HP Server Automation

Software Version: 10.22

SA User Guide: Software Management

Legal Notices

Warranty

The only warranties for HP products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HP shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HP required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

Copyright Notice

© Copyright 2001-2015 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number, which indicates the software version.
- Document Release Date, which changes each time the document is updated.
- Software Release Date, which indicates the release date of this version of the software.

To check for recent updates or to verify that you are using the most recent edition of a document, go to: **http://h20230.www2.hp.com/selfsolve/manuals**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to: **http://h20229.www2.hp.com/passport-registration.html**

Or click the **New users - please register** link on the HP Passport login page.

You will also receive updated or new editions if you subscribe to the appropriate product support service. Contact your HP sales representative for details.

Support

Visit the HP Software Support Online web site at: **http://www.hp.com/go/hpsoftwaresupport**

This web site provides contact information and details about the products, services, and support that HP Software offers.

HP Software online support provides customer self-solve capabilities. It provides a fast and efficient way to access interactive technical support tools needed to manage your business. As a valued support customer, you can benefit by using the support web site to:

- Search for knowledge documents of interest
- Submit and track support cases and enhancement requests
- Download software patches
- Manage support contracts
- Look up HP support contacts
- Review information about available services
- Enter into discussions with other software customers
- Research and register for software training

Most of the support areas require that you register as an HP Passport user and sign in. Many also require a support contract. To register for an HP Passport ID, go to:

http://h20229.www2.hp.com/passport-registration.html

To find more information about access levels, go to:

http://h20230.www2.hp.com/new_access_levels.jsp

HP Software Solutions Now accesses the HPSW Solution and Integration Portal Web site. This site enables you to explore HP Product Solutions to meet your business needs, includes a full list of Integrations between HP Products, as well as a listing of ITIL Processes. The URL for this Web site is **http://h20230.www2.hp.com/sc/solutions/index.jsp**

Contents

Chapter 1 # Software Management Quick Start

HP Server Automation (SA) enables you to govern the full spectrum of your software management requirements. With SA policy-based software management you can automate software installation and application configuration, and ensure that managed servers are compliant with software policies, as shown in The SA Software Management Process . (See About Policy-Based Software Installation and Management for more information).

- The **SA library** provides a secure folder hierarchy for organizing and sharing software resources and managing resource permissions. See About Software Resources in the SA Library.

- **SA software policies** enable you to specify the ideal deployment of an application including all the software packages, patches, scripts, and other objects to be installed on a server, as well as how configuration files for the application should be set on the server. See About Software Policiesand About Attaching Software Policies to Servers or Device Groups.

- The **SA remediation process** installs software and applies application configurations to managed servers according to the software policy specifications, making them compliant. See About Remediating Managed Servers Against Software Policies.

- **SA compliance scans** ensure that managed servers maintain compliance with their attached software policies and application configurations. See About Software Policy Compliance and About Software Policy Reports.

Figure: The SA Software Management Process
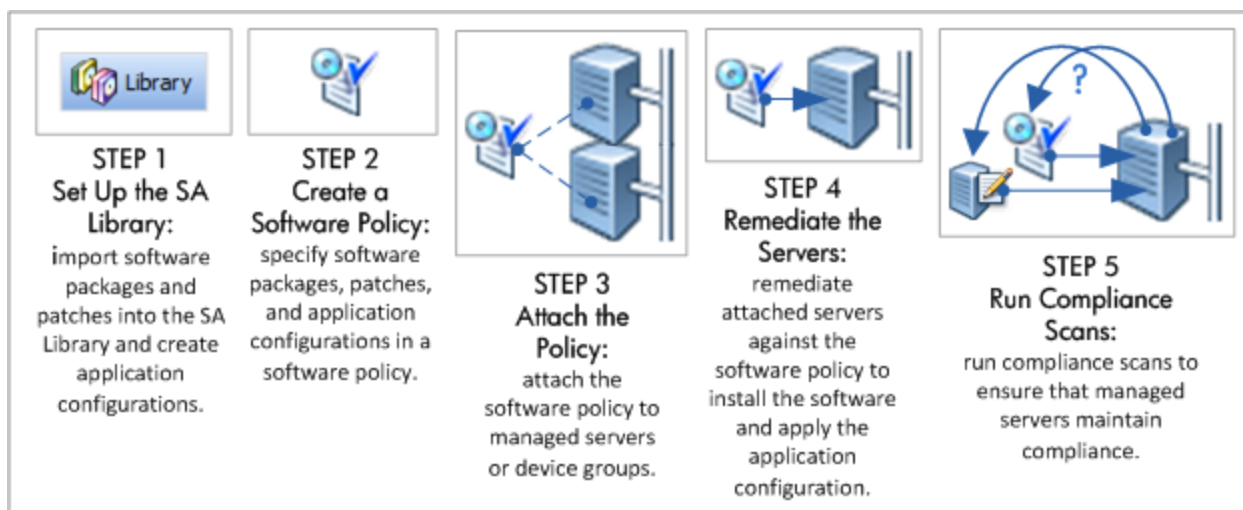
> **Note:** The SA Client is used for managing purchased software packages. To manage and deploy your own custom software applications to target servers in your data centers, use SA Application Deployment. For complete information, see the *SA User Guide: Application Deployment Manager*.

About Policy-Based Software Installation and Management

To manage software using software policies:

1   **Add software resources** (such as packages, patches, application configurations, scripts, and server objects) to the SA Library.

    Adding application configurations involves defining the configuration values that will be used to generate the configuration files. For example, if the software policy is being created to deploy an Apache Web Server, the application configurations would specify the default values for the httpd.conf file. For information about application configurations, see the *SA User Guide: Application Configuration*.

2   **Create a software policy** to specify the managed server, the order for installing the listed software resources, and the application configurations to be applied. See Creating Software Policies and Software Templates.

3   **Attach the software policy** to one or multiple managed servers. This associates that policy with the server, but does not enforced the policy or install the software it contains. See Attaching a Software Policy to a Server or Device Group.

4   **Remediate the managed servers** against the attached software policy to install the software as specified in the policy. This makes the servers compliant. See Remediating Servers with Software Policies.

    a   When you remediate a server or servers, you have the option of defining additional tasks to perform during the remediation process, such as system rebooting requirements, additional scripts to run, and job status email notifications.

    b   When the remediation process runs, it scans the server to determine areas of non-compliance with the software policy. It then installs the software resources identified in the policy in the order specified, applies the specified application configuration, and performs all the additional tasks defined in the remediation job such as rebooting systems, running additional scripts, and sending job status e-mails.

5   **Run compliance scans** to ensure that managed servers maintain compliance with their attached software policies and application configurations. See About Software Policy Compliance.

    a   When a software policy or application configuration is modified, the servers on which it is installed or applied, respectively, become non-compliant.

    b   The Software Compliance and Configuration Compliance scans identify non-compliant servers so that you can remediate them back into compliance with the modified software policy or application configuration respectively.

Best Practice: Validate new policies on a test server before remediating the servers in your operational environment. Attach the new policy to a test server, remediate the test server, and

then review the results. If everything is deployed correctly, attach the policy to the live servers and then remediate.

Terminology

The following list defines key terms and concepts used in Server Automation software management:

* Package: An installable package, such as an RPM package, or a Windows MSI package.

* Package Metadata: Information about a package that is stored in the HP SA Model Repository. Some package metadata is extracted from the package itself during the software import process, while other metadata is provided by the user.

* Remediation: A process that brings a server into compliance with its attached software policies.

* Server Script: A script that executes on a managed server. Server Scripts can be stored in the HP SA Software Repository, and be included in Software Policies.

* Software Inventory: The HP SA Model Repository contains a snapshot list of the packages installed on a managed server. Inventory is automatically performed on managed servers on an infrequent basis (about daily), and during software installation/uninstallation.

* Software Policy: An ordered list of packages, script, application configurations, and other items. A Software Policy is essentially a recipe for installing and configuring one of more pieces of software on a single server (and uninstalling, as well).

* Template: A set of rules that allow a configuration file to be generated by the HP SA Application Configuration feature. An Application Configuration can include multiple templates, if more than one configuration file needs to be maintained. Templates can either use Configuration Markup Language (CML), for text configuration files, or XML for XML configuration files.

* Value Set: Value Sets are typed data associated with various objects in the HP SA model. They are similar to, but more full-featured than custom attributes.

About Software Policies

SA software policies enable automation of software installation and application configuration. If a policy is changed after it has been deployed, the managed servers can be scanned and remediated to ensure that they maintain compliance with the policy.

* SA software policies allow you to define the ideal deployment of an application.In a software policy, you specify the software packages and patches to be installed, the server scripts to run, and the application configurations to be applied to the managed servers.

* Software policies can be attached to multiple managed servers or device groups.

* Managed servers are brought into compliance with the software policy through a configurable remediation process. When you remediate a server or group of servers, the software resources and application configurations specified in the attached policy are automatically installed and applied respectively.

- If modifications are made to software policies, installed software, or application configurations, the compliance scan identifies non-compliant managed servers, so you can remediate them back into compliance with the policy.

Software policies can specify:

- Software resources (such as packages, patches, application configurations, scripts, and server objects) to install
- Software installation order
- Custom Attributes
- Sub-policies (as long as they belong to the same operating system family)
- OS sequences
- Application configurations to apply

Software policy attributes and features include:

- Embedded Software Subpolicies
- Software Policy Templates
- Software Resources in a Software Policy
- Custom Attributes for Policies
- Software Policies for Patch Installation
- Software Policies for Script Execution
- ISM Controls in Policies

Embedded Software Subpolicies

Software policies that are embedded under another software policy are called subpolicies. Embedding sub-policies provides a way to organize your software and manage dependencies between the software resources across sub-policies.

Sub-polices are handled as one policy by the remediation and installation processes—all the software resources from all the sub-policies are grouped together and then installed as a unit. SA does not consider the install order specified in the sub-policies, it only considers the parent policy's install order. Once installed, the sub-policies are no longer recognized as discrete, separate policies.

> **Note:** Note that software policies with embedded sub-policies are different than software policy templates which define a set of polices that are handled as individual policies after installation. See Software Policy Templates.

Software Policies for Script Execution

A policy allows you to execute multiple scripts on servers or server groups simultaneously, and execute a sequence of scripts on a server by specifying an install order in the software policy.

In the SA Client, you can execute scripts in the following ways:

- Execute a server script directly on servers or server groups. See the *SA User Guide: Server Automation* for more information about script execution.

- Add a script to a policy and execute the script by attaching the policy to the server and then remediating the server against the software policy. See Step 2 (Optional): Specify Reboot, Error Handling, and Script Options for Remediationfor more information about adding scripts to the remediation settings.

Software Policy Templates

Software policy templates are a defined set of software polices that are handled as individual policies and can be installed, modified, or detached as discrete policies. The template itself is just the container and is not actually installed on the server.

The value of the software policy templates is that the software policies can be managed independently even after they are installed. For example, policies that were installed from a template can be detached, modified, and updated as individual policies, whereas policies that were installed as embedded sub-policies of another software policy cannot.

A software template can be associated with either a single operating system family or multiple operating system families. When you add software resources to a software template, the software resources must belong to the same operating system family as the software template. For example, if you define the operating system for a software template as HP-UX, you can only add software resources applicable to versions of HP-UX to the software policy.

About Installing Software Using a Software Policy Template:

You can install software by using a software template.You use the same procedure to create a software template as you use to create a software policy, however, you specify that the policy is to be a software template. See Remediating and Installing Software.

The difference is that when you attach, install, or remediate a server against a template, the template itself is not attached or installed, just the policies it contains. For example:

- When you attach a software policy template, the template itself is not attached, just the policies it contains.

- When you remediate a server against a software policy template, the software policies specified in the software template are installed individually; the template itself is not installed.

> **Note:** Note that software templates are different than software policies with embedded sub-policies which are handled as one flattened policy after installation and are not recognized as discrete policies. See Embedded Software Subpolicies.

Software Resources in a Software Policy

A policy can contain packages, RPM packages, patches, application configurations, scripts, and server objects. After you add the software resources to a software policy, you can specify the order in which you want them to be installed. When you attach a policy to a server and remediate the server, SA installs the software resources in the policy in the specified order.

A policy can be associated with either a single operating system family or multiple operating system families. When you add software resources to a software policy, the software resources must belong to the same operating system family as the software policy. For example, if you define the operating system for a policy as HP-UX, you can only add software resources applicable to versions of HP-UX to the software policy.

Similarly, if the operating system defined for a policy is Windows Server 2008 and Windows Server 2003, the software resources that are applicable to Windows Server 2008 and Windows Server 2003 operating systems can be added to the software policy.

You have the option to associate OS Sequences for added control over the manner in which a particular OS should be installed. For example, you can specify which OS Installation Profile to use, the application and patch policies to include, and how these policies should be remediated either before or after the OS is installed.

A software policy can also include sub-policies. The sub-policies and the parent policy must belong to the same operating system family. When a policy contains sub-policies, all the software resources from the sub-policies are grouped together and then installed as a unit. See Embedded Software Subpolicies.

You can also create software policy templates which contain a set of independent policies that can be attached, installed, and modified as discrete policies. During remediation, SA does not consider the install order for the set of policies in the template. However, within each policy, the install order of the software resources is honored. See Software Policy Templates.

Custom Attributes for Policies

You to set custom attributes for servers by using software policies. The custom attributes include miscellaneous parameters and named data values. You can write scripts that use these parameters and data values when you perform a variety of functions, including network and server configuration, notifications, and CRON script configurations.

You can set custom attributes for software policies or for servers or device groups directly. When you set a custom attributes for a software policy, the custom attributes and values affect all the servers attached to the policy. When a policy containing sub-policies is attached to a server, all the custom attributes and values from the parent policy and the included sub-policies are added to the server.

Setting custom attributes to servers or device groups directly allows you to override the attributes and values set by a software policy. For example, if a certain port is required for installing an application, you can set it as a custom attribute in a software policy. When you attach the policy to multiple servers, the attribute is added to those servers. If required, you can change the port settings of a particular server attached to the software policy, without changing the port settings of all the other servers attached to the software policy. You can achieve this by setting the custom attribute on the server directly. As a result, the custom attribute value set on the server directly supersedes the value set by the policy for that server.

See Adding Custom Attributes to a Software Policy for more information.

Software Policies for Patch Installation

With SA you can install patches on servers in the following ways:

* Using Windows patch policies to install Windows patches. See "Patch Management for Windows" in the *SA User Guide: Server Patching* for more information.

* Using Solaris patch policies to install Solaris patches. See "Patch Management for Solaris" in the *SA User Guide: Server Patching* for more information.

* Using patch policies to install HP-UX, AIX and Linux patches. See "Patch Management for Unix" in the *SA User Guide: Server Patching* for more information.

> **Note:** A policy can contain both Unix patches and Windows patches. It is recommended that you use Windows patch policies to install Windows patches, Solaris patch policies to install Solaris patches and policies to install other Unix patches on servers.

Patch policies provide you with an option of setting a policy exception. If you need to include or exclude a Windows patch in a patch policy from being installed, you can deviate from a patch policy by specifying that Windows patch in a policy exception. You can also set precedence rules for applying patch policies and policy exceptions. The precedence rules determine the Windows patches that are actually installed on a server. See the *SA User Guide: Server Patching* for more information about precedence rules for applying patch policies and patch policy exceptions.

After you attach a patch policy to a managed server, the remediation process installs the patches in a patch policy on the managed server. If you remove any patches from the patch policy and remediate the server again, the remediation process does not remove the patches from the server.

However, with a software policy, the remediation process removes the patches from the server. There are some patches like Service Packs that cannot be uninstalled. For example, if you remove a Service Pack from a policy and remediate the server again, the Service Pack is not uninstalled from the server.

About Attaching Software Policies to Servers or Device Groups

After creating a software policy, you can attach it to managed servers or device groups.

When you attach a software policy to a managed server or device group, the policy has a persistent association to that server. Therefore, whenever the software policy is updated, you receive a notification indicating which servers or groups of servers are affected by the updated software policy. You can then remediate the servers or device groups to reflect the changes to the software policy. See Attach a Software Policy to a Server or Device Group for more information.

About Remediating Managed Servers Against Software Policies

The remediation process works by comparing what is actually installed on a managed server to the software that should be installed per the software policy. SA then determines what operations are required to make the server compliant. Server Scripts attached to the policy are executed during each remediation, even if all patches/packages of the policy are compliant.

When you remediate a server or device group, SA installs the software resources (patches, packages, scripts, server objects, and application configurations) in the attached software policy in the order specified in the policy. See Remediating Servers with Software Policies for more information about the remediation process.

If a software policy specifies sub-policies, all the software resources from the sub-policies are grouped together and then installed as a unit. See About Software Policiesfor more information on how policies with sub-policies are handled.

About Software Policy Compliance

A software policy compliance scan determines whether a managed server's is compliant with the software resources, application configurations specified in its attached software policies. Scripts specified in a software policy are not used to determine software compliance. If the managed server does not match its attached software policies' requirements, the server is considered to be non-compliant.

If a managed server is not compliant with even a single attached software policy, it is considered non-compliant. Non-compliant servers must be brought into compliance by remediating the software policy against the server.

The SA Client displays the following compliance information for managed servers:

- **Compliant**: If a server is compliant with all software policies attached to it, the server is considered compliant and displays this icon ●.

- **Non-compliant**: If a managed server is not compliant with one or more of the software policies attached to it, the server is considered non-compliant and is represented by the icon ⊗.

- **Scan Started**: When a software compliance scan is in progress and information is currently being calculated, the server is represented by the icon ⊠.

- **Scan Needed**: If a server's software compliance information must be (re)calculated or its compliance information could be inaccurate, it is represented by the icon ▢.

- **Not Applicable**: Software compliance information is not applicable and the server is represented by a dash (—).

  For example, if you detach a software policy from a managed server but do not remediate the server against the detached software policy to remove the installed software, the server's compliance status is displayed as Not Applicable.

Using the SA Client, you can scan for software compliance by selecting servers from the server list or from the Compliance view of a server or device group. See Running the Software Policy Compliance Scan for information about performing a compliance scan from the server list. See "The Compliance View" in the *SA User Guide: Audit and Compliance* for information about the Compliance View for a device or device group.

Running the Software Policy Compliance Scan

Perform the following tasks to scan a managed server for software policy compliance:

1   From the SA Client navigation pane, select **Devices** > **Servers** >**All Managed Servers**. The server list appears in the content pane.

2   From the content pane, select a server to scan.

3   From the **Actions** menu, select **Scan** > **Software Compliance**. During the scan, a dialogue shows the status of the scan. After the scan, the compliance status of the server appears in the server list.

The results of this scan show you the servers that are in compliance and the servers that are out of compliance and specify the software policies that need to be synchronized.

Remediate non-compliant servers against the specified software policy to bring the servers back into compliance. The software compliance scan status is automatically updated after you install or uninstall software or remediate a software policy against a managed server. For more information, see Remediating Servers with Software Policies.

About Software Policy Reports

For information about viewing, launching, and scheduling reports, and building custom reports, see the "Reports" section of the *HP Automation Insight User Guide*.

For specific information about HP Automation Insight reports and universes, see the solution pack user guides that are provided with each solution pack available for download on HPLN.

About Software Resources in the SA Library

The SA Library stores software resources such as application configurations, policies, patches, patch policies, packages, OS sequences, OS profiles, Windows COM+, Users and Groups, Local Security Settings. The SA Library is organized by resource type and by folder. You can view software resources either by their type or by their location in the folder hierarchy.

*   The by type view is organized by the type of object (policy, package, OS, patch, script). This view is a popular starting point for most of the software management activities, such as creating application configurations, running scripts, attaching policies to servers.

*   The folder view allows you to manage user group access to the software resources and is organized by operating system as a default. Folders can be added, moved, etc. It is where the admin can organize and manage permissions to shared resources. When you add or import resources, you specify a folder location. The location you specify will determine which user groups can access it.

Note: For more information about the SA Library, see "Exploring the SA Library" in the *SA User Guide: Server Automation*.

About Importing and Creating Your Software Resources

Setting up your SA Library involves uploading packages and patches to SA, creating scripts, creating application configurations, setting up policies with the software resources that are required to be installed, and managing dependencies between software resources across policies.

Steps for setting up your SA Library:

- Importing software packages and patches
- For instructions on importing and managing software packages, see Managing Software Packages in this guide.
- For information on importing patches to SA, and managing patches and patch policies, see the *SA User Guide: Server Patching*.
- Importing or creating scripts
- For information on importing, creating, and managing scripts, see the *SA User Guide: Server Automation*.
- Creating Application Configurations
- For information on creating application configurations, see the *SA User Guide: Application Configuration*.
- Creating Software Policies
- For instructions on creating software policies and managing dependencies between software resources across policies, see Creating and Managing Software Policies
- Organizing Resources into Folders
- For instructions on creating folders and managing the folder hierarchy, see the *SA User Guide: Server Automation*
- Managing Server Objects
- For instructions on adding and managing server objects (such as services, COM+, Windows Registry, IIS Metabase, Unix User's and Groups, Local Security Settings, .NET Framework Configurations), see the *SA User Guide: Audit and Compliance*.

Note: For additional information about related tasks, see the *SA User Guide: Audit and Compliance*, *SA User Guide: Server Patching*, *SA User Guide: Application Configuration*, *SA User Guide: Provisioning*, and *SA User Guide: Server Automation*.

Software Discovery

The Server Automation (SA) Software Discovery module provides a signature-based software discovery mechanism for Windows and UNIX managed servers to help you manage applications and software that are not already managed by SA. Specifically, the Software Discovery feature:

- Discovers software by scanning the file system. The signature-based mechanism enables discovery of software even if it is unlicensed, unregistered, custom-built or not installed using one of the standard vendor packaging technologies.

- Creates an inventory of software programs that have not been installed as an OS-registered application, such as RPMs on a Linux system.

- Provides system administrators the ability to create snapshots of all the discovered software on a server and then periodically audit against the snapshot over time. This can help you upgrade a server, remove unwanted software and modify a server to conform to your organization's security policies.

- Gives auditors a convenient method of capturing the current state of a server's software and discovering unsupported or unlicensed software installed on a server. By running the audit on a regular schedule, you can monitor software changes over time.

Software Discovery is a read-only server module that provides a rich inventory of software on a managed server.

> **Note:** When importing the custom signature file (XML generated with the SAI Editor) into a SQLite-database, only files with file type: Main will be accepted. File types Associated and 3rdParty are ignored and will not be inserted in the footprints table in the generated SQL database. To mark the file as "Main," right-click the file in SAI Editor and select Relationship to Application > Main.

Software Discovery Prerequisites

To deploy the Software Discovery feature, you must meet the following requirements:

- Have a BSA Essentials account.

  — You can request a BSA Essentials account from the HP Live Network (HPLN) at:

    http://www.hp.com/go/livenetwork

    Login using your HP Passport credentials.

- Have the Live Network connector (LNc), installed and configured on your core server. The LNc is the client for the HP Live Network, which automates content updates, downloads, and imports into the product (SA, BSAE, SAR).

  The LNc is installed with Server Automation. Refer to the LNc documentation for configuration instructions.

> **Requirement: IMPORTANT**: LNc will not list, download, preview, or import content if you do not have the proper products specified! See the *Live Network connector Users Guide* (a.k.a. *LNc Users Guide*) on the HP Live Network for instructions on enabling products.

> **Note:** For additional information about Software Discovery see the SA Software Discovery Reference Guide available on the HP Live Network at **http://www.hp.com/go/livenetwork**. Login using your HP Passport credentials and select Server Automation Community to view announcements and associated projects pertaining to Server Automation, including Software Discovery.

Chapter 2 Creating and Managing Software Policies

The policy management tasks include:

- Creating Software Policies and Software Templates
- Opening a policy or Template
- Editing Software Policy Properties
- Adding Software Resources to a Software Policy
- Specifying the Installation/Uninstallation Order in a Software Policy
- Setting Installation and Update Options for a RPM
- Removing a Software Resource from a software policy
- Adding Custom Attributes to a Software Policy
- Editing Custom Attributes in a software policy
- Deleting Custom Attributes from a software policy
- Adding Custom Attributes to Servers
- Duplicating Zip Packages
- Editing the ZIP Installation Directory
- Viewing Servers Attached to a software policy
- Viewing All the policies Associated with a software policy
- Viewing the History of a software policy
- Viewing OS Sequence Associated with a software policy
- Locating policies in Folders

Creating Software Policies and Software Templates

A policy contains software resources such as packages, patches, RPM packages, scripts, application configurations, and server objects that need to be installed on managed servers. A software template is a policy that can only contain other policies.

In the SA Client, you can create a policy or template in the following ways:

- Creating a Software Policy or Template from the By Type View in the Library
- Creating a Software Policy or Template from the By Folder view in the Library

Creating a Software Policy or Template from the By Type View in the Library

To create a policy in the SA Client:

1 From the navigation pane, select **Library** > **By Type** > policies. The list of policies appears in the content pan. By default, the policies are organized by operating system families.
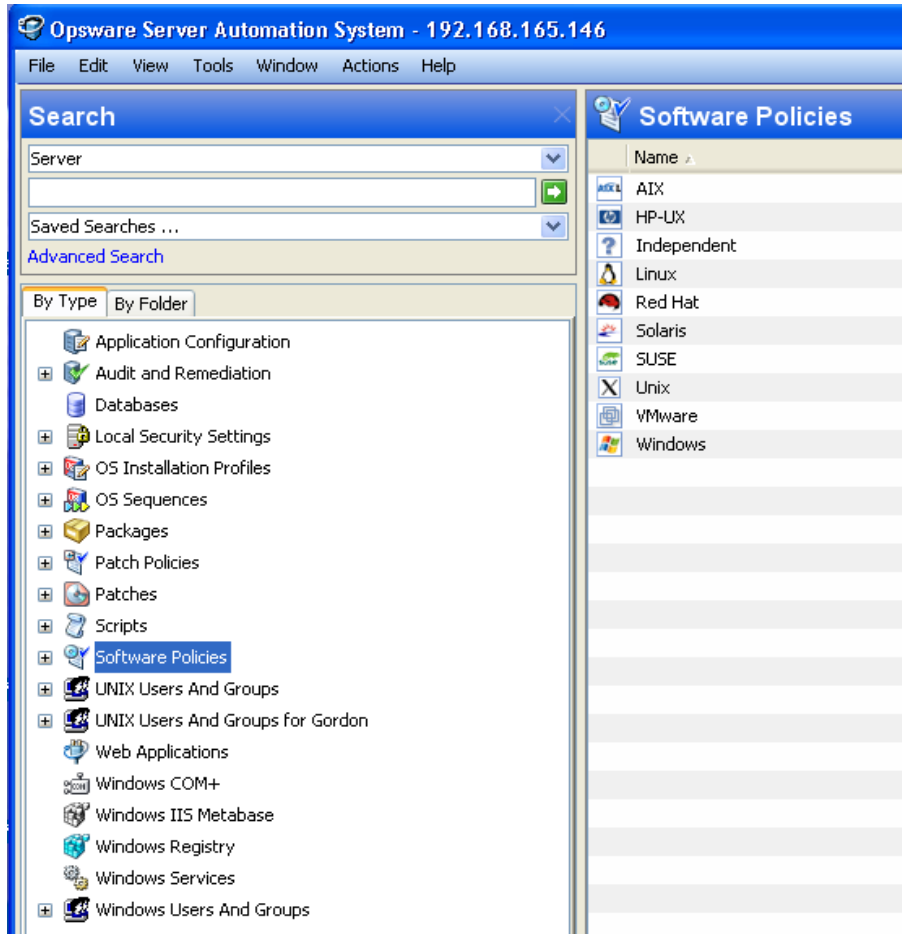
2 Select a specific operating system.

3 From the **Actions** menu, select **New**. The policy window appears.

4 In the Name field, enter the name of the software policy.

5 In the Description field, enter text that describes the purpose or contents of the policy.

6 Click **Select** to specify the location for the policy in the folder hierarchy. The Select Folder window appears. Select a folder in the Library to specify the location of the policy and then click **Select**.

7 From the Availability drop-down list, select the SA server life cycle values for the software policy.

8 From the OS drop-down list, select the operating system family or specific operating systems in that family.

9   In the *Template field*, select Yes to designate a policy as a template. A policy template is not persistently associated with a server. See the Software Policy Templates for information about policy templates.

10 To save the changes, select **Save** from the **File** menu.

Note: In the SA Client, a policy is represented by the icon ⬙. A software template is represented by the icon ⬙.

Creating a Software Policy or Template from the By Folder view in the Library

To create a policy in the SA Client:

1   From the navigation pane, select **Library** > **By Folder**. The folder hierarchy in the Library appears in the content pane.

2   Select the folder that should contain the software policy.

3   From the **Actions** menu, select **New software policy**. The policy window appears.

4   In the Name field, enter the name of the software policy.

5   In the Description field, enter text that describes the purpose or contents of the policy.

6   Click **Select** to change the location for the policy in the folder hierarchy. The Select Folder window appears. Select a folder in the Library to specify the location of the policy and then click **Select**.

7   From the Availability drop-down list, select the SA server life cycle values for the software policy.

8   From the OS drop-down list, select the operating system family or specific operating systems in that family.

9   In the *Template field*, select Yes to designate a policy as a template. A policy template is not persistently associated with a server. See the Software Policy Templates for information about policy templates.

10 To save the changes, select **Save** from the **File** menu.

Note: In the SA Client, a policy is represented by the icon ⬙. A software template is represented by the icon ⬙.

Opening a policy or Template

In the SA Client, there are several ways to open a policy or template. You can open a policy from:

•   The Search option in the navigation pane

•   The Devices option in the navigation pane

•   The By Type view in the Library

•   The By Folder view in the Library

Opening a policy from Search

1   From the navigation pane, select **Search**.

2   Select policy from the drop-down list and then enter the name of the policy in the text field.

3   Select ⬀. The search results appear in the content pane.

4   From the content pane, select the policy and then select **Open** from the **Actions** menu. The policy window appears.

Opening a Software Policy from Devices

1   From the navigation pane, select **Devices** > **Servers** > **All Managed Servers**. The server list appears in the content pane.

     Or

     From the navigation pane, select **Devices** > **Device Groups**. The device groups list appears in the content pane.

2   From the content pane, select a server and then from the **Actions** menu, select **Open**. The Server Explorer window opens.

3   From the Views pane, select **Management Policies** > **Software Policies**. The policies attached to the server appear in the content pane.

4   From the content pane, select the policy and then select **Open** from the **Actions** menu. The policy window appears.

