tr>
<tr>
<td></td>
<td>- If the password for <strong>Specified User</strong> fails to be re-encrypted, the Run As option is set to <strong>SYSTEM</strong>.</td>
</tr>
<tr>
<td></td>
<td>- If the passwords for Oracle and MySQL fail to be re-encrypted, the affected Oracle and MySQL credentials are removed.</td>
</tr>
<tr>
<td></td>
<td>If the credentials are not re-encrypted, you need to re-enter the credentials and save changes in the task.</td>
</tr>
</tbody>
</table>
To migrate custom inventory tasks using manual export and import, perform the steps in the following topic:

See "Migrating data using manual export and import" on page 27.

After you import the custom inventory tasks, do the following:

- You need to migrate the custom inventory data classes that you use in the tasks.

To migrate custom inventory data classes using manual export and import, perform the following steps in order:

- On the source Notification Server, in the Symantec Management Console, click **Settings > All Settings**.
- In the left pane, under **Settings**, expand **Notification Server > Resource and Data Class Settings > Data Classes > Inventory > Custom**, right-click the data class that you want to export, and then click **Export**.
- Click **Save**.
- In the Symantec Management Console of the destination Notification Server, click **Settings > All Settings**, and in the left pane, under **Settings**, expand **Notification Server > Resource and Data Class Settings > Data Classes > Inventory > Custom**. In the left pane, right-click the location, and then click **Import**. In the **Import Item** dialog box, choose the XML file to import, and then click **OK**.

- For the custom inventory tasks that have specified **Run As** credentials, you may need to re-enter the credentials and save changes in the task.
- For the custom inventory tasks that have configured schedules, you must manually re-configure the schedules and save changes in the task.

**Note:** After you run the imported custom inventory tasks, you can view gathered inventory data in custom reports and the **Resource Manager**. However, you cannot view the imported data class on the **Manage Custom Data classes** page.

### Application metering policies

Before migrating the policy that uses custom targets, you must migrate the policy targets separately.

To migrate application metering policies using manual export and import, perform the steps in the following topic:

See "Migrating data using manual export and import" on page 27.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom inventory tasks</td>
<td>To migrate custom inventory tasks using manual export and import, perform the steps in the following topic:</td>
</tr>
<tr>
<td></td>
<td>See &quot;Migrating data using manual export and import&quot; on page 27.</td>
</tr>
<tr>
<td></td>
<td>After you import the custom inventory tasks, do the following:</td>
</tr>
<tr>
<td></td>
<td>- You need to migrate the custom inventory data classes that you use in the tasks.</td>
</tr>
<tr>
<td></td>
<td>To migrate custom inventory data classes using manual export and import, perform the following steps in order:</td>
</tr>
<tr>
<td></td>
<td>- On the source Notification Server, in the Symantec Management Console, click <strong>Settings &gt; All Settings</strong>.</td>
</tr>
<tr>
<td></td>
<td>- In the left pane, under <strong>Settings</strong>, expand <strong>Notification Server &gt; Resource and Data Class Settings &gt; Data Classes &gt; Inventory &gt; Custom</strong>, right-click the data class that you want to export, and then click <strong>Export</strong>.</td>
</tr>
<tr>
<td></td>
<td>- Click <strong>Save</strong>.</td>
</tr>
<tr>
<td></td>
<td>- In the Symantec Management Console of the destination Notification Server, click <strong>Settings &gt; All Settings</strong>, and in the left pane, under <strong>Settings</strong>, expand <strong>Notification Server &gt; Resource and Data Class Settings &gt; Data Classes &gt; Inventory &gt; Custom</strong>. In the left pane, right-click the location, and then click <strong>Import</strong>. In the <strong>Import Item</strong> dialog box, choose the XML file to import, and then click <strong>OK</strong>.</td>
</tr>
<tr>
<td></td>
<td>- For the custom inventory tasks that have specified <strong>Run As</strong> credentials, you may need to re-enter the credentials and save changes in the task.</td>
</tr>
<tr>
<td></td>
<td>- For the custom inventory tasks that have configured schedules, you must manually re-configure the schedules and save changes in the task.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> After you run the imported custom inventory tasks, you can view gathered inventory data in custom reports and the <strong>Resource Manager</strong>. However, you cannot view the imported data class on the <strong>Manage Custom Data classes</strong> page.</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Application metering policies</th>
<th>Before migrating the policy that uses custom targets, you must migrate the policy targets separately.</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>To migrate application metering policies using manual export and import, perform the steps in the following topic:</td>
</tr>
<tr>
<td></td>
<td>See &quot;Migrating data using manual export and import&quot; on page 27.</td>
</tr>
</tbody>
</table>
Before migrating targeted software inventory policies, you must migrate the following dependencies:

- Custom policy targets if you use them in the policy
  See “Migrating data using manual export and import” on page 27.
- Software components that are included in the targeted software inventory policies
  See “About migrating software components” on page 60.
- Detection rules that are associated to the software components
  See “About migrating software components” on page 60.

