HP Server Automation

for the HP-UX, IBM AIX, Red Hat Enterprise Linux, Solaris, SUSE Linux Enterprise Server, VMware, and Windows® operating systems

Software Version: 9.10

User Guide: Software Management

Document Release Date: June 2011
Software Release Date: June 2011

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 Notices

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

Intel® and Itanium® are trademarks of Intel Corporation in the U.S. and other countries.

Microsoft®, Windows®, Windows® XP are U.S. registered trademarks of Microsoft Corporation.

Oracle and Java are registered trademarks of Oracle and/or its affiliates.

UNIX® is a registered trademark of The Open Group.

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://support.openview.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:

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

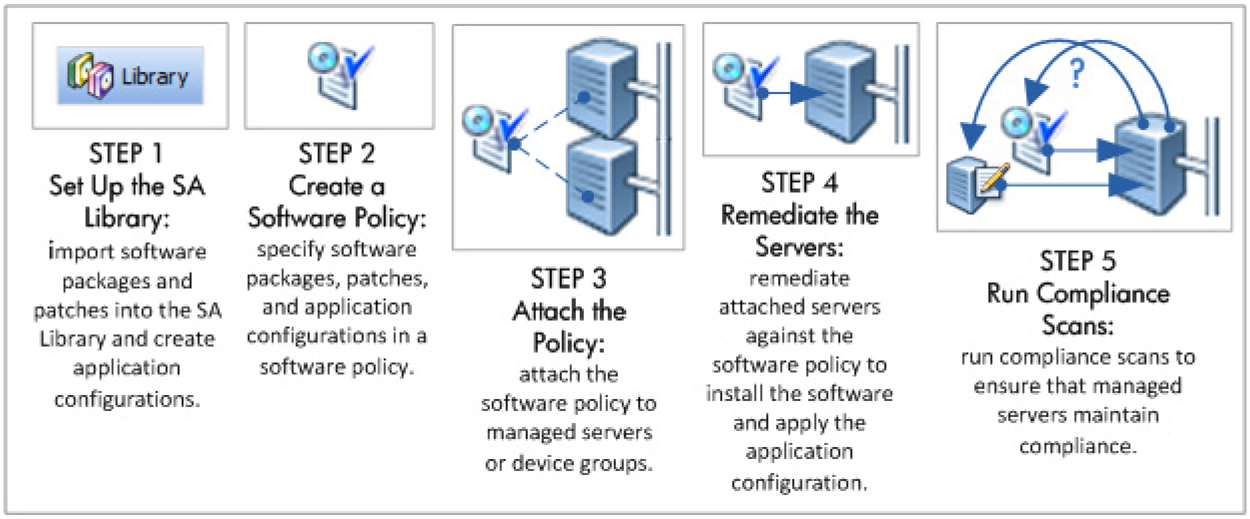
Contents

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 Figure 1. (See About Policy-based Software Installation and Management on page 12 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 on page 19.
- **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 Policies on page 13 and About Attaching Software Policies to Servers or Device Groups on page 17.
- 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 on page 17.
- **SA compliance scans** ensure that managed servers maintain compliance with their attached software policies and application configurations. See About Software Policy Compliance on page 18 and About Software Policy Reports on page 19.

Figure 1 The SA Software Management Process


Library
STEP 1
Set Up the SA Library:
import software packages and patches into the SA Library and create application configurations.
STEP 2
Create a Software Policy:
specify software packages, patches, and application configurations in a software policy.
STEP 3
Attach the Policy:
attach the software policy to managed servers or device groups.
STEP 4
Remediate the Servers:
remediate attached servers against the software policy to install the software and apply the application configuration.
?
STEP 5
Run Compliance Scans:
run compliance scans to ensure that managed servers maintain compliance.

➤ 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, RPMs, 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 on page 21.

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 on page 62.

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 on page 64.

   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 on page 18.

   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, RPMs, 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 Sub-policies on page 14
- Software Policy Templates on page 14
- Software Resources in a Software Policy on page 15
- Custom Attributes for Policies on page 16
- Software Policies for Patch Installation on page 16
- Software Policies for Script Execution on page 16
- ISM Controls in Policies on page 112

Embedded Software Sub-policies

Software policies that are embedded under another software policy are called sub-policies. 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 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 on page 14.

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 on page 61.

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 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 Sub-policies on page 14.

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 2000 and Windows 2003, the software resources that are applicable to Windows 2000 and Windows 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 Sub-policies on page 14.

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 on page 14.

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 Remediation on page 67 for more information about adding scripts to the remediation settings.

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 attribute 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 on page 29 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 the “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.

➤ 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 on page 62 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.

When you remediate a server or device group, SA installs the software resources (patches, packages, RPMs, scripts, server objects, and application configurations) in the attached software policy in the order specified in the policy. See Remediating Servers with Software Policies on page 64 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 Policies on page 13 for 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 on page 18 for information about performing a compliance scan from the server list. See The Compliance View on page 121 of 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 on page 64.

About Software Policy Reports

BSA Essentials (BSAE) provides both high level and detailed historical reporting on your data center's automation processes for Server Automation (SA). BSAE gives you insight through rich reporting on the cost effectiveness and return on investments (ROI) for the automated processes in your data center. BSAE also provides a window into the compliance state of your servers, devices, and business applications.

The following two SA report types are viewable in the BSA Essentials Java Client:

- **SA General Reports**

  General reports about various SA features, such as Windows Patching, Virtualization, Deployment Automation, and installed SA Server Agents.

  These reports can be downloaded from the BSA Essentials Network using the bsae_sa_reports stream.

  SA General Reports via BSAE in the *SA Reports Guide* describes these reports.

- **SA Compliance Reports**

  Reports that display the compliance state of your data center, such as overall server compliance status, overall compliance by policy, and specific compliance categories for features such as Application Configuration, Windows Patching, Audits, and Software Management.

  These reports can be downloaded from the BSA Essentials Network using the sar78_reports stream.

  SA Compliance Reports via BSAE in the *SA Reports Guide* describes these reports.

- **BSAE Custom Reports**

  See the BSAE Client Help for instructions on creating custom reports.

➤ For information on how to run and view these HP Server Automation reports available via BSA Essentials or the SA Client see Server Automation Reports or the *SA Reports Guide*.

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.

➤ 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 Chapter 3, Managing Software Packages, on page 35 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 Chapter 2, Creating and Managing Software Policies, on page 21
- 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*.

➤ 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: OS Provisioning*, and *SA User Guide: Server Automation*.

2 Creating and Managing Software Policies

The policy management tasks include:

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.

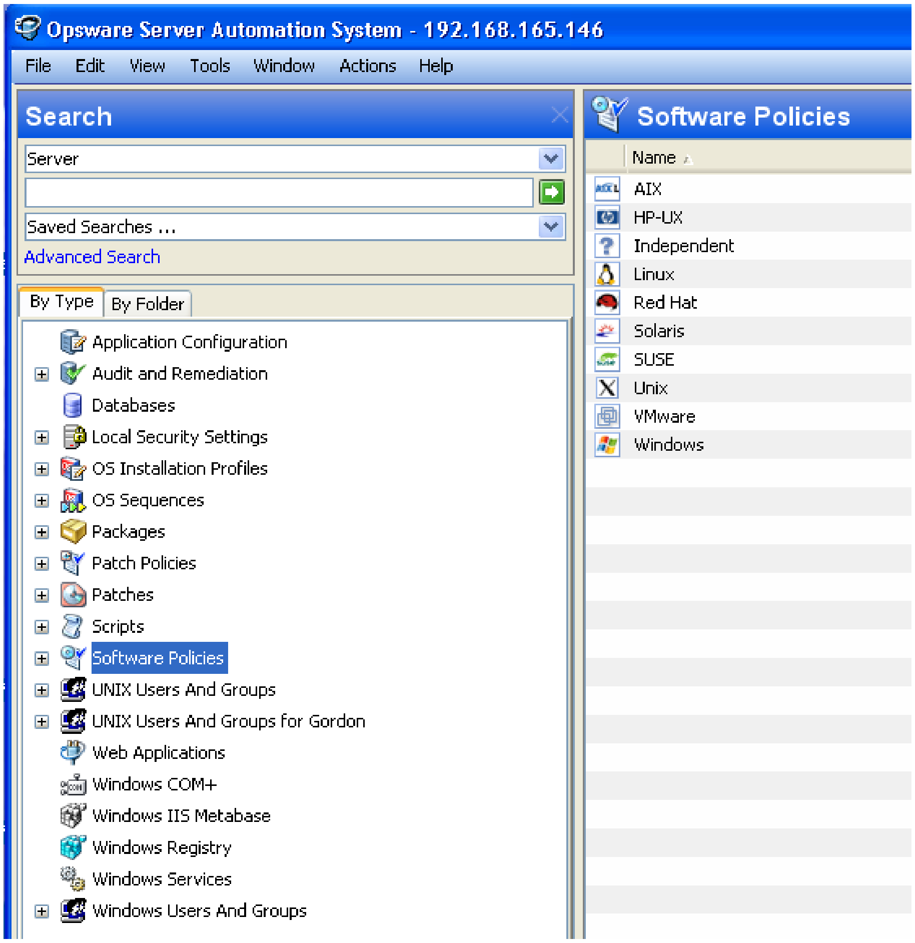
In the SA Client, you can create a policy or template in the following ways:

- Creating a Software Policy or Template from the By Type View in the Library on page 22
- Creating a Software Policy or Template from the By Folder view in the Library on page 23.

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 on page 14 for information about policy templates.
10. To save the changes, select **Save** from the **File** menu.

> 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 on page 14 for information about policy templates.
10. To save the changes, select **Save** from the **File** menu.

> 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.

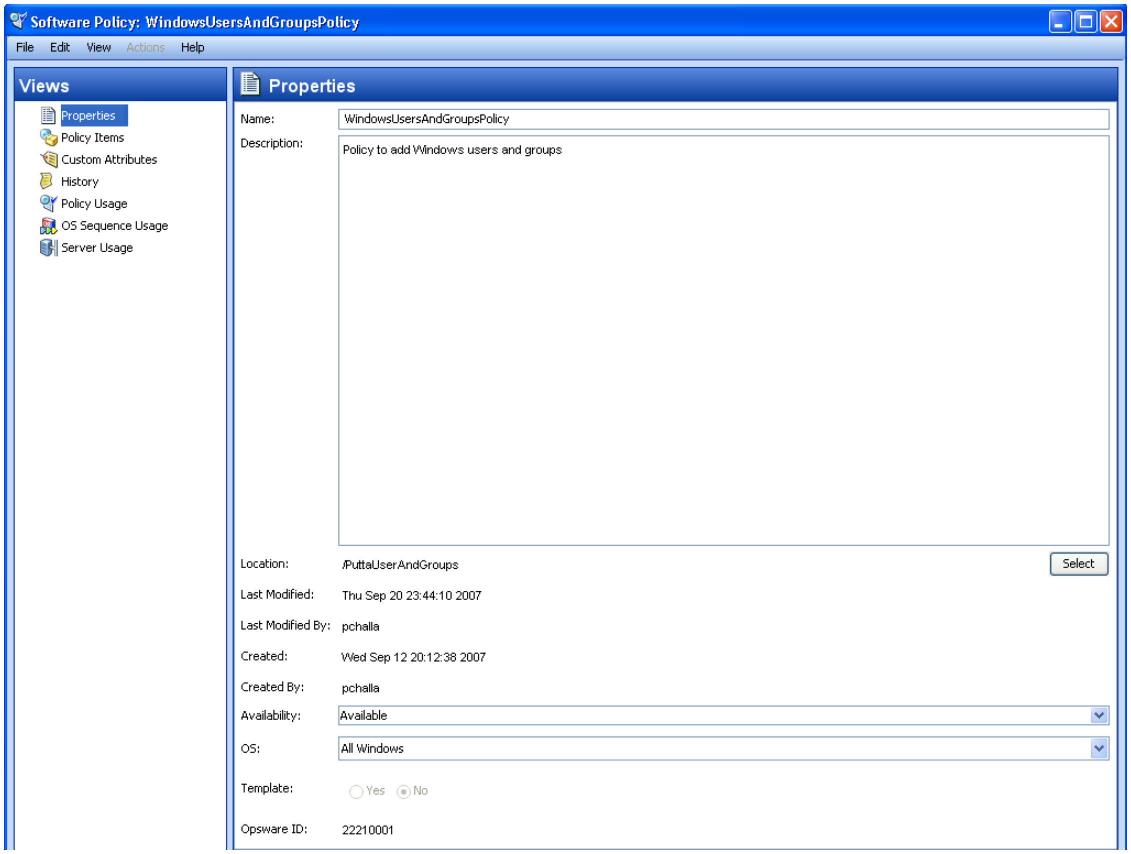
Editing Software Policy Properties

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.



Name: WindowsUsersAndGroupsPolicy

Description: Policy to add Windows users and groups

Location: /PuttaUserAndGroups

Last Modified: Thu Sep 20 23:44:10 2007

Last Modified By: pchalla

Created: Wed Sep 12 20:12:38 2007

Created By: pchalla

Availability: Available

OS: All Windows

Template: ○ Yes ● No

Opsware ID: 22210001

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 you change the operating system family of an existing software policy, you will see a dialog that shows any policy items that are no longer applicable and/ or any servers that are no longer applicable. You should remove non-applicable policy items and detach and remediate any servers that are no longer applicable to the modified policy.

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 on page 14 for information about policy templates.

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

In the SA Client, a policy is represented by the icon . A software template is represented by the 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 on page 61 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 an RPM Package on page 28 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.

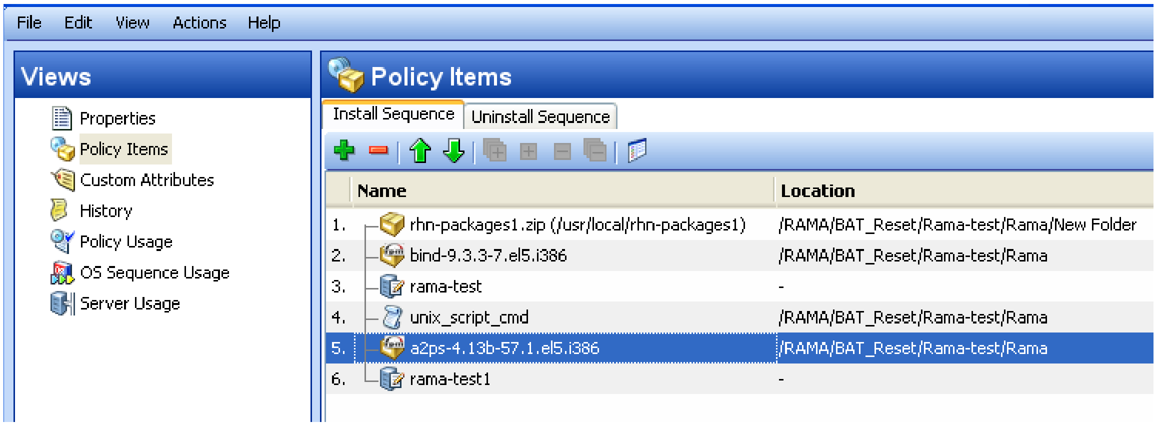
2 From the content pane, select the policy and open it. The policy window appears.

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 in Figure .
or

Select **Uninstall Sequence** to specify the uninstallation order.



	Name	Location
1.	rhn-packages1.zip (/usr/local/rhn-packages1)	/RAMA/BAT_Reset/Rama-test/Rama/New Folder
2.	bind-9.3.3-7.el5.i386	/RAMA/BAT_Reset/Rama-test/Rama
3.	rama-test	-
4.	unix_script_cmd	/RAMA/BAT_Reset/Rama-test/Rama
5.	a2ps-4.13b-57.1.el5.i386	/RAMA/BAT_Reset/Rama-test/Rama
6.	rama-test1	-

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 To save the changes, select **Save** from the **File** menu. 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 an RPM Package

Once you have added an RPM package to a software policy, you can specify if the RPM package 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.

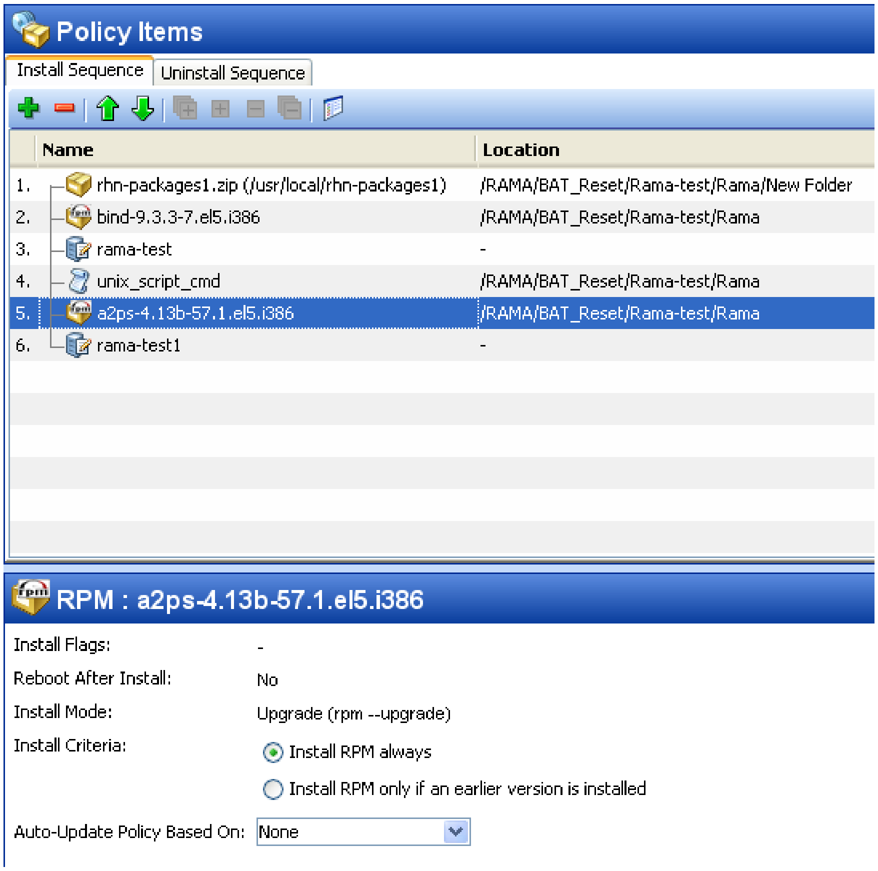
In a software policy, you can specify the installation and update options for RPM packages only if they are directly attached to the software policy.

To specify the installation options for an RPM package:

1 From the navigation pane, select **Library ➤ By Type ➤** 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 in the figure below.