Opening a Software Policy from the By Type view in the Library

1   From the navigation pane, select **Library** > **By Type** > policies. The policies appear in the content pane.

2   From the content pane, select the policy and then select **Open** from the **Actions** menu. The policy window appears.

Opening a Software Policy from the By Folder view in the Library

1   From the navigation pane, select **Library** > **By Folder**. The folder hierarchy in the Library appears in the content pane.

2   From the content pane, select the policy in a folder and then select **Open** from the **Actions** menu. The policy window appears.

Editing Software Policy Properties

After you create a software policy, you can view and modify its properties. You can view properties such as the SA user who created the software policy, the date when it was created, and the SA ID of the software policy. You can also modify the name, description, availability, the location of the policy in the Library and the operating systems of the software policy.

To define the properties of a software policy:

1 From the navigation pane, select **Library** > **By Type** > policies.

2 From the content pane, select the policy and open it. The policy window appears.
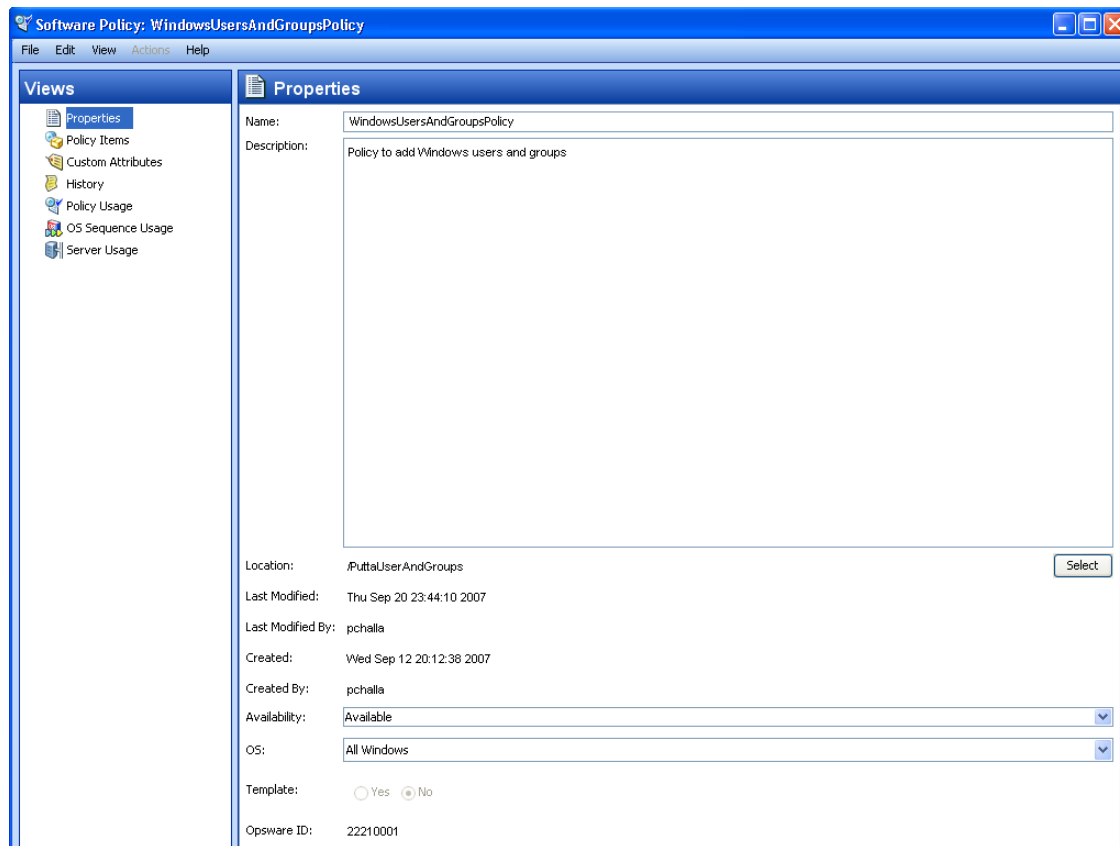
3 From the Views pane, select Properties. You can edit the name, description, location, life cycle, and operating systems for the policy in the content pane.

4 In the Name field, edit the name for the software policy.

5 In the Description field, edit the text that describes the purpose or contents of the policy.

6 Click **Select** to change the location for the policy in the folder hierarchy. The Select Folder window appears. Select a folder in the Library to specify the location of the policy and then click **Select**.

7 From the Availability drop-down list, select the SA server life cycle values for the software policy.

8 From the OS drop-down list, select the operating system family or specific operating systems in that family. If the chosen operating system family does not match any of the software packages in the policy, a dialog will appear displaying the non-matching items and providing the option to remove the non-matching items.

    • If you do not wish to remove the non-matching items, click Cancel to change the OS selection or to modify the packages included in the policy.

    • If you still wish to proceed, click Next.

Important: If you choose to remove the non-matching items and save the policy, the next time the attached servers are remediated, those packages will be uninstalled from the servers.

9   In the Template field, select Yes to designate a policy as a template. A policy template is not persistently associated with a server. See the Software Policy Templates for information about policy templates.

10 To save the changes, select **Save** from the **File** menu.

> **Note:** In the SA Client, a policy is represented by the icon ![icon] . A software template is represented by the icon ![icon] .

Adding Software Resources to a Software Policy

After you create a software policy, you can add software resources such as patches, packages, application configurations, scripts, and server objects to it. When you add software resources to a software policy, the software resources must contain at least one operating system as that of the software policy. Adding software resources to a policy does not install them on a managed server. After you add software resources to a software policy, you can install the software directly on the managed server or attach it to a managed server and then remediate the software policy. See the Installing Software Using a Software Policy for more information about installing software.

To add software resources to a software policy:

1   From the navigation pane, select **Library** > **By Type** > policies.

2   From the content pane, select the policy and open it. The policy window appears.

3   From the Views pane, select Policy Items.

4   From the **Actions** menu, select **Add Policy Items**. The Select Library Item window appears as shown

5   Select Browse Types to display a list of policy items that can be added to the software policy. Select the policy item and click **Select**. The selected policy item appear in the content pane.

   or

   Select Browse Folders to display the folder hierarchy in the Library and the list of software resources contained in the folders. Select the policy item and click **Select**. The selected policy item appear in the content pane.

6   To save the changes, select **Save** from the **File** menu.

Viewing Properties of Software Resources in a software policy

Once you have added software resources to a policy you can view the properties of the software resource in the software policy. For example for a package you can view the install flags and information on the reboot option. For Windows Services you can view the list of services and for Windows patch you can view the install path, install flags, and the information on the reboot information.

You cannot edit the properties of the software resources in the software policy. To edit the properties for a software resource, you must open the specific software resource window and edit.

Only for RPM packages and scripts, you can edit some of the properties in a software policy. For scripts you can specify the command options in a software policy. For RPM packages you can set the installation and update options in a software policy. See Setting Installation and Update Options for a RPM for more information.

To view the properties of a software resource in a software policy:

1   From the navigation pane, select **Library** > **By Type** > policies.
2   From the content pane, select the policy and open it. The policy window appears.
3   From the Views pane, select Policy Items. The policy items appear in the content pane.
4   Select a policy item. The properties of that policy item appear in the details pane.

Specifying the Installation/Uninstallation Order in a Software Policy

Once you have added the software resources to a software policy, you can specify the installation order among packages, patches, scripts, application configurations, included policies, and server objects in the software policy. When you specify the installation order for the included policies, all the software resources in the included policy are grouped together and installed as a unit.

When you specify the installation order for installing the software resources in a software policy, the software resources are installed in the same order. During Uninstallation, by default, SA will uninstall the software resources (except scripts and application configurations) defined in the policy in the reverse order.

You can also specify a separate uninstallation order for the software resources in a software policy. The uninstallation order can be completely different from the installation order. During Uninstallation, SA will uninstall all the software resources (except application configurations) defined in the software policy.

To specify the installation or uninstallation order in a software policy:

1   From the navigation pane, select **Library** > **By Type** > policies.
2   From the content pane, select the policy and open it. The policy window appears.
3   From the Views pane, select Policy Items. The list of all the software resources in the policy appear in the content pane.
4   (Optional) From the Actions menu, deselect **Automatic Uninstall Ordering** to specify the uninstallation sequence.
5   Select **Install Sequence** to specify the installation order as shown:
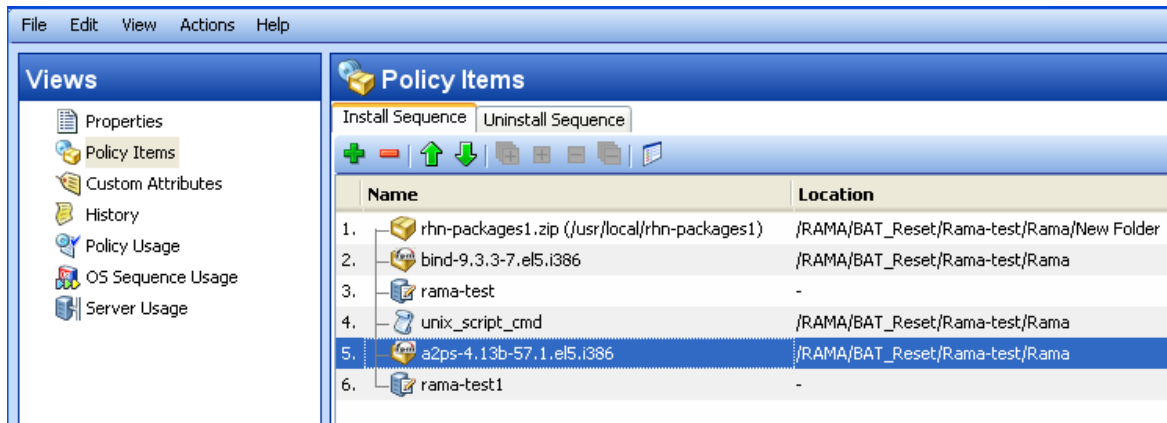
(Select **Uninstall Sequence** to specify the uninstallation order.)

6   Select the Policy Item and then from the **Actions** menu, select **Move up** or **Move down** to order the policy items.

Or select the Policy Item and then select 🔼 or 🔽.

7   Click **File > Save** to save the policy. When prompted, click **OK** to continue.

Deleting Install/Uninstall Sequences

You can delete install and uninstall sequences by highlighting the sequence and selecting delete. You will be prompted to confirm the deletion. Click **OK** to continue.

Setting Installation and Update Options for a RPM

Once you have added a RPM to a software policy, you can specify if the RPM needs to be installed on the server or upgraded to the latest version during remediation. To install or upgrade the RPMs on a managed server, you must remediate the server with the software policy attached.

> **Note:** RPMs are installed or upgraded *only* during remediation. Attaching or detaching a software policy and defining the installation and update options does not—by itself—install, update or uninstall the RPM.

You can specify policy-specific installation and update options for RPMs within the policy.

To specify the installation option for a RPM package:

1   From the navigation pane, select **Library** > **By Type** > **Software Policies**.

2   From the content pane, select the policy containing a RPM package and open it. The policy window appears.

3   From the Views pane, select Policy Items. The list of software resources contained in the policy appears in the content pane as shown below.

4   Select a RPM package. For every RPM package, you can specify the following options:

- Choose an Install Criteria option:

    — Select the **Install RPM always** option to install the selected RPM on the managed server.

    — Select the **Install RPM only if an earlier version is installed** option to update the RPM version on the managed server only if an existing version of that RPM is already installed on the server.

- Choose an Auto-Update Policy option:

    — Select **Version or Release** to automatically update the RPM in the policy to a newer version or release of the RPM.

    — Select **Release Only** to automatically update the RPM in the policy only when a new *release* of the RPM is available. The important distinction in this option is between RPM releases versus RPM versions. When this option is selected, the policy will *not* be updated if the new RPM is just a new *version* of an existing release; it will be updated if the new RPM is a new *release*.

    Based on the selected option, the policy will get updated when a newer version or release of the RPM is placed in the same folder location as the one specified in the policy. For details about the Auto-Update option, see Automatically Updating PPMs in a Software Policy

5   To save the changes, select **Save** from the **File** menu.

To specify the installation options for multiple RPM packages:

1   From the navigation pane, select **Library**>**By Type**>**Software Policies**.

2   From the content pane, select the policy containing a RPM package and open it. The policy window appears.

3   From the Views pane, select Policy Items. The list of software resources contained in the policy appears in the content pane as shown below.
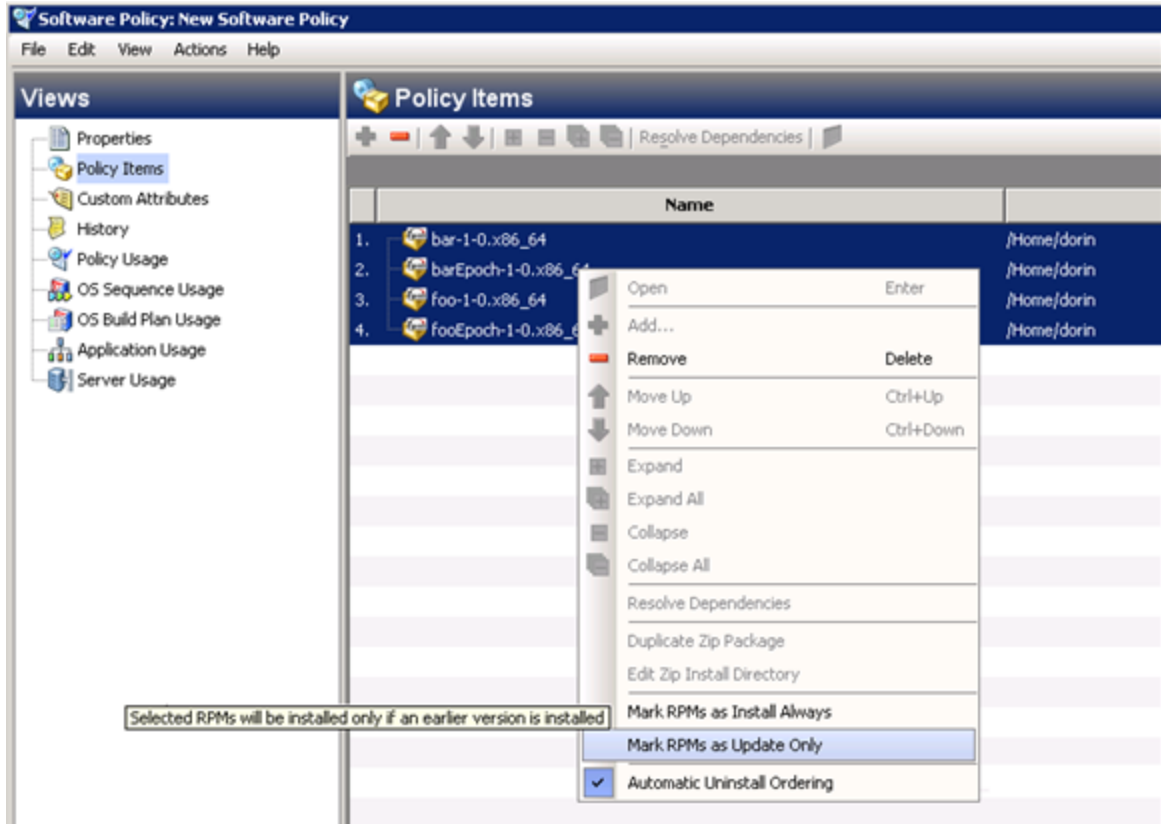
- Select multiple RPM packages and then right-click to choose an install criteria option:

- Use '**Mark RPMs as Install Always**' to set the install criteria of the selected RPM packages as "Install RPM always".

- Use '**Mark RPMs as Update Only**' to set the install criteria of the selected RPM as "Install RPM only" if an earlier version is installed.

4   To save the changes, select **Save** from the **File** menu.

Note: The RPM will become managed by the policy when the policy is remediated. If the RPM was already installed on the managed server, then it will be adopted by the policy during the remediation process.

Removing a Software Resource from a software policy

Removing a software resource from a policy does not uninstall it from a managed server. It only removes the software resource from the software policy. To uninstall the software resource from a managed server, you must uninstall or remediate the software policy. See the Installing Software Using a Software Policyfor more information about uninstalling software.

To remove a package from a software policy:

1   From the navigation pane, select **Library** > **By Type** > policies.
2   From the content pane, select the policy and open it. The policy window appears.
3   From the Views pane, select Policy Items.
4   Select the items that you want to remove from the list of policy items displayed in the content pane.
5   From the **Actions** menu, select **Remove Policy Item**.
6   To save the changes, select **Save** from the **File** menu.

Adding Custom Attributes to a Software Policy

When you add a custom attribute to a software policy, the attribute values affect the servers attached to the software policy. After you add a custom attribute to a software policy, you must attach it to a managed server and then remediate the software policy.

To add a custom attribute to a software policy:

1   From the navigation pane, select **Library** > **By Type** > policies.
2   From the content pane, select the policy and open it. The policy window appears.
3   From the Views pane, select Custom Attributes.
4   Click **Add**.
5   In the Name field, enter the name of the custom attribute.
6   In the Value field click ⟦…⟧. The Input dialog appears. Enter the value for the custom attribute.
7   To save the changes, select **Save** from the **File** menu.

Editing Custom Attributes in a software policy

To edit a custom attribute:

1   From the navigation pane, select **Library** > **By Type** > policies.
2   From the content pane, select the policy and open it. The policy window appears.
3   From the Views pane, select Custom Attributes.
4   Select the custom attribute that you want to edit.
5   Update the name and value for the custom attribute in the content pane.
6   To save the changes, select **Save** from the **File** menu.

Deleting Custom Attributes from a software policy

To delete a custom attribute:

1 From the navigation pane, select **Library** > **By Type** > policies.

2 From the content pane, select the policy and open it. The policy window appears.

3 From the Views pane, select Custom Attributes.

4 From the content pane, select the custom attribute that you want to delete and then click **Remove**.

5 To save the changes, select **Save** from the **File** menu.

Adding Custom Attributes to Servers

Using the SA Client, you can assign custom attributes to servers or groups of servers directly. This allows you to override the custom attribute set by a software policy.

To add a custom attribute to a managed server:

1 From the navigation pane, select **Devices** > **Servers** >**All Managed Servers**.

2 From the content pane, select the server and open it. The Server Explorer window appears.

3 From the Views pane, select Custom Attributes.

4 Click **Add**.

5 In the Name field, enter the name of the custom attribute.

6 In the Value field click ⬚. The Input dialog appears. Enter the value for the custom attribute.

7 To save the changes, select **Save** from the **File** menu.

Duplicating Zip Packages

The Software Management feature allows you to install multiple instances of an application on a single server by using ZIP packages in a software policy. (In SA, these ZIP packages are sometimes referred to as "relocatable ZIPs.") You can install the same ZIP package with different installation paths in multiple locations on a single server. SA supports installation of ZIP packages on both Unix and Windows operating systems. If the ZIP package was created with the IDK, then you cannot install the ZIP package into multiple locations on a single server.

To create ZIP packages with different installation paths:

1 From the navigation pane, select **Library** > **By Type** > policies.

2 From the content pane, select the policy containing the ZIP package and open it. The policy window appears.

3 From the Views pane, select Policy Items.

4 From the content pane, select the ZIP package.

5 From the **Actions** menu, select **Duplicate Zip Package**. The Duplicate ZIP Package window appears.
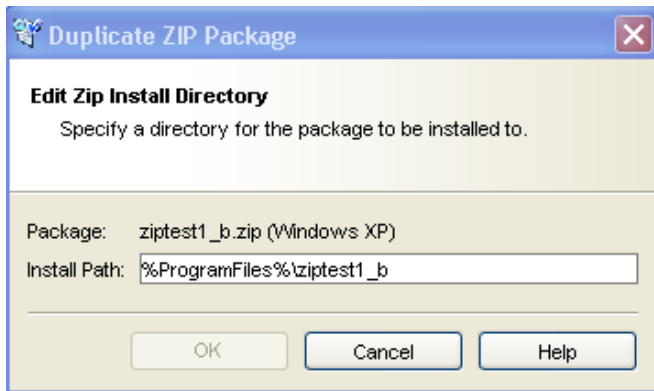
6   In the Install Path field, enter the path where you will install the ZIP file. If you do not enter a path, the default directory for the Windows ZIP package is:

```
%SystemDrive%\Program Files\[basename of zip file]
```

The default directory for Unix Zip is:

```
/usr/local/[basename of zip file]
```

7   Click **OK** to install the Zip file.

Editing the ZIP Installation Directory

To change the default installation directory for ZIP packages:

1   From the navigation pane, select **Library** > **By Type** > policies.

2   From the content pane, select the policy containing the ZIP package and open it. The policy window appears.

3   From the Views pane, select Policy Items.

4   From the content pane, select the ZIP package.

5   From the **Actions** menu, select **Edit Zip Install Directory**. The Edit ZIP Install Directory window appears.

6   In the Install Path field, enter the new path. If you do not enter a path, the default directory is for Windows ZIP package is:

```
%SystemDrive%\Program Files\[basename of zip file]
```

The default directory for Unix ZIP package is:

```
\usr\local\[basename of zip file]
```

7   Click **OK** to change the default installation directory for ZIP packages.

Viewing Servers Attached to a software policy

In the SA Client, you can view the list of all servers attached to a policy and servers that are detached from a policy and not yet remediated from the software policy. In the policy window, the servers that are detached from a policy and not yet remediated from the policy are represented by a gray icon as shown in Server Usage in the Policy Window .

Server Usage in the Policy Window
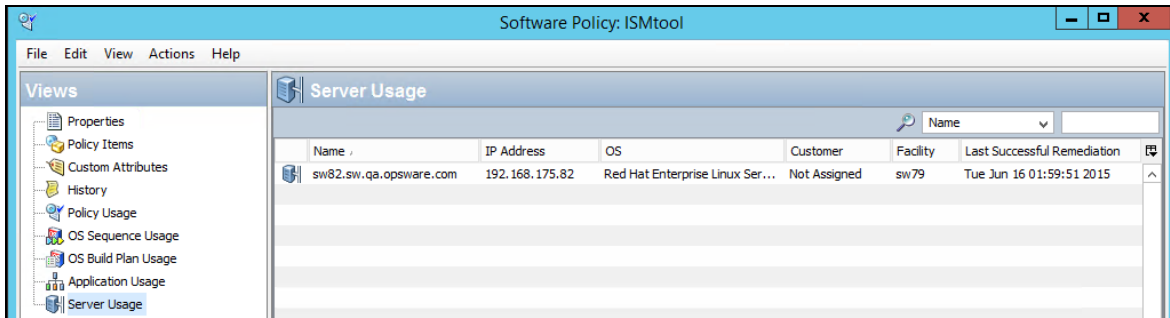
To view the servers attached to a software policy:

1   From the navigation pane, select **Library** > **By Type** > policies.

2   From the content pane, select the policy and open it. The policy window appears.

3   From the Views pane, select Server Usage.

4   (Optional) Enable "Last Successful Remediation" , to check when was a Software Policy last remediated successfully on the server .

Viewing All the policies Associated with a software policy

A policy can contain other policies. In the policy window, you can view all the policies that contain the selected policy.

To view policies associated with a software policy:

1   From the navigation pane, select **Library** > **By Type** > policies.

2   From the content pane, select the policy and open it. The policy window appears.

3   From the Views pane, select Policy Usage. The list of policies associated with the selected policy appears in the content pane.

Viewing OS Sequence Associated with a software policy

A policy can be associated with an OS Sequence. In the policy window, you can view all the OS Sequences a policy is associated with.

Note: OS Sequences are a deprecated method for provisioning. Use OS Build Plans if possible. See the SA User Guide: Provisioning for details.

To view the OS Sequence a policy is associated with:

1   From the navigation pane, select **Library** > **By Type** > policies.

2   From the content pane, select the policy and open it. The policy window appears.

3   From the Views pane, select OS Sequence Usage. The list of OS Sequences the selected policy is associated with appears in the content pane.

Viewing the History of a software policy

To view the events associated with a software policy:

1   From the navigation pane, select **Library** > **By Type** > policies.

2   From the content pane, select the policy and open it. The policy window appears.

3   From the Views pane, select **History**. The events associated with the policy will display in the content pane. You can view the action performed on a software policy (including custom-attribute changes), the user who performed the action, and the time when the action was performed.

Locating policies in Folders

To locate a policy in the folder hierarchy:

1   From the navigation pane, select **Library** > **By Type** > policies.

2   From the content pane, select the policy and then select **Locate in Folders** from the **Actions** menu. The folder hierarchy for the policy appears in the content pane.

Chapter 3 Managing Software Packages

Packages are made available in HP Server Automation (SA) by uploading the packages to the SA Library with the SA Client or by using the SA Command Line Interface 1.0 (OCLI 1.0). For information on OCLI 1.0, see the SA User Guide: Server Automation.

The SA Library provides a data store for all software that the SA Client manages. After you upload packages to the SA Library, you can install packages by adding packages to policies, attaching policies to servers, and then performing a server remediation.

Each operating system that SA supports has a list of package types that you can upload.

> **Note:** The ability to perform specific actions in SA is governed by your permission settings. To obtain additional permissions, contact your SA Administrator. See the *SA Administration Guide* for more information.
> See the *SA Support and Compatibility Matrix* for detailed information about supported operating systems.

Importing Software Packages

Software packages are downloaded from the vendor's web site and then imported (uploaded) into HP Server Automation. A package can be imported with the SA Client or the command line utility. This topic describes importing software packages into the SA Library using the SA Client.

> **Note:** See the *SA User Guide: Server Automation* for information about importing packages with a script using the SA Command Line Interface 1.0 (OCLI 1.0). See the *SA User Guide: Server Patching* for information about importing patches.

You can import multiple software packages simultaneously. If a software package that is being uploaded already exists in the SA Library, you can replace (overwrite) the contents of the existing package, skip the package import (useful when importing multiple packages), or cancel the import. When overwriting an existing software package, SA preserves any reboot options or flags previously set for the package.

To import a software package:

1   From the navigation pane, select **Library** > **By Type** > **Packages**. The packages organized by operating system appear in the content pane. Drill down to the operating system where the package should be imported.

Or

From the navigation pane, select **Library** > **By Folder** and then select the folder in which the package should be imported.

2 From the **Actions** menu, select **Import Software**. The Import Software window appears.

3 In the File section of the Import Software window:

a Click **Browse** to locate the packages to import.
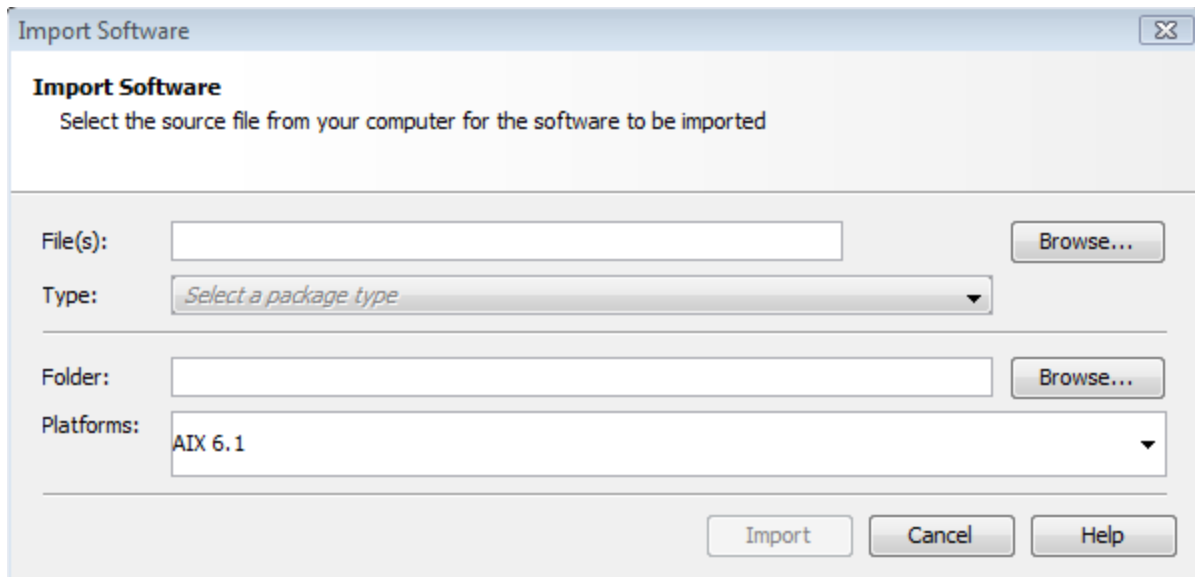
b In the Open window, select the packages to import and specify the character encoding to be used by the packages from the Encoding drop-down list.

You must specify the character encoding so that SA can extract the metadata contained in the packages and correctly display the information in non-ASCII characters in the SA Client (for example, in the Package Properties pages). Package metadata includes comments, READMEs, scripts, descriptions, and content lists.
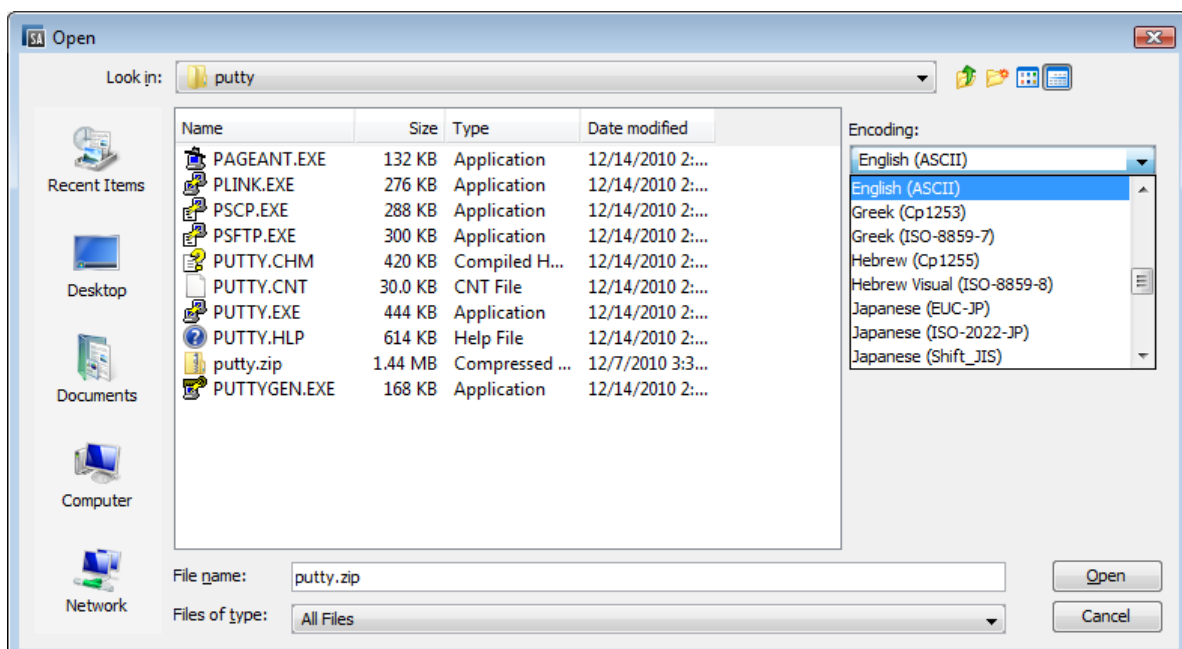
    c   Click **Open**. The Import Software window reappears.

    d   Select the file type from the **Type** drop-down list.