To migrate targeted software inventory policies using manual export and import, perform the steps in the following topic:

See “Migrating data using manual export and import” on page 27.

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Targeted software inventory policies</td>
<td>Before migrating targeted software inventory policies, you must migrate the following dependencies:</td>
</tr>
<tr>
<td></td>
<td>- Custom policy targets if you use them in the policy</td>
</tr>
<tr>
<td></td>
<td>See “Migrating data using manual export and import” on page 27.</td>
</tr>
<tr>
<td></td>
<td>- Software components that are included in the targeted software inventory policies</td>
</tr>
<tr>
<td></td>
<td>See “About migrating software components” on page 60.</td>
</tr>
<tr>
<td></td>
<td>- Detection rules that are associated to the software components</td>
</tr>
<tr>
<td></td>
<td>See “About migrating software components” on page 60.</td>
</tr>
<tr>
<td></td>
<td>To migrate targeted software inventory policies using manual export and import, perform the steps in the following topic:</td>
</tr>
<tr>
<td></td>
<td>See “Migrating data using manual export and import” on page 27.</td>
</tr>
</tbody>
</table>
To migrate software products that are configured for software-based usage tracking, use manual export and import and perform the following steps in order:

- On the source Notification Server, in the Symantec Management Console, on the Manage menu, click All Resources.
- In the left pane, expand Default > All Resources > Software Product, select the Software Product resource that you want to migrate, and then perform the steps in the following topic:
  See “Migrating data using manual export and import” on page 27.

Note that you can track usage of a migrated software product only if the following requirements are met:

- The software product is installed and discovered in your environment.
- The software product has at least one software component that is associated to it.
- At least one software component in the software product has the association with a key program file.

You need to run the Software Inventory scan on managed computers to discover and gather software inventory data. After software inventory data is gathered and entered into the Configuration Management Database, the required associations are automatically created for the following items:

- Predefined software products
- The software components that belong to the predefined or already metered software product
- The key program files that are installed with an MSI-based installer

Note: You need to create associations manually for the key program files that have been manually associated to the software components on your source Notification Server.

For more information, see the topics about tracking usage of the managed software products in the Inventory Solution User Guide.

---

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software-based usage tracking: software products and usage-tracking data</td>
<td>To migrate software products that are configured for software-based usage tracking, use manual export and import and perform the following steps in order:</td>
</tr>
<tr>
<td></td>
<td>- On the source Notification Server, in the Symantec Management Console, on the Manage menu, click All Resources.</td>
</tr>
<tr>
<td></td>
<td>- In the left pane, expand Default &gt; All Resources &gt; Software Product, select the Software Product resource that you want to migrate, and then perform the steps in the following topic:</td>
</tr>
<tr>
<td></td>
<td>See “Migrating data using manual export and import” on page 27.</td>
</tr>
<tr>
<td></td>
<td>Note that you can track usage of a migrated software product only if the following requirements are met:</td>
</tr>
<tr>
<td></td>
<td>- The software product is installed and discovered in your environment.</td>
</tr>
<tr>
<td></td>
<td>- The software product has at least one software component that is associated to it.</td>
</tr>
<tr>
<td></td>
<td>- At least one software component in the software product has the association with a key program file.</td>
</tr>
<tr>
<td></td>
<td>You need to run the Software Inventory scan on managed computers to discover and gather software inventory data. After software inventory data is gathered and entered into the Configuration Management Database, the required associations are automatically created for the following items:</td>
</tr>
<tr>
<td></td>
<td>- Predefined software products</td>
</tr>
<tr>
<td></td>
<td>- The software components that belong to the predefined or already metered software product</td>
</tr>
<tr>
<td></td>
<td>- The key program files that are installed with an MSI-based installer</td>
</tr>
<tr>
<td></td>
<td>Note: You need to create associations manually for the key program files that have been manually associated to the software components on your source Notification Server.</td>
</tr>
<tr>
<td></td>
<td>For more information, see the topics about tracking usage of the managed software products in the Inventory Solution User Guide.</td>
</tr>
<tr>
<td>The installation, upgrade, and uninstall policies for Inventory Plug-in, Application Metering Plug-in, and Inventory Pack for Servers Plug-in</td>
<td>Before migrating the policy that uses custom targets, you must migrate the policy targets separately.</td>
</tr>
<tr>
<td></td>
<td>To migrate the policies for Inventory Plug-in, Application Metering Plug-in, and Inventory Pack for Servers Plug-in using manual export and import, perform the steps in the following topic:</td>
</tr>
<tr>
<td></td>
<td>See “Migrating data using manual export and import” on page 27.</td>
</tr>
</tbody>
</table>
### Table 4-4  Migrating Inventory Solution components using manual export and import (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Custom inventory reports</td>
<td>To migrate custom inventory reports using manual export and import, perform the steps in the following topic: See “Migrating data using manual export and import” on page 27.</td>
</tr>
</tbody>
</table>