	Name	Location
1.	rhn-packages1.zip (/usr/local/rhn-packages1)	/RAMA/BAT_Reset/Rama-test/Rama/New Folder
2.	bind-9.3.3-7.el5.i386	/RAMA/BAT_Reset/Rama-test/Rama
3.	rama-test	-
4.	unix_script_cmd	/RAMA/BAT_Reset/Rama-test/Rama
5.	a2ps-4.13b-57.1.el5.i386	/RAMA/BAT_Reset/Rama-test/Rama
6.	rama-test1	-

RPM : a2ps-4.13b-57.1.el5.i386

Install Flags: -

Reboot After Install: No

Install Mode: Upgrade (rpm --upgrade)

Install Criteria: ● Install RPM always

○ Install RPM only if an earlier version is installed

Auto-Update Policy Based On: None

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

- In the Install Criteria, select the option **Install RPM always** to install the RPM packages specified in the policy on the managed server.
- In the Install Criteria, select the option **Install RPM only if an earlier version is installed** to update the RPM version on the managed server to the version specified in the software policy.
- From the Auto-Update based on drop-down list, select **Version or Release** to automatically update the RPM package in the policy to a newer version or release of the RPM.

➤ SA will update the RPM package in the policy to a version or release of the RPM only if the newer release or version is placed in the same folder as the RPM package specified in the software policy.

- From the Auto-Update based on drop-down list, select **Release Only** to automatically update the RPM package in the policy to a newer release of the same version of the RPM.

➤ SA will update the RPM package in the policy to a newer release of the RPM only if the newer release of the same version is placed in the same folder as the RPM package specified in the software policy.

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

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 Policy on page 61 for 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.

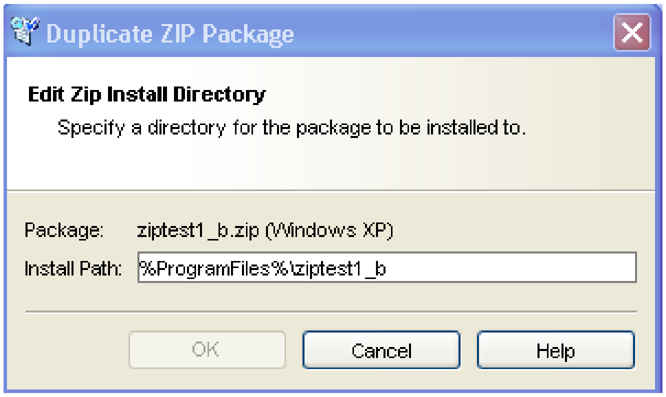
4. Click **Add**.
5. In the Name field, enter the name of the custom attribute.
6. In the Value field click ... . The Input dialog appears. Enter the value for the custom attribute.
7. To save the changes, select **Save** from the **File** menu.

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.



Edit Zip Install Directory

Specify a directory for the package to be installed to.

Package: ziptest1_b.zip (Windows XP)

Install Path: %ProgramFiles%\ziptest1_b

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:

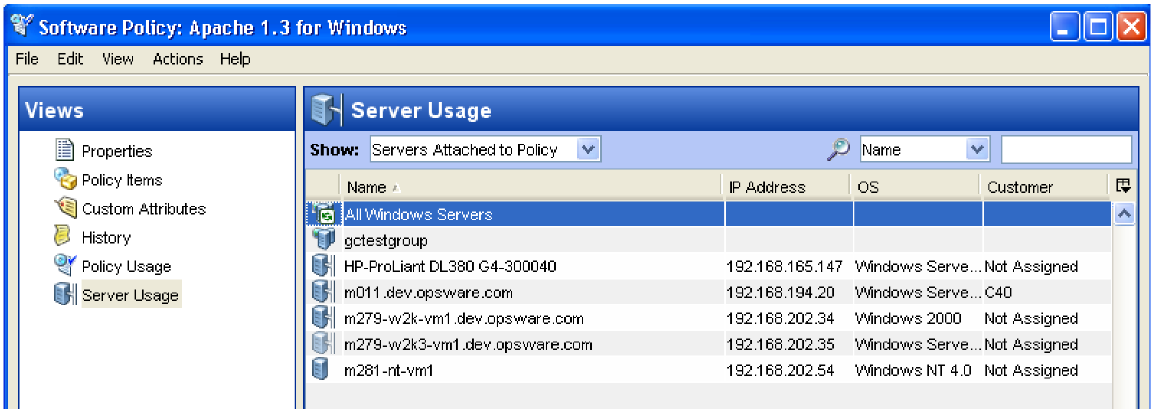
   ```
   \usr\local\[basename of zip file]
   ```

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 Figure 2.

Figure 2 Server Usage in the policy Window



Show: Servers Attached to Policy

Name

Name	IP Address	OS	Customer
All Windows Servers			
gctestgroup			
HP-ProLiant DL380 G4-300040	192.168.165.147	Windows Serve...	Not Assigned
m011.dev.opsware.com	192.168.194.20	Windows Serve...	C40
m279-w2k-vm1.dev.opsware.com	192.168.202.34	Windows 2000	Not Assigned
m279-w2k3-vm1.dev.opsware.com	192.168.202.35	Windows Serve...	Not Assigned
m281-nt-vm1	192.168.202.54	Windows NT 4.0	Not Assigned

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 Select Servers Attached to Policies from the Show drop-down list. The list of servers attached to the policy appears in the content pane.

5 (Optional) Use the Show drop-down list to display the compliance information for a server with respect to a software policy.

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.

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, 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.

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 (OCLI).

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.

➤ 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 *Server Automation 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 with a script. This topic describes importing software packages into the SA Library using the SA Client. See the *SA User Guide: Server Automation* for information about importing packages with a script using the SA Command Line Interface (OCLI). 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:

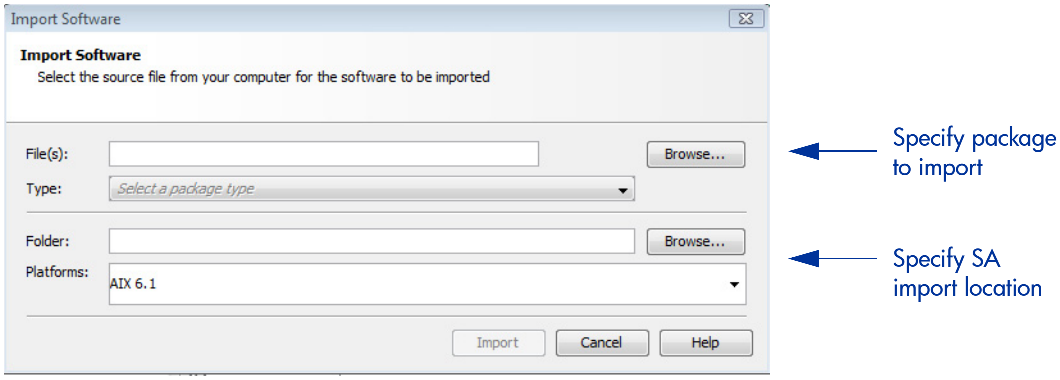
1. From the navigation pane, select **Library ➤ By Type ➤ Packages**. The packages organized by operating system appear in the content pane. Drill down to the operating system where the package should be imported.

   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 Import Software window, content pane, click **Browse** to locate the packages to import.



Import Software

Import Software

Select the source file from your computer for the software to be imported

File(s): Browse...

Type: *Select a package type*

Folder: Browse...

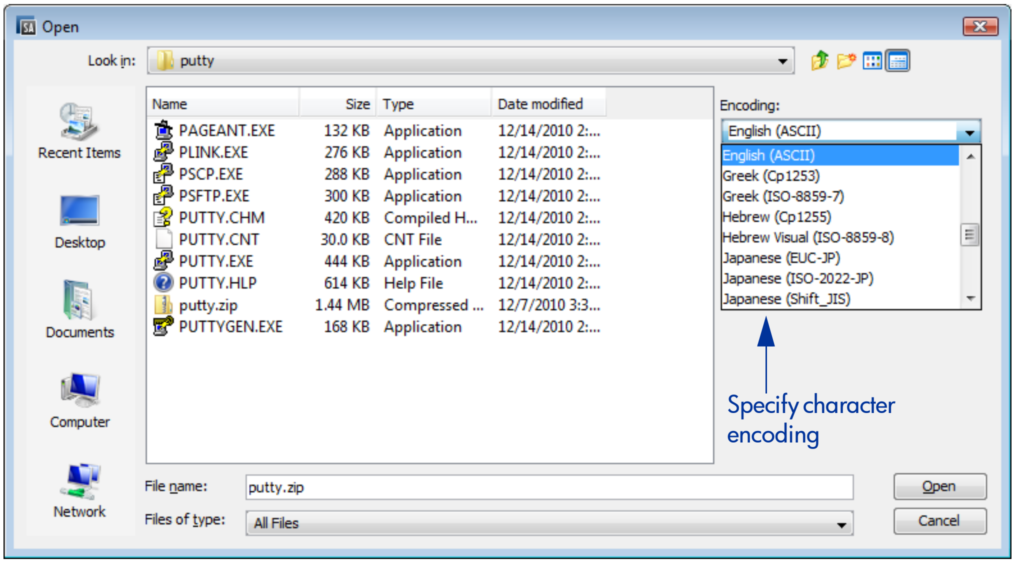
Platforms: AIX 6.1

Specify package to import

Specify SA import location

4 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.



Open

Look in: putty

Name	Size	Type	Date modified
PAGEANT.EXE	132 KB	Application	12/14/2010 2:...
PLINK.EXE	276 KB	Application	12/14/2010 2:...
PSCP.EXE	288 KB	Application	12/14/2010 2:...
PSFTP.EXE	300 KB	Application	12/14/2010 2:...
PUTTY.CHM	420 KB	Compiled H...	12/14/2010 2:...
PUTTY.CNT	30.0 KB	CNT File	12/14/2010 2:...
PUTTY.EXE	444 KB	Application	12/14/2010 2:...
PUTTY.HLP	614 KB	Help File	12/14/2010 2:...
putty.zip	1.44 MB	Compressed ...	12/7/2010 3:3...
PUTTYGEN.EXE	168 KB	Application	12/14/2010 2:...

Encoding: English (ASCII)

English (ASCII)
Greek (Cp1253)
Greek (ISO-8859-7)
Hebrew (Cp1255)
Hebrew Visual (ISO-8859-8)
Japanese (EUC-JP)
Japanese (ISO-2022-JP)
Japanese (Shift_JIS)

Specify character encoding

File name: putty.zip

Files of type: All Files

5 Select the file type from the Filetype drop-down list.

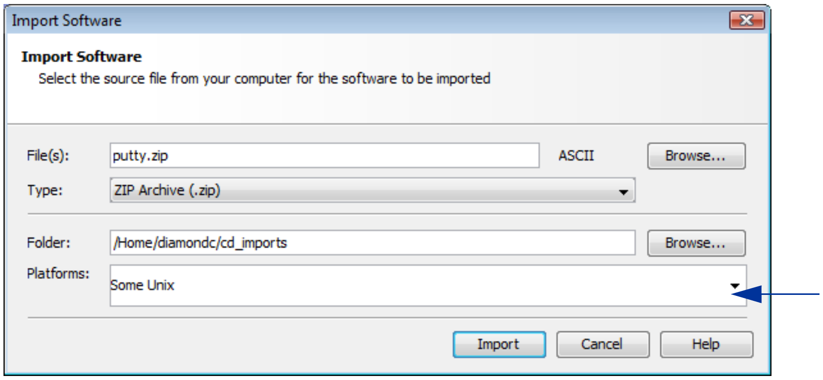
When importing multiple files, all files must be of the same type. Some of the package types include Windows MSI, ZIP, Executable, application installation media, RPM, Solaris Package.

6 Click **Open**. The Import Software window reappears.

7 Click **Browse** to specify the folder location for the packages.

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

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



Import Software

Import Software

Select the source file from your computer for the software to be imported

File(s): putty.zip

Type: ZIP Archive (.zip)

Folder: /Home/diamondc/cd_imports

Platforms: Some Unix

Specify platforms

10 Click **Import**.

You have the following options during the import process:

- **Run in Background**: Choose this option if you wish to have the process run in the background. The Import Software window will close.
- **Stop**: Click Stop to stop the import process.

11 (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.

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. See the Remediating and Installing Software on page 61 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

To import 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 Package

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

➤ Package types that are not physical files like APARs cannot be downloaded.

To download 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.

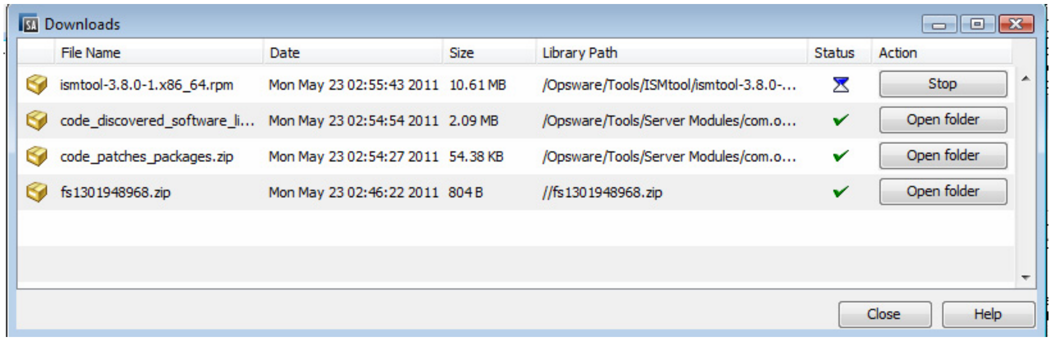
2 From the content pane, select a package to export.

3 From the **Actions** menu, select **Export Package**. 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 Downloads window displays the details and progress of the export. This window displays all the exports made within the session.



Downloads

File Name	Date	Size	Library Path	Status	Action
ismtool-3.8.0-1.x86_64.rpm	Mon May 23 02:55:43 2011	10.61 MB	/Opsware/Tools/ISMtool/ismtool-3.8.0-...	⧗	Stop
code_discovered_software_li...	Mon May 23 02:54:54 2011	2.09 MB	/Opsware/Tools/Server Modules/com.o...	✓	Open folder
code_patches_packages.zip	Mon May 23 02:54:27 2011	54.38 KB	/Opsware/Tools/Server Modules/com.o...	✓	Open folder
fs1301948968.zip	Mon May 23 02:46:22 2011	804 B	//fs1301948968.zip	✓	Open folder

Downloads window options:

- Click **Stop** if you wish to cancel an export process that is underway.
- Click **Open Folder** to open the folder where a completed export was stored locally.
- Click **Close** to close the window.
  — If you wish to open it later, select **Tools ➤ Downloads**.

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 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.

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 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.

Viewing Package Properties

To view the properties of a package:

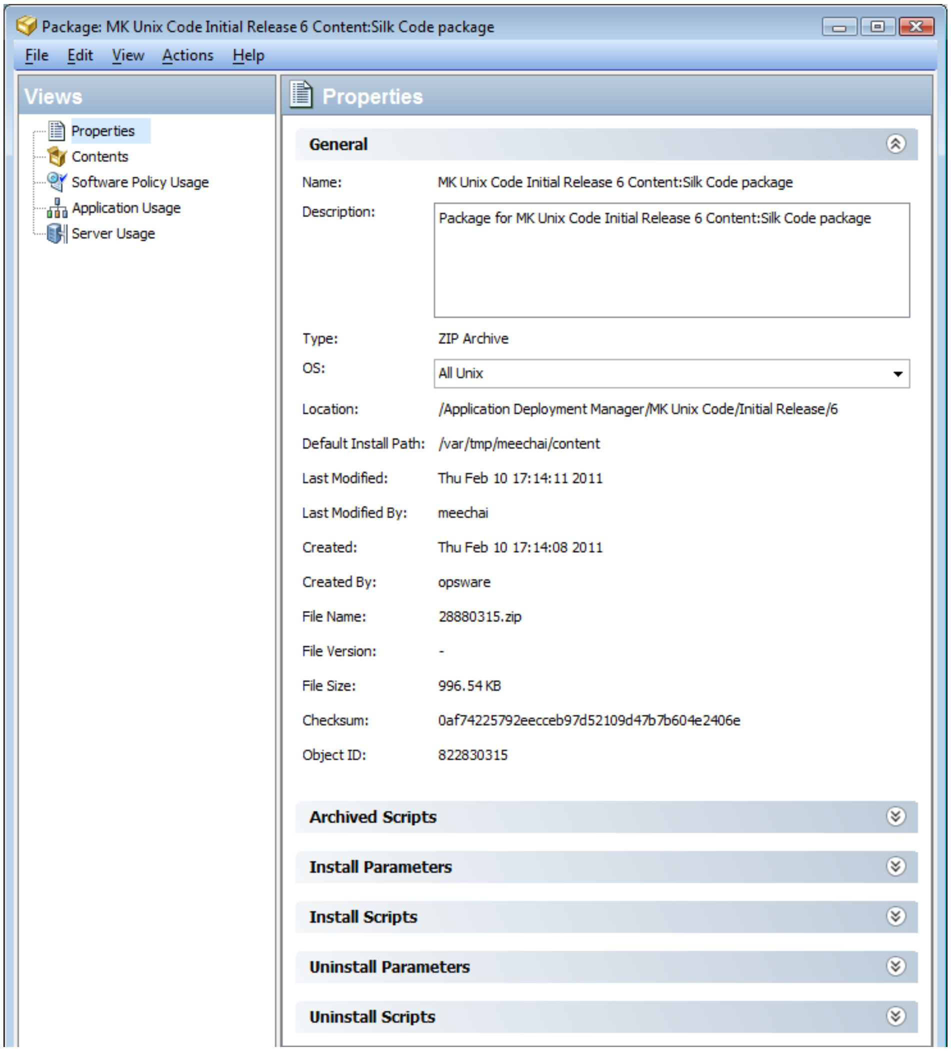
1 From the navigation pane, select **Library ➤ By Type ➤ Packages**. The packages organized by operating systems appear in the content pane.

  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.



Name: MK Unix Code Initial Release 6 Content:Silk Code package

Description: Package for MK Unix Code Initial Release 6 Content:Silk Code package

Type: ZIP Archive

OS: All Unix

Location: /Application Deployment Manager/MK Unix Code/Initial Release/6

Default Install Path: /var/tmp/meechai/content

Last Modified: Thu Feb 10 17:14:11 2011

Last Modified By: meechai

Created: Thu Feb 10 17:14:08 2011

Created By: opsware

File Name: 28880315.zip

File Version: -

File Size: 996.54 KB

Checksum: 0af74225792eecceb97d52109d47b7b604e2406e

Object ID: 822830315

4 From the Views pane, select **Properties**. The following package properties appear in the content pane:

General Properties

- **Name**: The name of the package.
- **Description**: The description of the package's contents.
- **Type**: The type of package.
- **OS**: The operating systems associated with the package.
- **Location**: The location of the package in the folder hierarchy.
- **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.
- **SA ID**: The unique SA ID for the package.