        When importing multiple files, all files must be of the same type. Some of the package types include Windows MSI, ZIP, Executable, application installation media, RPM, Solaris Package.

4   In the Folder section of the Import Software window, click **Browse** to specify the folder location for the packages.

    a   In the Select Folder window, select the import destination location and click **Select**. The Import Software window reappears.

    b   From the **Platform** drop-down list, select the operating system family or operating system. You can also select multiple operating system families.
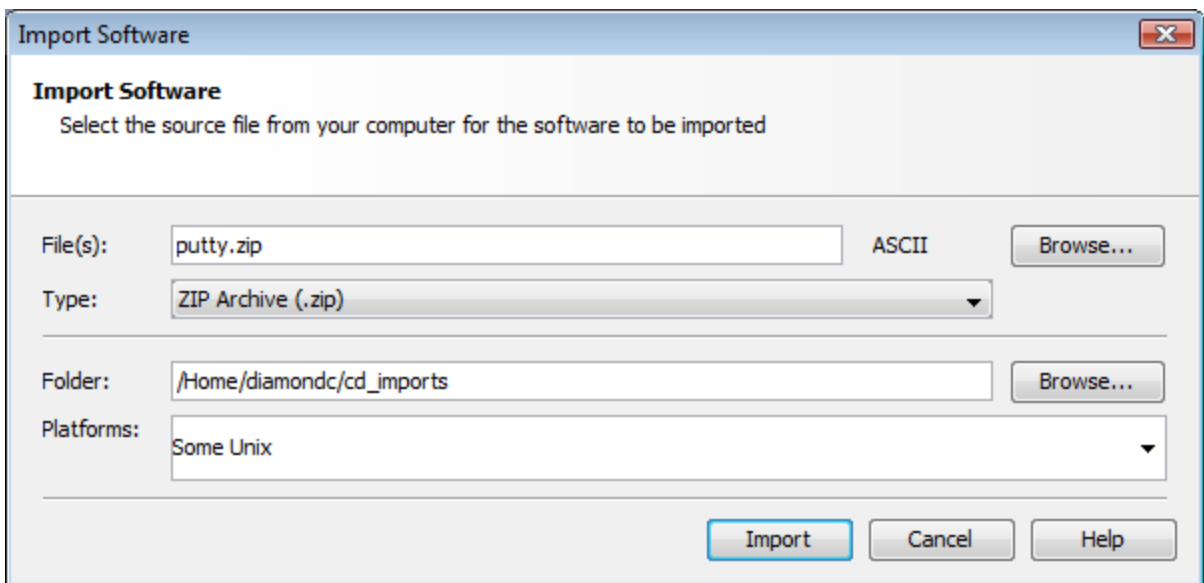
> **Note:** Most packages are specific to Unix platforms or Windows platforms and therefore cannot be imported for both Unix and Windows platforms at once. The only kind of package you can import for a mixture of Unix and Windows platforms are non-platform-specific server module results and unknown packages.

5   Click **Import**.

(Optional) If one of the packages you are importing already exists in the folder, you will be prompted with the following options for handling the duplicate file:

You have the following options:

- **Replace**: Replace (overwrite) the contents of the existing file.

- **Replace All**: When there are multiple existing files with the same name as the file you are importing, you can replace (overwrite) the contents of all the existing file.

- **Skip**: Skip the replacement of a single file. If you have multiple existing files with the same name as the file you are importing, you can select which files to skip or not. Skipping the import of a file does not affect other files with different names if you are

importing multiple files. Only the specified file(s) will be skipped, the other specified files will be imported.

- **Skip All**: All specified files with the same name as the file you are importing will be skipped and not replaced.

- **Cancel**: Cancels the Import Packages operation entirely. No files are imported.

- **Help**: Provides online help for the current dialog.

6   View the progress of the importing files in the Software Imports window

While the import is underway, the Software Imports window displays the details and progress of the import. This window displays all the imports made within the session.
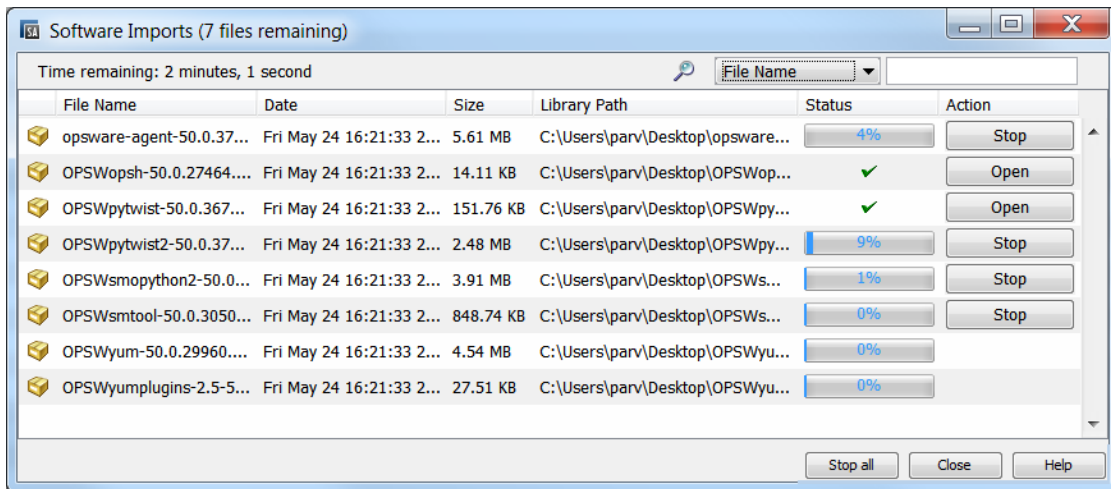
Software Imports window options:

- Click **Stop** if you wish to cancel an import process that is underway.

- Click Stop All to stop the processing of all packages at once.

- Click **Open** to open the imported package browser in SA.

- Click any column to sort the list of files by that value.

- For long lists, use the Search option at the top of the window to find any file in the list by the file name or path.

- Click **Close** to close the window.

  — If you wish to open it later, select **Tools** > **Software Imports**.

Importing Application Installation Media

SA allows you to import a software application such as Symantec Antivirus, provided by a software vendor using the SA Client and then deploy the software application by using policies.

Note: See the Remediating and Installing Software for information about installing software.

There are a few preparation steps you must preform before importing a software application from the software vendor using the SA Client.

To prepare for importing software from a vendor:

1 Obtain the application installation media from the software vendor on a CD or DVD, or download the application installation media.

2 Develop any required scripts or response files for the application media. The application must support silent install.

3 Create a ZIP file containing the application installer.

Once the ZIP file containing the application installer is created, you can use the SA Client to import the application installer to SA.

To import application installation media:

1 From the navigation pane, select **Library** > **By Type** > **Packages**. The packages organized by operating system appear in the content pane.

   Or

   From the navigation pane, select **Library** > **By Folder** and then select the folder in which the package should be located.

2 From the **Actions** menu, select **Import Package**. The Import Software window appears.

3 Click **Browse** to locate and select the packages to import.

4 In the Open window, select the character encoding to be used by the package from the Encoding drop-down list.

   You need to specify the character encoding so that SA can extract the metadata contained in the package and correctly display the information in non-ASCII characters in the SA Client (for example, in the Package Properties pages). Package metadata includes comments, READMEs, scripts, descriptions, and content lists.

5 In the Import Software window, select Application Installation Media from the Filetype drop-down list.

6 Click **Browse** to specify the folder location for the packages. The Select Folder window appears.

7 From the Platform drop-down list, select the operating system family or operating systems. You can also select multiple operating system families.

8 Click **Import**.

9 From the navigation pane, select **Library** > **By Type** > **Packages**. The packages organized by operating system appear in the content pane. Select the package and open.

10 In the Packages window, select **Properties** from the View pane. Enter the installation script and uninstallation script.

11 Select **Save** from the File menu.

Importing Executables

1 From the navigation pane, select **Library** > **By Type** > **Packages**. The packages organized by operating system appear in the content pane.

   Or

   From the navigation pane, select **Library** > **By Folder** and then select the folder in which the package should be located.

2 From the **Actions** menu, select **Import Package**. The Import Software window appears.

3 Click **Browse** to locate and select the packages to import.

4 In the Open window, select the character encoding to be used by the package from the Encoding drop-down list.

   You need to specify the character encoding so that SA can extract the metadata contained in the package and correctly display the information in non-ASCII characters in the SA Client (for example, in the Package Properties pages). Package metadata includes comments, READMEs, scripts, descriptions, and content lists.

5 In the Import Software window, select Executable from the Filetype drop-down list.

6 Click **Browse** to specify the folder location for the packages. The Select Folder window appears.

7 From the Platform drop-down list, select the operating system family or operating systems. You can also select multiple operating system families.

8 Click **Import**.

9 From the navigation pane, select **Library** > **By Type** > **Packages**. The packages organized by operating system appear in the content pane. Select the package and open.

10 In the Packages window, select **Properties** from the View pane. Enter the install command and uninstall command.

11 Select **Save** from the File menu.

Exporting a Software Package

You can export (download) a package to your local computer so that you can check the install-ation of the package on a test or staging machine.

> **Note:** Package types that are not physical files like APARs cannot be downloaded.

1 From the navigation pane, select **Library** > **By Type** > **Packages**. The packages organized by operating systems appear in the content pane.

   Or

   From the navigation pane, select **Library** > **By Folder** and then select the folder which contains the package.

2   From the content pane, select a package to export.

3   From the **Actions** menu, select **Export Software**. The Export Software window appears.

4   In the Browse window, specify the location for the package to be exported to.

5   Click **Export**.

While the export is underway, the Software Exports window displays the details and progress of the export. This window displays all the exports made within the session.
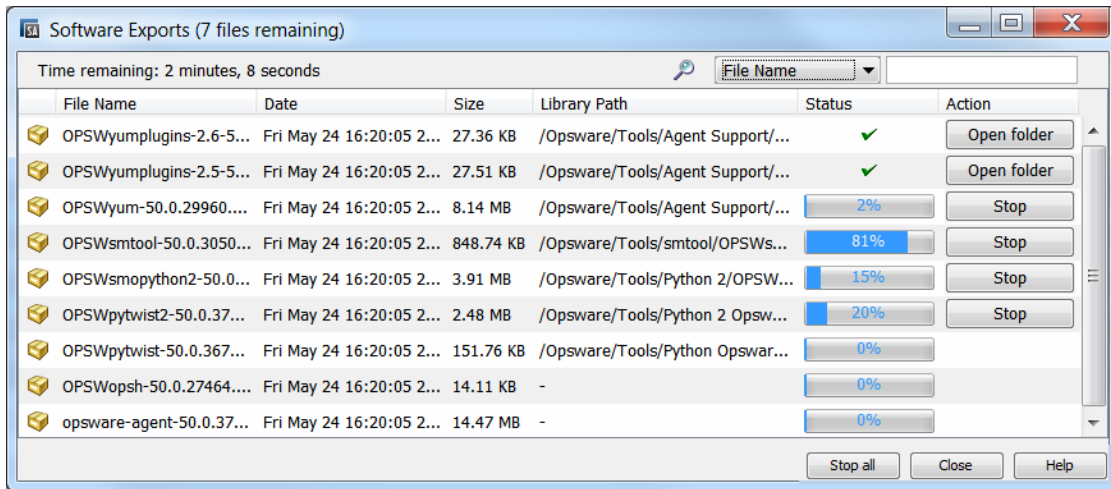
Software Exports window options:

- Click **Stop** if you wish to cancel an export process that is underway.

- Click Stop All to stop the processing of all packages at once.

- Click **Open Folder** to open the folder where a completed export was stored locally.

- Click any column to sort the list of files by that value.

- For long lists, use the Search option at the top of the window to find any file in the list by the file name or path.

-
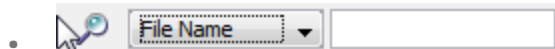
- Click **Close** to close the window.

    — If you wish to open it later, select **Tools** > **Software Exports**.

Ways to Open a Package

In the SA Client, you can open a package in the following ways:

- Opening a Package from the Search Pane

- Opening a Package from the By Type view in the Library

- Opening a Package from the By Folder view in the Library

Opening a Package from the By Folder view in the Library

To open a package from the By Folder tab in the Library:

1   From the navigation pane, select **Library** > **By Folder**. The folder hierarchy in the Library appears in the content pane.

2   From the content pane, select the package in a folder and then select **Open** from the **Actions** menu. The Package window appears.

Opening a Package from the By Type view in the Library

To open a package from the By Type tab in the Library:

1   From the navigation pane, select **Library** > **By Type** > **Packages**. The packages appear in the content pane.

2   From the content pane, select the package and then select **Open** from the **Actions** menu. The Package window appears.

Opening a Package from the Search Pane

To open a package from the Search pane:

1   From the navigation pane, select Search.

2   Select Software from the drop-down list and then enter the name of the package in the text field.

3   Select ➡. The search results appear in the content pane.

4   From the content pane, select the package and then select **Open** from the **Actions** menu. The Package window appears.

Viewing and Editing Package Properties

To view the properties of a package:

1   From the navigation pane, select **Library** > **By Type** > **Packages**. The packages organized by operating systems appear in the content pane.

    Or

    From the navigation pane, select **Library** > **By Folder** and then select the folder which contains the package.

2   From the content pane, select the package to view.

3   From the **Actions** menu, select **Open**. The Package window appears as shown below.
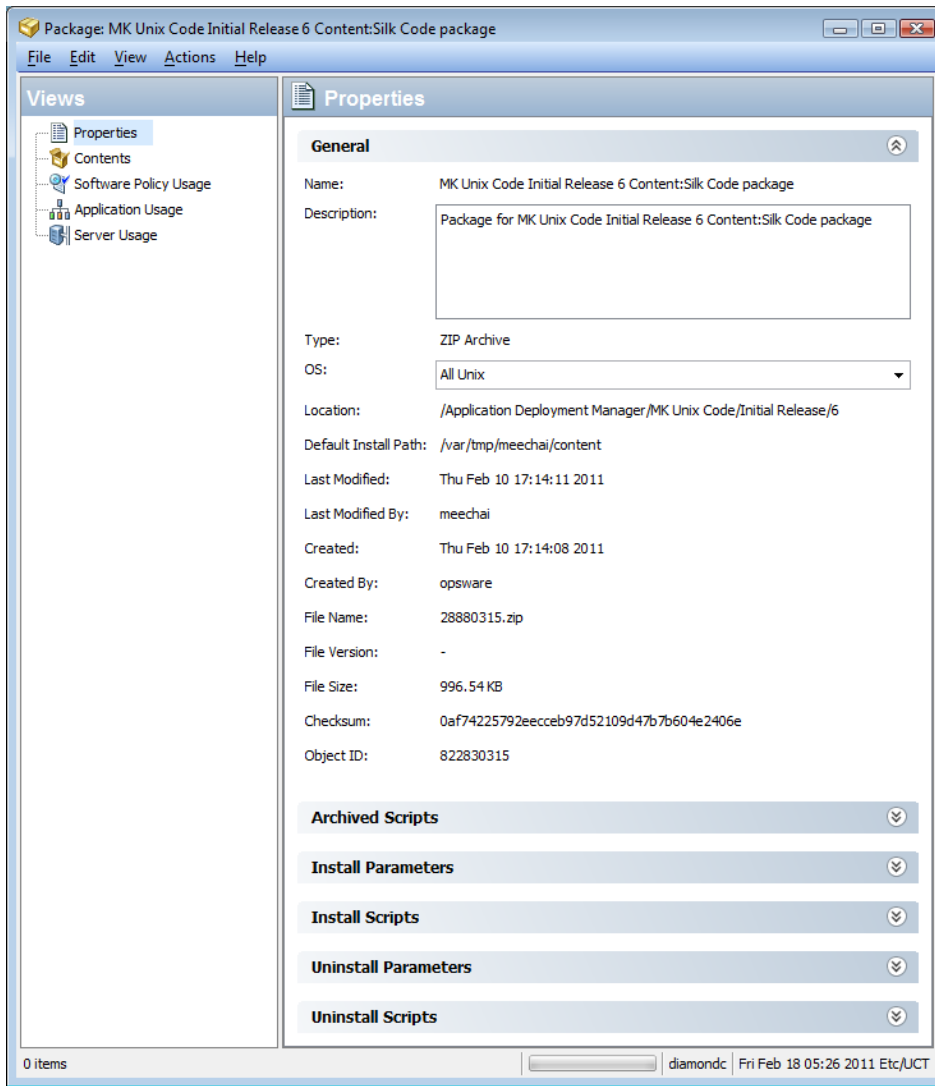
4   From the Views pane, select **Properties**. The package properties appear in the content pane. (See Package Properties Definedand Editing Package Properties)

Package Properties Defined

This is a description of the viewable package property fields, many of which are editable.

> **Note:** For instructions on viewing and editing package properties and contents, seeWays to Open a Package, Editing Package Properties, and Viewing Package Contents.

General Properties

Most of the general properties are predefined based on the package metadata. A few are editable fields, specified in the descriptions below.

– **Name**: The name of the package.

– **Description**: The description of the package's contents. (Editable.)

- **Type**: The type of package.
- **OS**: Select the operating systems associated with the package. (Editable.)
- **Location**: The location of the package in the folder hierarchy.
- **Default Install Path** (Only for Zip packages): The path where the package is installed on a server.
- **Last Modified**: The date when the package was last modified.
- **Last Modified By**: The SA user who last modified the package.
- **Created**: The SA user who created the package.
- **Created By**: The date when the package was created.
- **File Name**: The file name of the package.
- **File version**: The file version of the package.
- **File Size**: The file size of the package.
- **Checksum**: The hash computed by SA when the file is uploaded in order to verify consistency and detect corruption of a file
- **Object ID**: The unique SA ID for the package.

Most of the remaining properties in the expandable/collapsible sections are editable fields.
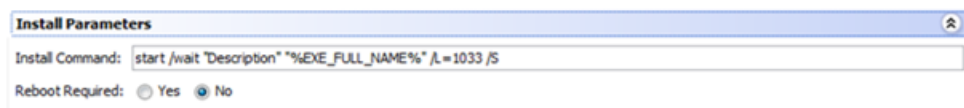
Archived Scripts (ZIP Packages only)

For ZIP packages you can specify additional scripts per unit beyond the install/uninstall scripts. These archived scripts enable you to specify extra steps when remediating ZIP packages to allow more granular control of install.

- **Post-Extraction Script**: The name of the post-extraction script to be run after installing the zip package.
- **Pre-Removal Script**: The name of the pre-removal script to be run before uninstalling the zip package.
- **If Script Returns Error**: An option that stops installation of the package if the script fails.

Install Parameters

- **Install Command**: (Only for Executables) The command that will be used to install the package. For executable packages you are required to enter the install command. For example:

The install command includes:

(Windows):

By default the install parameters are:
```
start /wait "Description" "%EXE_FULL_NAME%"
```

Extra arguments can be appended to the parameter also using this syntax:

```
start /wait "Description" "%EXE_FULL_NAME%" <arguments>
```

Extra arguments are needed for indicating application installation options, such as enabling a silent/unattended install, e.g., '`/S`':

```
start /wait "Description" "%EXE_FULL_NAME%" /S
```

(where '/S' is a Windows example only; actual arguments vary)

(UNIX):

By default the install command is:
```
"%EXE_FULL_NAME%"
```

Extra arguments can be appended to the parameter also using this syntax:
```
"%EXE_FULL_NAME%" <arguments>
```

Extra arguments are needed for indicating application installation options, such as enabling a silent/unattended install, e.g., '`/silent`':

```
"%EXE_FULL_NAME%" silent
```

(where '/silent' is a UNIX example only; actual arguments vary)

The environment variable EXE_FULL_NAME will be replaced by the fully qualified path to the executable when the Install command is run.

If the default install parameters do not work, the installation will time-out or the application window will become interactive.

In the above examples, the silent option prevents the application from becoming interactive or timing out, and enables it to run completely without demanding a response. Usually applications that are run this way should be verified with the vendor. These examples are only for illustration purposes. For instructions on running silent installs, see the vendor's documentation under silent, user-independent, or unattended installs.

- **Install Flags**: (Only for RPM, MSI, Build Customization Scripts) The optional arguments to be run when the package is installed on a managed server.

- **Temporary Path**: (Only for application media) The temporary directory where the zip package is downloaded.

- **Reboot Required**: An option that reboots the server when the package is successfully installed.

- **Response File** (Only for Solaris packages): The Response files that are associated with Solaris package instances.

- **Upgrade** (Only for RPM packages): An option that runs the `-U` parameter during package installation.

Install Scripts

- **Install Script**: (Only for Application Installation Media) A script required to perform a silent installation of the application.

  The environment variable EXTRACT_LOCATION will contain the fully qualified path to the directory where the Application Installation Media package was extracted.

- **Pre-Install Script**: A script required to run on a managed server before the package is installed.

- **Post-Install Script**: A script required to run on a managed server after the package is installed.

- **Stop install if script returns an error**: An option that stops installation of the package if the script fails.

Uninstall Parameters

- **Uninstall Command**: The command that will be used to uninstall the package.

    For executable packages you are required to enter the uninstall command.

- **Uninstall Flags**: The optional arguments to be run when the package is uninstalled on servers.

- **Reboot Required**: An option that reboots the server when the package is successfully uninstalled.

Uninstall Scripts

- **Uninstall Script**: (Only for Application Installation Media) A script required to perform a silent uninstallation of the application.

- **Pre-Uninstall Script**: A script required to run on a managed server before the package is uninstalled.

- **Post-Uninstall Script**: A script required to run on a managed server after the package is uninstalled.

- **Stop uninstall if script returns an error**: An option that stops uninstallation of the package if the script fails.

Editing Package Properties

After you upload a new package or select an existing package, you can add or edit the package properties in the SA Client.

You can edit a package's name, description, operating system association of the package, install parameters, install scripts, uninstall parameters, and uninstall scripts.

To edit the properties of a package:

1 From the navigation pane, select **Library** > **By Type** > **Packages**. The packages organized by operating system appears in the content pane.

Or

From the navigation pane, select **Library** > **By Folder** and then select the folder that contains the package.

2 From the content pane, select a package to edit.

3 From the **Actions** menu, select **Open**. The Package window appears.

4 From the Views pane, select **Properties**. The package properties will display in the content pane.

5 Edit the following properties for the package:

Specify the package properties. For a detailed list of the property fields see Package Properties Defined.

6   To save the changes, select **Save** from the **File** menu.

Viewing Package Contents

To view the contents of a package:

1   From the navigation pane, select **Library** > **By Type** > **Packages**. The packages organized by operating system appear in the content pane.

Or

From the navigation pane, select **Library** > **By Folder** and select the folder which contains the package.

2   From the content pane, select a package to view.

3   From the **Actions** menu, select **Open**. The Package window appears.

4   From the Views pane, select **Contents**. The package contents appears in the content pane.

5   From the content pane, select **Files** to display the list of files that will be installed by the package.

6   From the content pane, select **Scripts** to display the list of scripts that will be executed by the package. The Scripts tab is only available for package types that support embedded scripts. For example, the Scripts tab is not available for ZIP packages.

Note: The package contents are only available for ZIP, RPM and DEB packages.

- For Solaris packages, HPUX Depot, and AIX LPP, the package names of the children packages are displayed.

- For DEB packages with a data file (data.tar) compressed with xz (data.tar.xz) or lzma (data.tar.lzma), the package contents are only available if the tar archiving utility available on the SA Core server supports these compression methods.

Tip: If the tar archiving utility available on the SA Core server does not support compression methods that are compatible with DEB packages, attempting to retrieve the package contents for the DEB packages will result in an error. See Ubuntu Packages in the Package Type Reference for more details on DEB packages.

Package Management

This section describes how to perform package management activities, such as locating a package, viewing the servers or policies associated with a package, or deleting or renaming a package.

• Viewing Servers Associated with a Package

• Viewing All Software Policies Associated with a Package

• Deleting a Package

- Renaming a Package
- Locating Packages in Folders

Viewing Servers Associated with a Package

To view servers where the package is installed:

1 From the navigation pane, select **Library** > **By Type** > **Packages**. The packages organized by operating system appear in the content pane.

Or

From the navigation pane, select **Library** > **By Folder** and then select the folder which contains the package.

2 From the content pane, select a package to view.

3 From the **Actions** menu, select **Open**. The Package window appears.

4 From the Views pane, select Server Usage. The list of servers associated with the package will display in content pane.

Viewing All Software Policies Associated with a Package

To view software policies that contain the package:

1 From the navigation pane, select **Library** > **By Type** > **Packages**. The packages organized by operating system appear in the content pane.

Or

From the navigation pane select **Library** > **By Folder** and select the folder which contains the package.

2 From the content pane, select a package to view.

3 From the **Actions** menu, select **Open**. The Package window appears.

4 From the Views pane, select policy Usage. The list of policies associated with the package appears in content pane.

Deleting a Package

To delete a package:

1 From the navigation pane, select **Library** > **By Type** > **Packages**. The packages organized by operating system appear in the content pane.

Or

From the navigation pane, select **Library** > **By Folder** and then select the folder which contains the package.

2 From the content pane, select a package to delete.

3 From the **Actions** menu, select **Delete**.

Renaming a Package

To rename a package:

1 From the navigation pane, select **Library** > **By Type** > **Packages**. The packages organized by operating system appear in the content pane.

   Or

   From the navigation pane, select **Library** > **By Folder** and select the folder which contains the package.

2 From the content pane, select a package to rename.

3 From the **Actions** menu, select **Rename**. Enter the new name.

4 To save the changes, select **Save** from the **File** menu.

Locating Packages in Folders

To locate a package in the folder hierarchy:

1 From the navigation pane, select **Library** > **By Type** > **Packages**. The packages organized by operating system appear in the content pane.

   Or

   From the navigation pane, select **Library** > **By Folder** and select the folder which contains the package.

2 From the content pane, select the package and then select **Locate in Folders** from the **Actions** menu. The folder hierarchy for the package appears in the content pane.

RPM Deployment

With SA you can deploy RPM packages on Red Hat Linux and SUSE Linux servers without manually specifying all the dependent packages required for installing the RPM packages. When you deploy a RPM package, SA determines the dependencies and installation order for the RPM package, and identifies if any conflicts exists between the dependencies. After you resolve the conflicts, SA installs the RPM packages on the managed server.

In the SA Client, you can install and uninstall RPM packages on Linux servers using policies and also update the RPM packages in a policy to their latest version. SA also allows you to automatically download the Red Hat Linux Errata into SA and convert them to policies. See Automatically Importing Red Hat Errata for more information.

RPM Deployment Process Overview

Deploying RPM packages on Linux servers involves the following steps. Each step cited below includes a reference to detailed instructions for the specific step.

Table: RPM Deployment Process Steps

Step		Instructions
1	Upload the RPM Packages to the SA Library.	Importing Software Packages
2	Define the Software policy.	Creating Software Policies and Software Templates
3	Add RPM packages to the software policy, and then configure the installation and upgrade options for the RPM packages in the policy.	Setting Installation and Update Options for a RPM
	— *Auto-Update Policy* options provide additional upgrade efficiency. You can set up RPMs in your software policies to automatically update the policy whenever new RPMs are imported.	Automatically Updating RPMs in a Software Policy
4	Attach the software policy containing the RPMs to the managed servers.	About Attaching Software Policies to Servers or Device Groups
5	Remediate the servers to implement the attached policies and maintain the RPM updates on the servers.	Remediating and Installing Software
a	To install the RPMs on a managed server, remediate the server with a software policy attached that contains the RPMs. — The RPM will become managed by the policy when the policy is remediated. — If the RPM was already installed on the managed server, then it will be *adopted* by the policy during the remediation process. — *Adopted RPMs* are treated the same as RPMs that were deployed by SA.	Installing and Updating RPM Packages Using a Software Policy
b	To upgrade the RPMs that are already installed on a managed server, remediate the server with the software policy containing the newer RPMs.	Upgrade Options for an RPM
6	To uninstall an RPM, you can:	
a	Detach the policy containing the RPM from the server, and then remediate the server. — If an RPM resides in more than one attached software policy on a server, the RPM will *only* be uninstalled if *all* the software policies containing the RPM are detached from the server before the server is remediated. — If a software policy with adopted RPMs is	Uninstalling RPM Packages

Step		Instructions
	detached and remediated, then these *adopted* RPMs will be uninstalled the exactly same way as RPMs that were deployed by SA.	
b	Remove the RPM from the policy while keeping the policy attached to the server, and then remediate the server.	

Reminders:

- Upgrading a server's RPM *only* occurs during remediation:

  — Attaching or detaching a software policy from a server does not—by itself—install, update or uninstall the RPM.

  — Updating the software policy with a newer RPM does not—by itself—install or upgrade the server.

- To upgrade the RPMs on a managed server, the server must have a software policy attached that contains the updated RPM, and then the server must be remediated.

- Once a server is remediated with a software policy attached that contains an RPM, the RPM on that server will thereafter be managed by that policy.

- If an RPM was already installed on the managed server, and then you remediate a server with a software policy attached that contains that RPM, the pre-installed RPM will be *adopted* by the attached policy during the remediation process.

RPM Dependencies

After adding RPM packages to a policy when you remediate the policy on a managed server, SA identifies all the dependencies for the RPM packages specified in the policy and the install order requirements necessary for the RPM package to be installed on the server. The dependencies include all the packages that need to be installed or upgraded before or during the installation of the RPM package. SA also analyzes the server's package inventory and identifies any conflicts between what is already installed and what needs to be installed.