### Table 4-5  Inventory Solution components that you cannot migrate using export and import options

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standalone inventory packages</td>
<td>Migration of standalone inventory packages is not supported.</td>
</tr>
</tbody>
</table>
| File and registry baseline tasks | You can manually copy configuration and snapshot files from the following locations on your source Notification Server computer:  
\`\`\localhost\NSCap\bin\Win32\X86\Inventory\Application Management\FileBaselinePackage  
\`\`\localhost\NSCap\bin\Win32\X86\Inventory\Application Management\RegBaselinePackage  
Then you can paste the files to same locations on your destination Notification Server computer and use them to re-create your baseline tasks. |
| Agentless inventory tasks | You can export custom SNMP data mapping tables from the **SNMP Data Mapping Tables** page on your previous Notification Server computer. Then you can import the tables to your new Notification Server computer and create new agentless inventory task to collect inventory on required devices. |

### Migrating Patch Management Solution data using standalone replication

See “About data migration” on page 9.

See “Performing data migration using standalone replication” on page 11.

You can migrate the following Patch Management Solution components using standalone replication:

- Windows Patch remediation settings
- Software update policies for Windows computers
See “To migrate Patch Management Solution components using standalone Item Replication Rule” on page 53.

The standalone replication of the following Patch Management Solution components is not supported:

- Patch management import files
- Patch management reports
- Software update policies for Linux computers
- Linux Patch remediation settings

Before you replicate Patch Management Solution data, you need to perform the following steps in order:

- Run the **Import Patch Data for Windows** task on the destination Notification Server.
  See “To run Import Patch Data for Windows task” on page 53.

- Migrate physical packages.
  To migrate physical packages, use Symantec Notification Server Migration Wizard and perform the steps in the following topic:
  See “Migrating physical packages using Symantec Notification Server Migration Wizard” on page 62.

To migrate Patch Management Solution components using standalone Item Replication Rule

1. On the source Notification Server, in the Symantec Management Console, configure and run the standalone **Item Replication Rule** performing the steps in the following topic:
   See “Configuring and running standalone Item Replication Rule” on page 14.

2. While you specify the **Items** that you want to replicate, do the following:
   - Click **Settings > Software > Patch Management > Windows Settings**, and then select **Windows Patch Remediation Settings**.
   - Click **Policies > Software > Patch Management > Software Update Policies > Windows**, and then select the required software update policies.

To run Import Patch Data for Windows task

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

2. In the left pane, expand **Jobs and Tasks > System Jobs and Tasks > Software > Patch Management > Import Patch Data for Windows**.

3. In the right pane, under **Vendors and Software**, click **Update**.
4 When the available products list import is complete, under Vendors and Software, check the software for which you want to download the patch management metadata, and then make any other necessary changes.

**Note:** The settings of the Import Patch Data for Windows task must be the same on the source and destination Notification Servers.

5 Click Save changes.

6 Under Task Status, click New Schedule.

7 In the New Schedule dialog box, click Now, and then click Schedule.

---

**Migrating Patch Management Solution data using manual export and import**

See “About data migration” on page 9.

You can migrate the following Patch Management Solution components using manual export and import:

See Table 4-6 on page 55.

When you export and import Patch Management Solution components, you must consider the following limitations:

- Before migrating the components that contain dependent items, such as custom filters or collections as a target, you must export and import these dependent items performing the steps in the following topic:
  - See “Migrating data using manual export and import” on page 27.

- If policy or task credentials are not re-encrypted, you need to re-enter the credentials and save changes in the policy or task.

The manual export and import of the following Patch Management Solution components is not supported:

- Patch management import files
- Software update policies
  
  You can replicate software update policies for Windows computers using standalone replication.
  
  See “Migrating Patch Management Solution data using standalone replication” on page 52.
The lists of software channels in the **Import Patch Data for SUSE** and **Import Patch Data for Red Hat** tasks from Patch Management Solution lower than version 7.6 HF7.