Archived Scripts (Zip Packages only)

- **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. The install command includes:

  (Windows): Replace with install command, for example, start /wait "Description" "%EXE_FULL_NAME%" <arguments>

  (UNIX): Replace with install command, for example, "%EXE_FULL_NAME%" <arguments>

  The environment variable EXE_FULL_NAME will contain the fully qualified path to the executable when the Install command is run.
- **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:
   - **Name**: Specifies the name of the package.
   - **Description**: Specifies a short description that is used to indicate the package's contents.
   - **OS**: The operating systems associated with the package.
   - **Location**: The location of the package in the folder hierarchy.
   - **Post-Extraction Script** (Only for ZIP packages): The name of the post-extraction script to be run after installing the zip package. Quotes in the file name must be preceded by back slashes.

- **Pre-Removal Script** (Only for ZIP packages): The name of the pre-removal script to be run before uninstalling the zip package. Quotes in the file name must be preceded by back slashes.
- **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. The install command includes:

  (Windows): Replace with install command, for example, start /wait "Description" "%EXE_FULL_NAME%" <arguments>

  The Windows `Start` command can behave differently if the filename to run contains spaces. it is recommended that you always include a command Description as shown in the above example.

  (UNIX): Replace with install command, for example, EXE_FULL_NAME%" <arguments>
- **Temporary Path**: (Only for application media) The temporary directory where the zip packages is executed.
- **Install Flags**: Specifies the optional arguments to be run when the package is installed on servers.
- **Reboot Required**: Selecting this option reboots the server when the package is successfully installed.
- **Response File** (Only for Solaris packages): Specifies the Response files that are associated with the Solaris package instances.
- **Upgrade** (Only for RPM packages): Selecting this option runs the `-U` parameter when the package is installed.
- **Install Script**: (Only for Application Installation Media): Specifies a script required to perform a silent installation of the application.
- **Pre-Install Script**: Specifies the script required to run on a managed server before the package is installed.
- **Post-Install Script**: Specifies the script required to run on a managed server after the package is installed.
- **Stop install if script returns an error**: Selecting this option stops installation of the package if the script fails.
- **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**: Specifies the optional arguments to be run when the package is uninstalled on servers.
- **Reboot Required**: Selecting this option reboots the server when the package is successfully uninstalled.
- **Uninstall Script**: (Only for Application Installation Media): Specifies a script required to perform a silent uninstallation of the application.
- **Pre-Uninstall Script**: Specifies the script required to run on a managed server before the package is uninstalled.

- **Post-Uninstall Script**: Specifies the script required to run on a managed server after the package is uninstalled.
- **Stop uninstall if script returns an error**: Selecting this option stops uninstallation of the package if the script fails.

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 package contents are only available for ZIP and RPM packages. For Solaris packages, HPUX Depot, and AIX LPP, the package names of the children packages are displayed.

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 Network Errata on page 57 for more information.

RPM Deployment Process

Deploying RPM packages on Linux servers involves the following steps:

- Uploading RPM packages. See Importing Software Packages on page 35 uploading packages for more information.
- Creating a software policy. See Creating Software Policies and Software Templates on page 21 for more information.
- Adding RPM packages to a policy and then setting the installation and upgrade options for the RPM packages in the software policy. See Setting Installation and Update Options for an RPM Package on page 28 for more information.
- Attaching the policy to a managed server. See the About Attaching Software Policies to Servers or Device Groups on page 17 for information about attaching a policy to a server.
- Remediating the server against the software policy. See the Remediating and Installing Software on page 61 for information about remediating servers.

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 on page 61 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.

➤ During remediation SA does not support dependency solving for RPM packages for SUSE Linux Enterprise Server 8, SUSE Linux Standard Server 8 and all non Linux operating systems that support RPM packages.

Install and Update of 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 on page 35 and Setting Installation and Update Options for an RPM Package on page 28 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 RPM Packages in a software policy on page 54 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 Option for an RPM Package on page 54 for more information.

Install Criteria:

- If the **Install RPM always** option is selected, SA will install the RPM packages specified in the policy on the managed server when you remediate the policy on the managed server.
- If you select the **Install RPM if only an earlier version is installed** option is selected, SA updates the RPM version on the managed server to the version specified in the software policy. This will happen when you remediate the policy on the managed server.
- If the RPM package is not already installed on the managed server, SA does not install the RPM version specified in the software policy.
- See Setting Installation and Update Options for an RPM Package on page 28 for more information on how to set these options.

See also:

- Remediating Servers with Software Policies on page 64
- RPM Rollback on page 50

RPM Rollback

RPM is a Linux feature, so RPM Rollback feature is only available on Linux servers. Because Linux has discontinued the built-in rollback functionality of RPM, the SA 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.

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 wasn't 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 on page 51.
- **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 on page 52.
- **Delete old rollback points**: Rollback points accumulate over time. You can delete old rollback points to clean up the queue.
  - — See Deleting an RPM Rollback Point on page 53.

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 it's prior version;

b a package that was newly installed after that point in time will be uninstalled;

c a packaged 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 on page 61.

      — 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 on page 64.

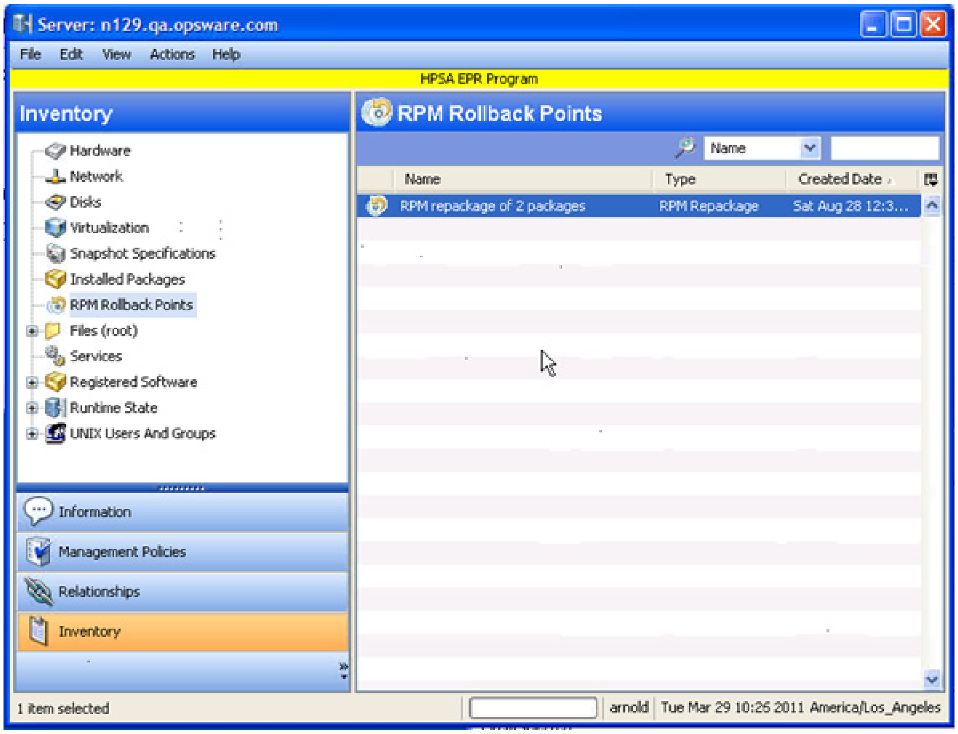
2 Select **Create RPM rollback point** option in the Options set of the installation or remediation process. This option will be enabled by default if the above requirements are met.

   - See Step 2 (Optional): Specify Reboot, Error Handling, and Script Options for Remediation on page 67

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.



Name	Type	Created Date
RPM repackage of 2 packages	RPM Repackage	Sat Aug 28 12:3...

1 item selected | arnold | Tue Mar 29 10:26 2011 America/Los_Angeles

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.

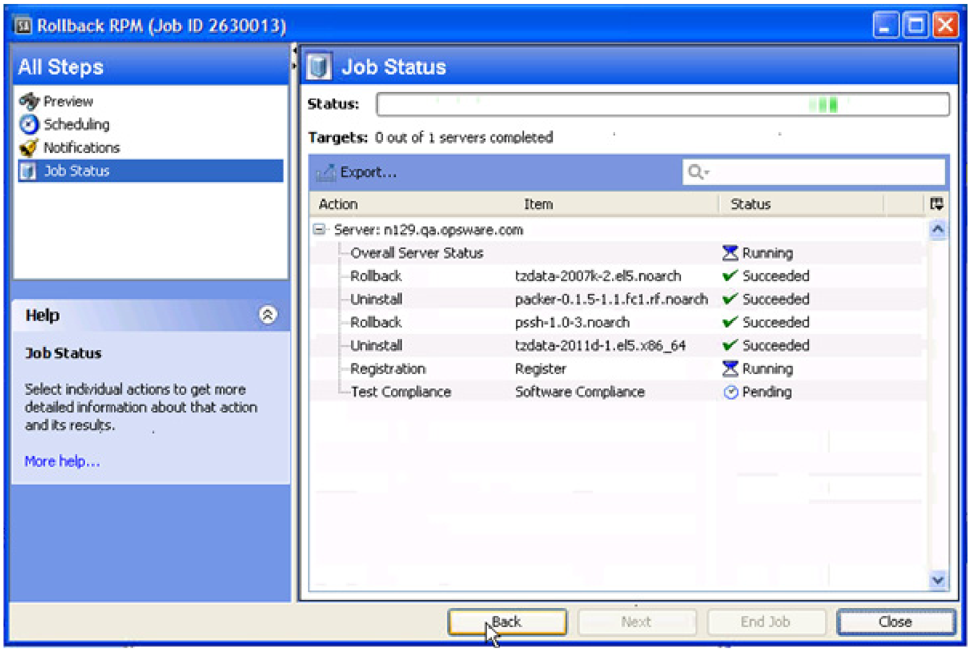
b **Scheduling**: specify if you want to start the job immediately or at a scheduled date and time.

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.



Status:

Targets: 0 out of 1 servers completed

Select individual actions to get more detailed information about that action and its results.

More help...

Action	Item	Status
Server: n129.qa.opsware.com		
Overall Server Status		Running
Rollback	tzdata-2007k-2.el5.noarch	✓ Succeeded
Uninstall	packer-0.1.5-1.1.fc1.rf.noarch	✓ Succeeded
Rollback	pssh-1.0-3.noarch	✓ Succeeded
Uninstall	tzdata-2011d-1.el5.x86_64	✓ Succeeded
Registration	Register	Running
Test Compliance	Software Compliance	Pending

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 an RPM 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 RPM Packages in a software policy

With SA you can automatically update the version and/or release of the RPM packages in a software policy. In a policy containing RPM packages, the Version and Release options determine whether the RPM package listed in the policy will be updated to the newer release or version. Also the newer release or version of the RPM package must be placed in the same folder as the RPM package specified in the software policy.

Thus, an RPM package in a policy is automatically updated if the Version or Release option is selected for an RPM package in the policy and if the newer version or release of the RPM package is present in the same folder as the RPM package in the software policy. The RPM packages in the folder are updated when you import an RPM package into the folder or when an RPM package is moved or copied from one folder to the other.

- **Version or Release**: This option allows you to automatically update the version or release of the RPM packages in a software policy. If you select this option, SA will automatically update the RPM packages in the policy to a newer version or release of the RPM. To upgrade the RPM packages on a managed server, you must remediate the server with the software policy.

➤ SA will update the RPM package in the policy to a newer version or release only if the newer release or version is placed in the same folder, as the RPM package specified in the software policy.

- **Release**: This option allows you to automatically update the version of the RPM package in a software policy. If you select this option, SA will automatically update the RPM package in the policy to a newer release of the same version of the RPM. To upgrade the RPM packages on a managed server, you must remediate the server with the software policy.

➤ SA will update the RPM package in the policy to a newer release only if the newer release of the same version is placed in the same folder, as the RPM package specified in the software policy.

See Setting Installation and Update Options for an RPM Package on page 28 for more information how to set these options.

Upgrade Option for an RPM Package

Upgrading a RPM package also depends on the Upgrade option for the RPM package (and the dependencies) specified in the Package properties window. After you upload an RPM package to SA, you can set the set the Upgrade option for the RPM package in the Package properties window. See Editing Package Properties on page 44 in this chapter for more information.

In the Package Properties window if you set the Install Mode option to Upgrade, then during remediation, SA first removes the previous version of the RPM package and its dependencies from the server and then installs the newer version of the RPM package and its dependencies on the server.

In the Package Properties window if you set the Install Mode option to Install, then during remediation SA installs the newer version of the RPM package and its dependencies on the server. The previous version of the RPM package and its dependencies are not removed from the server.

Updating an RPM package thus depends on the options you set for an RPM package on the policy window and the Package Properties window. Table 1 lists the action taken on the RPM package depending on the options set for the RPM package in the policy window and the Package Properties window.

Table 1 Setting Options for an RPM Package

Option selected for an RPM Package in the policy window	Option selected for an RPM Package in the Package Properties window	Action Taken
In the Install Criteria, the Install RPM only if an earlier version is installed option is selected	The Install Mode option is set to Upgrade	If a previous version of the RPM is installed, then SA will install the newer version of the RPM package as specified in the server's policy and uninstall the previous version. If the RPM package is not installed on the server, SA will not install the RPM version specified in the software policy.
In the Install Criteria, the Install RPM always option is selected	The Install Mode option is set to Upgrade	If the RPM is not already installed on the managed server, then SA will install the RPM packages specified in the policy on the managed server. If a previous version of the RPM package is installed on the server, then SA will install the newer version of the RPM package as specified in the policy on the server and uninstall the previous version from the managed server.
In the Install Criteria, the Install RPM only if an earlier version is installed option is selected	The Install Mode option is set to Install	If a previous version of the RPM package is installed on the server, then SA will not install the newer version of the RPM package as specified in the policy on the server. If the RPM package is not already installed on the server, then SA will not install the RPM version specified in the software policy.

Table 1 Setting Options for an RPM Package (cont'd)

Option selected for an RPM Package in the policy window	Option selected for an RPM Package in the Package Properties window	Action Taken
In the Install Criteria, the Install RPM always option is selected	The Install Mode option is set to Install	If the RPM package is not already installed on the managed server, then SA will install the RPM packages specified in the policy on the managed server. If a previous version of the RPM package is installed on the server, then SA will not install the newer version of the RPM package as specified in the policy on the server.

In SA, when you upload a non- kernel RPM package, by default the Upgrade option is set to Yes and when you upload a kernel RPM package, by default the Upgrade option is set to No. 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 the Detach a Software Policy from the Managed Server on page 74 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.

To downgrade to a previous version of an RPM packages:

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

2 Remediate the server to uninstall the RPM package.

3 Create a new software policy.

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

5 Attach the policy to the server.

6 Remediate the server to install the RPM package.

See also:

- Detach a Software Policy from the Managed Server on page 74
- Attaching a Software Policy to a Server or Device Group on page 62
- Setting Installation and Update Options for an RPM Package on page 28
- Creating Software Policies and Software Templates on page 21
- Remediating Servers with Software Policies on page 64
- RPM Rollback on page 50

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 RPM 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 Network Errata

Red Hat Network allows system administrators to manage their Red Hat servers on the network. Red Hat Linux publishes Errata which contains information describing security patches, bug fixes, and package updates for Red Hat Enterprise Linux. 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 policy in a folder in the Library in the SA Client.

Red Hat Network also consists of channels that contain packages. Using SA you can automatically download the packages in a channel, convert them to policies, and store the policy in a folder in the Library in the SA Client

The `rhn_import` CLI program provided by SA enables you to create policies, which correspond to Red Hat Network errata and channels. Using the `rhn_import` program, you can create the following types of policies:

- **Channel based software policy**: A Red Hat Network channel contains a list of packages. A channel allows you group packages as per your organizational requirements. For example, a channel may contain packages for a particular Red Hat operating system version or architecture. A channel may contain other child channels. When you run the `rhn_import` program, SA downloads the latest packages from the Red Hat Network channel and then imports the packages to the Library in the SA Client and creates a channel based software policy. Thus, a channel based policy reflects a particular channel. In the SA Client, you can view the name, description, location, availability, and the operating system version of the channel based policy in the Library. See Viewing Errata Based and Channel Based policies in the SA Client on page 58 for more information.
- **Errata based software policy**: Red Hat Network Errata 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. When you run the `rhn_import` program, SA downloads the latest packages from the Red Hat

Network 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 Network Errata: Bug Fix Advisories, Product Enhancement Advisories, and Security Advisories. The rhn_import program allows 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. See Viewing Errata Based and Channel Based policies in the SA Client on page 58 for more information.

- **Erratum-based software policy:** Erratum-based policies contain packages associated with a particular erratum. When you run the rhn_import program, SA downloads the latest packages from the Red Hat Network 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, log into the core server running the Software Repository component (part of the Slice Component bundle) and run the rhn_import program located in the following directory:

```
/opt/opsware/rhn_import/bin/rhn_import
```

➤ Importing RPM packages from the Red Hat Network 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 the Red Hat Network. It is recommended at least 5 GB of disk space is available in the Software Repository for every Red Hat Network channel you enable using the rhn_import program.