During remediation in the preview remediate step, you can view the list of packages dependent on the RPM package to be installed and any conflicts between the dependencies. You can then resolve the dependencies when more than one RPM satisfies a dependency. After you resolve the dependencies, SA installs the RPM packages specified in the software policy. See the Remediating and Installing Software for more information about remediation with software policies.

While remediating a server with policies containing multiple versions of an RPM package, SA will only install the latest version of the RPM package and its dependent packages.

Note: SA does not support dependency solving for RPM packages on non-Linux operating systems that support RPM packages.

The SA RPM Repository

SA builds a custom RPM repository for use by software management jobs. This is built on a server-by-server basis, taking into account several package and server properties and user defined settings.

The repository that SA downloads to a managed server before actually processing the RPM packages defined in the software policy is built by the following process:

- Packages whose platform set does not include the server platform are excluded from the RPM repository.

- Packages in folders whose customer constraints do not include the customer of the server are excluded from the RPM repository.

- If one or more repo.restrict custom attributes are applicable for this server, only packages in the folders defined by these custom attributes are included in the RPM repository. For more information, see Restricting Access to RPM Folders.

Restricting Access to RPM Folders

In SA, you can ensure that your Linux managed servers only have access to the set of RPMs in the SA Library that apply to each server. You simply specify in a custom attribute the folders in the SA Library that the server has access to. All other folders will be inaccessible to the server. This section describes how to set up these restrictions.

With this new mechanism, you can mimic the common Red Hat systems administration paradigm of having multiple, distinct yum (Yellowdog Updater, Modified) repositories. This gives you folder-level control over which versions of RPMs can be applied to a given server, allowing you to precisely manage platform update versions, for example Red Hat Advanced Server AS4 Update 5 versus Update 6.

This is not intended as a user-level access control mechanism, but rather to restrict the library and folder view of a managed server from access to the full set of RPMs in the SA Library. For information on user level folder access controls and folder permissions in the SA Library, see the SA Administration Guide.

How the RPM Folder Restrictions Work

During remediation, if a server has one or more of these custom attributes defined, SA reads the custom attribute values and only allows the managed server access to the RPMs in the SA Library folders specified in the custom attributes and their subfolders. Subfolders of all the specified folders are recursively searched for RPMs. All other folders are not accessible to the server.

Enabling RPM Folder Restrictions

To restrict a server or group of servers to a subset of RPMs in the SA Library, set a custom attribute in the format described below on your managed server or at a location that will be inherited by the server such as a device group, a software policy, a customer, a facility and so forth.

These custom attributes follow the custom attribute inheritance rules. For example, if you set a custom attribute at the facility level, the servers in that facility will inherit the custom attributes.

SA does not validate the SA Library folder paths you specify in these custom attributes so make sure the folder paths you specify are correct.

> **Note:** For instructions on how to manage custom attributes in software policies or managed servers, see Adding Custom Attributes to a Software Policy and Adding Custom Attributes to Servers. For more information about custom attributes, see the SA User's Guide: Application Automation.

Custom Attribute Format

The custom attributes that restrict access to RPMs must be in the following format:

```
repo.restrict.<name>
```

where `<name>` is any user-defined alphanumeric string.

Specify a `<name>` that is descriptive and helps you remember the purpose of the custom attribute. You can define multiple custom attributes as long as each `<name>` is unique.

Examples

The following defines custom attributes that grant access only to the SA Library directories `/Redhat/AS4/en/x86_64/U5` and `/Oracle/10/AS4/x86_64`:

```
repo.restrict.as4u5=/Redhat/AS4/en/x86_64/U5
repo.restrict.oracle_updates=/Oracle/10/AS4/x86_64
```

The custom attribute value can be multiple lines. The following defines custom attributes that grant access only to the SA Library directories listed:

```
repo.restrict.as4u5=/Redhat/AS4/en/x86_64/U5
                    /Redhat/AS4/en/x86_64/U5-extras
repo.restrict.s5u3=/Redhat/5Server/en/x86_64/U3
                   /Redhat/5Server/en/x86_64/U3-extras
                   /Redhat/5Server/en/x86_64/U3-VT
                   /Redhat/5Server/en/x86_64/U3-Cluster
```

Troubleshooting Errors

If you attempt to remediate a software policy that contains RPMs that are not accessible to the server, the following error message will be given:

```
The metadata needed to install this package is missing.
```

This indicates that SA was unable to access the RPM because the server does not have access to the RPM in the SA Library. To resolve this error, check the folder locations you have set in your custom attributes to ensure they are correct.

Installing and Updating RPM Packages Using a Software Policy

With SA you can install and update RPM packages on a server using policies. After you import RPM packages to SA, you can add the RPM packages to the software policy. See Importing Software Packages and Setting Installation and Update Options for a RPM for more information.

In a software policy, you can specify whether the RPM packages listed in the policy should be installed on the server or if the RPM package in the policy should be updated to the latest version. In a software policy, you can set the following options for an RPM Package:

- Install Criteria
- Auto Update Policy

The Install Criteria option determines whether the RPM package listed in the policy will be installed on the managed server. The Auto Update Policy option determine whether the RPM package listed in the policy will be updated to the newer release or version. See Automatically Updating RPMs in a Software Policy for more information.

In addition, the Upgrade option for the RPM package in the Package Properties page determines if the RPM package will be updated. See Upgrade Options for an RPM for more information.

Install Criteria:

- If the **Install RPM always** option is selected, the RPM packages specified in the policy will be installed on the managed server. This will happen when you remediate the server with that policy attached.

- If the **Install RPM only if an earlier version is installed** option is selected, the RPM version on the managed server will be updated to the version specified in the software policy. This will happen when you remediate the server with that policy attached.

  Note: If this option is selected but the RPM package specified in the software policy is not *already* installed on the managed server, then the RPM will not be installed.

- See Setting Installation and Update Options for a RPM for more information on how to set these options.

See also:

- Remediating Servers with Software Policies
- RPM Rollback
- Using the Native YUM to Remediate RPM Packages

Using the Native YUM to Remediate RPM Packages

The Yellowdog Updater Modified (YUM) plugin handles the analyze phase of the remediation process using the native YUM available on the managed server.

Server Requirement

In order to enable the YUM plugin option, the managed server must use native YUM 3.0.1 or later. The YUM version available on the managed server can be identified by running the following command in the command line:

```
yum --version
```

> **Note:** See the SA Support and Compatibility Matrix for updated YUM compatibility information on SA managed servers.

Setting the YUM Adapter Parameter

When available, the managed server's native YUM is used to analyze RPM package dependencies. When the managed server does not have a native YUM available, the SA YUM Adapter is used instead. This behavior is based on the default and recommended setting governed by the SA configuration parameter, way.analyze.yum, settings.

> **Requirement:** Only system administrators with the Opsware System Administrators user group or the 'Manage system configurations in SA' action permission can change the SA configuration parameter settings.

> **Caution:** Changes to SA Core configuration parameter values as documented herein are verified by HP and you can safely apply them as directed. However, exercise caution when modifying any default SA Core configuration parameter values as modifications can have a negative effect on core functionality and performance.

To view or edit these settings from the SA Client, navigate to Administration > System Configuration.

The way.analyze.yum parameter has the following available values:

0 - use the YUM adapter (YUM v2.6.1)

1 - use the native YUM when available, otherwise use the YUM adapter. (Default)

2 - use the native YUM

> **Note:** SA configuration parameters targeting YUM do not apply to managed servers running SuSE Linux Enterprise Server (SLES) 11 or newer. In this case, analysis and remediation is performed using Zypper, a native tool for SLES.

YUM Restrictions

Natively, YUM does not support the `--nodeps` command-line option as RPM does. Also, YUM does not natively support the src.rpm packages.

For other YUM known issues and limitations please check the Yellowdog documentation at http://yum.baseurl.org/wiki.

Using the Native Zypper To Remediate RPM Packages

The native tool Zypper is used to analyze and install the phase of the remediation process on the managed server.

Server Requirements

In order to work with Zypper, your managed server must be SLES 11 GA or later. This option is automatically selected when the managed server is SLES 11 GA ++ (no other remediation options

are provided for the selection).The installed zypper version can be identified by running the following command in the command line:

```
zypper –version
```

For complete SA support and compatibility information for this release, see the HP Server Automation Support and Compatibility Matrix .

> **Note:** In the SLES service pack upgrade process, all rpm packages from upgrade software policy have to be marked with the option *Install RPM only if an earlier version is installed.* See Setting Installation and Update Options for an RPM for more information.

Zypper Restrictions

Zypper does not support :

- –nodeps command-line option, as RPM does. This option is ignored during remediation, and remediated packages are remediated as regular packages.

- On SLES 11 GA, Zypper does not support installation of packages with an epoch that is not zero (0).

RPM Rollback

RPM Rollback feature is only available on Linux servers for remediation jobs where the installation is done using rpm. Because Linux has discontinued the built-in rollback functionality of RPM, the SA rollback function is only available with RPM versions 4.2 to 4.6. Additionally, the SA Agent must be version 45 or greater for the rollback process to work.

The user must have read/write permissions on the server/customer and the permission: *Allow Install/Uninstall Software*, to be able to start a rollback operation or delete a rollback point. To view rollback points the user may also need to have *Read/write* permission on the Manage Packages feature.

You can roll back an RPM upgrade to restore systems to a former working state. This can be used in the event of an RPM upgrade that caused a failure.

If you have ever performed an upgrade on one or more RPMs, and then discovered that the upgrade had undesirable consequences or was not compatible with one of the applications on the host, then you know the need for RPM Rollback. You can revert the set of installed RPMs on the server to the set it had prior to the upgrade in a single operation.

- **Set the rollback point**: Set the rollback point during RPM Installation. This preserves the current state so that you can restore it later.

    — See Creating an RPM Rollback Point.

- **Roll back to a previous RPM state**:In the Server Browser, view the list of rollback points in the RPM Rollback Points view in the Inventory section. Select the desired rollback point and run a rollback job.

    — See Rolling Back to a Previous RPM Rollback Point.

* **Delete old rollback points**: Rollback points accumulate over time. You can delete old rollback points to clean up the queue.

    — See Deleting a Rollback Point .

How RPM Rollback Mechanism Works

The SA RPM rollback function uses the built-in repackage/rollback mechanism of RPM, which repackages the current installed version and saves it to the repackage directory (`/var/spool/repackage` by default) at upgrade time. The repackage directory can be configured in the RPM configuration file.

The rollback process undoes all the operations down to a certain point in time (the time when the rollback point is created in SA) in reverse order:

a   A package that was upgraded will be downgraded to its prior version;

b   A newly installed package will be uninstalled;

c   A package that was removed will be re-installed.

The latter two actions, b and c, occur even if such operations were done after the upgrade and were not necessary related to the upgrade operation that resulted in the creation of the rollback point.

For example, let's say the following scenario occurs:

1   a policy install is done with SA that upgrades a number of RPMs, and a rollback point is created.

2   Then, the user installs another set of newly RPMs through SA—or manually on the server.In this case, when rolling back to the rollback point created by the RPM upgrade (step 1), the newly installed packages (step 2) will be uninstalled as well. (Note: This will not result in creating a rollback point for this operation because no RPMs were upgraded.)

Because Linux has discontinued the built-in rollback functionality of RPM, this rollback function is only available in RPM versions 4.2 to 4.6. Additionally, the SA Agent must be version .34 or greater for the installation process to work.

Creating an RPM Rollback Point

To create a rollback point as a result of an upgrade:

1   Start from either an RPM installation or remediate operation:

a   Start an install of one or more RPM packages on one or more Linux servers. One or more of the RPMs must have a previous version already installed on a target server and must have the upgrade flag set.

    — See Installing Software Using a Software Policy.

    — The upgrade flag is set in the RPM package in SA (It can be set to either install or upgrade. Upgrade is the default.)

Or

b   Start an uninstall of one or more RPM packages on one or more Linux servers.

Or

c Start a remediation of one or more software policies on one or more Linux servers. The software policy must contain one or more RPMs.

— See Remediating Servers with Software Policies.

2 Select **Create RPM rollback point** option in the Options set of the installation or remediation process. This option will be enabled by default if the above requirements are met.

• See Step 2 (Optional): Specify Reboot, Error Handling, and Script Options for Remediation

3 After the remediation/installation process is complete, the rollback points are established. For each rollback point created, a message will be displayed in the details pane of the Registration step for each server.

4 Open the Server Browser window of one of the servers on which the above operation has been successfully finished.

5 Go to the Inventory view and then open the **RPM Rollback Points** pane to view the newly created rollback point. The table displays the Name, Type, and Created Date, where type is RPM Repackage.
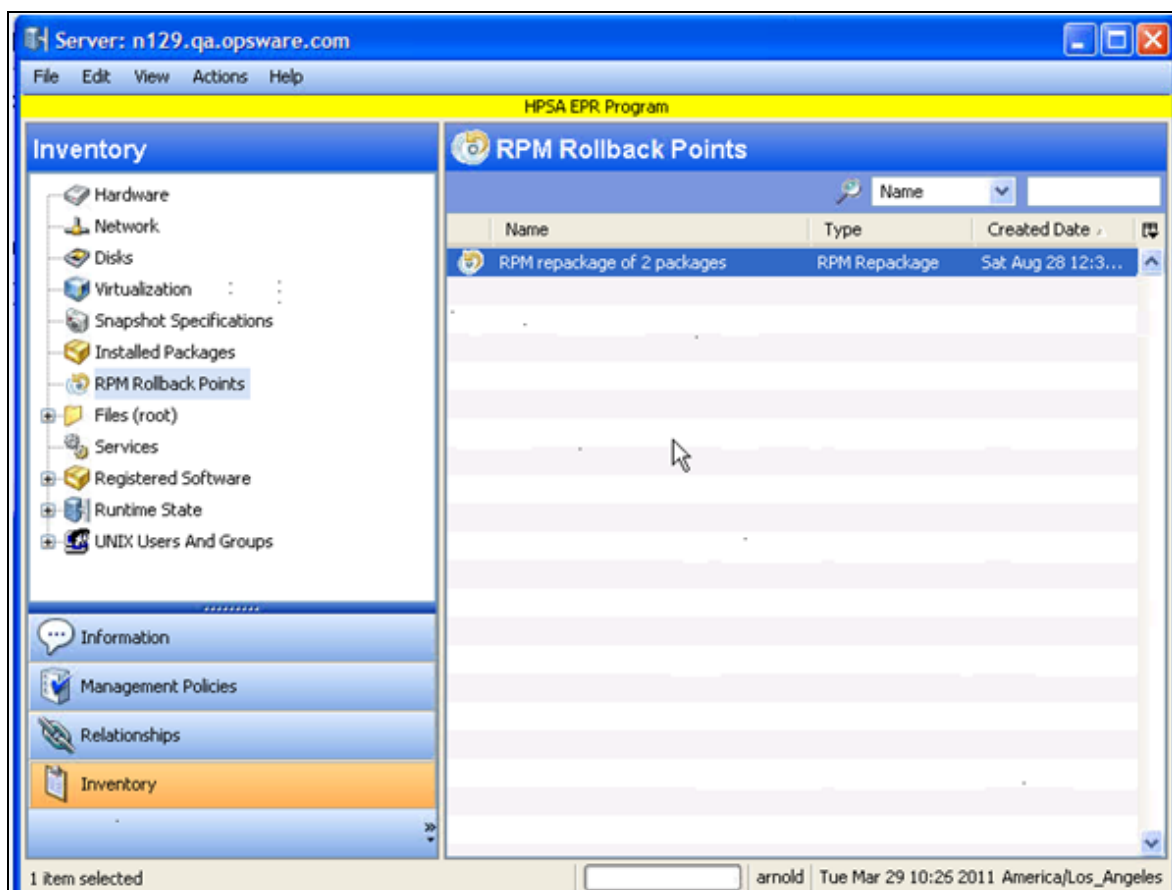
Rolling Back to a Previous RPM Rollback Point

To rollback to a previous RPM rollback point:

1. Open the server where the RPM rollback points were created.

   From the server browser window, select **Inventory** > **RPM Rollback Points**

2. The table in the content pane displays the list of available rollback points.
   - Rollback points can be filtered by Name, Type, and Created Date.
   - Only one rollback point can be selected

3. Right-click one of the rollback points and select **Rollback...**.

4. The Rollback window displays the options for setting up the Rollback job.

   a **Preview**: displays information about the rollback operation, including the exact steps that will be attempted:
      - the target device for the rollback
      - the targeted rollback point's name and creation date
      - an action step for each package that will be altered along with the corresponding operation (rollback or uninstall)
      - the final action step, Registration, will update the installed packages list.

   b **Scheduling**: specify if you want to start the job immediately or at a scheduled date and time.

   c **Notifications**: set up email notifications in case of failure or success.

   d **Status**:displays detailed progress about the rollback process.

Similar to the preview step, the Status view displays an action step for each of the packages being rolled back or uninstalled, including Registration as a last step.

5. As the rollback task is run, the steps will be displayed in detail in the status window.

6. When the rollback process is finished, the rollback point will be deleted.

Rolling Back Multiple Rollback Points: When multiple rollback points are available, if you roll back to one that is not the most recent, all the rollback points that are chronologically newer than that one will also be rolled back in reverse order. For example, if you roll back to the oldest rollback point available, everything will be rolled back to that point in reverse order.

Deleting a Rollback Point

To delete an RPM rollback point:

1. Open the server where the RPM rollback points were created.

   From the server browser window, select **Inventory** > **RPM Rollback Points**.

2. The table in the content pane displays the list of available rollback points.
   - Rollback points can be filtered by Name, Type, and Created Date.
   - Only one rollback point can be selected.

3. Right-click one of the rollback points and select **Delete**.

4. Accept the confirmation dialog window to begin the operation.

5. After the operation is finished the table items will be automatically refreshed.

Deleting Multiple Rollback Points: When multiple rollback points are available, if you delete one that is not the oldest, all the rollback points that are chronologically older than that one will also be deleted. For example, if you delete the newest rollback point available, all the rollback points will be deleted.

Automatically Updating RPMs in a Software Policy

With SA, you can set up a software policy to automatically update the version and/or release of its enclosed RPMs. In policies that contain RPMs, the **Auto-Update Policy** setting is available for each RPM, with two automatic-update options: *Release Only* and *Version or Release*.

The selection of one of these options will determine whether the RPM listed in the policy will be automatically updated for newer versions of an RPM, or just for newer releases of an RPM. In addition to specifying this setting, for the policy update to occur, the newer RPM must also be placed in the same folder as the RPM that is specified in the software policy.
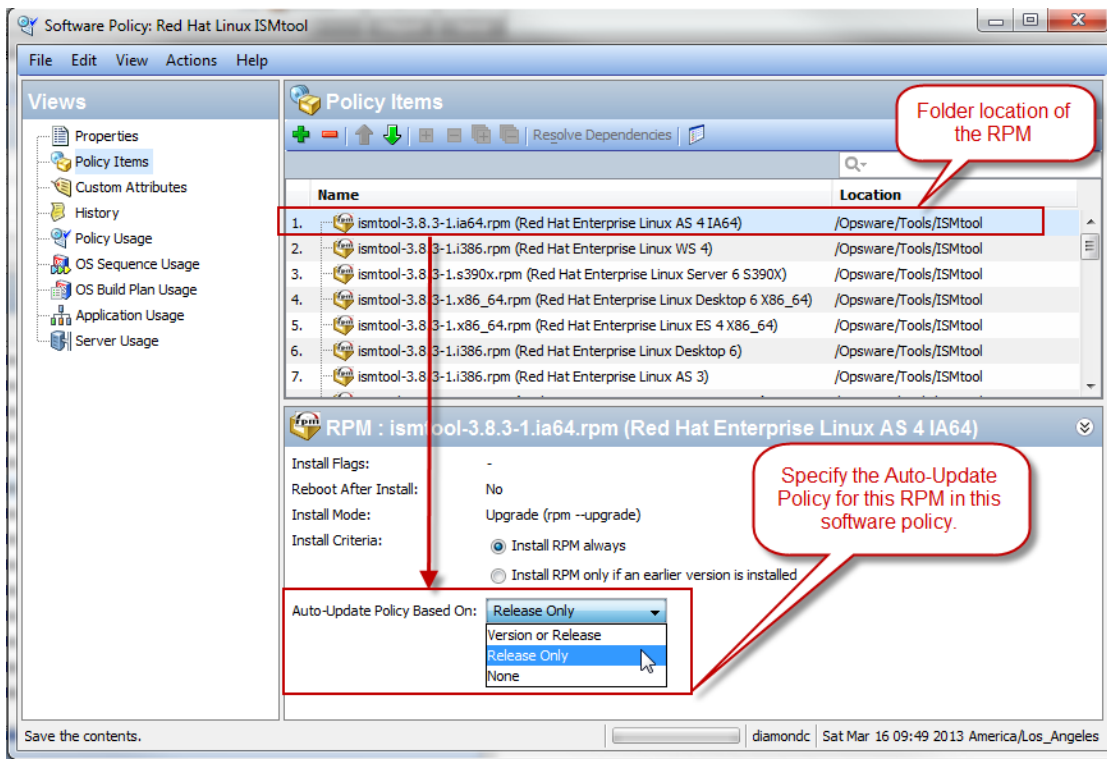
Choosing an Auto-Update Policy option:

If you enable one of these automatic update options in the software policy, and then save the policy, the policy will be instantaneously updated when a newer RPM is *moved* to the folder.

- This update only occurs if the newer RPM is added to the folder *after* the auto-update option is enabled.

- The policy will reflect the *most recent* version or release of the RPMs in the specified folder, respective of the setting:

  — If the **Version or Release** option is selected, the automatic policy update occurs when either a newer *version* or *release* of the RPM is added to the specified folder. Use this option if you want to update the policy for any RPM update, even new versions of the same release.

  — If the **Release only** option is selected, the automatic policy update occurs only when a newer *release* of the RPM is added to the specified folder.

  The important distinction in the **Release only** option is that the policy will *only* recognize the new RPM as an update if the RPM is a new *release*; not merely a new *version* of the same release. When this option is selected, adding a newer *version* of an RMP to the specified folder will *not* update the policy.

  Use this option if you only want to update the policy for major RPM releases and you do not want to update the policy for the minor release versions.

  — If the **None** option is selected, RPMs will not be automatically updated. This is the default setting.

Note: SA will update the RPM in this policy *only* if the newer release or version is placed in the same folder as the RPM specified in the software policy.

The Auto-Update Policy setting applies *only* to this RPM in this Policy. It does not apply to this RPM in other policies, nor does it apply to other RPMs in this policy.

Updating the RPM folder:

When one of the Auto-Update Policy options is enabled, the RPM in the software policy will be automatically updated the next time a newer RPM is placed in the same folder as the older RPM that is already specified in the policy. An RPM can be placed in the specified folder in a few different ways:

  — A new RPM unit can be created in the specified folder using the SA Client import action or an import script (rhn_import, CBT).

  — An existing RPM can be moved into the specified folder using either the SA Client or the SA API

Regardless of the method used to place the newer RPM file in the specified folder, the software policy that references that RPM in that directory will be automatically updated based on this setting in the software policy.

Automatic RPM Update Requirements:

An RPM within a software policy is automatically updated if *both* of the following conditions are met:

- The Auto-Update Policy setting for the RPM in the software policy must be set to **Release Only** or **Version or Release**.

and

- The newer RPM must be placed in the same folder as the older RPM that is already specified in the software policy.

    — If the **Release** option is selected, the newer RPM must be a new *release*, not just a *version* update, in order for the software policy to get updated.

    — If the **Version or Release** option is selected, the newer RPM can be a new *release* or even just a newer *version* of the same release.

Reminders:

- Updating the software policy with a newer RPM does not—by itself—install or upgrade the server. The server upgrade is performed *only* during remediation.

- To upgrade the RPMs on a managed server, the server must have a software policy attached that contains the updated RPM, and then the server must be remediated.

To specify the Auto-Update Policy setting for an RPM in a software policy:

1   In a software policy containing RPMs, navigate to **Policy Items** and select one of the RPMs. The content pane will display installation and upgrade options for this RPM.

    Note the folder location of the RPM.

2   In the Auto-Update Policy setting, select either **Release Only** or **Version or Release**.

3   Click **File > Save** to save the policy.

4   Place a newer RPM into the same folder as the RPM specified in the software policy.

    The RPM can be placed into the folder via any supported method—by importing, moving or copying the file into the folder using the SA Client, a script, or a command line action.

5   The software policy will automatically be updated to reference the newer RPM according to the specified setting.

    This process will update the software policy contents so that it reflects the newer RPMs. This process does not upgrade the servers. To upgrade the servers, you must remediate the servers with the software policy attached.

6   The next time a server is remediated with this updated policy attached, it will upgrade the server to the newer RPM version or release.

> **Note:** See Setting Installation and Update Options for a RPM for information on additional options. See Upgrade Options for an RPM for an explanation of how these options interact.

Upgrade Options for an RPM

Upgrading an RPM depends on multiple factors, including:

- the Install Parameters specified in the Package Properties window for the RPM,

- the RPM's dependencies, and the Install Parameter settings of those dependencies, and

- the install and upgrade settings specified for the RPM within the Software Policy

Setting Package Properties for the RPM and Its Dependencies:

After you upload an RPM package to SA, you can set the set the Install Mode option for the RPM package in the Package properties window.

The Install Mode setting in the RPM Package Properties window:

- If the **Upgrade** option is used, then during remediation, the previous version of the RPM package and its dependencies will be removed from the server *first*. Then, the newer version of the RPM package and its dependencies will be installed on the server.

- If you use the **Install** option, then during remediation SA will install the newer version of the RPM package and its dependencies on the server. The previous version of the RPM package and its dependencies *will not* be removed from the server.

- See Editing Package Properties.

Setting Package Properties for the RPM within the Software Policy:

The options defined in the Policy Items content pane of the Software Policy window govern how the policy maintains RPM updates within the policy as well as actual server upgrade behavior when remediating servers with that policy attached.

The Install Criteria setting for the RPM in the Software Policy:

- If the **Install RPM always** option is used if you want install the selected RPM on the managed server, whether or not a version is already installed on the server.

- If the **Install RPM only if an earlier version is installed** option is used if you want to restrict RPM installations to upgrades. This option will install the RPM on the managed server *only* if an existing version of that RPM is already installed on the server.

- See Installing and Updating RPM Packages Using a Software Policy.

Setting Options for an RPM Package lists the action taken on the RPM package based on the options set for the RPM package in both the Software Policy window and the Package.

Table: Setting Options for an RPM Package

Install Criteria setting for the RPM in the Software Policy	*Install Mode* setting in the RPM Package Properties	Action Taken During Remediation
Install RPM only if an earlier version is installed	**Upgrade**	SA will *only* install the specified RPM if a previous version of the RPM is already installed on the server. - If a previous version of the RPM is installed on the server, then SA *will uninstall* the previous version of the RPM, *and then install* the newer version, as specified in the server's policy.

Install Criteria setting for the RPM in the Software Policy	*Install Mode* setting in the RPM Package Properties	**Action Taken During Remediation**
		• If a previous version of the RPM is *not* already installed on the server, SA *will not* install the RPM on the server.
Install RPM always	**Upgrade**	SA *will install* the specified RPM in either case; whether the RPM is already installed or not. • If a previous version of the RPM is installed on the server, then SA *will uninstall* the previous version of the RPM, *and then install* the newer version, as specified in the server's policy. • If a previous version of the RPM is *not* already installed on the server, then SA *will install* the RPM specified in the policy on the server.
Install RPM only if an earlier version is installed	**Install**	SA *will not install* the specified RPM in either case; whether the RPM is already installed or not. • If a previous version of the RPM is installed on the server, then SA will *not install* the newer version of the RPM specified in the policy. • If a previous version of the RPM is *not* already installed on the server, then SA will *not install* the RPM version specified in the software policy.
Install RPM always	**Install**	SA will *only* install the specified RPM if there is no RPM already installed on the server. • If a previous version of the RPM is already installed on the server, then SA *will not* install the newer version of the RPM. • If a previous version of the RPM is *not* already installed on the server, then SA *will install* the RPM packages specified in the policy on the managed server.

When you upload a *non- kernel* RPM package, the Upgrade option is enabled by default. When you upload a *kernel* RPM package, the Install option is enabled by default. Therefore, when you remediate a server with a policy containing kernel RPMs (such as kernel, kernel-bigmem, kernel-enterprise, kernel-smp, kernel-modules, kernel-debug, kernel-unsupported, kernel-source, kernel-devel), then SA will always install the newer version of the kernel RPM packages and its dependencies on the server. The previous version of the kernel RPMs and its dependencies are not removed from the server.

Uninstalling RPM Packages

With SA you can uninstall RPM packages and downgrade to a previous version of the RPM package using policies. To uninstall an RPM package from a managed server, you must first detach the policy from the server and then remediate the server against the software policy. See Detach a Software Policy from the Managed Server for information on how to detach a policy from a server.

When you remediate the server, SA uninstalls the RPM package specified in the policy from the server and the dependent packages for the specified RPM package. You can uninstall the RPM packages only if they are not used by another software policy. When you uninstall an RPM package, SA also uninstalls any RPM packages which depend on the RPM packages being uninstalled.

SA also allows you to downgrade to a previous version of an RPM package using a software policy.

Uninstalling RPMs from a Managed Server

To uninstall RPMs from a managed server:

1   Detach the policy containing the newer version of the RPM package from the server.

2   Remediate the server to uninstall the RPM package.

- If the software policy with adopted packages is detached and remediated then these adopted packages will be uninstalled exactly like the packages that were actually deployed by SA.

- If an RPM resides in more than one attached software policy on a server, SA will only try to uninstall the RPM after all the software policies containing the RPM are detached from the server and the server is remediated.

Downgrading to a Previous Version of an RPM Package

To downgrade to a previous version of an RPM package:

1   Uninstall the RPM from the server.

    See Uninstalling RPMs from a Managed Server for details.

2   Create a new software policy.

3   Add the older version of the RPM package to the software policy.

4   Attach the new policy to the server.

5   Remediate the server to install the older RPM package.

Related topics:

- Detach a Software Policy from the Managed Server

- Attaching a Software Policy to a Server or Device Group

- Setting Installation and Update Options for a RPM

- Creating Software Policies and Software Templates

- Remediating Servers with Software Policies

- [RPM Rollback](#)

Server Compliance for RPM Packages

A server can be either compliant or non-compliant with respect to a policy attached to it. If the server's configuration does not match the packages, RPM packages, patches, and application configurations defined in a policy (attached to that server), then the server is said to be non-compliant with that software policy. For RPM packages, software compliance is calculated based only on the RPM packages specified in the software policy. The dependent packages for the RPMs specified in the policy are not used for calculating the software compliance.