**Table 4-6**  
Migrating Patch Management Solution components using manual export and import

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Patch Management Solution settings | To migrate Patch Management Solution settings using manual export and import, perform the steps in the following topic:  
  See "Migrating data using manual export and import" on page 27.  
  **Note:** After you import the settings that contain the locations not available on your destination Notification Server computer, you need to re-enter these locations. |
| Software update plug-in policies  | To migrate Software update plug-in policies using manual export and import, perform the steps in the following topic:  
  See "Migrating data using manual export and import" on page 27.  
  **Note:** Some **Default Software Update Plug-in Policy** settings cannot be migrated due to extensive changes in the restart dialog boxes in Patch Management Solution 8.0 and later.  
  To view and re-configure the **Default Software Update Plug-in Policy** settings, perform the following steps in order:  
  - In the Symantec Management Console, on the **Settings** menu, click **Agents/Plug-ins > Agents/Plug-ins**.  
  - In the left pane, expand **Software > Patch Management > Windows**, and then click **Default Software Update Plug-in Policy**.  
  - (Optional) In the right pane, view the policy settings and configure the policy according to your needs, and then click **Save changes**. |
### Table 4-6  Migrating Patch Management Solution components using manual export and import (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Patch Management Solution jobs and tasks | To migrate Patch Management Solution jobs and tasks using manual export and import, perform the steps in the following topic:  
  See "Migrating data using manual export and import" on page 27.  
  **Note:** While you prepare to run the migrated **Import Patch Data for Windows** task, you need to review and edit the imported list of available software channels. After you click **Update** on the task page, under **Vendors and Software**, some previously checked channels get unchecked for import because of the difference in channel naming. You must check the software channels for which you want to download the patch management metadata. |

---

**Migrating Software Management Solution data**

See “About data migration” on page 9.
### Table 4-7  Migrating Software Management Solution data

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Software Management Components Settings | You can migrate the following software settings using the export and import:  
  - Managed Delivery Settings  
  - Software Discovery  
  - Software Library Configuration  
  - Software Portal Settings  
  
  To migrate these software settings using the export and import, perform the steps in the following topic:  
  
  See "Migrating data using manual export and import" on page 27.  
  
  To migrate Software Portal Settings and Managed Delivery Settings using the standalone Item Replication Rule, do the following:  
  
  - To configure and run the standalone Item Replication Rule, perform the steps in the following topic:  
    See “Configuring and running standalone Item Replication Rule” on page 14.  
  
  - While you specify the Items that you want to replicate, click Notification Server > Settings > Software, and select the Managed Delivery Settings, then click Notification Server > Settings > Software > Software Portal Settings, and select the Software Portal Settings.  
  
  Note that you cannot migrate Software Discovery and Software Library Configuration using standalone replication. |
| Software components | You can migrate the following software components:  
  - Associations between components  
  - Command lines  
  - File Inventory  
  - Inventory rules  
  - Packages  
  - Service packs  
  - Software releases  
  - Software updates  
  
  See “About migrating software components” on page 60. |
Table 4-7  Migrating Software Management Solution data (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software tasks</td>
<td>You can migrate the following software tasks:</td>
</tr>
<tr>
<td></td>
<td>■ Package Delivery</td>
</tr>
<tr>
<td></td>
<td>■ Quick Delivery</td>
</tr>
<tr>
<td></td>
<td>■ Software Virtualization</td>
</tr>
<tr>
<td></td>
<td>■ Source Path Update</td>
</tr>
<tr>
<td></td>
<td>■ Windows Installer Repair</td>
</tr>
</tbody>
</table>

To properly migrate software tasks, perform the following steps:

1. Migrate the physical packages that are related to the corresponding software components using Symantec Notification Server Migration Wizard.
   
   See “Migrating physical packages using Symantec Notification Server Migration Wizard” on page 62.

2. Migrate the corresponding software components using the Software Resource Replicator utility.
   
   See “About migrating software components” on page 60.

3. Migrate software tasks using the Item Replication Rule as follows:
   
   ■ To configure the standalone Item Replication Rule, perform the steps in the following topic:
     
     See “Configuring and running standalone Item Replication Rule” on page 14.
   
   ■ While you specify the Items that you want to replicate, click Notification Server > Tasks > Jobs and Tasks > System Jobs and Tasks > Software, and then select the required items.

**Warning:** If you migrate software tasks using the Item Replication Rule first, and only then migrate the corresponding software components with the Software Resource Replicator utility, you need to do the following:

Use the Software Resource Replicator utility again with the unchecked option Do not import resources which already exist in NS on the Import Software Resources tab to re-import the software components that are used in the replicated tasks.