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

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

When you run the rhn_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
```

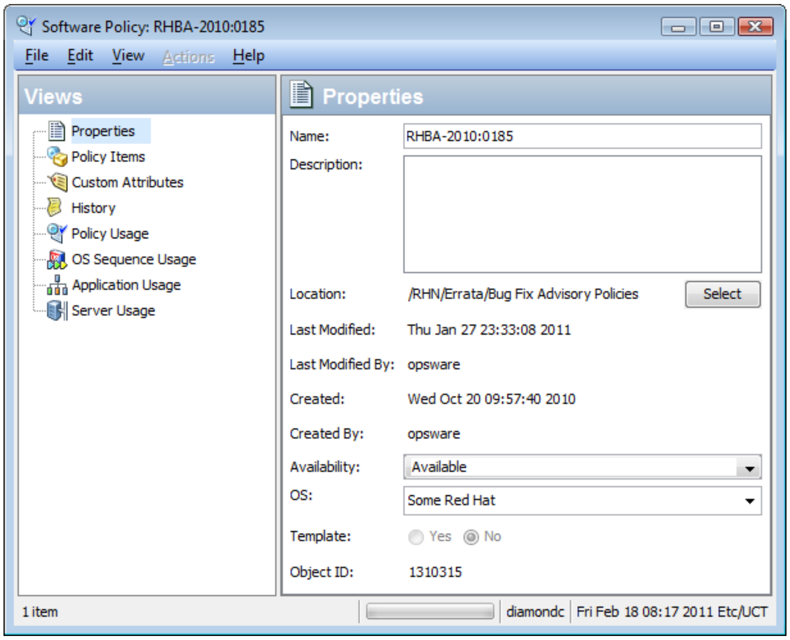
Viewing Errata Based and Channel Based policies in the SA Client

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.



Name: RHBA-2010:0185

Description:

Location: /RHN/Errata/Bug Fix Advisory Policies

Last Modified: Thu Jan 27 23:33:08 2011

Last Modified By: opsware

Created: Wed Oct 20 09:57:40 2010

Created By: opsware

Availability: Available

OS: Some Red Hat

Template: ○ Yes ● No

Object ID: 1310315

1 item | diamondc | Fri Feb 18 08:17 2011 Etc/UCT

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.

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
- Cancelling or Terminating Installation, Uninstallation or Remediation Jobs

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

➤ 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 on page 80.

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 on page 64.

Attach a Software Policy to a Server or Device Group

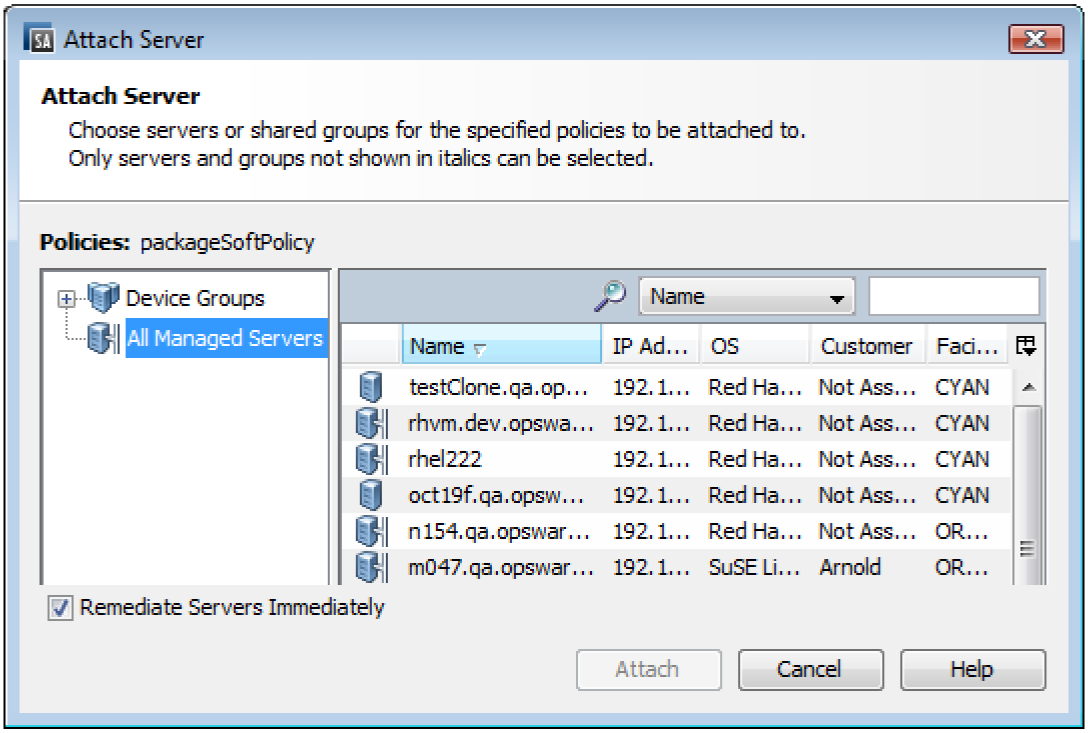
To attach a software policy to a server or device group:

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.



Attach Server

Attach Server

Choose servers or shared groups for the specified policies to be attached to.
Only servers and groups not shown in italics can be selected.

Policies: packageSoftPolicy

Name	IP Ad...	OS	Customer	Faci...
testClone.qa.op...	192.1...	Red Ha...	Not Ass...	CYAN
rhvm.dev.opswa...	192.1...	Red Ha...	Not Ass...	CYAN
rhel222	192.1...	Red Ha...	Not Ass...	CYAN
oct19f.qa.opsw...	192.1...	Red Ha...	Not Ass...	CYAN
n154.qa.opswar...	192.1...	Red Ha...	Not Ass...	OR...
m047.qa.opswar...	192.1...	SuSE Li...	Arnold	OR...

☑ Remediate Servers Immediately

(*Optional*) Enable **Remediate Servers Immediately** to remediate the attached servers against the software policy. See Remediating Servers with Software Policies on page 64 in this chapter for more information.

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 widow will appear. See Remediating Servers with Software Policies on page 64 in this chapter for more information.

Attach a Server to a Software Policy

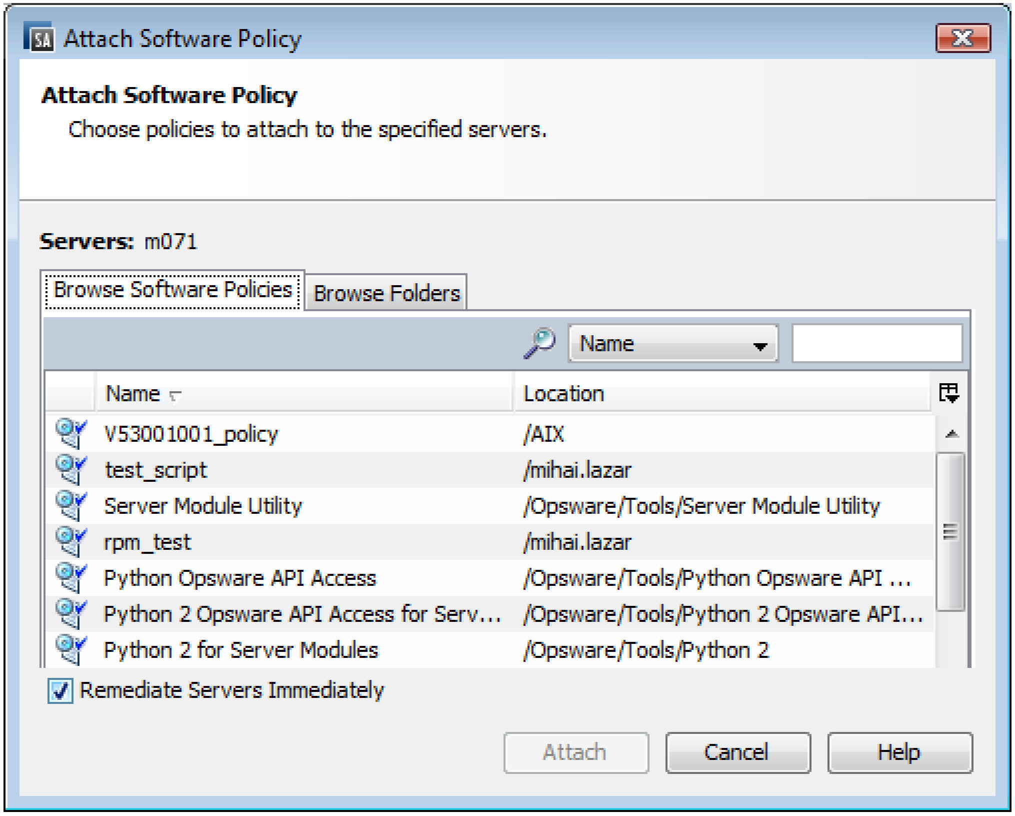
To attach a server or device group to a software policy:

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.



Attach Software Policy

Attach Software Policy

Choose policies to attach to the specified servers.

Servers: m071

Name	Location
V53001001_policy	/AIX
test_script	/mihai.lazar
Server Module Utility	/Opsware/Tools/Server Module Utility
rpm_test	/mihai.lazar
Python Opsware API Access	/Opsware/Tools/Python Opsware API ...
Python 2 Opsware API Access for Serv...	/Opsware/Tools/Python 2 Opsware API...
Python 2 for Server Modules	/Opsware/Tools/Python 2

☑ Remediate Servers Immediately

(*Optional*) Select **Remediate Servers Immediately** to remediate the servers against the software policy. See Specifying the Remediation Options on page 65.

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 widow will appear. See Remediating Servers with Software Policies on page 64 in this chapter for more information.

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, RPMs, 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 on page 77.

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.

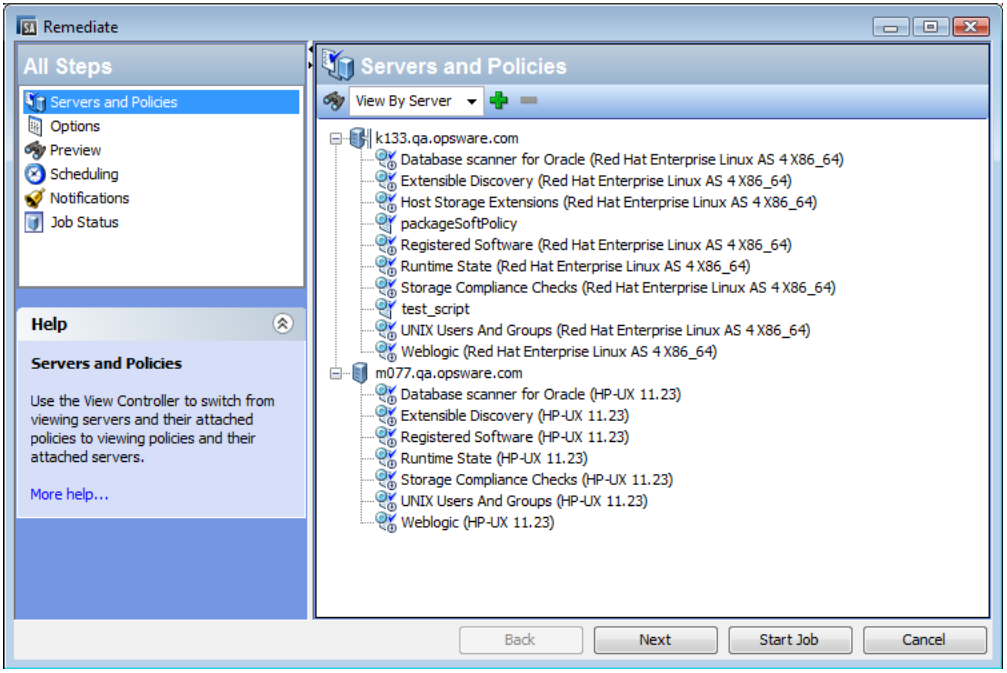
There are several ways to open the Remediate window, depending on what you are trying to accomplish. For example, this section provides instructions for the following methods:

- 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 on page 66.

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.



Servers and Policies

k133.qa.opsware.com
- Database scanner for Oracle (Red Hat Enterprise Linux AS 4 X86_64)
- Extensible Discovery (Red Hat Enterprise Linux AS 4 X86_64)
- Host Storage Extensions (Red Hat Enterprise Linux AS 4 X86_64)
- packageSoftPolicy
- Registered Software (Red Hat Enterprise Linux AS 4 X86_64)
- Runtime State (Red Hat Enterprise Linux AS 4 X86_64)
- Storage Compliance Checks (Red Hat Enterprise Linux AS 4 X86_64)
- test_script
- UNIX Users And Groups (Red Hat Enterprise Linux AS 4 X86_64)
- Weblogic (Red Hat Enterprise Linux AS 4 X86_64)

m077.qa.opsware.com
- Database scanner for Oracle (HP-UX 11.23)
- Extensible Discovery (HP-UX 11.23)
- Registered Software (HP-UX 11.23)
- Runtime State (HP-UX 11.23)
- Storage Compliance Checks (HP-UX 11.23)
- UNIX Users And Groups (HP-UX 11.23)
- Weblogic (HP-UX 11.23)

Servers and Policies

Use the View Controller to switch from viewing servers and their attached policies to viewing policies and their attached servers.

More help...

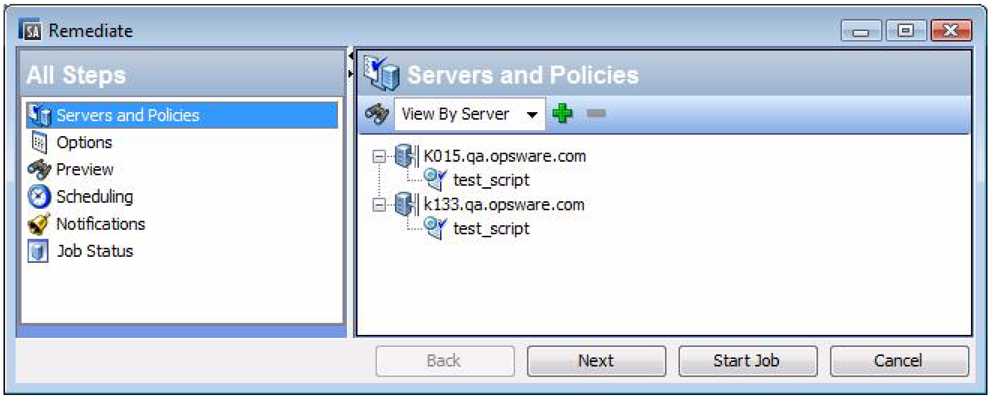
To access the Remediate window from the software policy list:

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.



Servers and Policies

K015.qa.opsware.com
- test_script

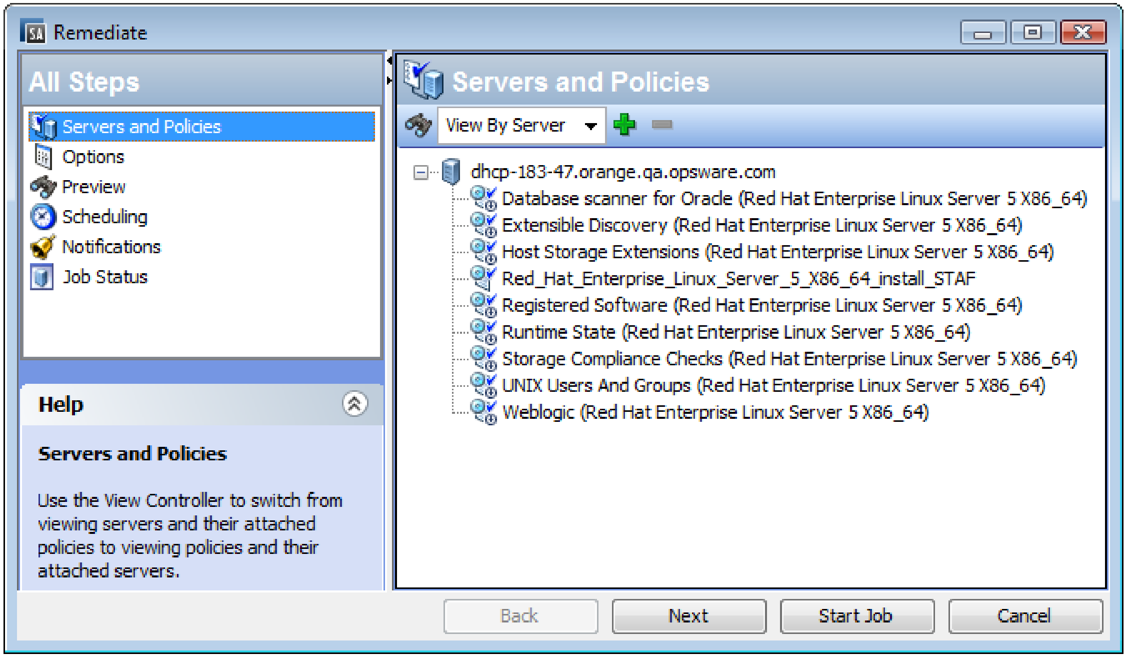
k133.qa.opsware.com
- test_script

Specifying the Remediation Options

Use the Remediate window (Figure 3) 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

Figure 3 The Remediate Window in the SA Client



dhcp-183-47.orange.qa.opsware.com
- Database scanner for Oracle (Red Hat Enterprise Linux Server 5 X86_64)
- Extensible Discovery (Red Hat Enterprise Linux Server 5 X86_64)
- Host Storage Extensions (Red Hat Enterprise Linux Server 5 X86_64)
- Red_Hat_Enterprise_Linux_Server_5_X86_64_install_STAF
- Registered Software (Red Hat Enterprise Linux Server 5 X86_64)
- Runtime State (Red Hat Enterprise Linux Server 5 X86_64)
- Storage Compliance Checks (Red Hat Enterprise Linux Server 5 X86_64)
- UNIX Users And Groups (Red Hat Enterprise Linux Server 5 X86_64)
- Weblogic (Red Hat Enterprise Linux Server 5 X86_64)

Use the View Controller to switch from viewing servers and their attached policies to viewing policies and their attached servers.

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 on page 64.

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 on page 67.
- **Reboot servers after each installation or uninstallation**: This option reboots servers after installing or uninstalling each software item.
- **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 2 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 all RPM-type packages are set to reboot, the remediate process will reboot the server only once after all the RPM packages are installed.

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 **RPM Rollback** section, select the **Create RPM Rollback point** option to set the current server state as a rollback point. This preserves the current state in case you want to restore it later if something about a subsequent update fails.

This option only appears on Linux servers in one of these conditions:

a The RPMs have previous versions already installed and the target servers are set to upgrade.

Or

b You are remediating one or more Linux servers with software policies containing one or more RPMs that will result in at least one upgrade/erase operation on the target servers.

The RPM Package Manager on the target servers must be version 4.2 to 4.6. The SA Agent must be version .34 or greater. (See RPM Rollback on page 50.)

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-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.

To skip the remaining setting steps and run the job, see Step 6: Run the Remediation Job and View Job Status on page 71.

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.

(Optional) To export the job status results to a text file, click **Export**.

4 Click **Next** to proceed to the to the Scheduling step.

To skip the remaining setting steps and run the job, see Step 6: Run the Remediation Job and View Job Status on page 71.

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.

To skip the remaining setting steps and run the job, see Step 6: Run the Remediation Job and View Job Status on page 71.

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 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 6: Run the Remediation Job and View Job Status on page 71.

Step 6: Run the Remediation Job and View Job Status

When you run the remediation job, the Job Status window provides summary information about the 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.

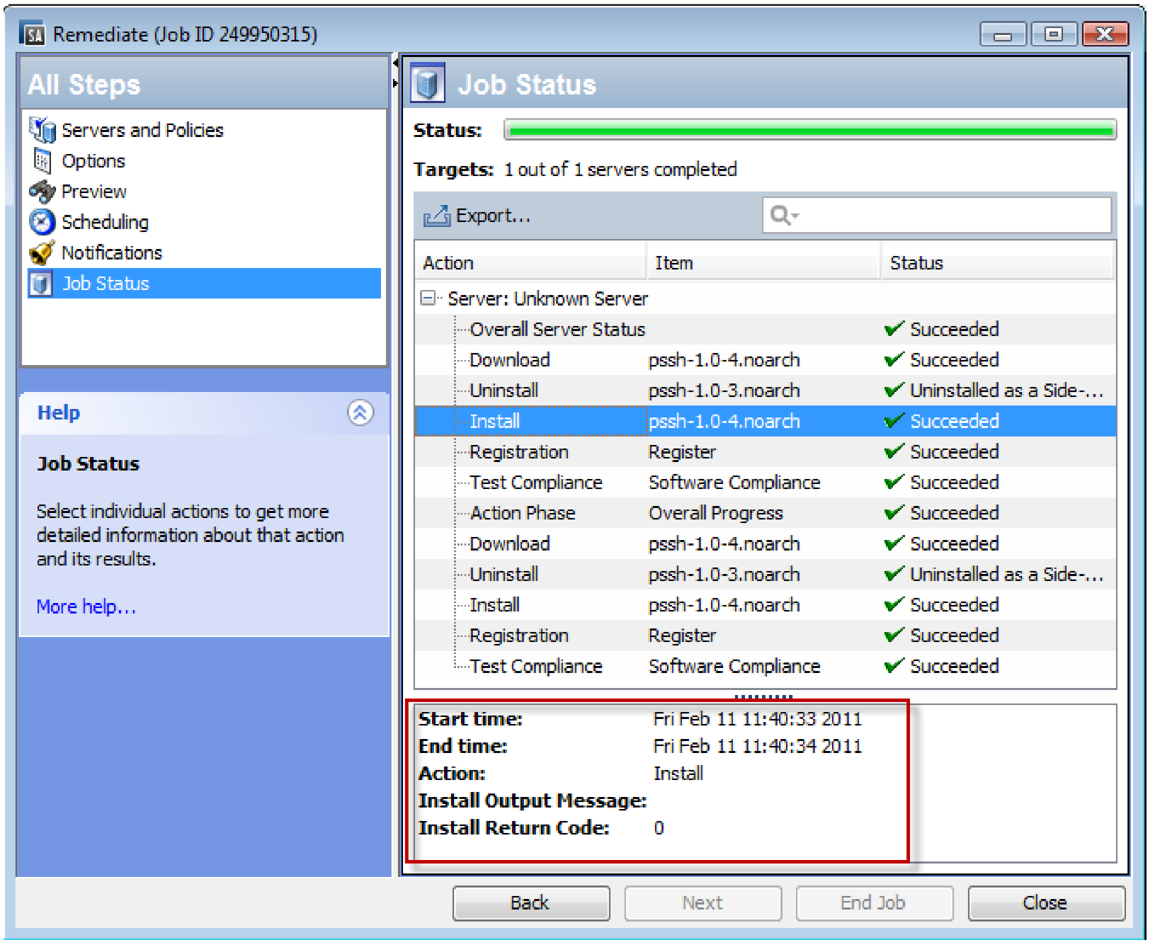
3 To view the details of each action, select an action row in the table. The details for the selected action appear in the lower panel of the content pane. See Viewing Job Status on page 73 for an illustration.

4 You can also perform any of the following optional actions:

- Click **Export** to export the job status results to a text file.
- Click **End Job** to stop the job. See Terminating an Active Installation/Uninstallation or Remediation Job on page 77.
- 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.

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.



Select individual actions to get more detailed information about that action and its results.

More help...

Status:

Targets: 1 out of 1 servers completed

Action	Item	Status
⊟ Server: Unknown Server		
Overall Server Status		✓ Succeeded
Download	pssh-1.0-4.noarch	✓ Succeeded
Uninstall	pssh-1.0-3.noarch	✓ Uninstalled as a Side-...
Install	pssh-1.0-4.noarch	✓ Succeeded
Registration	Register	✓ Succeeded
Test Compliance	Software Compliance	✓ Succeeded
Action Phase	Overall Progress	✓ Succeeded
Download	pssh-1.0-4.noarch	✓ Succeeded
Uninstall	pssh-1.0-3.noarch	✓ Uninstalled as a Side-...
Install	pssh-1.0-4.noarch	✓ Succeeded
Registration	Register	✓ Succeeded
Test Compliance	Software Compliance	✓ Succeeded

Start time: Fri Feb 11 11:40:33 2011
End time: Fri Feb 11 11:40:34 2011
Action: Install
Install Output Message:
Install Return Code: 0

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.

➤ 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:

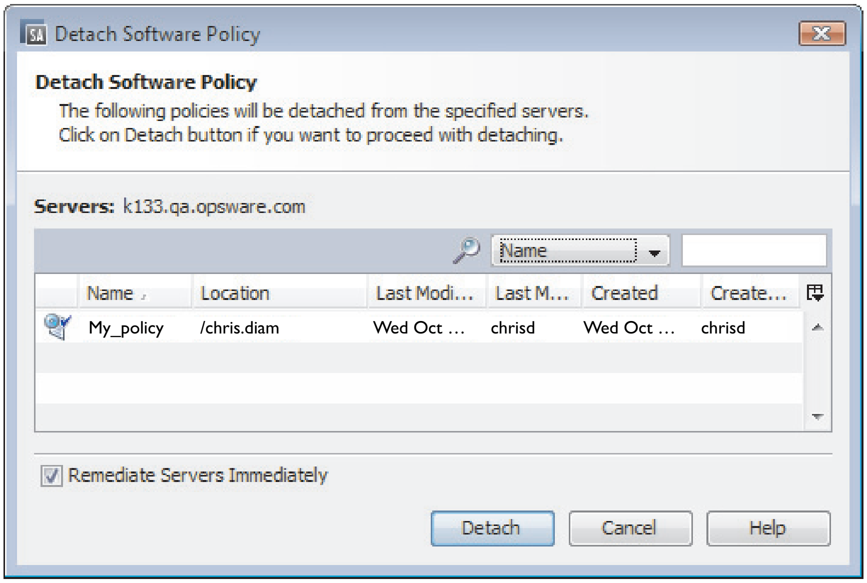
- Detach a Software Policy from the Managed Server
- Remediate a Server to Remove Software

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.



Detach Software Policy

Detach Software Policy

The following policies will be detached from the specified servers.
Click on Detach button if you want to proceed with detaching.

Servers: k133.qa.opsware.com

Name	Location	Last Modi...	Last M...	Created	Create...
My_policy	/chris.diam	Wed Oct ...	chrisd	Wed Oct ...	chrisd

☑ Remediate Servers Immediately

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.

Remediate a Server to Remove Software

Perform the tasks described in Specifying the Remediation Options on page 65. 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 or Terminating Installation, Uninstallation or Remediation Jobs

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 on page 79.

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, however, phases that are already running must complete before the entire job can stop. For instructions, see Terminating an Active Installation/Uninstallation or Remediation Job on page 77.

Table 3 Phases in the Installation, Uninstallation and Remediation Processes

Phase	Actions performed
Analyze	Figures out exactly what packages need installation and removal from the server. May include running pre-download scripts.
Download	Downloads any packages that need to be staged onto the server. May include running post-download scripts.
Action (Install/ Uninstall/Remediate)	Performs all the installations, upgrades, removals and reboots. Depending on the installation or remediation settings, additional actions may also occur, and are also subject to cancellation. For example: • Rebooting servers • Registering software • Testing compliance • Running scripts