See the *SA User Guide: Audit and Compliance* for more information about policy compliance and how to perform a compliance scan.

Automatically Importing Red Hat Errata

Red Hat allows system administrators to manage their Red Hat servers on the network. Red Hat provides two hosted technologies for managing subscriptions: Red Hat Network and Red Hat Subscription Management. Red Hat Subscription Management is the replacement for Red Hat Network.

> **Note:** Red Hat Subscription Management is available for the following Red Hat Enterprise Linux versions: 5.7+, 6.1+ and 7+. Red Hat Enterprise Linux 7 is the first version that can only be managed through Red Hat Subscription Management and does not support Red Hat Network.

Red Hat publishes Errata which contains information describing security patches, bug fixes, and package updates for Red Hat Enterprise Linux and other Red Hat products. To install the packages in the Errata, the Errata must be downloaded from the Red Hat web site and imported into SA. Using SA you can automatically download the Errata released by Red Hat, convert them to policies, and store the policies in a folder in the Library in the SA Client.

The main content for Red Hat products is distributed through Red Hat Network channels and Red Hat Subscription Management contents (available through Red Hat Content Delivery Network).Using SA you can automatically download the packages in a Red Hat Network channel or Content Delivery content, convert them to policies, and store the policies in a folder in the Library in the SA Client.

The `rhn_import` and `redhat_import` CLI programs provided by SA enable you to create policies, which correspond to Red Hat Network errata and channels and to Red Hat Subscription Management errata and contents. `rhn_import` allows for content import from Red Hat Network. `redhat_import` provides all the capabilities of `rhn_import` and additionally allows for importing content from Red Hat Subscription Management.

> **Note:** HP recommends the usage of `redhat_import`, `rhn_import` is only provided for backward compatibility.

Using the `rhn_import` and `redhat_import` programs, you can create the following types of policies:

- **Channel / Content based software policy**: A Red Hat Network channel / Red Hat Subscription Management content contains a list of packages. For example, a channel / content may contain packages for a particular Red Hat operating system version and architecture. When you run the `rhn_import` or `redhat_import` program, SA downloads the latest packages from the Red Hat Network channel / Red Hat Subscription Management content and then imports the packages to the Library in the SA Client and creates a channel / content based software policy. Thus, a channel based policy reflects a particular channel while a content based policy reflects a particular Red Hat Subscription Management content. In the SA Client, you can view the name, description, location, availability, and the operating system version of the channel / content based policy in the Library.

- **Errata based software policy**: A Red Hat Erratum contains information on a particular problem and the associated packages to resolve the problem. An Errata based policy contains all the individual Erratum-based policies for a given channel / content. When you run the `rhn_import` or `redhat_import` program, SA downloads the latest packages from Red Hat errata and then imports the packages to the Library in the SA Client and creates an errata based software policy. There are three types of RED Hat Errata: Bug Fix Advisories, Product Enhancement Advisories, and Security Advisories. The `rhn_import` and `redhat_import` programs allow you to create errata policies for Bug Fix Advisories, Product Enhancement Advisories, and Security Advisories in the SA Client. In the SA Client, you can view the name, description, location, availability, and the operating system version of the errata based policy in the Library.

- **Erratum-based software policy**: Erratum-based policies contain packages associated with a particular erratum. When you run the `rhn_import` or `redhat_import` program, SA downloads the latest packages from the Red Hat erratum and then imports the packages to the Library in the SA Client and creates an Erratum-based software policy.

To create and maintain policies from the Red Hat Linux errata, erratum, and channels / contents, log into the core server running the Software Repository component (part of the Slice Component bundle) and run the `rhn_import` or `redhat_import` program located in the following directory:

`/opt/opsware/rhn_import/bin`

The software policies created by `rhn_import` / `redhat_import` will, by default, have an empty uninstall sequence. This setting prevents the inadvertent uninstall of the RPMs in the policy when it is detached.

Importing RPM packages from the Red Hat to SA requires a large amount of disk space. Over a period of time, the amount of disk space required increases as new versions of packages are released by Red Hat.

For example, importing only the latest packages for the x86_64 flavor of Red Hat Enterprise Linux 5 takes up to 20 GB of space (channel and errata), while importing all packages would use about 80-100 GB.

The documentation for the `rhn_import` and `redhat_import` programs is available online. To view the complete documentation run the program with the following option:

`/opt/opsware/rhn_import/bin/rhn_import-manual`

`/opt/opsware/rhn_import/bin/redhat_import-manual`

When you run the `rhn_import` or `redhat_import` program, you can specify the options listed the documentation provided online or use the Configuration File provided by HP. The Configuration file provided by HP with the `rhn_import` program is located in the following directory:

`/etc/opt/opsware/rhn_import/rhn_import.conf`

The Configuration file provided by HP with the redhat_import program is located in the following directory:

`/etc/opt/opsware/rhn_import/redhat_import.conf`

Reusing a RedHat Import Configuration File with Encrypted Passwords

You can reuse an `rhn_import.conf` or `redhat_import.conf` file that contains encrypted passwords on another core, however you must clear all the encrypted passwords before copying the file and reuse the `--hide_passwords` option on the new core.

The sequence of the steps matters. It is important that you change the encrypted passwords into clear text and use the `--hide_passwords` option. If you attempt to reuse an `rhn_import.conf` or `redhat_import.conf` file with encrypted passwords on another core without performing these steps, an error (500 Internal Server) will occur.

To reuse an `rhn_import.conf` or `redhat_import.conf` file containing encrypted passwords on another core:

1. Change all encrypted passwords in the file into clear text.

2. Copy the `rhn_import.conf` or `redhat_import.conf` file to the other core.

3. Reuse the `--hide_passwords` option when running the RedHat import on the new core.

Viewing Errata Based and Channel / Content Based policies in the SA Client

The `rhn_import` and `redhat_import` programs, allow you to create errata-based, erratum-based and channel / content based policies in the SA Client. After successfully running the program, you can view the properties of errata-based, erratum-based, and channel / content based policies in the SA Client. You can view properties such as the SA user who created the software policy, the date when it was created, the name, the description, the availability, the location of the policy in the Library, the operating systems applicable to the policy and the HP ID of the

software policy. HP recommends that you do not edit the policies which have been created by the `rhn_import` or `redhat_import` program.

To view the properties of a software policy:

1. From the navigation pane, select Library > By Folder.
2. Select the Red Hat Network Folder (RHN) or Red Hat Subscription Management Folder (RHSM).
3. From the content pane, select the errata-based or channel / content based policy and open it. The policy window appears.
4. From the Views pane, select Properties. You can view the properties for the policy in the content pane.
   - Name: Contains the errata reference for the errata based software policy.
   - Description: Includes all the errata documentation for the errata.
   - Location: Specifies the location of the policy in the folder hierarchy. To change the location click Select to specify the location for the policy in the folder hierarchy. The Select Location window appears. Select a folder in the Library to specify the location of the policy and then click Select.
   - Created: Corresponds to the time when the errata was downloaded by HP to create the software policy.
   - Last Modified: Corresponds to the time when the errata based policy was modified.
   - Availability: Contains the HP server life cycle values for the errata based software policy. The default value for an errata based policy is set to Available.
   - Platform: Specifies all operating systems applicable to the errata. You can expand the list to see the selected platforms.
5. To save the changes, select **Save** from the **File** menu.

Errata caching

When importing errata, SA Red Hat Import tool keeps track of the imported errata. Details of each imported erratum are stored in a cache file and subsequent runs will skip the cached errata completely. This improves performance as it avoids some calls to Red Hat and to SA Library. In the absence of the cached data these calls are being made even for errata that has not been modified and is up to date in the SA Library. Errata that has been modified by Red Hat is updated anyway so there is no danger of having outdated errata after import.

A cache file is created for each imported Red Hat Network channel / Red Hat Subscription Management content.

The cache files are kept in the following folder on the SA core server:

`/var/opt/opsware/rhn_import`

The file name uses the following pattern:

`prev_import_ch_<label>.dat`

where <label> is the Red Hat Network channel label or the Red Hat Subscription Management content label. Some example file names are presented below:

- `prev_import_ch_rhel-x86_64-server-6.dat`
- `prev_import_ch_rhel-7-server-rpms{7Server-x86_64}.dat`

As a result of the caching mechanism described above the following scenarios are possible:

- An erratum is imported into SA Library and then it is removed / renamed / moved to another folder. When `rhn_import` or `redhat_import` are run next time the erratum will not be reimported into the SA Library. This is because the erratum details are present in the cache file so it is skipped during the import.
- The errata roll-up policy is created and then it is removed / renamed / moved to another folder (e.g. by using the SA Client). When `rhn_import` or `redhat_import` are run next time the errata roll-up policy will be recreated but it will contain only the errata that has been published by Red Hat since the last import. If there is no new errata the errata roll-up policy will not be recreated. This is because the errata present in the cache file is skipped during the import.

If you would like to fully synchronize the errata in SA Library (including the errata roll-up policy), remove the cache file for the concerned channels / contents and run `rhn_import` or `redhat_import`. In this case an erratum policy is created for each erratum available from Red Hat, provided that such a policy is not already present in the SA Library and the errata roll-up policy is created if not present and updated to include all erratum policies. The cache file is also recreated so next runs will benefit from the performance improvements offered by the caching mechanism.

Reusing a RedHat Import Configuration File with Encrypted Passwords

You can reuse an `rhn_import.conf` file that contains encrypted passwords on another core, however you must clear all the encrypted passwords before copying the file and reuse the `--hide_passwords` option on the new core.

> **Caution:** The sequence of the steps matters. It is important that you change the encrypted passwords into clear text and use the --hide_passwords option. If you attempt to reuse an rhn_import.conf file with encrypted passwords on another core without performing these steps, an error (500 Internal Server) will occur.

To reuse an rhn_import.conf file containing encrypted passwords on another core:

1 Change all encrypted passwords in the file into clear text.
2 Copy the `rhn_import.conf` file to the other core.
3 Reuse the `--hide_passwords` option when running the RHN import on the new core.

Viewing Errata Based and Channel Based policies in the SA Client

The `rhn_import` program, allows you to create errata-based, erratum-based and channel-based policies in the SA Client. After successfully running the program, you can view the

properties of errata-based, erratum-based, and channel-based policies in the SA Client. You can view properties such as the SA user who created the software policy, the date when it was created, the name, the description, the availability, the location of the policy in the Library, the operating systems applicable to the policy and the HP ID of the software policy. HP recommends that you do not edit the policies which have been created by the `rhn_import` program.

To view the properties of a software policy:

1   From the navigation pane, select **Library** > **By Folder**.

2   Select the Red Hat Network Folder (RHN).

3   From the content pane, select the errata-based or channel-based policy and open it. The policy window appears.

4   From the Views pane, select **Properties**. You can view the properties for the policy in the content pane.

- **Name**: Contains the errata reference for the errata based software policy.

- **Description**: Includes all the errata documentation for the errata.

- **Location**: Specifies the location of the policy in the folder hierarchy. To change the location click Select to specify the location for the policy in the folder hierarchy. The Select Location window appears. Select a folder in the Library to specify the location of the policy and then click **Select**.

- **Created**: Corresponds to the time when the errata was downloaded by HP to create the software policy.

- **Last Modified**: Corresponds to the time when the errata based policy was modified.

- **Availability**: Contains the HP server life cycle values for the errata based software policy. The default value for an errata based policy is set to Available.

- **Platform**: Specifies the all operating systems applicable to the errata. You can expand the list to see the selected platforms.

5   To save the changes, select **Save** from the **File** menu.

Installing Packages on Servers with Low Disk Space

By default, packages to be installed are downloaded from the Software Repository. This presents a problem on managed servers with low disk space.

To avoid this problem, administrators can specify locations such as shared network drives, or a CD-ROM, where SA should look for packages to install without downloading the package onto the managed server.

Specifying Paths for Package Installation

Using the SA Client, you can assign the `OPSWpackage_paths` custom attribute to servers or groups of servers.

To add the *OPSWpackage_paths* custom attribute to a managed server:

1   From the navigation pane, select **Devices** > **Servers** >**All Managed Servers**.

2   From the content pane, select the server for which you are defining the new custom attribute and select **Action > Open**. The Server Explorer window appears.

3   From the Views pane, select **Custom Attributes**.

4   Click the **Add** icon .

5   In the **Name** field, enter `OPSWpackage_paths`.

Be sure to use this exact spelling and case for each server for which you are specifying paths for package installation.

6   In the **Value** field click . The Input dialog appears. Enter each path for SA to look for the package to install. For example:

```
/mnt/cdrom
/shared/hpux_depots
```

or

```
/networkshare/packages/SunOS/5.6/
/mnt/cd0
```

Tip: You can enter any number of paths. You can also specify the Software Repository as a path by using `opsware_repository` as one of the values. This is useful in cases where you have entered a number of path names and want to disable the feature temporarily without having to re-enter the path names when you are ready to enable the feature again. To do this, enter `opsware_repository` at the top of the list of values.

7   To save the changes, select **File > Save** from the menu.

During subsequent package installations, each of the specified paths will be searched, in the sequence listed, until the package is located.

If the package is not found in any of the specified locations, SA will then search in the Software Repository. If it is found in the Software Repository, SA will attempt to download the package. If there is not enough disk space, an error message will appear, and the packages will not be downloaded.

Requirement: Verify that permissions on the files are set so that the SA Agent has read access.

Custom Attributes

Table: *Custom Attributes for Package Installation*

Custom Attribute	Description
`package_download_dir`	This custom attribute specifies the temporary directory where the agent stages (downloads) packages on a managed server before installing them.
	The Microsoft Offline Catalog file, and several other files used for Windows Patch Management, will also be downloaded at the location specified by this custom attribute [provided there is enough space].
`OPSWpackage_paths`	This custom attribute specifies a list of locations where the agent will look for packages.
	If the package is not found in any of the specified locations, SA will then search in the Software Repository. If it is found in the Software Repository, SA will attempt to download the package. If there is not enough disk space, an error message will appear, and the packages will not be downloaded.

Chapter 4 Remediating and Installing Software

SA Remediation is the policy-based method for installing software. This process involves attaching a software policy to managed servers or device groups and then remediating the servers or device groups against the policy.

Running the remediation job involves defining the job options, which provide flexibility and control of the software installation process. For example, the installation process is clearly delineated into stages: analysis, download, and installation. The remediation options allow you to independently schedule each stage. You can also define system reboot settings, run scripts, associate a ticket ID to each job and receive a job status notification by email upon successful completion of a stage.

The SA Remediation process compares what is actually installed on a server to the software that should be installed on the server according to the software policy, and determines what operations are required to make the server compliant. It then installs the software and applies the application configurations to the managed servers according to the software policy specifications, making them compliant.

In this section:

- Installing Software Using a Software Policy
- Attaching a Software Policy to a Server or Device Group
- Remediating Servers with Software Policies
- Viewing Job Status
- Uninstalling Software Using a Software Policy
- Installing/Uninstalling Software without a Software Policy
-

Installing Software Using a Software Policy

Using a software policy to install software has two phases:

1 Attaching a Software Policy to a Server or Device Group
2 Remediating Servers with Software Policies

> **Note:** You can also install software directly on a managed server using the SA Client. To install or uninstall software without a policy, see Installing/Uninstalling Software without a Software Policy.

Attaching a Software Policy to a Server or Device Group

You can attach a software policy and a server or device group in one of two ways:

* Attach a Software Policy to a Server or Device Group—use this method when you want to associate a specific policy with one or multiple devices.

* Attach a Server to a Software Policy—use this method when you want to associate a specific server or device group with one or multiple software policies.

When you attach a software policy and a managed server or device group, the software policy is only associated with that server or group, not installed. To install the software, remediate the server against the policy. See Remediating Servers with Software Policies.

Attach a Software Policy to a Server or Device Group

To attach a software policy to a server or device group:

1 From the SA Client navigation pane, select **Library** > **By Type** > **Software Policies**. A list of available software policies appears in the content pane. You may need to drill down the hierarchy a few levels to see the list of software policies.

2 Select a software policy. The policy details will appear in the lower pane.

   (Optional) To view the servers or device groups that are already attached with this policy, select **Server Usage** from the View drop-down list. Attached servers or device groups will be listed in the lower pane.

3 From the **Actions** menu, select **Attach...**. The Attach Server window appears.
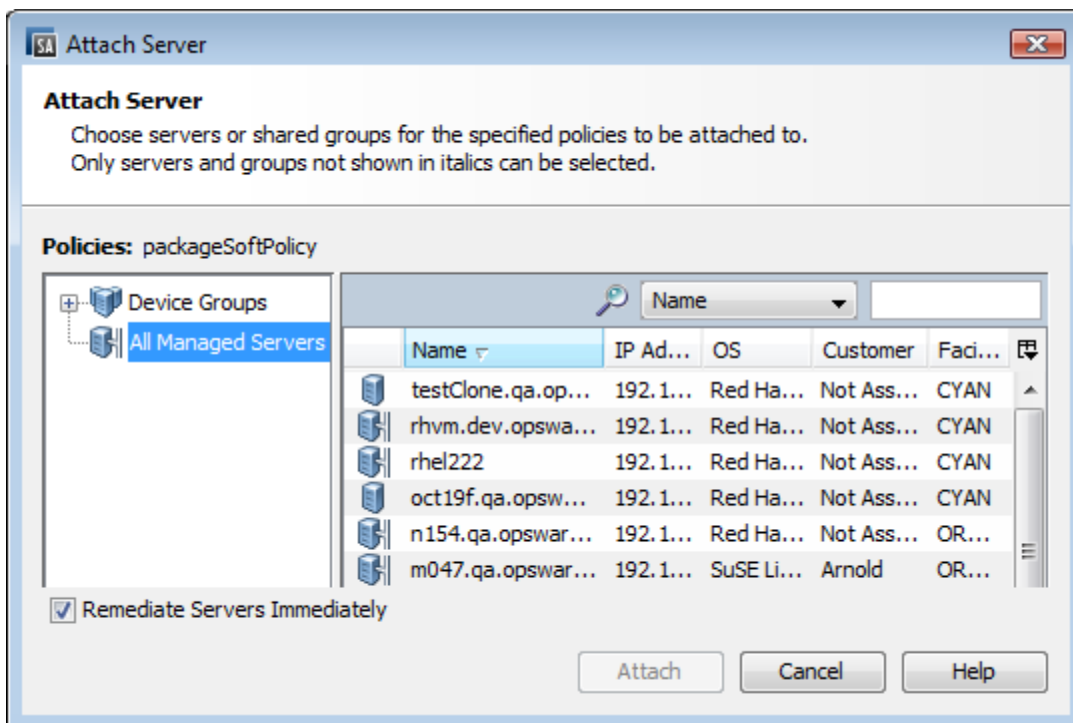
(*Optional*) Enable **Remediate Servers Immediately** to remediate the attached servers against the software policy. See Remediating Servers with Software Policies.

4   Navigate to the list of managed servers or device groups:

- •   Select **All Managed Servers** to view the server list.

- •   Select **Device Groups** to view the device group list.

5   From the content pane, select the servers or device groups that you want to attach to this policy.

You can only select servers that are not in *italics*. Servers in italics indicate that you do not have the necessary permissions to attach a software policy to that server.

6   Click **Attach**. The Remediate window will appear. See Remediating Servers with Software Policies.

Attach a Server to a Software Policy

To attach a server or device group to a software policy:

1   From the SA Client navigation pane, access the list of managed servers or device groups:

- •   Select **Devices** > **Servers** > **All Managed Servers** to view the server list.

- •   Select **Devices** > **Device Groups** to view the device group list.

2   From the content pane, select the servers or device groups.

3   From the **Actions** menu, select **Attach** > **Software Policy**. The Attach Software Policy window appears.
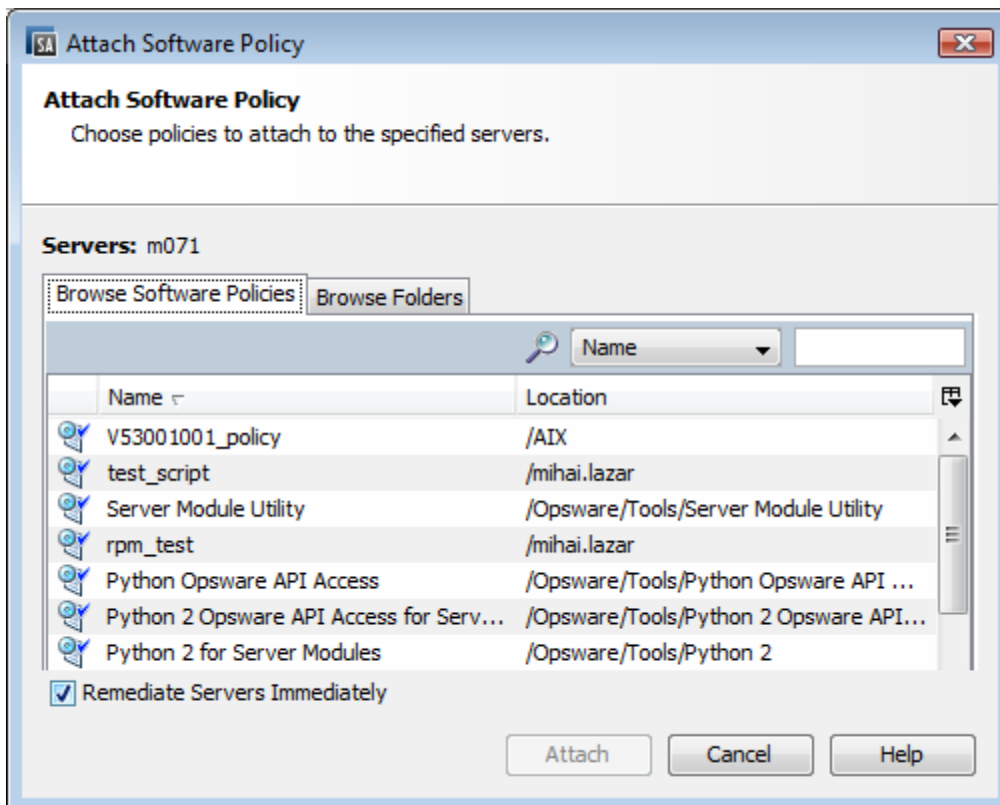
(*Optional*) Select **Remediate Servers Immediately** to remediate the servers against the software policy. See Specifying the Remediation Options.

4 Navigate to the policy you want to attach. The tabs present different navigation views:

- Select **Browse Software Policies** to view a flat list of software policies.

- Select **Browse Folders** to view the folder hierarchy. You may need to drill down the hierarchy a few levels to find the software policy you want.

5 Select the policy you want to attach.

6 Click **Attach**. The Remediate window will appear. See Remediating Servers with Software Policies.

Remediating Servers with Software Policies

Remediation brings servers into compliance with their attached software policies. The remediation process has three stages: 1) Analysis, 2) Download, and 3) Installation.

1 In the Analysis stage, SA compares the software that is actually installed on a managed server to the software that should be installed per the software policy. SA then determines what operations are required to make the server compliant with the software policy.

2 In the Download stage, SA downloads the necessary software resources (patches, packages, scripts, server objects, and application configurations) from the attached software policy to prepare for installation.

3 In the Installation stage, SA installs the downloaded software resources in the order specified in the policy and performs any of the other activities specified in the installation settings, such as running additional scripts and rebooting servers.

You can monitor the remediation job progress from the Job Status window. From this window you can view a summary of the actions performed in the job and the details of each action.

You can also cancel/terminate the job if you notice an error. See Terminating an Active Installation/Uninstallation or Remediation Job.

Accessing the Remediate Window

Access the Remediate window to specify the servers and software policies you want to remediate, define the conditions for remediation, and then run the job. Remediation conditions include reboot and error handling settings, the schedule for running the job (immediately or at scheduled times for each stage), and the email settings to notify users of the job status.

There are several ways to open the Remediate window, depending on what you are trying to accomplish. For example, this section provides instructions for the following methods:

- To remediate one or multiple servers against multiple attached software policies, access the Remediate window from the server list.

- To remediate one or multiple servers against a single policy, access the Remediate window from the software policy list.

- You can also revise the set of servers and policies that you want to remediate from the Remediate window. See Step 1: Select Servers and Policies for Remediation.

To access the Remediate window from the server list:

1   From the SA Client navigation pane, access the list of managed servers or device groups:

- Select **Devices** > **Servers** > **All Managed Servers** to view the server list.

- Select **Devices** > **Device Groups** to view the device group list.

2   From the content pane, select the server(s) or device group(s) you want to remediate. If you select one server, summary information about that server appears in the lower pane. If you select multiple servers, summary information is not provided.

3   From the **Actions** menu, select **Remediate...**. The Remediate window displays the selected server(s) and all of its attached software policies.
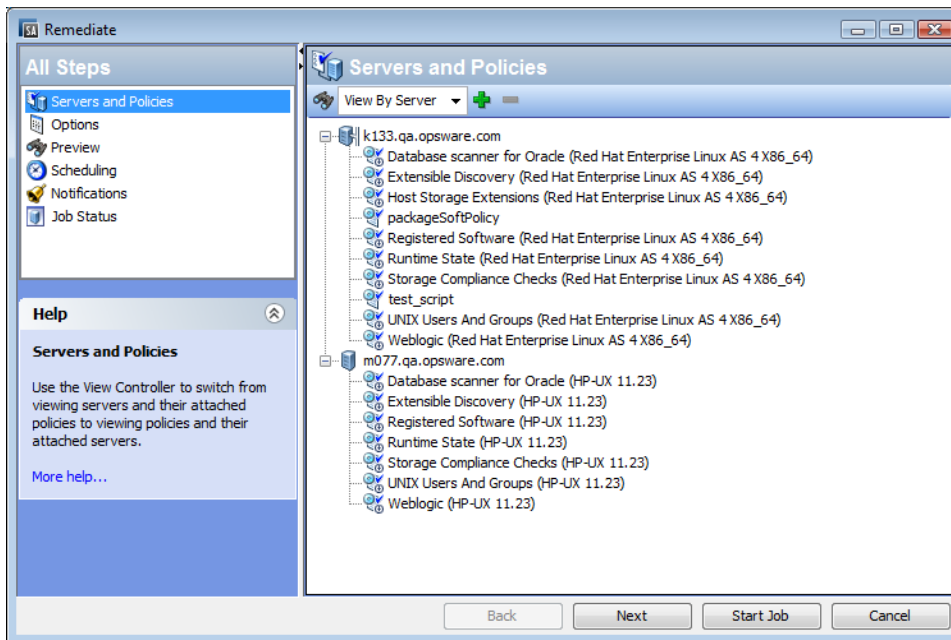
To access the Remediate window from the software policy list:

1   From the SA Client navigation pane, select **Library** > **By Type** > **Software Policies**. The Software Policy List appears in the content pane.

2   From the content pane, select a software policy. (You can only select one software policy in this step.)

3   From the **View** drop-down list, select **Server Usage**. A list of the servers attached to this policy appears in the lower pain.

4   Select a server or multiple servers, and then select **Remediate** from the **Actions** menu. The Remediate window appears displaying the selected server(s) with the attached software policy.
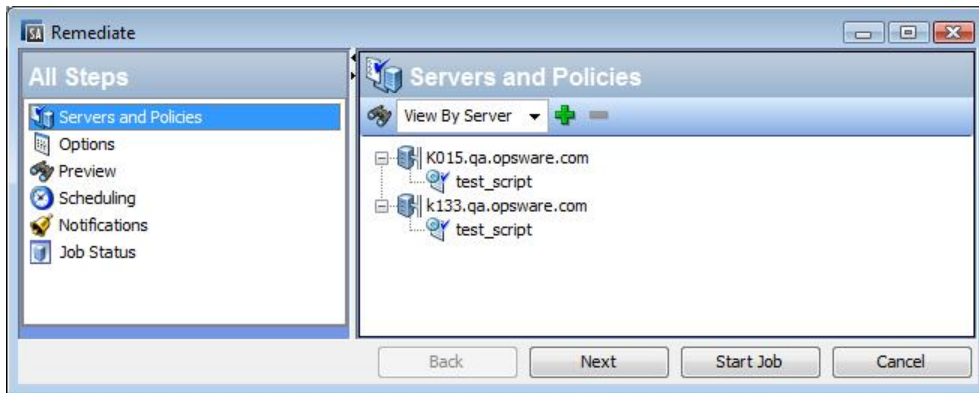
Specifying the Remediation Options

Use the Remediate window (The Remediate Window in the SA Client) to specify the remediation job options, run the job, and view the job status. The navigation pane in the Remediate window walks you through the following steps:

- Step 1: Select Servers and Policies for Remediation

- Step 2 (Optional): Specify Reboot, Error Handling, and Script Options for Remediation

- Step 3 (Optional): Preview the Remediation Job

- Step 4 (Optional): Schedule the Remediation Stages

- Step 5 (Optional): Set Email Notifications for Remediation

- Step 6: Run the Remediation Job and View Job Status

The Remediate Window in the SA Client
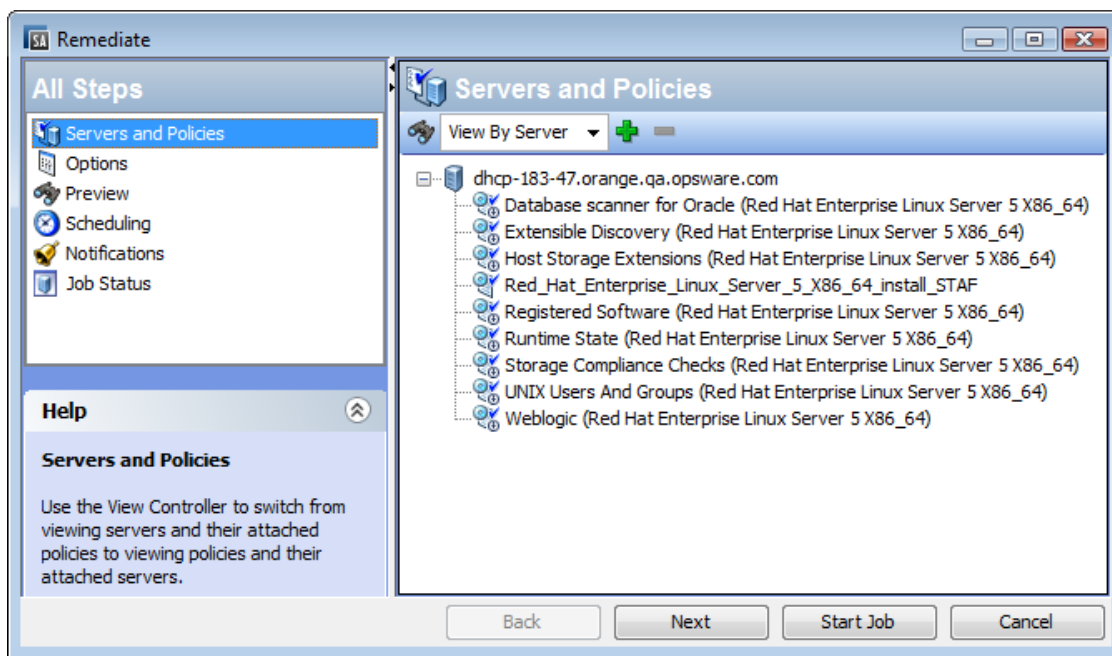
You can navigate between remediation setup steps from the All Steps pane on the left or by clicking the **Next** button after performing each step.