See “Migrating software components using the Software Resource Replicator utility” on page 65.
### Table 4-7  Migrating Software Management Solution data (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Custom filters and targets that are based on predefined filters and targets | - You can migrate filters using manual export and import.  
  See "Migrating data using manual export and import" on page 27.  
  You can also import filters using the ImportExportUtil.exe tool.  
- You can migrate targets using the ImportExportUtil.exe tool.  
  See "Migrating data using the ImportExportUtil.exe tool" on page 28.  
- Alternatively, you can migrate filters and targets using the standalone Item Replication Rule.  
  See “Configuring and running standalone Item Replication Rule” on page 14. |
| Managed Software Delivery policies | To properly migrate Managed Software Delivery policies, perform the following steps:  
  1. Migrate the physical packages that are related to the corresponding software components using Symantec Notification Server Migration Wizard.  
  See “Migrating physical packages using Symantec Notification Server Migration Wizard” on page 62.  
  2. Migrate the corresponding software components using the Software Resource Replicator utility.  
  See “About migrating software components” on page 60.  
  3. Migrate the filters and targets that are used in Managed Software Delivery policies.  
  4. Migrate Managed Software Delivery polices using the Item Replication Rule as follows:  
    - To configure the standalone Item Replication Rule, perform the steps in the following topic:  
      See “Configuring and running standalone Item Replication Rule” on page 14.  
    - While you specify the Items that you want to replicate, click Notification Server > Policies > Software > Managed Software Delivery, and then select the required items.  

**Warning:** If you migrate Managed Software Delivery polices using the Item Replication Rule first, and only then migrate the corresponding software components with the Software Resource Replicator utility, you need to do the following:  

Use the Software Resource Replicator utility again with the unchecked option Do not import resources which already exist in NS on the Import Software Resources tab to re-import the software components that are used in the replicated policies.  

See “Migrating software components using the Software Resource Replicator utility” on page 65. |
### Table 4-7  Migrating Software Management Solution data (continued)

<table>
<thead>
<tr>
<th>Component</th>
<th>Description</th>
</tr>
</thead>
</table>
| Custom reports          | **Note:** Custom reports are migrated without the data.  
  ■ You can migrate custom reports using the standalone Item Replication Rule.  
  See “Configuring and running standalone Item Replication Rule” on page 14.  
  ■ You can manually export and import a single custom report or a folder that contains several reports.  
  **Note:** If you import a folder and a folder with the identical GUID already exists on the target Notification Server, the existing folder and its content get overwritten.  
  See “Migrating data using manual export and import” on page 27. |
| Software security roles | You can migrate software security roles using the following standalone Security Replication Rules:  
  ■ The Role Replication Rule lets you migrate roles and accounts.  
  ■ The Privilege Replication Rule lets you migrate privileges.  
  Migration of software security roles using manual export and import is not supported. |

### About migrating software components

Migrating software components is a step in the process of data migration of the following IT Management Suite solutions:

- **Software Management Solution**  
  See “Migrating Software Management Solution data” on page 56.

- **Inventory Solution**  
  See “Migrating Inventory Solution data using standalone replication” on page 40.  
  See “Migrating Inventory Solution data using manual export and import” on page 46.

When migrating software components, consider the following:

- The migration of software components without an associated physical package or a command line is not supported.

- Before migrating the software components that are located in the Software Library, you must perform one of the following actions:
  
  ■ Define a new Software Library on destination Notification Server.  
  Software Library can be same UNC share as on the source Notification Server, or a new one. If you specify a new Software Library, ensure that
physical packages are migrated there from the UNC share that you use on the source Notification Server. If you reuse your old UNC share, its security settings for the destination Notification Server should satisfy the Software Library Configuration conditions (APP ID, ACC, DPC account permissions).

- Migrate Software Library from the source Notification Server.
  You can export and import Software Library Configuration settings performing the steps in the following topic:
  See “Migrating data using manual export and import” on page 27.
  Note that the Software Library Configuration settings cannot be replicated with the standalone Item Replication Rule.

- To correctly migrate the software components that are associated with physical packages or command lines, use the Software Resource Replicator utility.
  See “Migrating software components using the Software Resource Replicator utility” on page 65.

---

**Note:**
Physical package files must be accessible from the destination Notification Server, and it is verified during the import by the Software Resource Replicator utility. Packages must be migrated manually or using Symantec Notification Server Migration Wizard.

See “Migrating physical packages using Symantec Notification Server Migration Wizard” on page 62.

If the package source location (UNC, URL, or local) is not the same or not accessible from the destination Notification Server, you must change the location path in the Software Resource Replicator utility, on the Import Software Resources tab.