Step 1: Select Servers and Policies for Remediation

This step allows you to specify the servers (with attached software policies) for remediation. In this step, you can add and remove servers from the list, view all the policies attached to a server, and remove policies attached to servers.

To select the servers and policies for remediation:

1 Open the Remediate window from one of the methods described in Accessing the Remediate Window.

2 From the All Steps navigation pane, select **Servers and Policies**.

   By default, the content pane displays the selected servers and device groups with attached software policies and patch policies. To switch the view and display a list of policies with attached servers, select **By Policies** from the View drop-down list.

   • The 🔯 icon indicates a software policy.

   • The 🔯 icon indicates a patch policy.

3 (*Optional*) You can add or remove managed servers or device groups from the list:

   • To remove a server, select the server in the list and then click 🟥.

   • To add additional servers to the list, click 🟢. In the Select Servers and Device Groups window, select the servers to add and click **Select**. The added devices will now appear in the device list in the content pane of the Remediate window.

4 (*Optional*) You can remove software policies from the list:

   • To remove a policy from under a server, select the policy in the list and then click 🟥.

   • You cannot add software policies to the list.

5 Click **Next** to proceed to the Options step.

Step 2 (Optional): Specify Reboot, Error Handling, and Script Options for Remediation

You can specify how the remediation process will handle errors and rebooting, and if it will run any pre- or post-install scripts.

To specify these additional options:

1 In the **Rebooting** section, select one of the reboot options:

   You can control when to reboot servers during the software installation or uninstallation. For example, you may want to reboot the servers after each installation or you may want to hold all server reboots until all the software is installed to minimize downtime. You can also choose to suppress all server reboots.

   • *(Default)* **Reboot servers as specified by individual software items**: This option reboots servers per the reboot requirement specified in the software resource. See About Software Resource Reboot Requirement Settings.

   • **Reboot servers after each installation or uninstallation**: This option reboots servers after installing or uninstalling each software item.

> **Exception**: If the native package manager will use several transactions in order to complete the job, a reboot will be performed only after each transaction.

- **Hold all server reboots until all actions are complete**: This option suppresses server reboots until all the install/uninstall actions are complete. Then, it reboots the servers per the reboot requirement specified in the software resource.

- **Suppress all reboots**: This option suppresses the reboots even if the reboot option is selected in the software resource.

About Software Resource Reboot Requirement Settings

To view the reboot requirement of a software resource: Find the package in the SA Library: **Library** > **Packages** > drill down to the individual software resource > **Actions** > **Open**. In the Properties view expand the Install Parameters section to view the **Reboot Required** setting (yes or no).

The following table describes how the remediation process handles the software resource reboot requirements when the **Reboot servers as specified by individual software items** setting is selected:

Table: Software Resource Reboot Requirement Handling

Reboot Required?	Remediation Process
no	The remediate process will not reboot the server after installing that software resource
yes	The remediate process will reboot the server after installing that software resource
yes (all)	Even if all the resources are set to reboot, the remediate process will still reboot the server after each installation.
	Exception: If the native package manager will use several transactions in order to complete the job, a reboot will be performed only after each transaction.

2 In the **Error Handling** section, specify if you want to skip error handling when possible to minimize downtime.

- *(Default)* Select **Attempt to continue running if an error occurs** if you want the processes to continue even when an error occurs with any of the software, patches or scripts.

- Deselect this option if you want to see and respond to errors before the process continues.

3 In the Rollback Points section you can choose to create rollback points that enable you to restore your systems to a former working state in the event of a RPM upgrade, install or erase. More information about this functionality can be found in the RPM Rollback section of this guide.

4 In the **Scripts** section, specify if you want any scripts to run on a server before or after installation or uninstallation. There are four tabs in this section:

- Pre-Analyze: (Installation Only) Use this tab to enable a script that runs before software analysis.

- Post-Analyze: (Installation Only) Use this tab to enable a script that runs after software analysis.

- Pre-Download: (*Installation Only*) Use this tab to enable a script that runs before software or patches are downloaded from the software repository to the managed server.

- Post-Download: (*Installation Only*) Use this tab to enable a script that runs after software or patches are downloaded, but before the software or patch is installed

- Pre-Install/ Pre-Uninstall: Use this tab to enable a script that runs before software or patches are installed or uninstalled.

- Post-Install/ Post-UnInstall: Use this tab to enable a script that runs after software or patches are installed or uninstalled.

You can specify different scripts on each of the tabs, which provide the same options:

a   Select **Enable Script** to enable the remainder of the fields on the tab. Enable Script must be selected for a script to run.

b   In the **Select** drop-down list, select the type of script you want to run.

   — A **Saved Script** is stored for future use after you upload the script to SA.

      If you choose Saved Script, click **Select** to specify the script. The **Select Script** window appears. Select the script(s) to run and click **Select**.

   — An **Ad-Hoc Script** must be entered manually and is intended only for a single operation and is not stored in SA.

      If you choose Ad-Hoc Script, select the type of script from the **Type** drop-down list and then enter the script content in the **Script** field.

c   In the **Command** field, enter any command-line flags.

d   In the **Script Timeout** field, enter the script time-out value in minutes.

e   In the **Retain output of** field, enter the amount of output to retain in kilobytes.

f   In the **User** section, indicate whether you want to run the script as root or as a specified user:

   — To execute the script as root, select **Root**.

   — To execute the script as a specified user, select Name and enter the user name and password.

      To enter a Windows Domain Name in the pre-download, post-download, pre-install, post-install scripts, use the following format in the **Name** field: `DomainName\UserName`.

g   In the **Error** field, indicate your error handling preference:

   — Select **Stop job if script returns an error** if you want the installation to stop if the script returns an error.

   — Deselect this option if you want the script to continue running even when errors occur.

5   Click **Next t**o proceed to the Preview step.

Tip: To skip the remaining setting steps and run the job, see Step 6: Run the Remediation Job and View Job Status.

Step 3 (Optional): Preview the Remediation Job

You can preview a detailed list of actions that will be performed on a server as a result of the software remediation job. Information is displayed for each server or device group where the job will be run.

To preview the remediation process:

1   From from the All Steps navigation pane, select **Preview**. A blank content pane will appear with a **Preview** button.

2   Click **Preview** to view the actions that will be performed during the remediation process.

The Preview process only performs the Analyze phase and cannot be cancelled. While it is running, the **Start Job** button will be disabled.

Depending on the size of the job, the preview process may take a while. You can review the other settings while it is running, and then return to this view. When the preview is done running, the **Start Job** button will become enabled again.

3   To view the details of each of the actions, select a row in the table. The details for each action appear, including:

— the software resources that will be installed on or uninstalled

— the application configurations that will be applied to a server

— the dependency information required for the software packages or patches

— any reboots required during the remediation process

— any scripts that will be executed

The details vary depending on the item and action that is selected. If you select an object that has other software dependencies, you may see other objects (such as packages and ZIP files) listed in the preview.

If you select an application configuration, you have two options for inspecting the configuration:

Preview...   This option enables you to preview the details of the application configuration in this job. If you have multiple configurations in the job, the preview screen displays each configuration in a separate tab.

Each configuration preview tab presents the existing configuration on the server in the left pane. The modification defined in the selected configuration is shown in the right pane.

Configure...   This option opens the selected application configuration in the value set editor so you can define the values for the template variables at the server- instance level.

Preview...	This option enables you to preview the details of the application configuration in this job. If you have multiple configurations in the job, the preview screen displays each configuration in a separate tab.
	Each configuration preview tab presents the existing configuration on the server in the left pane. The modification defined in the selected configuration is shown in the right pane.

For more information about previewing application configurations, see the SA User Guide: Application Configuration.

(Optional) To export the job status results to a text file, click **Export**.

4   Click **Next** to proceed to the to the Scheduling step.

> **Tip:** To skip the remaining setting steps and run the job, see Step 6: Run the Remediation Job and View Job Status.

Step 4 (Optional): Schedule the Remediation Stages

The remediation process has three stages: 1) Analysis, 2) Download, and 3) Remediate. You can schedule specific times to run each stage, or set each stage to run immediately after the previous one completes.

To schedule the remediation stages:

1   In the Schedule Analysis section, select one of the following options:

- *(Default)* **Run at Job Start**: Runs the job immediately when you click **Start Job**.

  (Alternate Default) **Use Preview Results**: If you run a preview, this option appears as the default, indicating that it will use the preview results as the analysis step.

- **Start time**: Specify a later date and time to schedule the job.

2   In the Schedule Download section, select one of the following options: (*Installation Only*)

- *(Default)* **Run Immediately After Analysis**: Download software immediately after completing the analysis.

- **Start time**: Specify a later date and time to the download software.

3   In the Schedule Remediate section, select one of the following options:

- *(Default)* **Run Immediately After Download**: Install or Uninstall software immediately after completing the download.

- **Start time**: Specify the date and time to install or uninstall software.

4   Click **Next** to proceed to the Email Notifications step.

> **Tip:** To skip the remaining setting steps and run the job, see Step 6: Run the Remediation Job and View Job Status.

Step 5 (Optional): Set Email Notifications for Remediation

Set email notifications to alert you or other users on the success or failure of the remediation pro-cess. You can associate a Ticket ID to identify and track this job.

To specify email notifications:

1   By default, your email address will appear in the list of recipient email addresses.

   •   To add additional recipients, click **Add Notifier** and enter the email addresses in the Email Address of Recipient field.

   •   To remove a recipient, select the recipient and click **Remove**.

2   For each recipient, select the options for when to send an email notification:

   •   On Success: sends email to recipient if the job succeeds.

   •   On Failure: sends email to recipient if the job fails.

   •   On Termination: sends email to recipient if the job is terminated.

      –   Termination occurs when you stop an actively running job via the End Job action.

      –   This notification does *not* apply to jobs that are cancelled before they are run.

3   In the Ticket **ID** field, enter a unique text string to identify this job. This string will appear in the email notifications.

4   Click **Next** to proceed to the Job Status step.

   The Job Status window will appear without any details until you start the job. See Step 6: Run the Remediation Job and View Job Status.

Step 6: Run the Remediation Job and View Job Status

When you run the remediation job, the Job Status window provides summary information about its progress. You can also view the status of each action required to complete the job.

To run the remediation job and view the job status:

1   Click **Start Job** from one of the following locations to run the installation.

   a   After specifying the servers and software policy to remediate, you can run the remediation job immediately by clicking **Start Job**.

   b   Alternatively, you can complete the any of the optional setting steps before starting the job:

      —   Step 2: Options—Specify how the remediation process will handle errors and rebooting, and if it will run any pre- or post-install scripts.

      —   Step 3: Preview—View a snapshot preview of the actions that will be performed in the remediation process that you have defined.

      —   Step 4: Scheduling—Schedule the remediation stages: 1) Analysis, 2) Download, 3) Install. You can specify specific times to perform the actions in the stage, or set each stage to run immediately after the previous one completes.

      —   Step 5: Notifications—Indicate if you want to receive an email notification when the job succeeds, fails or is cancelled. You can also specify a ticket id for the job.

   From any of these steps, click **Start Job** to run the remediation job.

2   The Job Status window will appear without any details until the job actually begins. When the job starts depends on the settings defined in the Scheduling step.

- If you set the job to run immediately, which is the default setting, then the job will begin immediately after you click **Start Job** from any of the setting steps. When the job starts, the Job Status window will appear showing the progress of the job.

- If you scheduled the job for a later time, the job will run at the scheduled time and only then will the Job Status window show progress details.

3   To view the details of each action, select an action row in the table. The details for the selected action appear in the lower panel of the content pane. See Viewing Job Status for details.

Viewing Job Status

The Job Status window displays detailed results of a job that has completed or is in progress. The Status bar displays relative progress throughout the job.

To view the details of each action in a job, select an action row in the table. The detail steps for the selected action appear in the details pane.

You can also perform any of the following optional actions:

- Click **Export** to export the job status results to a text file.
- Click **Expand All** or **Collapse All** to expand or collapse all the action sets.
- Click **End Job** to stop the job. See .
- Click **Close** to close the window. To view job status later, click **Job Status** from the SA Client navigation pane, and then double-click on the job to view details.

Note: For more information about SA Client job logs, see the *SA User Guide: Server Automation* for information about job logs.

Uninstalling Software Using a Software Policy

You can uninstall software installed using a software policy by detaching the policy from a managed server or device group and then remediating the server. The remediation process recognizes that the software policy has been detached and uninstalls the software. You can also remove specific software resource from the attached software policy to uninstall specific software while keeping the policy attached.

Uninstalling software by detaching a software policy has two phases:

- Detach a Software Policy from the Managed Server
- Remediate a Server to Remove Software

Detach a Software Policy from the Managed Server

Simply detaching a software policy from a server does not delete the software policy itself nor does it uninstall the software from the managed server or device group. To uninstall the software, you must detach the software policy from the server or group and then remediate the server.

To detach a software policy from a server:

1   From the SA Client navigation pane, access the list of managed servers or device groups:
- Select **Devices** > **Servers** > **All Managed Servers** to view the server list.
- Select **Devices** > **Device Groups** to view the device group list.
2   From the content pane, select the servers or device groups.
3   From the **View** drop-down list, select **Software Policies**. The software policies attached to the server appear in lower pane.
4   Select the policy or policies that you want to detach. (Note that inherited policies cannot be detached.)
5   From the **Actions** menu, select **Detach**. The **Detach Software Policy** window appears.
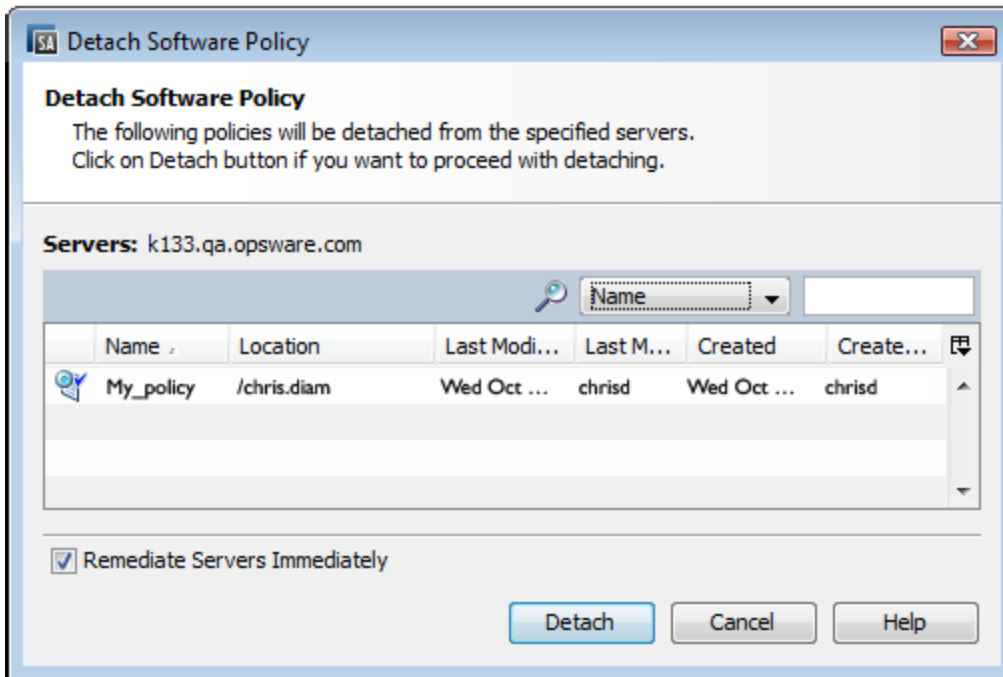
6 *(Optional)* Select **Remediate Servers Immediately** to remediate the servers against the software policy immediately after detaching the policy. (This is the default setting.)

7 Click **Detach**. The policy is removed from the list of policies for that server.

- If you selected **Remediate Servers Immediately**, in the Detach Software Policy window, the Remediate window will appear.

- If you did not select **Remediate Servers Immediately**, the policy will not be uninstalled from the server until you remediate the server.

Remove (Server-Software Policy) attachment

Detaching and remediating large policies from managed devices can render the devices unusable due to the large number of packages and their dependencies being uninstalled.

As a solution, this functionality simply removes the association between the software policy and the device without requiring a subsequent remediation job, thus without affecting the device in any way. For example, no package will be uninstalled.

This action can also be applied for detached but not yet remediated policies.

If the device was compliant before this action, the compliance status is preserved.

To remove a server-policy attachment:

1 From the SA Client navigation pane, access the list of managed servers or device groups:

- a Select **Devices** > **Servers** > **All Managed Servers** to view the server list.

- a Select **Devices** > **Device Groups** to view the device group list.

2 From the content pane select the servers or device groups.

3   From the **View** drop-down list, select **Management Policies** > **Software Policies** .The software policies attached to the server appear in the lower pane.

4   Select the policy or policies whose server attachment you want to be removed (Note that attachments for inherited policies cannot be removed)

5   From the **Actions** menu, select **Remove Attachment** . The **Remove Policy Attachment** window appears.
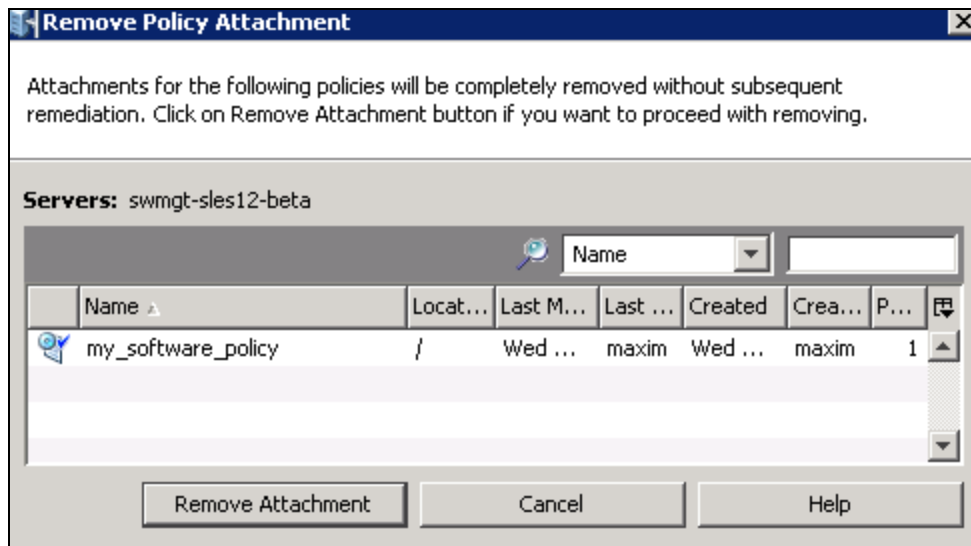
6   Click **Remove Attachment** . The association between the policy and the server is removed.

Remediate a Server to Remove Software

Perform the tasks described in Specifying the Remediation Options. The software specified in the detached software policy will be removed from the managed server.

When you detach a software policy from a server and then remediate:

a   Any software packages contained in the policy are physically uninstalled from the server during the remediation process, unless:

  —   the same package(s) are also contained in other software policies that are attached to the server, or

  —   SA has determined that the package is a prerequisite for other packages currently installed on the server

b   Application configurations contained in the policy are detached, but the configuration files are left on the server

Cancelling a Scheduled Installation/Uninstallation or Remediation Job

When you cancel a scheduled installation, uninstallation or remediation job, the entire job is cancelled and it appears in the Job Log queue with Cancelled status.

To cancel a schedule job, perform these steps:

1   From the SA Client navigation pane, select **Jobs and Sessions**. The Job Logs window appears in the content pane.

2   In the Status filter, select: Scheduled.

3   Select the scheduled job that you want to cancel.

4   From the menu, select **Action** > **End Job**. The job appears in the Job Log with Cancelled status.
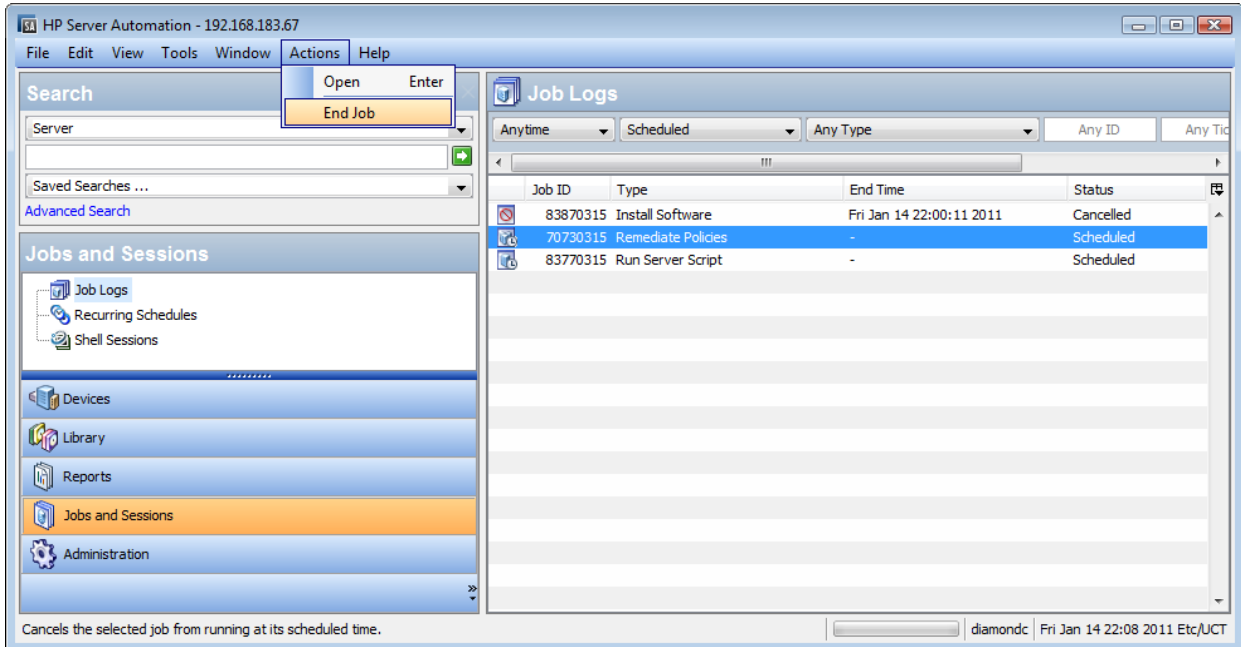
Cancelling Scheduled or Recurring Jobs

You can cancel a scheduled or recurring job that is not running from the Job Log window. (For example, scheduled job types that can be cancelled include installation, uninstallation, remediation, and application configuration push jobs.) When you cancel a scheduled or recurring job, the entire job is cancelled. For instructions, see Cancelling a Scheduled Installation/Uninstallation or Remediation Job.

Terminating Active Jobs

You can also terminate certain jobs that are actively running. For example, you may need to stop a job that is producing erroneous results or will run beyond an allotted maintenance window. The types of active jobs that can be stopped include installation, uninstallation, remediation, or application configuration push jobs.

Actively running jobs respond differently to being terminated than scheduled or recurring jobs. When you terminate an actively running job, forthcoming and scheduled phases are immediately cancelled. For instructions, see Terminating an Active Installation/Uninstallation or Remediation Job.

An active installation/ uninstallation or remediation job can be stopped in any job phase. Depending on the phase that is running when the job is being terminated, the following behaviors apply:

- Analyze: the job terminates after the Analyze phase is completed. The next phases does not start.

- Download or Install/ Uninstall/ Remediate: execution stops as soon as the phase finishes processing the item it is currently handling.

Further, pending items, from the job item list will be skipped. The next phase, if any, will not be executed.

Terminating an active installation, uninstallation or remediation job has the following results:

* No processes will be started on additional servers.

* If a job phase has already started on a server, then the currently running tasks from that phase will be completed. No new tasks will be started within that job phase. Also no new phases will be started.

* Any staged packages downloaded to the server will be removed, no matter what phase the job was processing when it was cancelled.

* The Job Status view displays each job step and indicates whether or not they were performed.

Status	Explanation
Server Status	
Cancelled	The job was cancelled before completing all of the steps on the device.
Succeeded	All the steps were completed on the device.
Step Status	
Skipped	The step did not get executed on the listed device.
Succeeded	The step was completed on the listed device.

* The Job Logs view displays the status of the job.

Job Status	Explanation
Terminating	The termination request has been received and the job is in the process of ending.
Terminated	The termination process has completed.

Permissions for Terminating Active Jobs

In general, users with the permission to start a job will also be able to terminate that job. In addition, users having *Edit or Cancel Any Job* permission are able to soft-cancel any running job.

See "Permissions Reference" in the *SA Administration Guide* for SA permissions details.

> **Note:** For Windows Patch Policy Remediation jobs, *Servers - Allow Remediate Servers* permission must be granted in order to soft-cancel and display Remediation Policies jobs in Jobs & Session table panel. Notice that this permission is different than the one used to start the job.

Terminating an Active Installation/Uninstallation or Remediation Job

You can terminate a software installation, uninstallation or remediation job that is actively running. For example, you may need to stop a job that is producing erroneous results or will run beyond an allotted maintenance window.

To stop an active remediation or installation job:
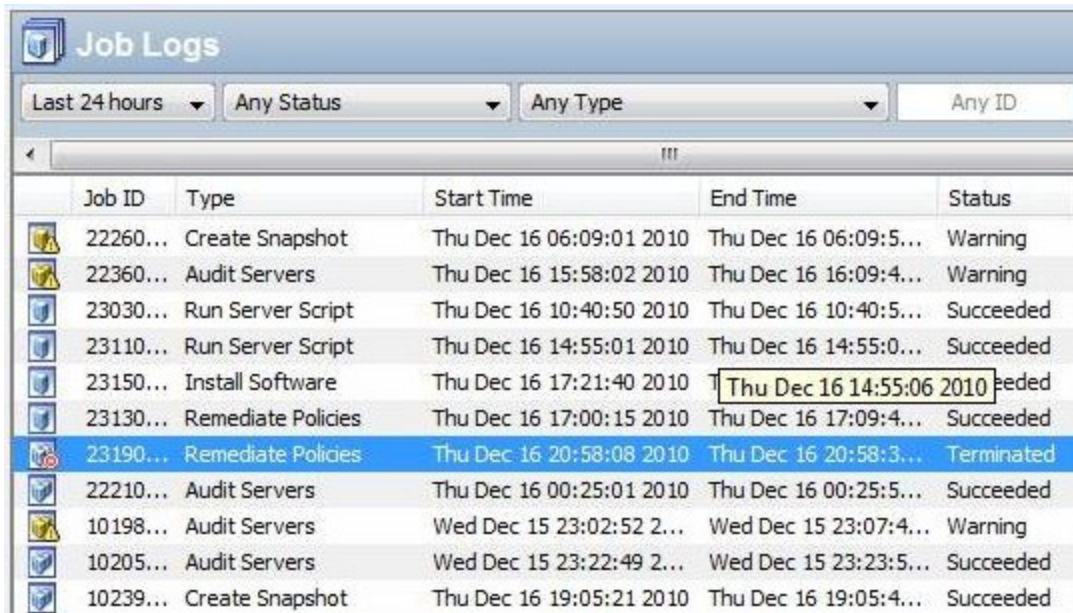
1   From the Job Status window, click **End Job**. (This button only appears if the job is in progress.)

2   The End Job warning dialog will be displayed advising you how job termination works:

- the job will not initiate work on any additional servers

- if work has started on a server, the job will cancel any steps that can be skipped

- the Job Status will indicate the steps that were completed or skipped

- if the job ends successfully, the final job status will be "Terminated"

3   Click **OK** to confirm that you wish to terminate the job. The Job Status window displays the progress of the termination.
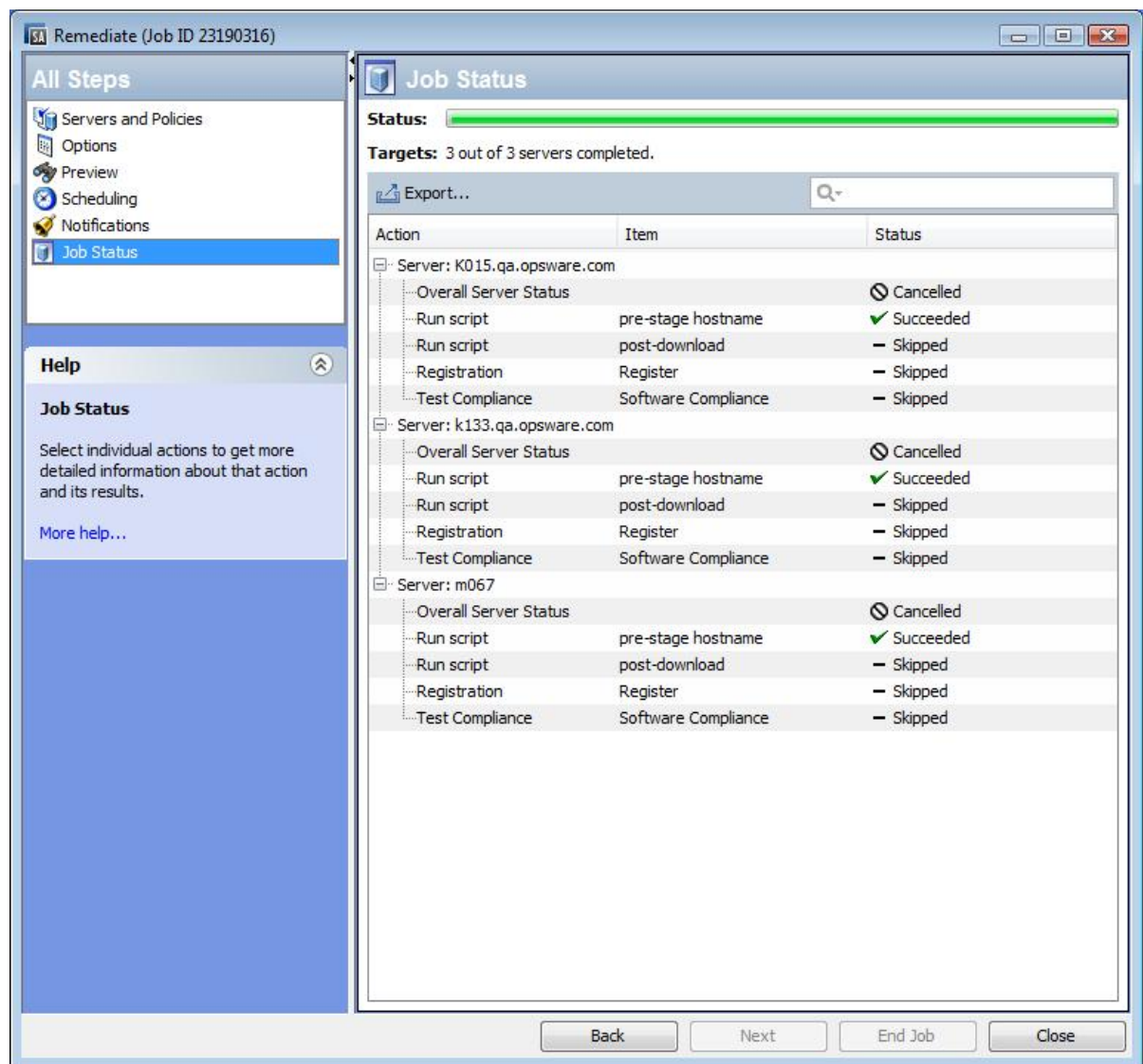
The job status will be Terminated. The server status will be Cancelled. The task statuses will be Succeeded or Skipped.

4 When the termination is complete, you can also view the job in the SA Client Job Log.

From the SA Client navigation pane, click **Jobs and Sessions**. The Job Logs view appears with your job listed with Terminated status.

See also for an explanation of how the job cancellation process works and what the individual statuses mean.

Terminating an Active Job from the SA Client Job Logs

You can terminate an active job from the SA Client Job Logs.

To terminate an active job from the SA Client Job Logs, perform these steps:

1 From the SA Client navigation pane, select **Jobs and Sessions**. The Job Logs window appears in the content pane.

2 In the Status filter, select In Progress to find running jobs.

3 Select **View** > **Refresh** from the menu to refresh the list. The content pane displays jobs with In Progress status.

   You can additionally filter the list by the type of job (such as Remediate Policies) from the Type filter.

4 In the content pane, select the job that you want to terminate.

5 Select **Action** > **End Job** from the menu. (This option only appears if the selected job is in progress.)

   When the termination process is complete, the job will have Terminated status.
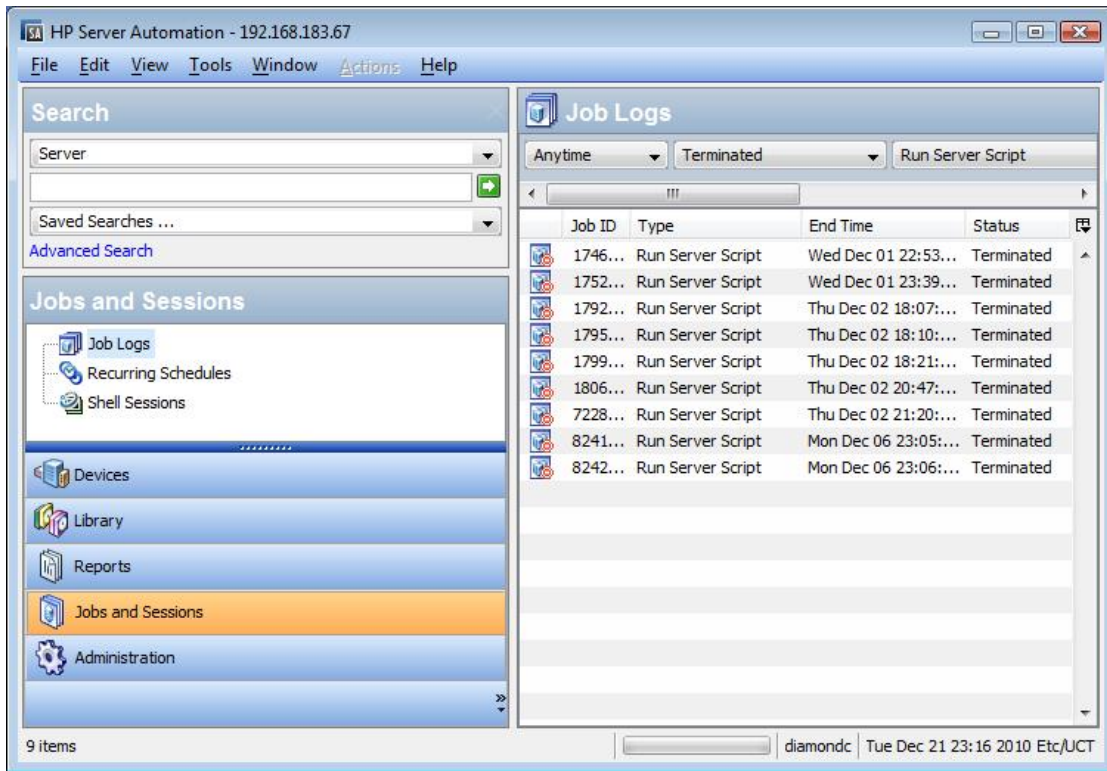
Installing/Uninstalling Software without a Software Policy

You can install software without the use of a software policy directly on a managed server using the SA Client, as described in this section.

Best Practice: Using a software policy is the recommended method for installing software on an SA managed server. This involves attaching a software policy to a managed server and then remediating the server against the policy to install the software. See Installing Software Using a Software Policy.

Accessing the Install or Uninstall Window

To access the Install or Uninstall window from the server or device group list:

1   From the SA Client navigation pane, access the list of managed servers or device groups:

 • Select **Devices** > **Servers** > **All Managed Servers** to view the server list.

 • Select **Devices** > **Device Groups** to view the device group list.

2   From the content pane, select the servers or device groups on which you want to install or uninstall software.

3   From the **Actions** menu select the action you want to perform:

 • Select **Install** > **Software** to open the Install Software window.

 • Select **Uninstall** > **Software** to open the Uninstall Software window.

   The Install or Uninstall Software window appears listing the selected servers or devices. Proceed to Specifying the Install or Uninstall Options.

To access the Install window from the software policy list:

1   From the SA Client navigation pane, select **Library** > **By Type** > **Software Policies**. The software policies list appears, organized by operating system.

2   Navigate to the software policy that you want to install. You may need to drill down a few levels within a given operating system to find the software policy list.

3   From the content pane, select the software policy you intend to install.

4   From the **Actions** menu, select **Install Software**. The Install Software window appears listing the selected software policy. Proceed to Specifying the Install or Uninstall Options.

Specifying the Install or Uninstall Options

You can install or uninstall software directly on an SA managed server. The Install Software window as shown in Install Software Window and the Uninstall Window provide the following options:

•   Step 1: Select Devices

•   Step 2: Select Software

•   Step 3 (Optional): Specify Reboot, Error Handling, and Script Options

•   Step 4 (Optional): Preview the Installation/Uninstallation Job

•   Step 5 (Optional): Schedule the Installation/Uninstallation Stages

•   Step 6 (Optional): Setting Email Notifications for Installation/Uninstallation

•   Step 7: Run the Installation/Uninstallation and View Job Status

Note: All steps outlined in this section are performed from the Install Software or Uninstall Software window. See Accessing the Install or Uninstall Window.

Install Software Window
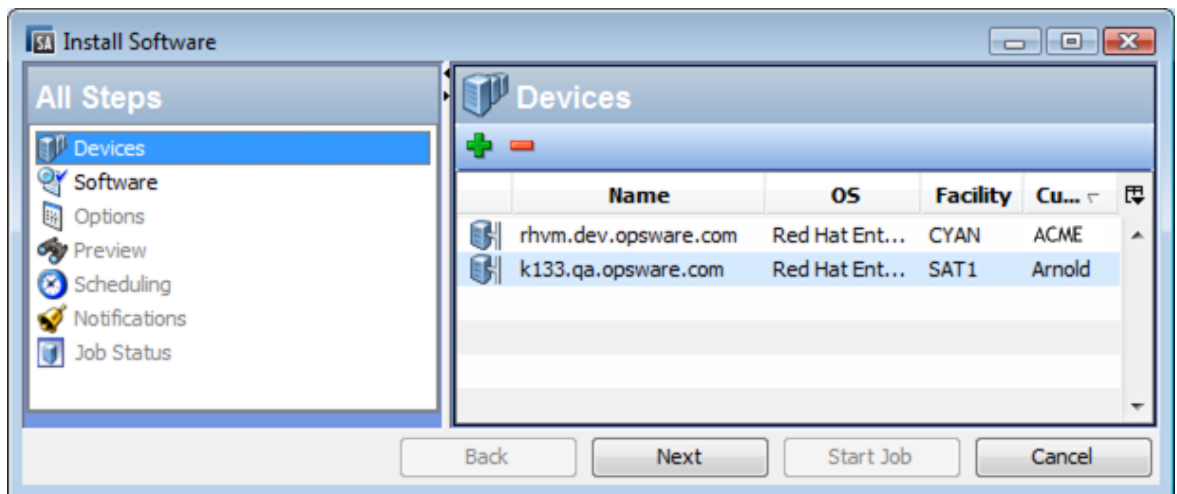
> **Tip:** You can navigate between installation setup steps from the All Steps pane on the left or by clicking the **Next** button after performing each step.

Step 1: Select Devices

Specify the servers or device groups on which to install or uninstall software.

To select devices:

1. From the All Steps navigation pane, select **Devices**. The content pane displays a list of servers and device groups on which to install or uninstall software.

2. *(Optional)* Add or remove servers or device groups:

   - To remove a server, select the server in the list and then click ▬.

   - To add additional servers to the list, click ✚. In the Select Servers and Device Groups window, select the servers to add and click **Select**. The added devices will now appear in the device list in the Install Software window.

3. Click **Next** to proceed to the Select Software step.

Step 2: Select Software

Specify the software (packages, patches, etc.) to install or uninstall. You can also specify the order in which you want to install or uninstall the software.

To select the software:

1. From from the All Steps navigation pane, select **Software**. The software list in the content pane will be empty until you add the software.

2. Click ✚ to open the Select Library Item window.

3. In the Select Library window, select the software to be installed or uninstalled and click **Select**.

   a. Click the Browse Types tab to browse the list of items by type, such as Software Policy, Patch, Package.

   b. Click the Browse Folders tab to browse the item list by folders.

   The added software items will now appear in the software list in the Install Software window.

4. *(Optional)* Reorder or remove listed software:

   — To reorder the software in the list, click ⬆ or ⬇.

   - To remove any of the software you have added, select the software and click ▬.

5. Click **Next** to proceed to the Specify Additional Options step.

> **Tip:** After adding the software you want to install, you can run the install or uninstall job, or you can complete the additional setting options before running the job. To skip the remaining setting steps and run the job immediately, see Step 7: Run the Installation/Uninstallation and View Job Status.

Step 3 (Optional): Specify Reboot, Error Handling, and Script Options

You can specify how the installation/uninstallation process will handle errors and rebooting, and if it will run any pre- or post-install scripts.

To specify these additional options:

1   From from the All Steps navigation pane, select **Options**. Additional job options are displayed in the content pane.

2   In the **Rebooting** section, select one of the reboot options:

    You can control when to reboot servers during the software installation or uninstallation. For example, you may want to reboot the servers after each installation or you may want to hold all server reboots until all the software is installed to minimize downtime. You can also choose to suppress all server reboots.

    • *(Default)* **Reboot servers as specified by individual software items**: This option reboots servers per the reboot requirement specified in the software resource.

    • **Reboot servers after each installation or uninstallation**: This option reboots servers after installing or uninstalling each software item.

       Exception: If the native package manager will use several transactions in order to complete the job, a reboot will be performed only after each transaction.

    • **Hold all server reboots until all actions are complete**: This option suppresses server reboots until all the install/uninstall actions are complete. Then, it reboots the servers per the reboot requirement specified in the software resource.

    • **Suppress all reboots**: This option suppresses the reboots even if the reboot option is selected in the software resource.

> **Tip:** To view the reboot requirement of a software resource: Find the package in the SA Library: **Library** > **Packages** > drill down to the individual software resource > **Actions** > **Open**. In the Properties view expand the Install Parameters section to view the **Reboot Required** setting (yes or no). See About Software Resource Reboot Requirement Settings

3   In the **Error Handling** section, specify if you want to skip error handling when possible to minimize downtime.

    • *(Default)* Select **Attempt to continue running if an error occurs** if you want the installation or uninstallation process to continue even when an error occurs with any of the software, patches or scripts.

    • Deselect this option if you want to see and respond to errors before the process continues.

4   In the Rollback Points section you can choose to create rollback points that enable you to restore your systems to a former working state in the event of a RPM upgrade, install or erase. More information about this functionality can be found in the RPM Rollback section of this guide.

5   In the **Scripts** section, specify if you want any scripts to run on a server before or after installation or uninstallation. There are four tabs in this section:

   •   Pre-Analyze: (Installation Only) Use this tab to enable a script that runs before software analysis.

   •   Post-Analyze: (Installation Only) Use this tab to enable a script that runs after software analysis.

   •   Pre-Download: (*Installation Only*) Use this tab to specify a script that runs before software or patches are downloaded from the software repository to the managed server.

   •   Post-Download: (*Installation Only*) Use this tab to specify a script that runs after software or patches are downloaded, but before the software or patch is installed .

   •   Pre-Install/ Pre-Uninstall: Use this tab to specify a script that runs before software or patches are installed or uninstalled.

   •   Post-Install/ Post-UnInstall: Use this tab to specify a script that runs after software or patches are installed or uninstalled.

   You can specify different scripts on each of the tabs, which provide the same options:

   a   Select **Enable Script** to enable the remainder of the fields on the tab. Enable Script must be selected for a script to run.

   b   In the **Select** drop-down list, select the type of script you want to run.

      —   A **Saved Script** is stored for future use after you upload the script to SA.

         If you choose Saved Script, click **Select** to specify the script. The **Select Script** window appears. Select the script(s) to run and click **Select**.

      —   An **Ad-Hoc Script** must be entered manually and is intended only for a single operation and is not stored in SA.

         If you choose Ad-Hoc Script, select the type of script from the **Type** drop-down list and then enter the script content in the **Script** field.

   c   In the **Command** field, enter any command-line flags.

   d   In the **Script Timeout** field, enter the script time-out value in minutes.

   e   In the **Retain output of** field, enter the amount of output to retain in kilobytes.

   f   In the **User** section, indicate whether you want to run the script as root or as a specified user:

      —   To execute the script as root, select **Root**.

      —   To execute the script as a specified user, select Name and enter the user name and password.

         To enter a Windows Domain Name in the pre-download, post-download, pre-install, post-install scripts, use the following format in the **Name** field:
         `DomainName\UserName.`

g   In the **Error** field, indicate your error handling preference:

   —   Select **Stop job if script returns an error** if you want the installation to stop if the script returns an error.

   —   Deselect this option if you want the script to continue running even when errors occur.

6   Click **Next t**o proceed to the Preview step.

   To skip the remaining setting steps and run the job immediately, see Step 7: Run the Installation/Uninstallation and View Job Status

Step 4 (Optional): Preview the Installation/Uninstallation Job

You can preview a detailed list of actions that will be performed on a server as a result of the software installation or uninstallation job. It displays information for each server or device where the job will be run.

To preview the installation or uninstallation process:

1   From from the All Steps navigation pane, select **Preview**. A blank content pane will appear with a **Preview** button.

2   Click **Preview** to view the actions that will be performed during the installation or uninstallation process.

   The Preview process only performs the Analyze phase and cannot be cancelled. While it is running, the **Start Job** button will be disabled.

   Depending on the size of the job, the preview process may take a while. You can review the other settings while it is running, and then return to this view. When the preview is done running, the **Start Job** button will become enabled again.

3   To view the details of each of the actions, select a row in the table. The details for each action appear, including:

   —   the software resources that will be installed on or uninstalled

   —   the application configurations that will be applied to a server

   —   the dependency information required for the software or patches

   —   any reboots required during the installation or uninstallation process

   —   any scripts that will be executed

   The details vary depending on the item and action that is selected. If you select an object that has other software dependencies, you may see other objects (such as packages and ZIP files) listed in the preview.

   If you select an application configuration, you have two options for inspecting the configuration:

Preview...	This option enables you to preview the details of the application configuration in this job. If you have multiple configurations in the job, the preview screen displays each configuration in a separate tab.
	Each configuration preview tab presents the existing configuration on the server in the left pane. The modification defined in the selected configuration is shown in the right pane.
Configure...	This option opens the selected application configuration in the value set editor so you can define the values for the template variables at the server- instance level.

For more information about previewing application configurations, see the SA User Guide: Application Configuration.

4 Click **Next to** proceed to the to the Scheduling step.

To skip the remaining setting steps and run the job immediately, see Step 7: Run the Installation/Uninstallation and View Job Status.

Step 5 (Optional): Schedule the Installation/Uninstallation Stages

The installation and uninstallation processes have three stages: 1) Analysis, 2) Download, and 3) Install. You can schedule specific times to run each stage, or set each stage to run immediately after the previous one completes.

To schedule the installation or uninstallation stages:

1 In the Schedule Analysis section, select one of the following options:

- *(Default)* **Run at Job Start**: Runs the job immediately when you click **Start Job**.

  (Alternate Default) **Use Preview Results**: If you run a preview, this option appears as the default, indicating that it will use the preview results as the analysis step.

- **Start time**: Specify a later date and time to schedule the job.

2 In the Schedule Download section, select one of the following options: (*Installation Only*)

- *(Default)* **Run Immediately After Analysis**: Download software immediately after completing the analysis.

- **Start time**: Specify a later date and time to the download software.

3 In the Schedule Install or Schedule Uninstall section, select one of the following options:

- *(Default)* **Run Immediately After Download**: Install or Uninstall software immediately after completing the download.

- **Start time**: Specify the date and time to install or uninstall software.

4 Click **Next** to proceed to the Email Notifications step.

To skip the remaining setting steps and run the job immediately, see Step 7: Run the Installation/Uninstallation and View Job Status.

Step 6 (Optional): Setting Email Notifications for Installation/Uninstallation

Set email notifications to alert you or other users on the success or failure of the installation or uninstallation process. You can associate a Ticket ID to identify and track this job.

To specify email notifications:

1   By default, your email address will appear in the list of recipient email addresses.

- To add additional recipients, click **Add Notifier** and enter the email addresses in the Email Address of Recipient field.
- To remove a recipient, select the recipient and click **Remove**.

2   For each recipient, select the options for when to send an email notification:

- On Success: sends email to recipient if the job succeeds.
- On Failure: sends email to recipient if the job fails.
- On Termination: sends email to recipient if the job is terminated.
  - Termination occurs when you stop an actively running job via the End Job action.
  - This notification does *not* apply to jobs that are cancelled before they are run.

3   In the Ticket **ID** field, enter a unique text string to identify this job. This string will appear in the email notifications.

4   Click **Next** to proceed to the Job Status step.

The Job Status window will appear without any details until you start the job. See Step 7: Run the Installation/Uninstallation and View Job Status.

Step 7: Run the Installation/Uninstallation and View Job Status

When you run the installation or uninstallation job, the Job Status window provides summary information about its progress. You can also view the status of each action required to complete the job.

To run the installation/uninstallation job and view job status:

1   Click **Start Job** from one of the following locations to run the installation.

a   After specifying the software to install, you can run the installation job immediately by clicking **Start Job**.

b   Alternatively, you can complete the any of the optional setting steps before starting the job:

— Step 3: Options—Specify how the installation/uninstallation process will handle errors and rebooting, and if it will run any pre- or post-install scripts.

— Step 4: Preview—View a snapshot preview of the actions that will be performed in the installation or uninstallation process that you have defined.

— Step 5: Scheduling—Schedule the installation stages: 1) Analysis, 2) Download, 3) Install. You can specify specific times to perform the actions in the stage, or set each stage to run immediately after the previous one completes.

— Step 6: Notifications—Indicate if you want to receive an email notification when the job succeeds, fails or is cancelled. You can also specify a ticket id for the job.

From any of these steps, click **Start Job** to run the installation or uninstallation job.

2   The Job Status window will appear without any details until the job actually begins. When the job starts depends on the settings defined in the Scheduling step.

- If you set the job run immediately in the Scheduling step, which is the default setting, then the job will begin immediately after you click **Start Job** from any of the setting steps. When the job starts, the Job Status window will appear showing the progress of the job.

- If you scheduled the job for a later time in the Scheduling step, the job will run at the scheduled time and only then will the Job Status window show progress details.

3   To view the details of each action, select a row in the table. The details for each action appear in the lower panel of the content pane. See Viewing Job Status for details.

Note: For more information about SA Client job logs, see the *SA User Guide: Server Automation* for information about job logs.

Uninstalling Software From the Server Inventory

SA periodically scans, and then stores, the full software inventory of a managed device, containing software that was installed using SA and other external tools. For more information, see the UG: Server Automation section on software and hardware inventory.

Even for SA-installed software, the software inventory does not maintain relationships between the SA library packages used in the install job and the items in the inventory, because the same package can be duplicated in several folders of the SA Library, with each package having its own properties, including uninstall parameters and scripts. As a result, uninstalling a package from the server inventory will not use the uninstall parameters and scripts of any package in the SA Library. To uninstall a package using uninstall parameters and scripts, see Installing/Uninstalling Software without a Software Policy.

Timeout Handling for Remediation and Installation Jobs

A timeout can occur during a software remediation or installation job. When this happens the job execution stops to prevent further changes to the server.

> **Note:** The error handling option set for the job (see Step 2 (Optional): Specify Reboot, Error Handling, and Script Options for Remediation) does not apply to timeouts. A timeout, unlike a general error, describes a situation where the job had been running successfully until a specified time interval passed. This is not considered an error, and the job does not attempt to run the remaining phases irrespective of the above flag.

Execution exceeds maximum defined duration

The main reason remediation and installation jobs time out is, when processing a job phase or job item exceeds the maximum defined duration for the specific phase or item (Example: package, script or patch).

These timeout values can be adjusted in the Command Engine section of System Configuration (for more information contact your HP Server Automation Administrator).

When encountering this type of timeout, the job attempts to stop as soon as possible. This behavior depends on phase active when the timeout occurred:

- Analyze: the analyze phase gets completed, but the next phases will not be started

- Download: the download stops after the current package is downloaded. Pending packages will not be downloaded and the next phases will not be started.

- Action: the installation that is currently running will complete but no remaining items will be processed.

After the timeout occurs and until the job execution stops, the status of the server will be changed to Stopping. After the job execution stops the server will be marked as Timed Out.
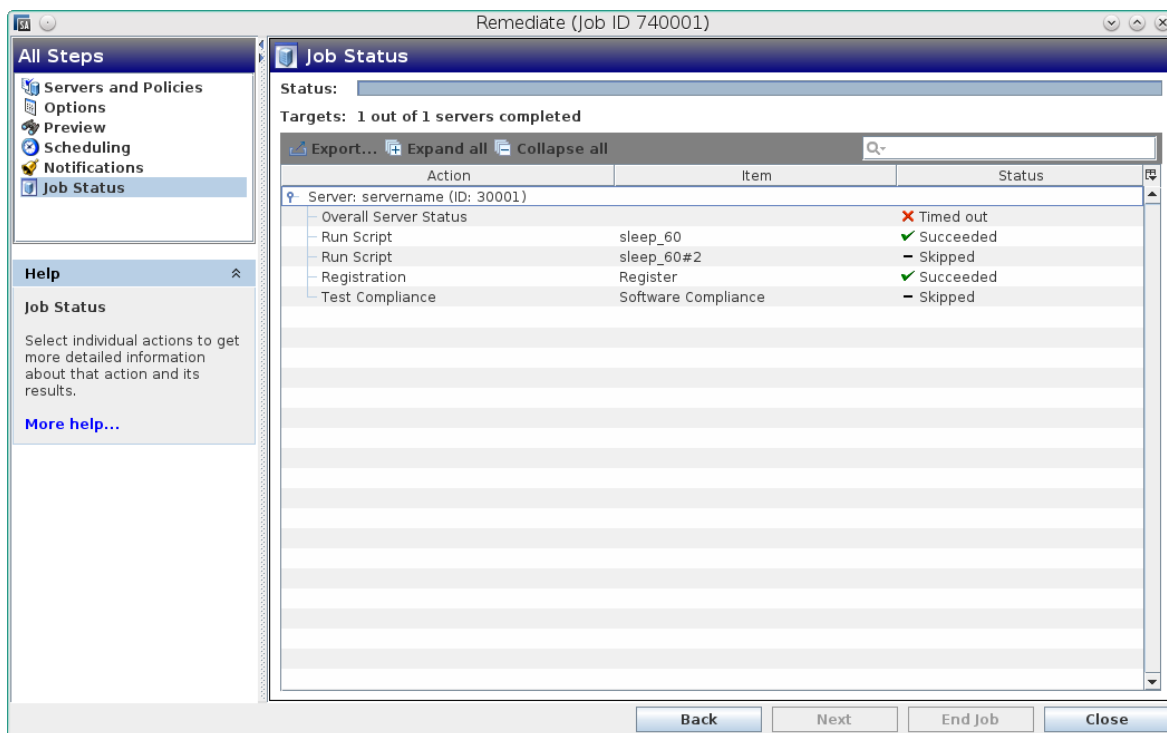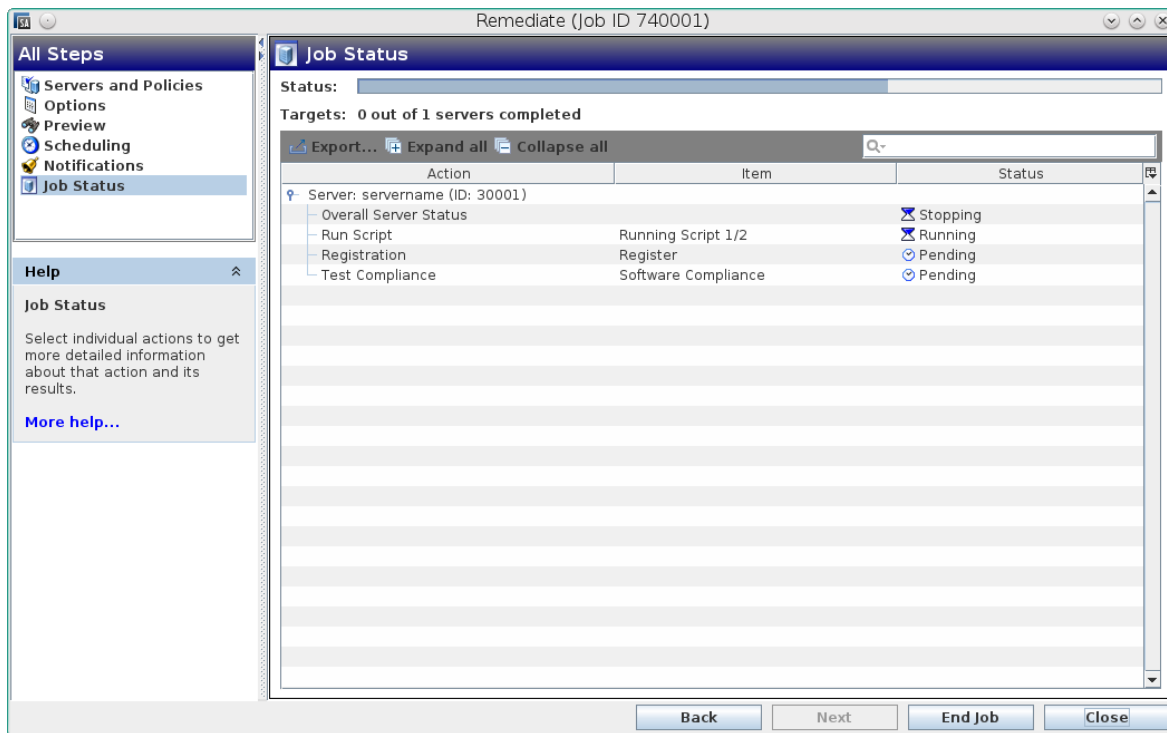
Communication problems between the agent and the core

An SA core considers a job as timed out, if communication problems prevent it from reaching the agent during job execution.

Timeouts and server reboots

When a timeout is detected during the Action phase the job prevents the server reboots requested by the packages imported into SA.

If the timeout occurs during a reboot, then after restarting, the agent will not continue with the job. This addresses the situation when servers stay offline for a long time before managing to start again.

Chapter 6 ISM Controls Reference

An Intelligent Software Module (ISM) is an installable software package created with the ISM Development Kit (IDK). An ISM can contain control scripts that perform day-to-day, application-specific tasks such as starting software servers. For example, an ISM for Apache might contain control scripts that start and stop the HTTP server. For additional information about ISM Controls in Policies, see ISM Controls in Policies.

You can run control scripts in an ISM with the SA Client. To run the control scripts in an ISM, you must first add the ISM package to a software policy and then attach the software policy to a Managed Server. See Adding Software Resources to a Software Policy and Attach a Software Policy to a Server or Device Group.

Accessing the Run ISM Control Window

Access the Run ISM Control window to run the control scripts in an ISM (Intelligent Software Module). There two ways to access the Run ISM Control window, from the server list or from the software policy:

To access the Run ISM Control window from the server list:

a From the SA Client navigation pane, access the list of managed servers or device groups:

— Select **Devices** > **Servers** > **All Managed Servers** to view the server list.

— Select **Devices** > **Device Groups** to view the device group list.

b From the content pane, select the server or device group on which you want to run the script.

c From the **Actions** menu, select **Run** >**ISM Control**. The Run ISM Control window appears.