See “Migrating software components using the Software Resource Replicator utility” on page 65.

---

- Migrate physical files by moving them manually or by using Symantec Notification Server Migration Wizard.
  See “Migrating physical packages using Symantec Notification Server Migration Wizard” on page 62.
Warning: Symantec does not recommend to migrate software components using standalone Resource Replication Rule.

Software components may be replicated using Resource Replication Rule. However, the Resource Replication Rule does not replicate all dependent items. For example, physical packages, detection or applicability rules may not be replicated. Because of this limitation, the replicated software components may become inconsistent and may not be delivered to the clients.

Do not re-run the Resource Replication Rule for the software component with physical packages that has already been migrated using the Software Resource Replicator utility. The standalone replication may corrupt some dependencies for this software component. To restore the dependencies, you must again run the Software Resource Replicator utility with the option Do not import resources which already exists in NS unchecked.

Migrating physical packages using Symantec Notification Server Migration Wizard

Before you migrate software components that are used in Software Management Solution and Patch Management Solution, you must migrate the physical packages related to these software components.

See “Migrating Software Management Solution data” on page 56.

See “Migrating Patch Management Solution data using standalone replication” on page 52.

You can migrate physical packages using Symantec Notification Server Migration Wizard that you must install on your destination and source Notification Servers.

When you use the wizard to migrate physical packages for Software Management Solution items, consider the following:

- If you want to use a new Software Library configuration or a new UNC share, you must manually migrate physical packages to the new location. You may continue to use your old Software Library configuration and UNC shares but then you need to ensure that these locations are accessible from the destination Notification Server.

- If you used a custom local path for the software components on the source Notification Server, you must recreate the same file structure on the destination Notification Server. For example, if the software resources were located on disk F, then disk F must also be on the destination Notification Server computer.
If a path that is used in a software component 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.

To export physical packages using Symantec Notification Server Migration Wizard

1. On the destination Notification Server, in the Symantec Installation Manager installation directory, copy one of the two migration wizard installation files: Symantec_Migration_Package_xxxx_x64.exe or Symantec_Migration_Package_xxxx_x64_silent.exe

   The default Symantec Installation Manager installation directory is C:\Program Files\Altiris\Symantec Installation Manager\MigrationPackage

2. On the source Notification Server, paste the copied migration wizard installation file and install it.

3. (Optional) If you use the Symantec_Migration_Package_xxxx_x64_silent.exe file, after the installation finishes, in the migration wizard installation directory, start NSUpgradeWizard.exe to open Symantec Notification Server Migration Wizard.

   The default migration wizard installation directory is C:\Program Files\Altiris\Upgrade

   If you use the Symantec_Migration_Package_xxxx_x64.exe file, Symantec Notification Server Migration Wizard opens automatically after the installation finishes.

4. In Symantec Notification Server Migration Wizard, do the following:

   - On the Export / Import Task Selection page, select Export data from a Symantec Notification Server to a file store, specify the location where you want to place the exported data (the Package Files folder and the Store.adb file), and then click Next.

   - On the Password Protection page, enter the password to encrypt the data, and then click Next.

   - On the Exporter Configuration page, select the data that you want to export, and then click Next.

     - For Patch Management Solution, select Patch Management Package Items Physical Files Exporter.

     - For Software Management Solution, select Software Package Resource Exporter.
On the **Product Readiness Check** page, verify that all requirements for Patch Management and Software Management are met, and then click **Next**.

On the **Task Summary** page, check if the database settings and the **Into file source** location are correct, and then click **Next**.

After the successful export, click **OK**, and then click **Finish**.

To import physical packages using Symantec Notification Server Migration Wizard

1. Before importing the physical software update packages for Patch Management Solution to destination Notification Server, check if you have specified the required location where the packages will be stored after the import.

To check the location, in the Symantec Management Console, on the **Settings** menu, click **All Settings**, in the left pane, expand **Settings > Software > Patch Management > Windows Settings > Core Services**, and then on the **Core Services** page, click the **Locations** tab.

   The default location is `C:\Program Files\Altiris\Patch Management\Packages\Updates`

2. On the source Notification Server, copy the **Package Files** folder and the **Store.adb** file, and then paste them to the destination Notification Server.


   The default migration wizard installation directory is `C:\Program Files\Altiris\Upgrade`

4. In **Symantec Notification Server Migration Wizard**, do the following:

   - On the **Export / Import Task Selection** page, select **Import data from a file store to a Symantec Notification Server**, specify the location of the **Store.adb** file, and then click **Next**.