To access the Run ISM Control window from the software policy list:

a From the SA Client navigation pane, select **Library** > **By Type** > **Software Policies**. The software policy list appears in the content pane.

b From the content pane, select a software policy that specifies an ISM.

c From the **View** drop-down list, select **Server Usage**. A list of the servers attached to this policy appears in the lower pain. Select a server, and then select **ISM Control** from the **Actions** menu. The Run ISM Control window appears.

Running ISM Controls

Use the Run ISM Control window (The Run ISM Control Window in the SA Client) to specify the ISM Control job options, run the job, and view the job status. The navigation pane in the Run ISM Control window walks you through the following steps:

- Step 1: Select Managed Servers
- Step 2: Specify Control Parameters
- Step 3: Schedule ISM Control Script Execution

- Step 4: Set Email Notifications

- Step 5: Run Job and View Job Status

The Run ISM Control Window in the SA Client
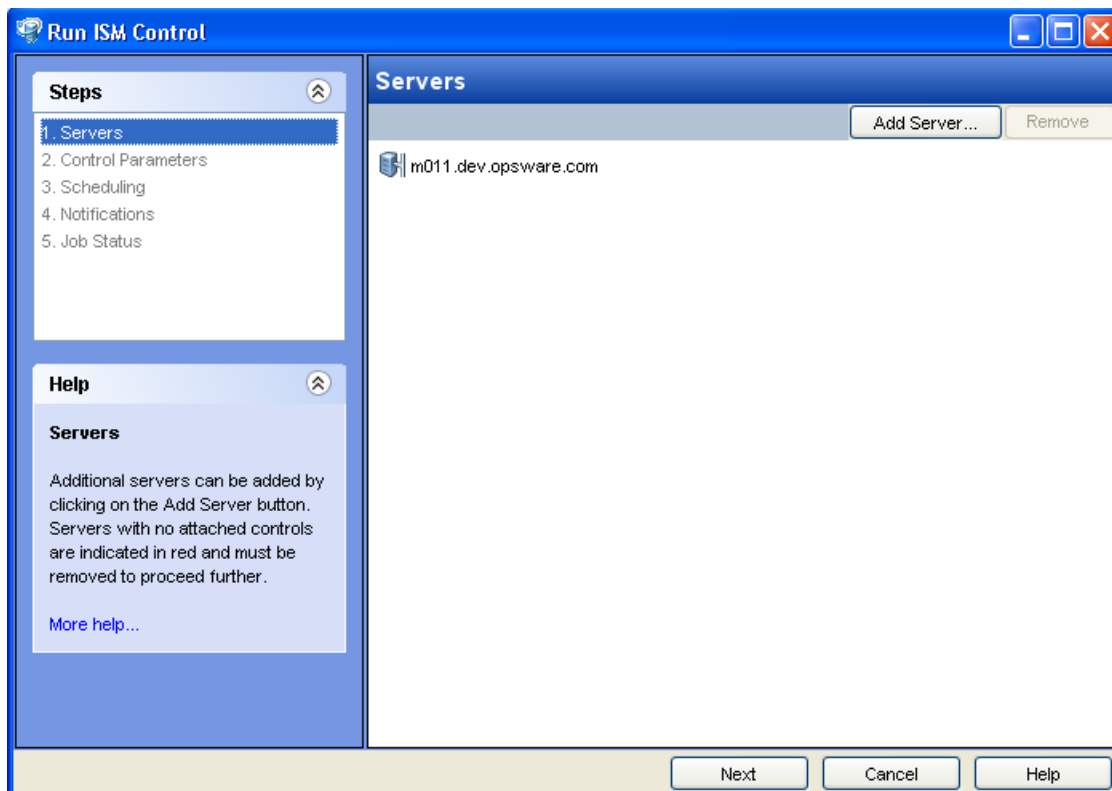
Step 1: Select Managed Servers

Perform the following steps to select the managed server(s) on which to run an ISM Control script:

1 Open the Run ISM Control window from one of the methods described in Accessing the Run ISM Control Window.

2 From the All Steps navigation pane, select **Servers**. A list of managed servers is displayed.

3 Specify the server(s) on which to run this script. Servers that appear in the list are included by default.

   a To add a server to the list, click **Include Server**. Navigate the list of managed servers or device groups. Select the device you want to add and click **Select**.The added devices will appear in the list of servers in the content pane.

   b To remove a server from the list, select it and click **Exclude**.

4 Click **Next** to proceed to the Control Parameters step.

Step 2: Specify Control Parameters

Perform the following steps to specify the control parameters:

1 From the **Software Policy** drop-down list, select an ISM package.

2 From the **Control Script** drop-down list, select a control script. The drop-down list contains only the control scripts assigned to the ISM package selected in the previous step.

3 In the **Parameters** section, the name of a parameter matches the name of its corresponding custom attribute name. The value of a custom attribute determines the value of the parameter.

4 Click **Next** to proceed to the Scheduling setup.

Step 3: Schedule ISM Control Script Execution

Perform the following steps to schedule an ISM Control script to be run immediately or at a specified date and time:

1 Select one of the following options:

 • To run the ISM control script immediately, select **Run Task Immediately**.

 • To specify a later date and time to run the ISM control script, select **Run Task At:** and enter the desired date and time.

2 Click **Next** to proceed to the Notifications step.

Step 4: Set Email Notifications

Set email notifications to alert users on the success or failure of ISM control script. You can associate a Ticket ID with the ISM Control script job.

Perform the following steps to set email notifications:

1 To add email addresses, click **Add Notifier** and enter the email addresses in the **Notification Email Address** field.

2 To trigger the notification on the success of a job, select the [✔] icon.

 To trigger the notification on the failure of a job, select the [✘] icon.

3 Enter a unique text string to be identify the job in the **Ticket ID** field.

4 Click **Next** to go to the **Job Status** display.

Step 5: Run Job and View Job Status

View summary information about the progress of the ISM Control script job and the status of each action required for the job to be completed:

1 Click Start Job to run the ISM Control Script.

 a If you selected **Run Task Immediately** in the Scheduling setup, the job begins immediately. The Job Status appears.

 b If you scheduled the job for a later time, the job will run at the scheduled time.

2　To view the details of each action from the Job Status window, select a row in the table. The details for each action will appear.

3　Click **End Job** to stop the Job or click **close** to close the Run ISM Control window.

> **Note:** You can also view all your jobs in theSA Client job logs. See the *SA User Guide: Server Automation* for information about job logs.

ISM Controls in Policies

An Intelligent Software Module (ISM) is an installable software package created with the ISM Development Kit (IDK). An ISM can contain control scripts that perform day-to-day, application-specific tasks such as starting software servers. For example, an ISM for Apache might contain control scripts that start and stop the HTTP server.

You can create a control script with a text editor, package the script into an ISM, and then upload the ISM to SA using the ISM tool in the IDK. See the *SA Content Utilities Guide* for more information about the ISM Development Kit (IDK) and ISM control scripts.

The ISM appears in the SA Library as a package. You can add the ISM package to a policy and then attach the policy to managed servers. See Adding Software Resources to a Software Policy for information about adding software packages to policies.

You can run the control scripts in the ISM from the SA Client. An ISM control script can have parameters corresponding to custom attributes. See ISM Controls Reference for more information about running ISM controls.

The name of a parameter matches the name of its corresponding . The value of a custom attribute determines the value of the parameter. The source of a custom attribute is an SA object, such as a facility, customer, server, group of servers, or software policy. Custom attributes with the same name (but with different values) can be specified on different SA objects. If a server is associated with objects that have identically named custom attributes, SA uses a predefined search order to determine the custom attribute that provides the parameter value. In the Run ISM Control window of the SA Client, you can view the name and value of the control parameter. See the *SA Content Utilities Guide* for more information on the search order for custom attributes.

Chapter 7 **Package Type Reference**

This appendix describes the SA supported software packages, including:

- Supported Operating Systems and Package Types
- LPP Packages
- HP-UX Packages
- RPM Packages
- Solaris Packages (prior to Solaris 11)
- Solaris 11 Packages
- Ubuntu Packages
- Windows Packages
- ZIP Packages
- Windows Performance for Uploading Packages
- Character Encoding for Package Metadata and Scripts

Supported Operating Systems and Package Types

SA supports these package types on the supported operating systems, as shown in Supported Operating Systems and Package Types.

Table: Supported Operating Systems and Package Types

Operating System	Package Type	File Formats	Additional Metadata
AIX	LPP (contains an update fileset or base filesets)	.bff, .I, .U, .lpp	N/A
	RPM	.rpm	N/A
	ZIP	.zip	N/A
	Application Install-ation Media	.zip	N/A
	Executable	.sh	N/A
HP-UX	Depot (contains products and file-sets)	.tar, .depot	N/A

Operating System	Package Type	File Formats	Additional Metadata
	ZIP	.zip	N/A
	Application Install-ation Media	.zip	N/A
	Executable	.sh	N/A
Linux	RPM	.rpm	N/A
	ZIP	.zip	N/A
	Application Install-ation Media	.zip	N/A
	Executable	.sh	N/A
Solaris	Patch	.jar, .tar, tar.gz, .tar.Z, t.gz, .zip	N/A
	Patch Cluster (con-tains patches)	.tar, .tar.gz, tar.Z, .tgz, .zip	N/A
	Solaris package (con-tains package instances)	.pkg, .tar	N/A
	Solaris IPS package	.p5p	N/A
	RPM	.rpm	N/A
	ZIP	.zip	N/A
	Application Install-ation Media	.zip	N/A
	Executable	.sh	N/A
Ubuntu	Debian packages	.deb	N/A
	ZIP	.zip	N/A
Windows	Hotfix	.exe	N/A
	Security Patch	.exe	N/A
	MSI	.msi	N/A
	OS Service Pack	.exe	Service Pack Level
	Windows Utility	.exe	N/A

Operating System	Package Type	File Formats	Additional Metadata
	(Microsoft Security Baseline Analyzer and qchain)		
	Microsoft Patch Database (contains a description of available patches) See "Patch Management for Windows" in the *SA User Guide: Server Patching* for more information.	.xml, .cab	N/A
	ZIP	.zip	N/A
	Application Installation Media	.zip	N/A
	Executable	.exe, .sh	N/A
OS Independent	Unknown	All	N/A

* For certain package types, SA requires that you provide additional metadata for the package.

LPP Packages

LPPs are the container packages for AIX. LPPs have the following characteristics:

- An LPP contains either one or more base filesets or an update fileset.

- When an LPP contains multiple filesets, frequently only a subset of those filesets is installed because users might want to install only certain filesets.

The basic unit of AIX packages is the fileset. Filesets have the following characteristics:

- Filesets are versioned.

- The two types of filesets are base and update.

- Users add filesets to policies. Therefore, SA adds filesets to and removes filesets from servers through remediation.

Filesets are delivered as part of an LPP file, which users upload to the Software Repository. SA automatically creates package entries for all the filesets that the LPPs contain. When viewing an LPP in the SA Client, users see which filesets it contains.

The Agent reports which filesets and Authorized Program Analysis Reports (APARs) are installed on servers because servers only report filesets and APARs (and cannot report LPPs). The SA Client shows filesets and APARs in the Installed Packages list for a server.

LPP Metadata

SA uses the metadata contained in LPPs when creating the package entries in the list of packages. An LPP contains the following metadata:

- The name of the LPP

- The name, version, and description of each fileset in the LPP

- For an updated fileset, a list of APARs addressed by the fileset

- For each APAR listed, the list of filesets that make up that APAR

> **Note:** SA does not support bundles (which are abstract sets of filesets, drawn from multiple LPPs) or Program Temporary Fix (PTFs), which are similar to APARs without the metadata. However, users can still model a bundle or PTF by creating a policy and attaching the filesets included in the bundle or PTF to that software policy.

When a user uploads an LPP, SA performs the following actions:

- Opens the LPP and parses its metadata.

- Automatically creates entries in the list of packages for the filesets in the LPP and registers them as installable.

- Automatically creates entries in the list of packages for the APARs defined by the update filesets in the LPP (if any).

- Registers the LPP as a non-installable package.

HP-UX Packages

Depots are the container packages for HP-UX. Depots have the following characteristics:

- A depot either contains products that contain filesets, or it contains patch products that contain patch filesets.

- When a depot contains multiple products and filesets, frequently only a subset is installed because users might want to install only certain products or filesets.

- A depot is a special type of directory formatted for use by HP Software Distributor (SD-UX) commands. SD-UX, a software management system, is the distribution mechanism for all HP software for HP-UX.

- A depot can be a local directory, a CD-ROM, tape, or it can reside on a server on the network.

- Multiple depots can be created for different applications or purposes.

- Users upload depots to the Software Repository in TAR format.

- When the software in a depot is compatible with multiple versions of HP-UX, upload the depot to the Software Repository for all appropriate versions.

- Depots cannot be differentiated by a hardware platform, such as s700 or s800.

- HP-UX depots have two basic formats:

  — **Directory**: The format for depots saved on a server or CD-ROM.

  — **Tape**: The format for standalone depot files and the format required for uploading HP-UX packages into SA.

Products and filesets are the installable packages for HP-UX. They have the following characteristics:

- Products and filesets are versioned.

- Filesets are the smallest installable unit. A fileset can belong to only one product, but can be included in multiple subproducts or bundles.

- Subproducts are logically related filesets and are not versioned; for example, X11.Manuals.

- Products are supersets of filesets.

- Bundles are logical groups of filesets; for example, HP-UX Support Tools Bundle.

- SA supports products, filesets, and patch products as installable software.

Note: SA does not support bundles (which are abstract sets of filesets, drawn from depots) or subproducts by automatically creating policies for bundles and subproducts when users upload depots. However, users can still model bundles and subproducts by creating policies for them and attaching the filesets for the bundles and subproducts. SA does not support using HP-UX code words.

When a user uploads a depot, SA performs the following actions:

- Opens the depot and parses its metadata.

- Automatically creates entries in the list of packages for the products and filesets in the depot and registers them as installable.

- Registers the depot as a non-installable package.

Requirement: If a depot contains different software for specific versions of HP-UX, create OS-specific depots for each HP-UX version and upload the depots to the Software Repository. The SA Client does not check the OS compatibility of the products and filesets in a depot when a user uploads the depot. When adding products or filesets to a software policy, the products and filesets can be added only when the associated OS of their depot matches the OS specified for the software policy.

The format of HP-UX version information can be inconsistent, making it difficult to determine whether one version is older than another when installing a package that has another version already installed. SA attempts to install it anyway. An error results if a newer version is already installed.

Note: SA does not provide alternate root support for HP-UX. Do not include commands that require alternate root support in the Install Flags text box of the Packages: Properties page.

> By default, the HP-UX `swinstall` command does not replace a newer version of a fileset or product with an older version. However, SA does overwrite newer versions of filesets and products with older versions. SA does not support relocating packages for HP-UX.

Depot Metadata

SA uses the metadata contained in depots when creating the package entries in the list of packages. A depot contains the following metadata:

- The name, version, and description of each product in the depot
- The list of filesets in each product in the depot
- The name, version, and description of each fileset in the depot

Preparing for HP-UX Package Management

Before you upload a depot to the Software Repository, perform the following tasks:

1 Convert the depot on the installation media (CD-ROM) from directory format to tape format by using the `swpackage` command:

```
swpackage -x media_type=tape -s <directory depot> <software
selection> @ <file depot>
```

2 Split the depot into depots for each product.

> **Tip:** For more information on creating a script to automate this step, see Example: File – Script to Split a Depot by Product and Example: File – Script to Split a Depot by Bundle.

Example: Commands – Converting a Depot

The following example shows the commands used to create a Quality Pack file depot from the Support Plus CD-ROM for HP-UX 11.00:

1 Mount the directory on the CD-ROM that contains the Quality Pack file depot:

```
mount -F cdfs /dev/dsk/c2t1d0 /cdrom
```

2 Convert the depot on the CD-ROM from directory format to tape format by using the swpackage command:

```
swpackage -x media_type=tape -s /cdrom/QPK1100 QPK1100 @ \
 /var/tmp/QPK1100.depot
```

Entering this command copies the QPK1100 bundle contained in the depot to a file that can be uploaded into SA.

Example: File – Script to Split a Depot by Product

```
# This is an example script that splits a depot into individual
# product depots that can then be uploaded to the HP
# Software Repository
```

```
for product in `swlist -l product -s <location of depot> | \
cut -f1 | grep -v ^# | grep '[A-z]'`
do
swpackage -x media_type=tape -s <location of depot> $product \
@ /var/tmp/$product.depot
done
```

Example: File – Script to Split a Depot by Bundle

```
# This splits a depot into individual bundle depots that can
# then be uploaded to the HP Software Repository

for bundle in `swlist -l bundle -s <location of depot> | \
cut -f1 | grep -v ^# | grep '[A-z]'`
do
swpackage -x media_type=tape -s <location of depot> $bundle \
@ /var/tmp/$bundle.depot
done
```

RPM Packages

Linux packages are RPMs, which have the following characteristics:

- RPMs are both uploaded and installed as a unit so there is no distinction between container and installable packages.

- RPMs are versioned.

RPM Metadata

SA uses the metadata contained in RPMs when creating the package entries in the list of packages. An RPM contains the following metadata - the name, epoch, version, architecture and release of the RPM.

When a user uploads an RPM, SA performs the following actions:

- Opens the RPM and parses its metadata.

- Registers the RPM as an installable package.

When you upload a Linux RPM package to SA, the policies related to that RPM may be updated. See Setting Installation and Update Options for a RPM for more information.

Solaris Packages (prior to Solaris 11)

Note: See also Solaris 11 Packages.

Solaris packages are the container packages for Solaris. Solaris packages have the following characteristics:

- A Solaris package contains one or more package instances.

- When a Solaris package contains multiple instances, frequently only a subset of those instances will be installed because users might want to install only certain instances.

- Solaris packages have two basic formats:

  — **File system format**: The format for packages stored in a directory structure.

  — **Data stream format**: The format for standalone package files. This format is required for uploading Solaris packages into SA.

The basic unit of Solaris packages is the package instance. Package instances have the following characteristics:

- Package instances are versioned.

- Platform assignment of Solaris packages is immutable.

- Users add package instances to a software policy. SA adds package instances to and removes package instances from servers by using the remediate function. See Remediating and Installing Software for more information about remediate.

In the SA Client, you can upload, view, download, and delete Solaris packages, and you can view, deprecate, and attach instances to policies.

SA supports Solaris packages in the following ways:

- Users upload Solaris packages in the uncompressed data stream file format.

- SA can install interactive and non-interactive Solaris package instances. Interactive Solaris package instances require response files.

- SA displays the name and version number for Solaris packages in the following way:

  ```
  SUNW125f-1.0,REV=2001.03.21.17.00
  SUNW1394h-11.9.0,REV=2002.04.06.15.27
  ```

- The Solaris utilities (such as `pkgadd`) use an admin file. The admin file stores settings regarding how the utilities should work. Each Agent on managed servers includes its own admin file that it uses when installing Solaris package instances. The admin file that the Agent uses is only used by SA and does not set defaults for other applications using pkgadd.

- In some instances, a Solaris package might only get partially installed. A partial installation generally occurs when a package contains an installation script (other than the checkinstall script - for example, a preinstall or postinstall script) and that script exits with a non-zero exit code during package installation. A partially installed Solaris package can be removed as if it were installed as a full package by removing it, or by overwriting it with a new package.

- For more information on `pkginfo, pkgadd, and pkgrm,` see the man pages.

Response files are text files. The entries in a response file occur as name = value pairs; for example, `BASEDIR="/opt/SUNWexplorer"` is a valid entry.

SA supports response files in the following ways:

- Users create response files outside of SA by using the `pkgask` Solaris utility.

- By using the Solaris Instance Package Properties page in the SA Client users upload and overwrite the response files that are associated with Solaris package instances.

- Each response file is accessible only in the context of the Solaris package instance to which it belongs.

- Each Solaris package instance can have zero or one response file. Response files are not shared by different Solaris package instances.

- Attaching an interactive package to a policy includes the response file because SA stores the response file with the package. You do not need to attach the response file to the software policy.

- After a Solaris package instance has a response file, SA uses that response file whenever the Solaris package instance is installed.

- If a Solaris package instance requires a response file and that file is missing in the SA Client, SA might report an error when any server is remediated with that Solaris package instance.

When a user uploads a Solaris package, SA performs the following actions:

- Opens the package and parses its metadata.

- Automatically creates entries in the list of packages for the package instances in the package and registers them as installable.

- Registers the Solaris package as uninstallable.

Solaris Metadata

SA uses the metadata contained in Solaris packages when creating the package entries in the list of packages. A Solaris package contains the following metadata - the name, version, and description of each package instance in the package.

Prerequisites to Solaris Package Management

The Solaris package must be in data stream format before you can upload it to the SA Software Repository. If it is in file system format, you can convert it by using the pkgtrans command:

```
pkgtrans -s <location of package> <new package> all
```

Solaris 11 Packages

With Solaris 11 Oracle takes a new approach to package management by introducing Image Packaging System (IPS) as a replacement of the old SVR4 packages used in previous versions. According to Oracle, IPS packages have the following characteristics:

- an IPS package is a collection of directories, files, links, drivers, dependencies, groups, users, and license information in a defined format. This collection represents the installable objects of a package.

- IPS was designed to cope with the complete life cycle of software, addressing software packaging, deployment and installation, updates, system upgrades, and removal of software packages.

- IPS is also tightly integrated with ZFS, and uses ZFS features (such as snapshots and clones) to minimize risk and downtime associated with maintenance.

- an IPS package is made up of a series of actions which are described in the manifest of a package. Actions are used for defining the files and directories of the package, setting package attributes, declaring dependencies on other packages, creating users and groups, and installing device drivers. Actions represent the installable objects on a system.

IPS Metadata

Each IPS package is represented by a Fault Management Resource Identifier (FMRI). The FMRI includes descriptive information about the package, such as the publisher of the package, package name, version information, and date.

Example for pkg: `//solaris/library/libc@5.11,5.11-0.75:20071001T163427Z`:

```
Scheme: pkg
Publisher: solaris
Category: library
Package name: libc
Version string
Component version: 5.11
   Build version: 5.11
   Branch version: 0.75
   Time the package was published, in ISO-8601 basic format:
   20071001T163427Z
```

Note: SA allows special characters (e.g. '@') in package names only for IPS packages.

Prerequisites to Solaris IPS Package Management

In order to remediate IPS packages to a managed server you need to have the package dependencies available in SA.

Ubuntu Packages

Ubuntu natively supports *Debian* packages, which usually have a filename ending in .deb and contain the files needed to implement a set of related commands or features.

There are two types of Debian packages: *binary* and *source* packages.

- *Binary packages* contain executable files, configuration files, man/info pages, copyright information and other documentation. The binary packages are directly used by *dpkg* during .deb package installation.

- *Source packages* contain the source code as well as the instructions for building binary packages. Source packages are not installable; they are just unpacked in whatever directory you want to build the binary packages they produce.

SA exclusively uses *Debian binary packages*, which have the following characteristics:

- They conform to the following naming convention:

```
<PackageName>_<VersionNumber>-<DebianRevisionNumber>_
<DebianArchitecture>.deb
```

> **Note:** By convention, the .deb package names should be lowercase. When a package that does not conform to the naming convention is uploaded to SA, the package name is converted to respect the convention. The original file name will still be displayed in the SA Client, however. This difference has no impact on the compliance.

- They have the following structure:

```
debian-binary
control.tar.gz
data.tar.gz
```

Where:

— *debian-binary* - This is a text file which simply indicates the version of the .deb file used.

— *control.tar.gz* - This archive file contains all of the available meta-information, such as the name and version of the package. Some of this meta-information is used by the package management tools during package operations. For example, it may be used to determine if it is possible to install or uninstall the package according to the list of packages already on the machine. Usually, this archive contains a control file, the manifest of the .deb package, and some executable scripts (*preinst*, *postinst*, *prerm* and *postrm*) that are automatically run before or after a package is installed.

> **Note:** SA will not honor the reboot requests in the *preinst*, *postinst*, *prerm* and *postrm* scripts. By default, when a DEB package is imported to SA, the "Reboot Required" option is set to *No*. If the Reboot Required option is enabled in the installation/remediation job, the system will be rebooted as requested.

— *data.tar.gz* - This archive contains all of the files to be extracted from the package; this is where the executable files, documentation, etc., are all stored.

> **Note:** By default, if you want to install package A on your Ubuntu system and this package recommends package B, if package B is available, it will be installed as side-effect. However, because package B is not an explicit dependency, it will not be uninstalled when package A is uninstalled. This behavior is due to the Ubuntu native tools.

Debian Metadata

The package metadata is available in the *control.tar.gz* archive file, described in Ubuntu Packages.

Windows Packages

SA supports the following Windows packages:

- Microsoft Installer Packages
- Microsoft Hotfixes, Security Patches, and Service Packs

Microsoft Installer Packages

Microsoft Installer packages (MSI) have the following characteristics:

- They contain all the information that the Microsoft Installer requires to install an application or product.
- They contain information that the installer requires to run the setup user interface.

MSI packages contain:

- An installation database
- A summary information stream
- Data streams for various parts of the installation

SA supports .msi files as installable software.

MSI Package Metadata

SA catalogs each MSI package by its ProductName and ProductVersion. These properties are defined in the Properties table of the MSI installation database.

Prerequisites to MSI Package Management

SA supports Microsoft Windows Installer, which is included with most versions of Windows. Windows NT does not include a version of the Windows Installer, but the Microsoft Windows redistributable can be obtained for download at http://www.microsoft.com or by including the --withmsi option on the Agent Installer command line.

See the *SA User Guide: Server Automation* for more information about the steps to install an Agent on a server.

Microsoft Hotfixes, Security Patches, and Service Packs

These packages include:

- Hotfixes
- Service Packs
- Security Patches

Hotfixes are issue-specific and should only be applied if you experience the exact issue addressed by the hotfix, and only if you are using the current operating system version that has had the latest service pack applied.

Service packs are groups of hotfixes. They are more thoroughly tested than individually released hotfixes, and are available to all customers, not just those with the specific problem.

Security patches are similar to hotfixes, but are mandatory if you are experiencing the specific problem they are created to address, and they need to be deployed as soon as they are made available.

When you upload a Service Pack, SA requires the user to provide the version of the service pack. When you upload Hotfixes and Security Patches, SA requires the user to provide the operating system version and the patch type.

ZIP Packages

ZIP Package Support

The SA Client adds support for ZIP packages on the following platform families:

- Windows
- Unix

ZIP Packaging

When you install a ZIP package on a server, the files are automatically extracted and saved to a directory that you select; otherwise, a default directory is used. SA keeps track of all ZIP packages that it has installed, which prevents you from installing a ZIP package with the same name twice.

A ZIP package has no limits or restrictions on the size, format, or number of files that it contains.

SA supports ZIP encapsulation for application package files that were built using other stan-dalone installation programs, for example, InstallShield.

SA requires silent install operation for programs designed for interactive installation. When you package these program files to upload to SA, use the silent install options to play back automatic responses to provide unattended installation.

Info-Zip Compatible ZIP Packages

SA offers package management support for Info-Zip compatible ZIP packages. The files that are archived within Info-Zip are installable in SA. You can download this package creation tool from www.info-zip.org.

Info-Zip Compatible Package Metadata

SA uses the ZIP package file name to uniquely identify a ZIP package.

Prerequisites of Info-Zip Compatible Package Management

Full support for managing ZIP packages on a server is included with the Windows SA Agent.

Windows Performance for Uploading Packages

When you upload packages from a Windows computer, users can improve the performance of the computer used to upload by changing TCP stack registry settings that affect upload speeds. The recommended change to the Windows registry file increases the default tcp-send buffer size from 8 KB to 16 KB.

> **Requirement:** Consult your system administrator before you make this change.

Perform the following steps to change the tcp-send buffer setting:

1   Using regedit, navigate to the following registry key:

```
HKEY_LOCAL_MACHINE
 SYSTEM
 CurrentControlSet
 Services
 Afd
 Parameters (Create this key if it does not already exist)
```

2   Set the following value for the key:

```
Name: DefaultSendWindow
Value Type: REG_DWORD
Value: 16384 (decimal)
```

After you set the value, reboot the machine for the changes to take effect.

Character Encoding for Package Metadata and Scripts

In SA, you can specify the character encoding for package metadata and scripts in the following ways:

• Specify the encoding for package metadata when uploading packages in the SA Client or by using the SA Command Line Interface 1.0 (OCLI 1.0). For information on OCLI 1.0, see the SA User Guide: Server Automation.

When the encoding is specified, the SA Web Client correctly displays in non-ASCII any package metadata, description fields, and error and status message returned by the operating system of the managed servers.

• Specify the encoding for scripts when uploading them in the SA Web Client (in the Run Distributed Script Wizard and Scripts channel).

SA converts the script contents from the UTF-8 encoding to the encoding that you select. Internally, SA stores the script in the UTF-8 encoding.

After a script runs, you can download a ZIP file that contains the results encoded in UTF-8 format. For example, on Unix you can use the `iconv` program to interpret the downloaded results of the script execution.

The SA Client includes the following selections for character encodings:

• Arabic (ISO-8859-6)

• Baltic (Cp1257)

• Baltic (ISO-8859-13)

• Baltic (ISO-8859-4)

• Central European (Cp1250)

• Central European (ISO-8859-2)

- Chinese Hong Kong, Taiwan (Cp950)
- Chinese Simplified (EUC-CN)
- Chinese Simplified (GB18030)
- Chinese Simplified (GBK)
- Chinese Traditional (Big5)
- Chinese Traditional (Big5-HKSCS)
- Chinese Traditional (EUC-TW)
- Cyrillic (Cp1251)
- Cyrillic (ISO-8859-5)
- Cyrillic (KOI8-R)
- English (US-ASCII)
- Greek (Cp1253)
- Greek (ISO-8859-7)
- Hebrew (Cp1255)
- Hebrew Visual (ISO-8859-8)
- Japanese (EUC-JP)
- Japanese (ISO-2022-JP)
- Japanese (Shift_JIS)
- Korean (Cp949)
- Korean (EUC-KR)
- Korean (JOHAB)
- South European (ISO-8859-3)
- Thai (TIS-620)
- Turkish (Cp1254)
- Turkish (ISO-8859-9)
- Unicode (UTF-8)
- Vietnamese (Cp1258)
- Western (Cp1252)
- Western (ISO-8859-1)
- Western (ISO-8859-15)

Chapter 7: Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

Feedback on SA User Guide: Software Management (Server Automation 10.22)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to hpe_sa_docs@hpe.com.

We appreciate your feedback!