   - On the **Password Protection** page, enter the password that you specified during the export of data, and then click **Next**.

   - On the **Importer Configuration** page, select the data that you want to import, and then click **Next**.

   - On the **Product Readiness Check** page, click **Next**.

   You can ignore the **Failed to meet baseline requirements** message for Altiris Monitor Solution 6.0, RTCI, and RTSM.

   - On the **Task Summary** page, check if the database settings and the **Into file source** location are correct, and then click **Next**.

   - After the successful import, click **OK**, and then click **Finish**.
Migrating software components using the Software Resource Replicator utility

Note that with the **Software Resource Replicator** utility you can migrate only the software components that are associated with physical packages or command lines. See “About migrating software components” on page 60.

To migrate software components using the Software Resource Replicator utility

1. Download the **Software Resource Replicator** utility from the following location: [http://www.symantec.com/docs/TECH166711](http://www.symantec.com/docs/TECH166711)

   Note that you must download the **Software Resource Replicator** utility both to source Notification Server and destination Notification Server.

2. On the source Notification Server, start **SoftwareReplicator.exe**.

3. In the **Software Resource Replicator** utility, on the **Export Software Resources** tab, do the following:
   - Select the software items that you want to export.
   - As **Export Path**, specify the location, where you plan to save exported XML files.
   - Configure the **Export Parameters**.
   - Click **Export Now**.

   After successful export, you have an XML file for each software component.

4. Move the exported XML files to destination Notification Server.

5. On the destination Server, start **SoftwareReplicator.exe**.

6. In the **Software Resource Replicator** utility, on the **Import Software Resources** tab, do the following:
   - As **Import Path**, specify the location of the imported XML files.
   - Click **Refresh** to check the available software components to be imported.
Note: Before importing the software components that are located in Software Library, specify Software Library on destination Notification Server. Software Library can be same UNC share as on the source Notification Server, or a new one. If you specify a new Software Library, ensure that physical packages are migrated there from the UNC share that you use on the source Notification Server.

During the import, it is verified whether physical package files are accessible from the destination Notification Server. If you reuse your old UNC share, its security settings for the destination Notification Server should satisfy the Software Library Configuration conditions (APP ID, ACC, DPC account permissions). Packages may be migrated manually or using Symantec Notification Server Migration Wizard.

See “Migrating physical packages using Symantec Notification Server Migration Wizard” on page 62.

If the package source location (UNC, URL, or local) is not the same or not accessible from the destination Notification Server, you must change the path to the location in the Software Resource Replicator utility, on the Import Software Resources tab.

Warning: If software component has been replicated by a replication rule previously, it must be overwritten on destination Notification Server. To do so, uncheck Do not import resources which already exists in NS.

7 Select the required software components, and then click Import Now.
8 On the destination Notification Server, in the Symantec Management Console, on the Software Releases page, you can check the list of available and imported software components.

Migrating ITMS Management Views Data

Data migration using the standalone replication rules is not supported for ITMS Management Views data.

You can migrate data using the manual export and import

See “Migrating data using manual export and import” on page 27.

You can export Targets, Computers Views and Groups, Jobs/Tasks, Policies, and Software folders from the ITMS Management views pages, or you can export single items from these folders.
Note: If you import an item or a folder that already exists on the destination Notification Server, the item or folder is relocated to the latest indicated location. Note that this happens only if the item or folder has the same name and GUID.

Migrating Real-Time System Management Data

Data migration using the standalone replication rules is not supported for Real-Time System Management Solution data.

You can only export **Network Filter** items. You can migrate data using the manual export and import.

See “Migrating data using manual export and import” on page 27.

Migrating IT Analytics Server and content pack Data

Data migration using the standalone replication rules or manual export and import is not supported for IT Analytics Server and content pack data.

**Note:** You can use the MultiCMDB feature during IT Management Suite 7.X to 8.X migration. The MultiCMDB feature lets you report on a mix of 7.X data and 8.X data.

For more information, see topics on MultiCMDB reporting with IT Analytics in the *IT Management Suite Planning for Implementation Guide*.

You can create an additional connection to a new CMDB (on the destination Notification Server) for IT Analytics, located on the source Notification Server. To view data from the new CMDB, you must configure additional External CMDB Connection.

For more information, see topics on configuring external Symantec CMDB in the *Client Server Management Pack for IT Analytics Guide*.

Although data migration is not supported for IT Analytics, you can copy the custom Cube View data records from source Notification Server database and restore them on the destination Notification Server.

The following knowledge base article contains useful information that can help perform custom Cube View data backup and restore:  
Migrating Server Management Suite component data

You can migrate the Server Management Suite component data as follows:

Table 4-8  Data migration of Server Management Suite components

<table>
<thead>
<tr>
<th>Component</th>
<th>Migration</th>
</tr>
</thead>
<tbody>
<tr>
<td>Network Discovery (ND)</td>
<td>You can migrate Tasks, Filters, and Reports using export and import.</td>
</tr>
<tr>
<td>Credential Manager (CM)</td>
<td>You can migrate Policies using export and import.</td>
</tr>
<tr>
<td></td>
<td>You can use the Migration Wizard to migrate the keys. For the keys to work, you must migrate the database as well.</td>
</tr>
<tr>
<td>Pluggable Protocol Architecture (PPA)</td>
<td>You can migrate Policies using export and import.</td>
</tr>
<tr>
<td></td>
<td>Replication is not supported.</td>
</tr>
<tr>
<td></td>
<td>You can use the Migration Wizard to migrate the keys. For the keys to work, you must migrate the database as well.</td>
</tr>
<tr>
<td>Management Information Base Browser (MIB)</td>
<td>You can migrate the Browser Task using the export and import or standalone replication.</td>
</tr>
</tbody>
</table>

See “Performing data migration using export and import” on page 25.
See “Performing data migration using standalone replication” on page 11.
See “Migrating physical packages using Symantec Notification Server Migration Wizard” on page 62.

Migrating Monitor Solution data

You can migrate the following Monitor Solution items using data export and import:

- Filters
- Reports
- Server and client jobs
- Server and client tasks

See “Performing data migration using export and import” on page 25.

To migrate Monitor Solution policies (including dependent Metrics and Rules) using manual export and import, perform the following steps:
To migrate Monitor Solution policies using manual export and import

1. On the source Notification Server, in the Symantec Management Console, on the Home menu, click Monitoring and Alerting.

2. In the left pane, under Monitoring and Alerting, expand Monitor > Policies > Monitor Policies, right-click the folder that you want to export, and then click Export Monitor Policy Folder.

3. Click Save.

To change the default location of the exported file, click Save As, select the required location, and then click Save.

4. Copy and paste the exported XML policy file to the destination Notification Server.

5. In the Symantec Management Console of the destination Notification Server, on the Home menu, click Monitoring and Alerting.

6. In the left pane, under Monitoring and Alerting, expand Monitor > Policies > Monitor Policies, click Import Monitor Pack.

7. On the Import Monitor Pack page, click Add and use the file browser to import the exported XML policy file.

8. On the Import Monitor Pack page, select the imported pack and on the top toolbar, click Schedule.

9. In the Schedule Monitor Pack dialog box, select the Run now option and click OK.

Migrating Virtual Machine Management data

You can migrate the following items of Virtual Machine Management using data export and import:

- Filters
- Policies
- Reports
- Server and client jobs
- Server and client tasks

See “Performing data migration using export and import” on page 25.
Migrating Power Scheme Task component data

See “About data migration” on page 9.

You can migrate the following Power Scheme Task component data:

- Power Scheme Task Plug-in policies
- Power Scheme Inventory task
- Predefined and custom power scheme tasks

**Note:** When you migrate the predefined power scheme policies or tasks from your source Notification Server, they replace the corresponding and already existing predefined power scheme policies or tasks on your destination Notification Server.

When you migrate custom power scheme tasks from your source Notification Server, they replace the corresponding power scheme tasks with the same GUID on your destination Notification Server.

To avoid the replacement, it is recommended to clone the required policies or tasks and migrate the cloned items.

To migrate Power Scheme Task component data using manual export and import, perform the steps in the following topic:

See “Migrating data using manual export and import” on page 27.

To migrate Power Scheme Task component data using the standalone Item Replication Rule

1. To configure and run the standalone Item Replication Rule, perform the steps in the following topic:

   See “Configuring and running standalone Item Replication Rule” on page 14.

2. While you specify the Items that you want to replicate, do the following:

   - To replicate the Power Scheme Task Plug-in policies, click Settings > Agents/Plug-ins > Power Scheme, and then select the required items.
   - To replicate the Power Scheme Inventory task, click Tasks > Jobs and Tasks > System Jobs and Tasks > Power Scheme Tasks, and then select the required item.
   - To replicate power scheme tasks, click Tasks > Jobs and Tasks > System Jobs and Tasks > Power Scheme Tasks > Set Power Scheme, and then select the required items.
Migrating Workflow Solution

You can migrate the following Workflow items using data export and import:

- Critical Error report

You can access the Critical Error report from **Reports > Service and Asset Management > Workflow**.

See "Performing data migration using export and import" on page 25.