➤ Because individual phases must complete, you cannot stop a job when it is in the final action phase (install, uninstall, remediate). To stop a job that is installing or remediating, it must be in either the Analyze or Download phase of the process. To stop a job that is uninstalling, it must be in the Analyze phase. (There is no Download phase when uninstalling.)

Terminating an active installation, uninstallation or remediation job has the following results:

- No processes will be started on additional servers.
- If a process (job phase) has already started on a server, all remaining tasks in that process will be completed; however, 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 be able 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.

➤ 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 that the one used to start the job.

Terminating an Active Installation/Uninstallation or Remediation Job

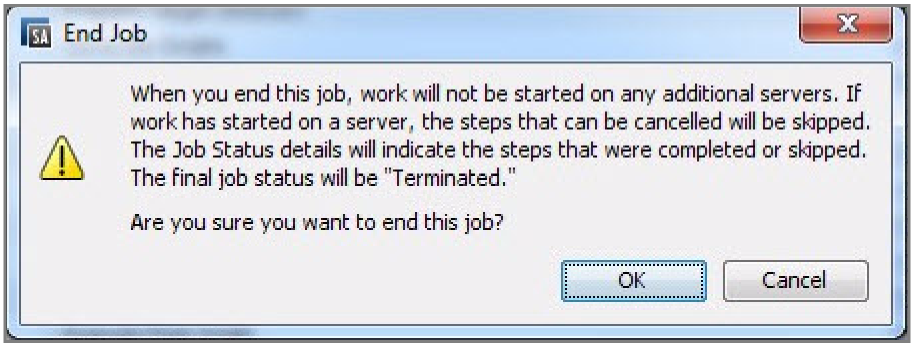
You can terminate a software installation, uninstallation or remediation job that is actively running. For example, you may need to stop a job that is producing erroneous results or will run beyond an allotted maintenance window. This option is only available for active remediation or installation jobs that are in the Analyze or Download phase and for uninstallation jobs that are in the Analyze phase.

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:

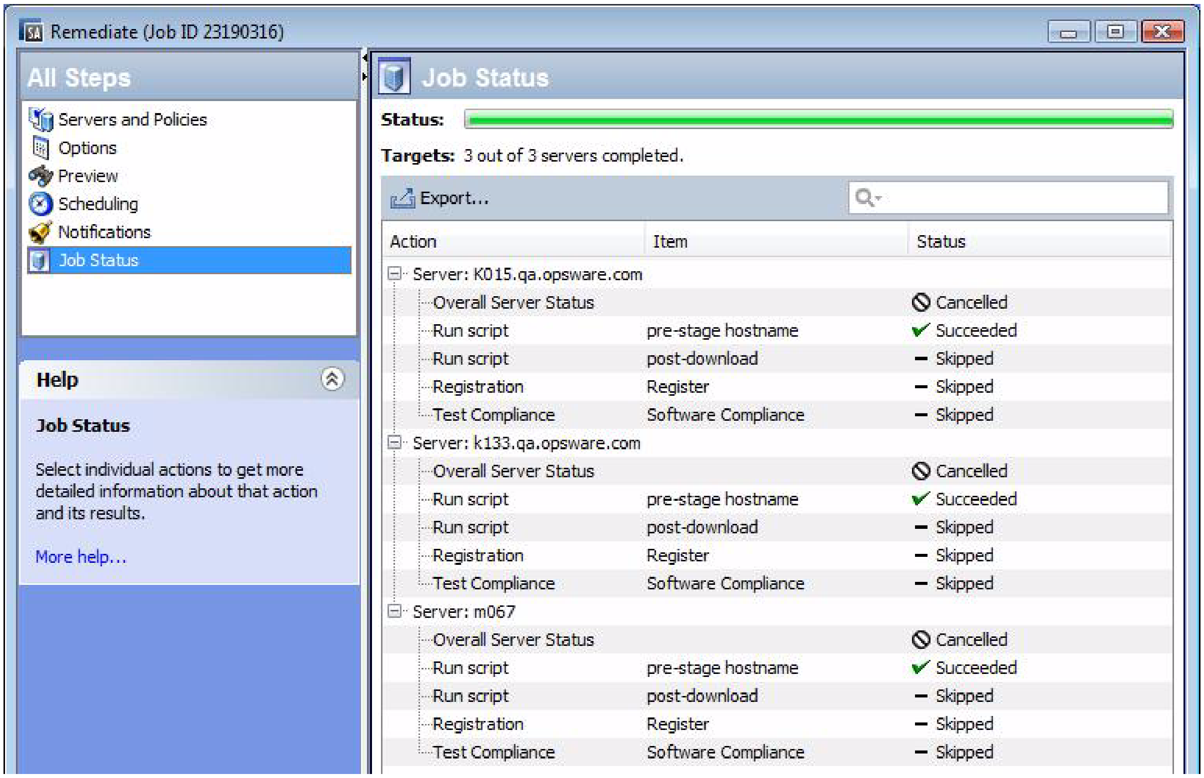
  - the job will not initiate work on any additional servers
  - if work has started on a server, the job will cancel any steps that can be skipped
  - the Job Status will indicate the steps that were completed or skipped
  - if the job ends successfully, the final job status will be “Terminated”



When you end this job, work will not be started on any additional servers. If work has started on a server, the steps that can be cancelled will be skipped. The Job Status details will indicate the steps that were completed or skipped. The final job status will be "Terminated."

Are you sure you want to end this job?

3 Click **OK** to confirm that you wish to terminate the job. The Job Status window displays the progress of the termination.



Remediate (Job ID 23190316)

All Steps

- Servers and Policies
- Options
- Preview
- Scheduling
- Notifications
- Job Status

Help

Job Status

Select individual actions to get more detailed information about that action and its results.

More help...

Job Status

Status:

Targets: 3 out of 3 servers completed.

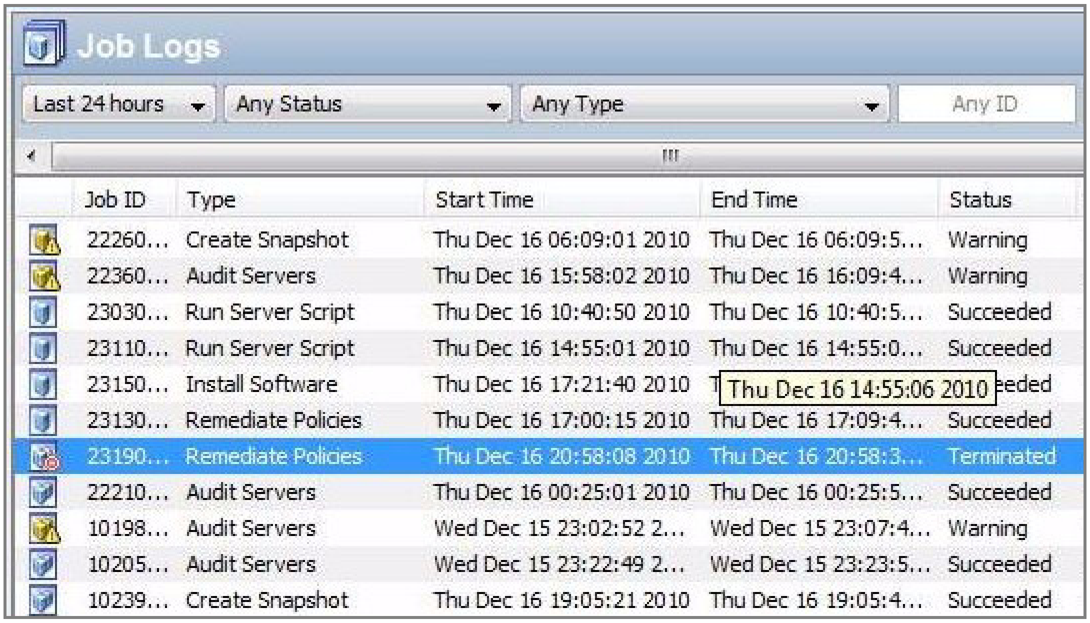
Export...

Action	Item	Status
⊟ Server: K015.qa.opsware.com		
Overall Server Status		⊘ Cancelled
Run script	pre-stage hostname	✓ Succeeded
Run script	post-download	— Skipped
Registration	Register	— Skipped
Test Compliance	Software Compliance	— Skipped
⊟ Server: k133.qa.opsware.com		
Overall Server Status		⊘ Cancelled
Run script	pre-stage hostname	✓ Succeeded
Run script	post-download	— Skipped
Registration	Register	— Skipped
Test Compliance	Software Compliance	— Skipped
⊟ Server: m067		
Overall Server Status		⊘ Cancelled
Run script	pre-stage hostname	✓ Succeeded
Run script	post-download	— Skipped
Registration	Register	— Skipped
Test Compliance	Software Compliance	— Skipped

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.



Job Logs

Last 24 hours ▾ | Any Status ▾ | Any Type ▾ | Any ID

Job ID	Type	Start Time	End Time	Status
22260...	Create Snapshot	Thu Dec 16 06:09:01 2010	Thu Dec 16 06:09:5...	Warning
22360...	Audit Servers	Thu Dec 16 15:58:02 2010	Thu Dec 16 16:09:4...	Warning
23030...	Run Server Script	Thu Dec 16 10:40:50 2010	Thu Dec 16 10:40:5...	Succeeded
23110...	Run Server Script	Thu Dec 16 14:55:01 2010	Thu Dec 16 14:55:0...	Succeeded
23150...	Install Software	Thu Dec 16 17:21:40 2010	T Thu Dec 16 14:55:06 2010	eded
23130...	Remediate Policies	Thu Dec 16 17:00:15 2010	Thu Dec 16 17:09:4...	Succeeded
23190...	Remediate Policies	Thu Dec 16 20:58:08 2010	Thu Dec 16 20:58:3...	Terminated
22210...	Audit Servers	Thu Dec 16 00:25:01 2010	Thu Dec 16 00:25:5...	Succeeded
10198...	Audit Servers	Wed Dec 15 23:02:52 2...	Wed Dec 15 23:07:4...	Warning
10205...	Audit Servers	Wed Dec 15 23:22:49 2...	Wed Dec 15 23:23:5...	Succeeded
10239...	Create Snapshot	Thu Dec 16 19:05:21 2010	Thu Dec 16 19:05:4...	Succeeded

See also, Cancelling or Terminating Installation, Uninstallation or Remediation Jobs on page 75 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.

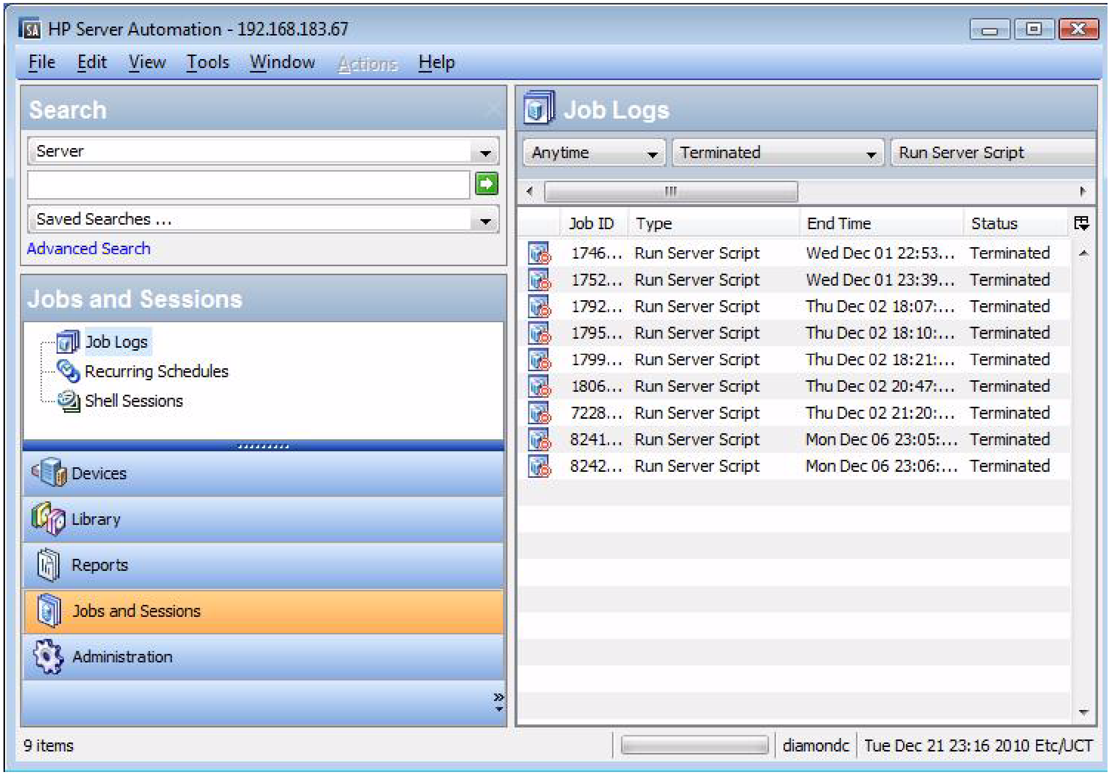
3 Select **View ➤ Refresh** from the menu to refresh the list. The content pane displays jobs with In Progress status.

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.



Anytime | Terminated | Run Server Script

Job ID	Type	End Time	Status
1746…	Run Server Script	Wed Dec 01 22:53:…	Terminated
1752…	Run Server Script	Wed Dec 01 23:39:…	Terminated
1792…	Run Server Script	Thu Dec 02 18:07:…	Terminated
1795…	Run Server Script	Thu Dec 02 18:10:…	Terminated
1799…	Run Server Script	Thu Dec 02 18:21:…	Terminated
1806…	Run Server Script	Thu Dec 02 20:47:…	Terminated
7228…	Run Server Script	Thu Dec 02 21:20:…	Terminated
8241…	Run Server Script	Mon Dec 06 23:05:…	Terminated
8242…	Run Server Script	Mon Dec 06 23:06:…	Terminated

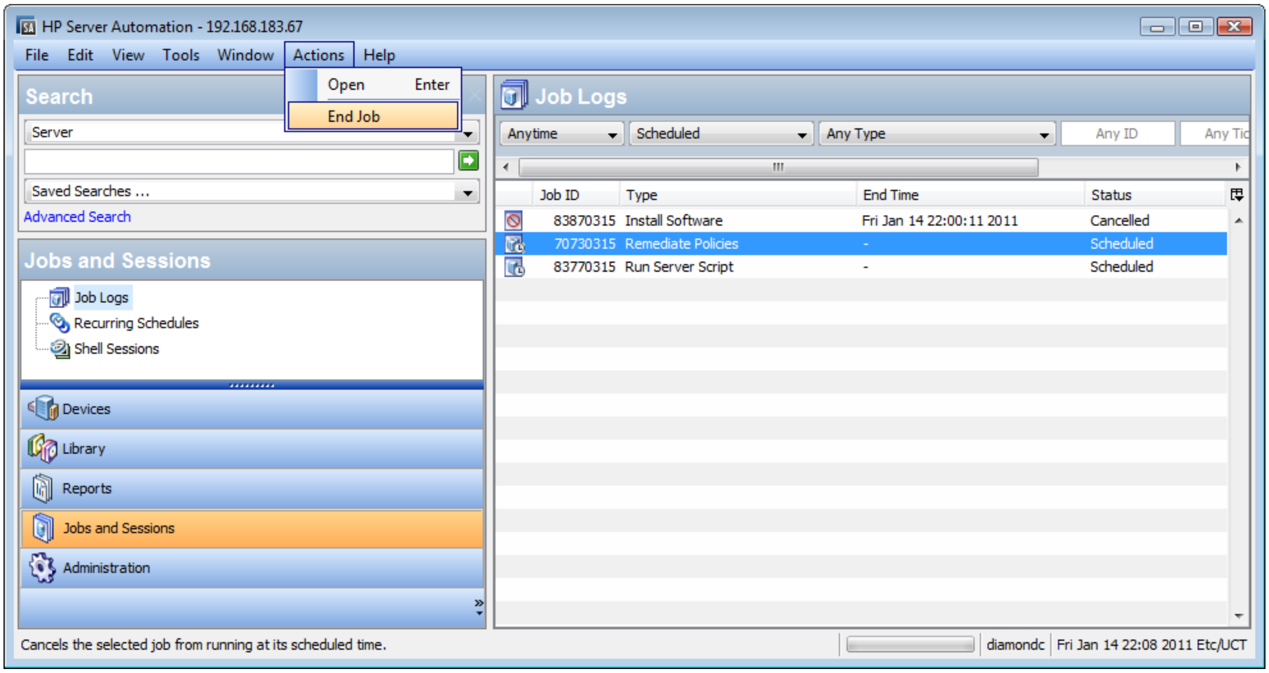
9 items | diamondc | Tue Dec 21 23:16 2010 Etc/UCT

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.



Job ID	Type	End Time	Status
83870315	Install Software	Fri Jan 14 22:00:11 2011	Cancelled
70730315	Remediate Policies	-	Scheduled
83770315	Run Server Script	-	Scheduled

Cancels the selected job from running at its scheduled time.

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 on page 61.

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 on page 81.

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.

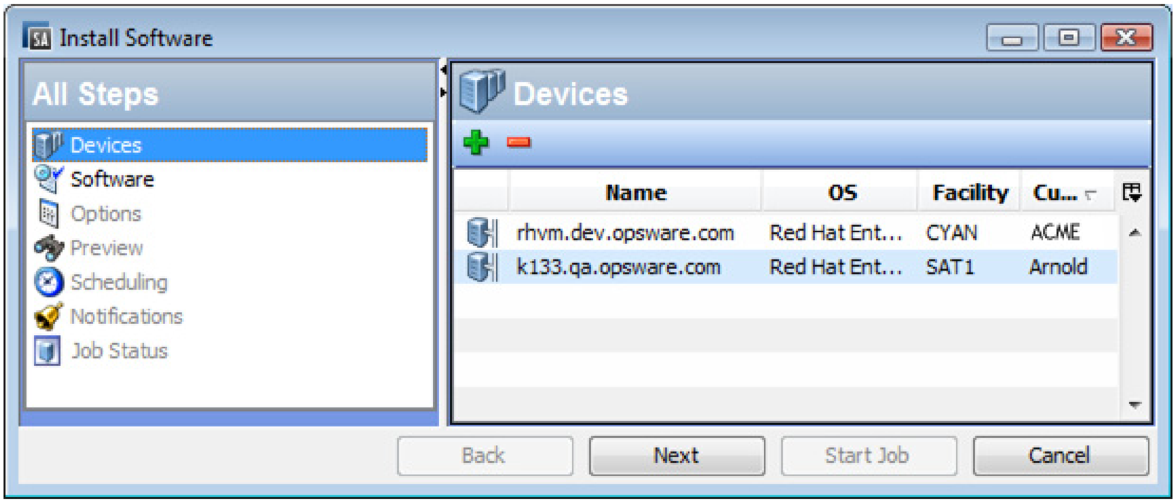
Specifying the Install or Uninstall Options

You can install or uninstall software directly on an SA managed server. The Install Software window as shown in Figure 4 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

➤ All steps outlined in this section are performed from the Install Software or Uninstall Software window. See Accessing the Install or Uninstall Window on page 80.

Figure 4 Install Software Window



Name	OS	Facility	Cu...
rhvm.dev.opsware.com	Red Hat Ent…	CYAN	ACME
k133.qa.opsware.com	Red Hat Ent…	SAT1	Arnold

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 t**o proceed to the Select Software step.

Step 2: Select Software

Specify the software (packages, RPMs, 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**.
   - Click the Browse Types tab to browse the list of items by type, such as Software Policy, Patch, Package.
   - 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 t**o proceed to the Specify Additional Options step.

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 on page 86.

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.
   - **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.

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 on page 67

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 **RPM Rollback** section, select the **Create RPM Rollback point** option to set the current server state as a rollback point. This preserves the current state in case you want to restore it later if something about a subsequent update fails.

   This option only appears on Linux servers in one of these conditions:

   a. The RPMs have previous versions already installed and the target servers are set to upgrade.

   Or

   b. You are installing one or more RPMs—either directly or through a software policy—that will result in at least one upgrade/erase operation on the target servers.

   The RPM Package Manager on the target servers must be version 4.2 to 4.6. The SA Agent must be version .34 or greater. (See RPM Rollback on page 50.)

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-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 on page 86.

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.
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 on page 86.

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 on page 86.

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 on page 86.

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.
4. You can also perform any of the following optional actions:
   - Click **Export** to export the job status results to a text file.
   - Click **End Job** to stop the job. See Cancelling or Terminating Installation, Uninstallation or Remediation Jobs on page 75.
   - 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.

➤ For more information about SA Client job logs, see the *SA User Guide: Server Automation* for information about job logs.

A Software Discovery Reference

IMPORTANT: Get the latest version of documentation for Server Automation Software Discovery from the HP Live Network at http://www.hp.com/go/livenetwork. Streamed product content may change between releases and the documentation on the portal may have important updates that are not contained in this document.

The Server Automation (SA) Software Discovery feature 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 unlicensed software, unregistered software, custom-built software and software that was not installed using one of the standard packaging technologies for Windows or UNIX.
- Creates an inventory of software programs that have not been installed as an OS-registered application.
- 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.

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.

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 at:

    http://www.hp.com/go/livenetwork
- Have the HP Live Network connector (LNc), installed and configured on your core server. This is the client for the HP Live Network, which automates content updates, downloads, and imports into the product (SAS, BSAE, SAR).

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

‼ **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* on the HP Live Network for instructions on enabling products.

- If you want to use the BSA Essentials (BSAE) Java client to create reports about discovered software, you must subscribe to the software_discovery_reports stream.
  - Use the following command to display the SAR streams:

    ```
    live-network-connector list-streams --product=sar
    ```

    Additional information may be available on the individual streams by using the "`describe`" command. This information may provide a long text description and a URL for where to locate additional information on the specified Stream/content.
  - Enable the software_discovery_reports stream

    ```
    live-network-connector write-config
    --stream=content.software_discovery_reports --enable
    ```

    (where the above statement is all one line)

➤ If you do not download this stream, some of the discovered software data will not appear in your reports generated from BSAE. If you do not plan to use BSAE for software discovery reports, you do not need to download this stream.

Information about additional BSAE Reports for SA are also available in the *SA Reports Guide*.

Supported Platforms and Configurations

Software Discovery is supported on all UNIX platforms and Windows versions which the SA Agent supports for managed servers.

Software discovery is ISO-8859-1 compliant.

➤ Software Discovery is not supported on all operating systems. Please see the *Server Automation Compatibility Matrix* for the latest and most accurate version support information.

Downloading the Software Discovery Package

The Software Discovery package is available from the BSA Essentials Network. To get the Software Discovery package, you must use the HP Live Network connector (LNc).

➤ For more information on BSA Essentials and to request a BSA Essentials account, visit the BSA Essentials web site at http://www.hp.com/go/livenetwork.

The LNc downloads the Software Discovery package in the form of a zip file with the following name:

```
OPSWsmo_discovered_software-<version>.zip
```

This zip file is placed in the following directory on your SA core server:

```
/var/opt/opsware/ogfs/mnt/root/var/opt/opsware/sm
```

This directory can also be accessed from the SA Global Shell at the following directory:

```
/var/opt/opsware/sm
```

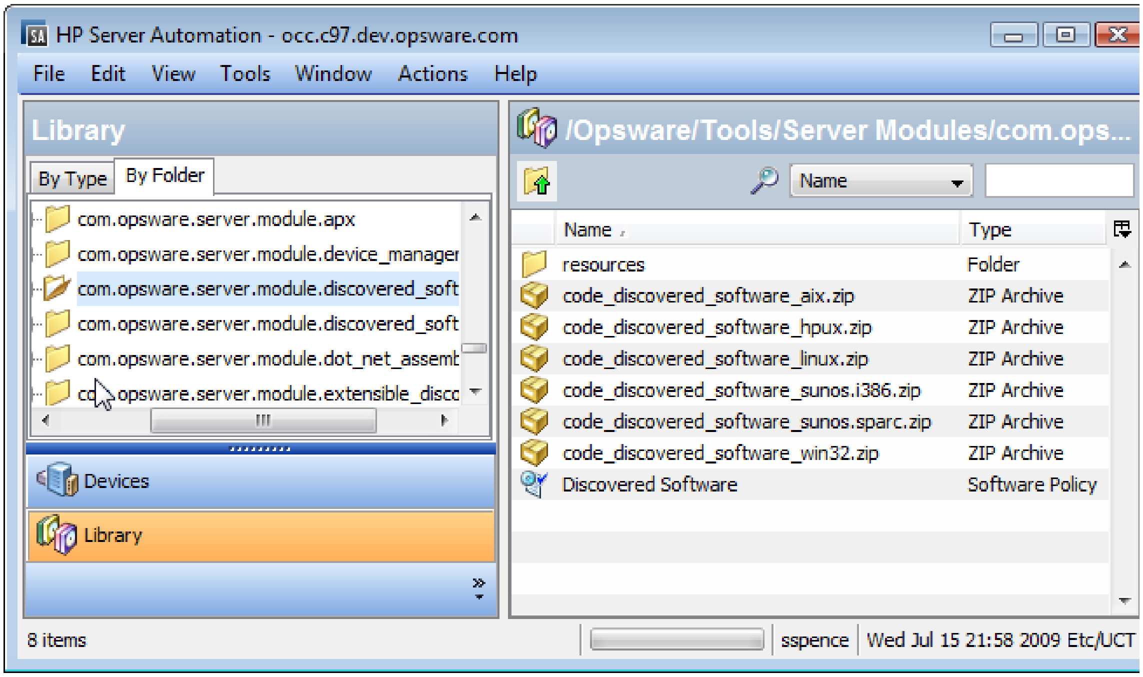
Contents of the Software Discovery Package

After you install the Software Discovery package, you can see the contents in the SA Client as follows.

1. In the SA Client, select Library in the navigation pane.
2. In the Library, select the By Folder tab.
3. Navigate to Library/Opsware/Tools/Server Modules/ com.opsware.server.module.discovered_software. This displays the following contents of the Discovered Software package as shown in Figure 5.
   - A set of zip file packages, one for each supported managed server platform.
   - A software policy named Discovered Software that contains all the zip file packages.
   - A subdirectory named resources.

The Discovered software policy is automatically remediated (installed) when you initiate a snapshot with the “Perform Inventory” option selected, as described in Deploying Software Discovery Using Inventory Snapshots on page 93.

Figure 5 SA Client Library Showing Location of Software Discovery Packages


HP Server Automation - occ.c97.dev.opsware.com
File
Edit
View
Tools
Window
Actions
Help
Library
By Type
By Folder
Devices
Library
/Opsware/Tools/Server Modules/com.ops...
Name
8 items
sspence
Wed Jul 15 21:58 2009 Etc/UCT

com.opsware.server.module.apx
com.opsware.server.module.device_manager
com.opsware.server.module.discovered_soft
com.opsware.server.module.discovered_soft
com.opsware.server.module.dot_net_assemb
co opsware.server.module.extensible_disco

Name	Type
resources	Folder
code_discovered_software_aix.zip	ZIP Archive
code_discovered_software_hpux.zip	ZIP Archive
code_discovered_software_linux.zip	ZIP Archive
code_discovered_software_sunos.i386.zip	ZIP Archive
code_discovered_software_sunos.sparc.zip	ZIP Archive
code_discovered_software_win32.zip	ZIP Archive
Discovered Software	Software Policy

Software Discovery Permissions

The Software Discovery feature can be run on a server by any SA user with read access to the server and belongs to a user group that has the client feature permission “Allow Execute Server Modules: Yes”.

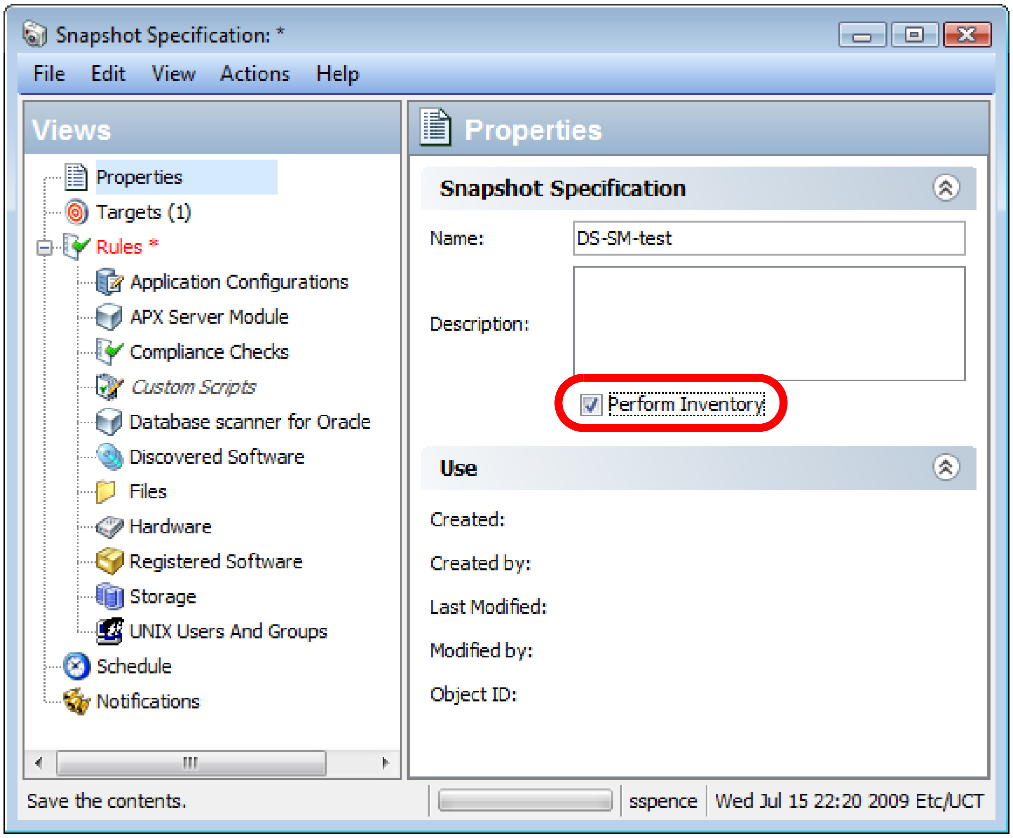
If a user wants to add or modify custom entries for Software Discovery, then the user will require the “Manage Server Modules: Read & Write” permission. Permissions are granted in the SAS Web Client.

For more information on SA permissions, see the *SA Administration Guide*.

Deploying Software Discovery Using Inventory Snapshots

To deploy the Software Discovery feature to discover software installed on a server, you must run a snapshot with the “Perform Inventory” option selected, as shown in Figure 6. For details, see “Creating a Snapshot Specification” and “Running a Snapshot Specification” in the *SA User Guide: Audit and Compliance*.

Figure 6 Snapshot with Perform Inventory Option Selected to Enable Software Discovery



Name: DS-SM-test

Description:

☑ Perform Inventory

Created:

Created by:

Last Modified:

Modified by:

Object ID:

Save the contents. | sspence | Wed Jul 15 22:20 2009 Etc/UCT

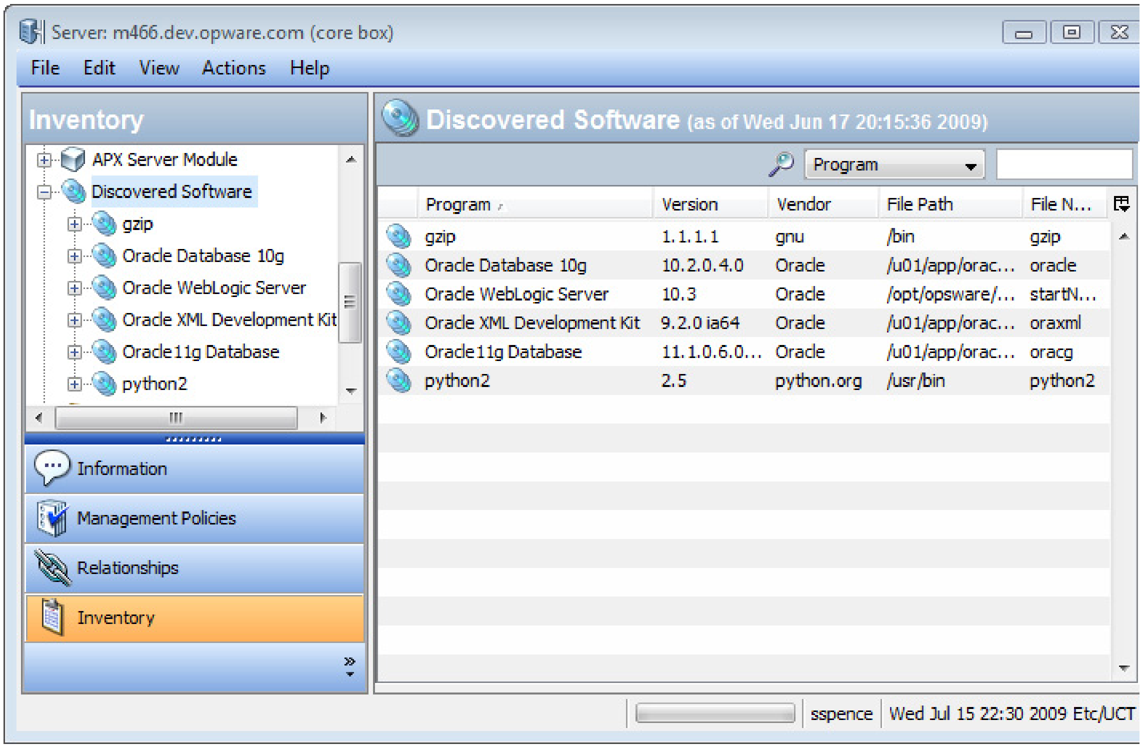
Each time a snapshot is run on a server with Perform Inventory selected, SA verifies that the Software Discovery server module is installed on the managed server. If the Software Discovery server module is not on the target server, a remediate job is launched automatically by the core that installs the contents of the Software Discovery software policy. The policy remediation occurs automatically when the snapshot is run.

This installs the Software Discovery server module on the server, including the signature zip package, which in turn enables you to view Software Discovery on a managed server’s Device Explorer, and use the Snapshot’s software inventory in an Audit.

Viewing Discovered Software on a Managed Server

The SA Client displays the software that has been discovered on the server in the Device Explorer in the Inventory view, as shown in Figure 7.

Figure 7 Device Explorer Showing Software Discovered



Program	Version	Vendor	File Path	File N...
gzip	1.1.1.1	gnu	/bin	gzip
Oracle Database 10g	10.2.0.4.0	Oracle	/u01/app/orac...	oracle
Oracle WebLogic Server	10.3	Oracle	/opt/opsware/...	startN...
Oracle XML Development Kit	9.2.0 ia64	Oracle	/u01/app/orac...	oraxml
Oracle11g Database	11.1.0.6.0...	Oracle	/u01/app/orac...	oracg
python2	2.5	python.org	/usr/bin	python2

Unlike other server objects in the managed server inventory that fetch data in real time from a server, the Discovered Software server object is configured to only show data from the latest inventory Snapshot (a Snapshot that has the Perform Inventory check box selected when the snapshot specification is created). If there are no inventory snapshots available, the server browser will show an error message suggesting that an inventory Snapshot should be made.

The Device Explorer displays a time stamp at the top of the Device Explorer window indicating the last time the inventory Snapshot was run on the server. For example, in Figure 7, the Contents pane (right side) of the window shows the label: “(as of Thu May 29th 23:45:29 2008)”. This indicates the last time the inventory Snapshot was run.

For more information, see “Creating a Snapshot Specification” and “Running a Snapshot Specification” in the *SA User Guide: Audit and Compliance*.

Inventory Snapshots in Audits

Once you have performed an inventory Snapshot, you can add it as the source of an audit, so whenever the audit runs, it will compare the original state of the snapshot with the current state of the server, and you can determine if the installed software has changed since you last ran the Snapshot.

For more information on Snapshots and Audits, see “Audit and Remediation” in the *SA User Guide: Audit and Compliance*.

Inventory Snapshot Job Error Messages

The following error codes and messages are specific to Software Discovery when running an inventory Snapshot:

* 1-TADNSW unexpectedly quit!

* 2-Invalid JSON format

* 3-Another instance of DS-SM is running.

* 4-Database merge failed

* 6-TADNSW run failure

* 8-TADNSW Error: `<error>`

How Software Discovery Works

Software Discovery provides a signature-based software discovery mechanism for SA Windows and UNIX managed servers. It consists of discovery logic, module metadata, and a signature database. This signature database contains application signatures from HP's Asset Management Tool, Discovery Dependency Mapping Inventory (DDMI), which is the Software Application Index (SAI) used by DDMI to discover software.

➤ This feature is not designed to allow you to install or remediate software on a managed server. For information on using software policies to install and remediate software onto managed servers, see Chapter 4, Remediating and Installing Software, on page 61.

➤ For complete information on DDMI and the DDMI scanner, see the *HP DDMI Configuration and Customization Guide*. For complete information on the DDMI SAI editor, see the *HP DDMI Scan Data Analysis Guide*. These manuals are available from http://support.openview.hp.com/selfsolve/manuals.

Application Discovery

Software Discovery uses DDMI SAI content for discovering applications on SA managed servers. The SAI signatures are used to generate the SCT (Signature Component Table) for use with Software Discovery. The SCT contains all the signatures imported from the DDMI SAI which are to be used by Software Discovery.

SCT application signatures are grouped together by product IDs and compared to the results retrieved by a file system scan. For every file found on the file system, a hash is computed using the DDMI hash algorithm. The signatures collected from the file scan are referred as 'raw' signatures. Application signatures represented in the DDMI SAI and corresponding SCT contain the same hash values computed from the same algorithm. The 'raw' signatures are then compared to the DDMI SAI signatures stored in SCT and a rating is calculated off the best possible match. The highest rated match is then reported as the application back to the user who initiated the scan.

All components are compared to the corresponding properties obtained from raw signatures. When a match occurs in any one of the components, the rating is incremented and used for gauging the best possible match among various product versions. When the best match is found, the product is reported using the display components:

```
DISPLAY PRODUCT: <display product-name>
DISPLAY VENDOR: <display vendor-name>
DISPLAY VERSION: <display version-number>
```

There are a few differences to note between the DDMI and Software Discovery results that are accepted around specific boundary conditions. The first difference in comparison is that Software Discovery will report all instances of software discovered on a server. For example, when evaluating multiple installs of the Java JRE. DDMI will only report the first install of a series of products of the same version. On the other hand, Software Discovery will report all instances of the installed product.

The second difference occurs when no exact matching signature is available in the SAI. In this situation, DDMI and the Software Discovery feature will attempt to find the next best match based off the ratings calculated. DDMI will evaluate all signatures, along with all 'associated' entries, to generate a high rating during guess estimates and find more accurate results. The Software Discovery feature will sometimes reach the same results in the guess. However, the guess does occasionally differ due to remaining 'associated' entries not being imported into SCT from the SAI.

Please note again that due to sizing constraints, not all SAI associated entries are imported into SCT. Only overlapping 'associated' entries between concurrent applications versions will be imported as well. As a result, SA will not pinpoint or discover suites or editions of applications.

Application Signatures

All application signatures are generated using the `DDMI SAI Master.xml` (WIN32) and `unix.xml` (UNIX). All application signatures are stored in a database for processing and identification during the scan process. SCT is used for the software discovery process in the database.

During a core install, these application signature packages must be uploaded to the core and attached to the Software Discovery software policy to which the Software Discovery package is attached. During upload, each package is associated with all UNIX or all Windows platforms. These packages are automatically installed onto a managed server when the server is remediated with respect to this policy. These signatures are used by the underlying scanning software to determine what software is discovered on a server.

Application Signatures from BSA Essentials Network

The Software Discovery feature comes with a database consisting of application signatures derived from the DDMI SAI content. When the Software Discovery package is imported into the SA core, all applications represented by those signatures are discovered. This signature database is updated periodically (usually monthly). These updates are provided through BSA Essentials Network and must be imported into the SA core.

The Software Discovery signature update package is a zip file, which has a file name similar to:

```
OPSWsmo_discovered_software_sig_prod-<version>.zip
```

After the BSA connector downloads the zip file, it is stored in the following directory on the SA core:

```
/var/opt/opsware/ogfs/mnt/root/var/opt/opsware/sm/data
```

This location can also be accessed from the Global Shell with the following command:

```
/var/opt/opsware/sm/data
```

The zip file can be uploaded to the core with the following dstool command:

```
/opt/opsware/smtool/dstool --user=<username> --pass=<password>
OPSWsmo_discovered_software_sig_prod-<version>.zip
```

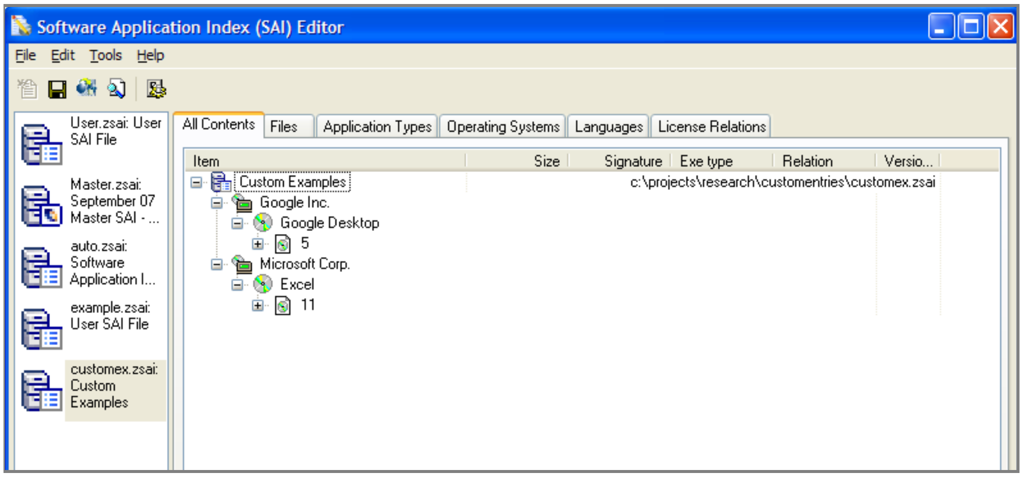
The --help option gives additional details on how to use dstool:

```
/opt/opsware/smtool/dstool --help
```

Custom Signatures

You can add custom application signatures using the DDMI SAI editor and corresponding platform scanners as shown in Figure 8. For complete information on the DDMI SAI editor, see the *HP DDMI Scan Data Analysis Guide*, available from http://support.openview.hp.com/selfsolve/manuals.

Figure 8 Software Application Index (SAI) Editor



User.zsai: User SAI File
Master.zsai: September 07 Master SAI - ...
auto.zsai: Software Application I...
example.zsai: User SAI File
customex.zsai: Custom Examples

Custom Examples — c:\projects\research\customentries\customex.zsai
Google Inc.
Google Desktop
5
Microsoft Corp.
Excel
11

The SAI editor provides a convenient way to add new publishers and applications. Its scanners retrieve raw application signatures related to the specific applications you are interested in reporting as applications to SA.

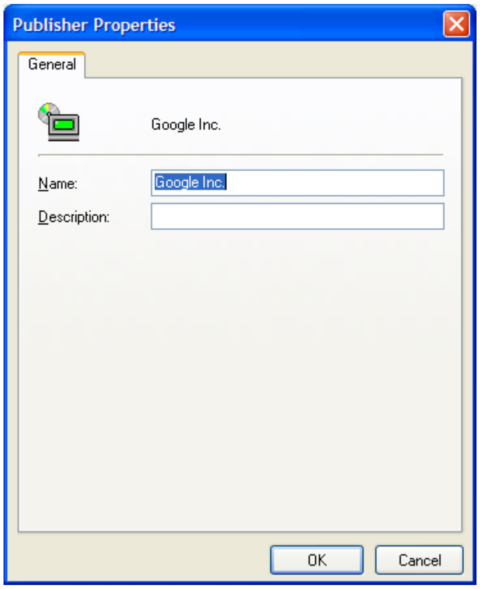
It is recommended that you run the scanner prior to working with the SAI editor. The entire file system or specific directories can be targeted with the scanner by using the following command line options:

```
scanwin32-x86-2.50.000.7199.exe -fast -p:C:\projects\research\edscan\
-paths:"C:\Program Files"
```

(`scanwin32-x86-2.50.000.7199.exe` is the latest version of the executable and may change without notice.)

In the SAI Editor, you can add the publisher, application, release, and version details for the specific applications that need to be categorized in SAI as shown in Figure 9 through Figure 12.

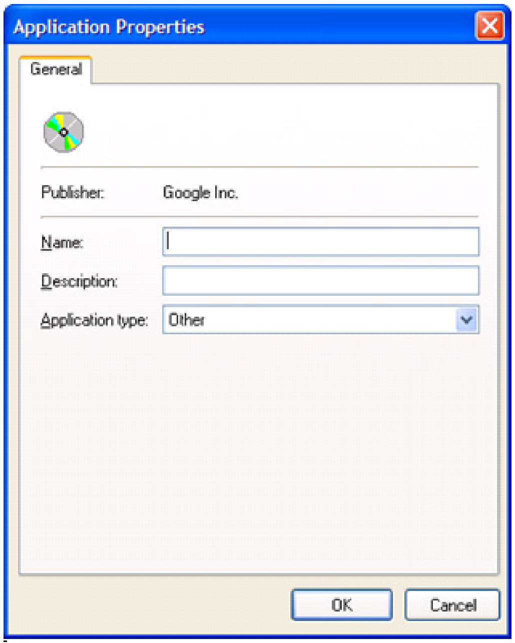
Figure 9 Publisher Properties



Name: Google Inc.

Description:

Figure 10 Application Properties



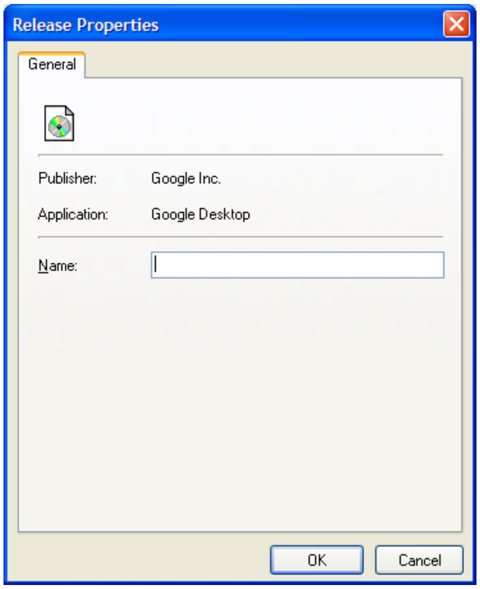
Publisher: Google Inc.

Name:

Description:

Application type: Other

Figure 11 Release Properties

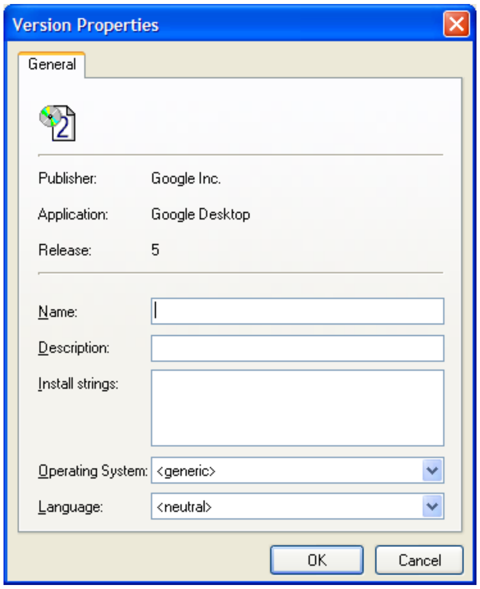


Publisher: Google Inc.

Application: Google Desktop

Name:

Figure 12 Version Properties



Publisher: Google Inc.

Application: Google Desktop

Release: 5

Name:

Description:

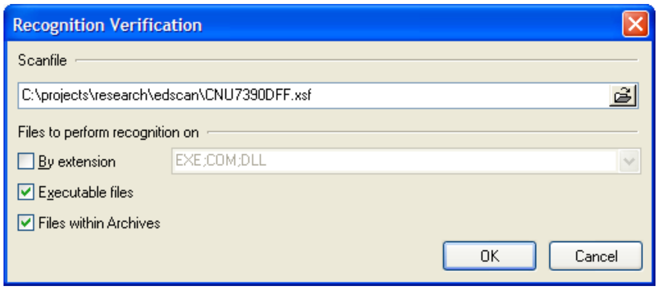
Install strings:

Operating System: <generic>

Language: <neutral>

At this stage, you can open the scan results in the SAI Editor and begin adding corresponding signatures to the versions previously added in the SAI Editor as shown in Figure 13 and Figure 14.

Figure 13 Recognition Verification



Scanfile

C:\projects\research\edscan\CNU7390DFF.xsf

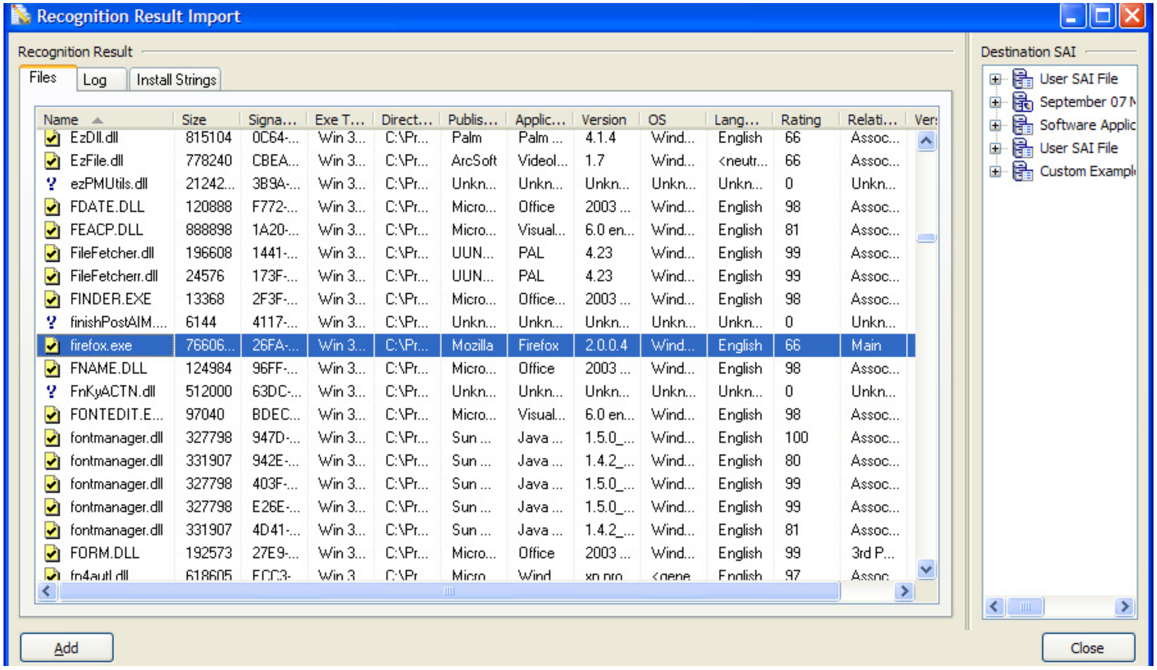
Files to perform recognition on

☐ By extension EXE;COM;DLL

☑ Executable files

☑ Files within Archives

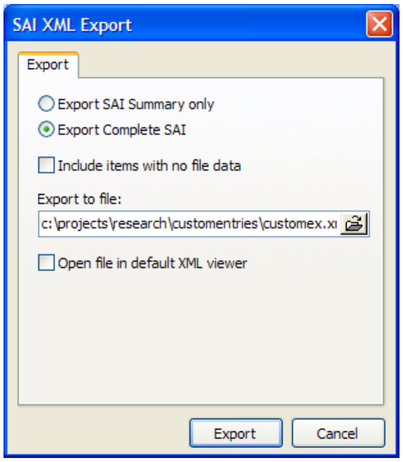
Figure 14 Recognition Result Import



Name	Size	Signa...	Exe T...	Direct...	Publis...	Applic...	Version	OS	Lang...	Rating	Relati...	Ver
☑ EzDll.dll	815104	0C64-...	Win 3...	C:\Pr...	Palm	Palm ...	4.1.4	Wind...	English	66	Assoc...	
☑ EzFile.dll	778240	CBEA...	Win 3...	C:\Pr...	ArcSoft	Videol...	1.7	Wind...	<neutr...	66	Assoc...	
? ezPMUtils.dll	21242...	3B9A-...	Win 3...	C:\Pr...	Unkn...	Unkn...	Unkn...	Unkn...	Unkn...	0	Unkn...	
☑ FDATE.DLL	120888	F772-...	Win 3...	C:\Pr...	Micro...	Office	2003 ...	Wind...	English	98	Assoc...	
☑ FEACP.DLL	888898	1A20-...	Win 3...	C:\Pr...	Micro...	Visual...	6.0 en...	Wind...	English	81	Assoc...	
☑ FileFetcher.dll	196608	1441-...	Win 3...	C:\Pr...	UUN...	PAL	4.23	Wind...	English	99	Assoc...	
☑ FileFetcherr.dll	24576	173F-...	Win 3...	C:\Pr...	UUN...	PAL	4.23	Wind...	English	99	Assoc...	
☑ FINDER.EXE	13368	2F3F-...	Win 3...	C:\Pr...	Micro...	Office...	2003 ...	Wind...	English	98	Assoc...	
? finishPostAIM....	6144	4117-...	Win 3...	C:\Pr...	Unkn...	Unkn...	Unkn...	Unkn...	Unkn...	0	Unkn...	
☑ firefox.exe	76606...	26FA-...	Win 3...	C:\Pr...	Mozilla	Firefox	2.0.0.4	Wind...	English	66	Main	
☑ FNAME.DLL	124984	96FF-...	Win 3...	C:\Pr...	Micro...	Office	2003 ...	Wind...	English	98	Assoc...	
? FnKyACTN.dll	512000	63DC-...	Win 3...	C:\Pr...	Unkn...	Unkn...	Unkn...	Unkn...	Unkn...	0	Unkn...	
☑ FONTEDIT.E...	97040	BDEC...	Win 3...	C:\Pr...	Micro...	Visual...	6.0 en...	Wind...	English	98	Assoc...	
☑ fontmanager.dll	327798	947D-...	Win 3...	C:\Pr...	Sun ...	Java ...	1.5.0_...	Wind...	English	100	Assoc...	
☑ fontmanager.dll	331907	942E-...	Win 3...	C:\Pr...	Sun ...	Java ...	1.4.2_...	Wind...	English	80	Assoc...	
☑ fontmanager.dll	327798	403F-...	Win 3...	C:\Pr...	Sun ...	Java ...	1.5.0_...	Wind...	English	99	Assoc...	
☑ fontmanager.dll	327798	E26E-...	Win 3...	C:\Pr...	Sun ...	Java ...	1.5.0_...	Wind...	English	99	Assoc...	
☑ fontmanager.dll	331907	4D41-...	Win 3...	C:\Pr...	Sun ...	Java ...	1.4.2_...	Wind...	English	81	Assoc...	
☑ FORM.DLL	192573	27E9-...	Win 3...	C:\Pr...	Micro...	Office	2003 ...	Wind...	English	99	3rd P...	
☑ fn4autl.dll	618605	FCC3-	Win 3	C:\Pr	Micro	Wind	xp pro	<gene	English	97	Assoc	

Once the content is modified, you can export the content to the SAI XML database (User XML) as shown in Figure 15.

Figure 15 SAI XML Export



○ Export SAI Summary only

● Export Complete SAI

□ Include items with no file data

Export to file:

c:\projects\research\customentries\customex.xı

□ Open file in default XML viewer

The User XML database is then copied using the following command to the core where it is used by dstool:

```
/opt/opsware/smtool/dstool --username=<username> --password=<password>
customex.xml
```

dstool generates a new (User) SCT database which is uploaded as a custom dependency to Software Discovery. During the next inventory snapshot, Software Discovery checks for the custom database and uses it along with the production database to categorize new applications.

If at any stage a mistake is made or you choose to remove all custom entries, invoke the dstool with the following command line options:

```
/opt/opsware/smtool/dstool --remove --username=<username>
--password=<password>
```

Use the following --help option for additional details about the usage of dstool:

```
/opt/opsware/smtool/dstool --help
```

For complete information on DDMI and the DDMI scanner, see the *HP DDMI Configuration and Customization Guide*. For complete information on the DDMI SAI editor, see the *HP DDMI Scan Data Analysis Guide*. These manuals are available from http://support.openview.hp.com/selfsolve/manuals.

Configuration and Customization

UNIX and Windows Software Discovery support configuration attributes which drive how they run and the profile of resource usage on a managed server.

Configuration Attributes

The name of the custom attribute is `HPSW DS SM_CONFIG`.

The value of this custom attribute is in INI file format in Windows. Windows filters are grouped under the FILTERS_WINDOWS section while UNIX filters are grouped under the FILTERS_UNIX section. The METHODS section specify the scanning settings and the CONFIGURATION section contains other configuration settings.

The following is the syntax of a custom attribute:

```
[FILTERS_WINDOWS]
FILTER#={INCLUDE | EXCLUDE | EXIST}, { FILENAME | FILEPATH | FILESYSTYPE |
VOLUME | PRODUCT | VENDOR | VERSION},  criteria

[FILTERS_UNIX]
FILTER#={INCLUDE | EXCLUDE | EXIST}, { FILENAME | FILEPATH | FILESYSTYPE |
VOLUME | PRODUCT | VENDOR | VERSION},  criteria

[METHODS]
DELTA_SCAN= {TRUE | FALSE}

[CONFIGURATION]
LOG_MODE= {LOW | MEDIUM | HIGH | DEBUG}
INCLUDE_SYMBOLIC_LINKED_FILES={TRUE | FALSE}
INCLUDE_SYMBOLIC_LINKED_DIRS={TRUE | FALSE}
```

Configuration Options

Table 4 describes the configuration options used within the HPSW_DS_SM_CONFIG custom attribute.

Table 4 Configuration Options

Attribute	Platform	Description
`'FILTER#'`	All	Create a list of filters for the Software Discovery Gauntlet for Cataloged and/or Uncataloged software. Filters are separated into two categories under INI format according to platform, [FILTERS_WINDOWS] and [FILTERS_UNIX]. Filter arguments are provided below their corresponding platform in the format of FILTER#=Action,Type,Criteria. Action can be one of 'Include', 'Exclude', or 'Exist'. Supported types are 'VOLUME', 'FILEPATH', 'FILENAME', 'PRODUCT', 'VENDOR', 'VERSION', 'FILESYSTYPE'. Criteria must correspond to the type.
`'INCLUDE_SYMBOLIC_LINKED_FILES'`	UNIX	True/False Default is False. Enable if you want to include symbolic linked files in the scan.
`'INCLUDE_SYMBOLIC_LINKED_DIRS'`	UNIX	True/False Default is False. Enable if you wish for tadnsw to traverse into symbolic linked directories.
`'DELTA_SCAN'`	All	Enabled/Disabled or True/False. Default is False. Enable/Disable the delta scanning module.
`'LOG_MODE'`	All	Value is one of "LOW", "MEDIUM", "HIGH or "DEBUG", default is "LOW". Sets the amount of information written to the log file. "LOW" is used to provide general runtime progress. "MEDIUM" will provide additional details regarding progress along with location if performing filescan. If “DEBUG”or "HIGH" is selected, the module will write enough information to the file so developers can diagnose obscure problems.

Syntax Errors

Refer to Inventory Snapshot Job Error Messages on page 94 to see all the Software Discovery error messages and codes. Prior to using the syntax, the values in the custom attributes in Table 4 are validated for proper syntax. If the configuration values violate the syntax, Software Discovery returns errors. Such messages are reported in place of `<error>` referenced in the list in Inventory Snapshot Job Error Messages on page 94. Validation only applies to the INCLUDE/EXCLUDE action assignments. If other invalid configuration options are specified, the default values override

Discovery Filtering Process

The use of Software Discovery filters benefits users by preventing unwanted data from consuming valuable network and database resources. The filtering scheme supports three actions, which are Include, Exist and Exclude.

The Software Discovery feature first checks the Include list to see what files should be examined. If a file is included, it progresses to the next step called Exist, which checks to make sure that selected fields contain certain data. Last, the discovery module compares the scanned data with all required fields against the Exclude list to see if the file should be excluded. If a file passes all configured filters, it is reported, otherwise the file is discarded and the discovery module continues scanning. All criteria fields accept inputs of `<criteria>`, prefix, postfix, as well as wild cards. If a wild card is specified at the end of the path string, the exact path is matched and sub-directories are not affected.

How Filters Affect Scanning

Include and exclude filters can affect the Software Discovery in a variety of ways. In general, the rules listed below apply.

Directory Scanning:

- If a directory is excluded, exclude all files and subdirectories.
- If a directory is included, include all files and subdirectories.
- If a directory does not match the include set, the status stays neutral and only the selected directories are scanned.
- If no directories are included or excluded, the status is set to include.

File Scanning:

- If a file is excluded, that file is not reported.
- If a file is included, that file is reported.
- If no files are included or excluded, the default status is set to include.

Sample Configuration

The following is a sample of a custom attribute in INI format.

```
[FILTERS_WINDOWS]
FILTER0=INCLUDE, VOLUME, "C:"
FILTER1=EXCLUDE, FILEPATH, "<WINDIR>\INSTALL*"
FILTER2=EXCLUDE, FILEPATH, "<WINSYSDIR>\DLLCACHE\"
```

```
FILTER3=EXCLUDE, FILEPATH, "<WINSYSDIR>\DRIVERS\"
FILTER4=EXCLUDE, FILENAME, "SETUP*"
FILTER5=EXCLUDE, FILEPATH, "\RECYCLE*"
FILTER6=EXCLUDE, FILEPATH, "\SYSTEM VOLUME INFORMATION*"
FILTER7=EXCLUDE, FILEPATH, "*\TEMPORARY INTERNET FILES\*"
FILTER8=EXCLUDE, FILEPATH, "*\LOCAL SETTINGS\TEMP\*"
FILTER9=EXCLUDE, FILEPATH, "*\LOCAL SETTINGS\HISTORY\*"
FILTER10=EXCLUDE, FILEPATH, "*DLLCACHE*"
FILTER11=EXCLUDE, FILEPATH, "*$NTUNINST*"
FILTER12=EXCLUDE, FILEPATH, "*$NTSERVICEPACKUNINSTALL$*"
FILTER13=EXCLUDE, FILEPATH, "\I386"
FILTER14=EXCLUDE, FILEPATH, "*SP4\*"
FILTER15=EXCLUDE, FILEPATH, "*$HF_*"
FILTER16=EXCLUDE, FILEPATH, "*SERVICEPACKFILES*"
FILTER17=EXCLUDE, FILEPATH, "<WINSYSDIR>\WinSxS\"
FILTER18=INCLUDE, FILEPATH, "\DOCUMENTS AND SETTINGS*"
FILTER19=INCLUDE, FILEPATH, "\PROGRAM FILES*"
FILTER20=EXIST, PRODUCT
FILTER21=EXIST, VERSION

[FILTERS_UNIX]
FILTER0=EXCLUDE, FILENAME, "*.dll"
FILTER1=EXCLUDE, FILENAME, "*.com"
FILTER2=EXCLUDE, FILENAME, "*.cmd"
FILTER3=EXCLUDE, FILENAME, "*.html"
FILTER4=INCLUDE, FILEPATH, "/etc*"
FILTER5=INCLUDE, FILEPATH, "/opt*"
FILTER6=INCLUDE, FILEPATH, "/bin*"
FILTER7=INCLUDE, FILEPATH, "/usr/bin*"
FILTER8=INCLUDE, FILEPATH, "/usr/lib*"
FILTER9=INCLUDE, FILEPATH, "/usr/games*"
FILTER10=INCLUDE, FILEPATH, "/usr/sbin*"
FILTER11=EXCLUDE, FILEPATH, "/cygdrive*"
FILTER12=EXCLUDE, FILEPATH, "/lost+found*"
FILTER13=EXCLUDE, FILEPATH, "/proc*"
FILTER14=EXCLUDE, FILEPATH, "/tmp*"

[METHODS]
DELTA_SCAN=TRUE

[CONFIGURATION]
LOG_MODE=LOW
INCLUDE_SYMBOLIC_LINKED_FILES=FALSE
INCLUDE_SYMBOLIC_LINKED_DIRS=FALSE
```

Concurrency and Multi-User Considerations

Software Discovery is configured to look at a Snapshot before attempting to run the inventory Snapshot. If an inventory Snapshot is available, the results are immediately displayed instead of running a new inventory Snapshot. However, if two users initially run an inventory

Snapshot, one of the instances will be accepted and run an inventory Snapshot. The other user will see a message when attempting to view the Discovered Software server module in the Device Explorer alerting them that an inventory Snapshot is already in progress.

If Software Discovery is used during an ad-hoc or scheduled Snapshot job, the data from the Discovered Software server module is persisted as a Snapshot package (snapshot.zip) on the SA core. These zip packages are used, for example, by the SAS Web Client when it needs to perform an Audit operation.

Software Discovery Usage Examples

The Software Discovery discovery mechanism can be useful in case of inherited servers and other usage examples. Some examples are listed below:

Example 1

You are an IT Administrator at a company that has 500 managed servers in your data center. You want to know how many servers have 1.3 Java JRE installed. You create a new Audit and select a source server that you know has Java JRE installed. You perform the following steps:

1. From the Discovered Software tab under Rules select and expand Software Node.
2. Selects JRE installed on the source server and add an additional regex property check for version='1\.3.*'.
3. Form the Targets tab select all the active servers in the lab.
4. Save and run the audit to check all the managed servers in the lab for 1.3 versions of Java JRE.

The results come back and you see there are still some servers that are not compliant and proceed to update the remaining servers.

Example 2

For the next task, you want to check all 64-bit machines and see what 32-bit applications were installed. You create a new policy and add your own configuration for Software Discovery using the `HPSW_DS_SM_CONFIG` custom attribute. In that attribute, you assign the following options:

```
[FILTERS_WINDOWS]
FILTER0=INCLUDE, VOLUME,   "C:"
FILTER1=INCLUDE, FILEPATH, "\PROGRAM FILES (X86)*"

[METHODS]
DELTA_SCAN=TRUE

[CONFIGURATION]
LOG_MODE=LOW
```

You attach all the 64-bit Windows 2003 Servers to the new policy and remediate the machines. Next, you create a new snapshot including all 64-bit Windows 2003 Servers and select the wildcard under the Discovered Software tab.

You save the snapshot and proceed to run the snapshot against all the 64-bit Windows 2003 Servers. Results come back and now you have a list of all the 32-bit applications deployed across all the 64-bit Windows 2003 Servers.

Example 3

You are auditing the lab to make sure all Windows servers have the appropriate virus detection software installed. You create a new Audit and select a source server you know has the correct software installed. You navigate to the Discovered Software tab and select Norton Antivirus under the Software node.

You include all the Windows machines in the lab as target machines and then save the Audit. The Audit is then run and the results come back with half the machines in the lab non-compliant. You proceed to install Norton Antivirus on the remainder noncompliant servers.

Extending Software Discovery

While Software Discovery can discover a very large number and a wide variety of applications, you can extend this feature by adding your own Python scripts to perform custom software discovery. To extend Software Discovery, perform the following steps.

1. Write your custom software discovery code in Python as described in Writing Custom Software Discovery Code on page 107.
2. Package your Python file into a zip file.
3. In the SA Client, select Library in the navigation panel.
4. Select the By Folder tab.
5. Create the following folder. You will import your zip file and create a software policy in this folder. Make sure you have adequate permission to create this folder. See the *SA Administration Guide* for details on permissions.

   ```
   Library/Opsware/Tools/Server Modules/
   com.opsware.server.module.discovered_software.ext/
   ```

   To create this folder, you need write permission on the parent folder. For more information, see “Folder Permissions” in the *SA Administration Guide*.
6. Import your zip file to this folder. Right click and select **Import Software...** or select the **Actions ➤ Import Software...** menu item. For details, see Importing Software Packages on page 35.
7. Open the zip package and set the Default Install Path to one of the following.
   - For UNIX servers set the default install path to:

   ```
   /opt/opsware/sm/com.opsware.server.module.discovered_software.ext
   ```

   - For Windows servers set the default install path to:

```
%PROGRAMFILES%\Opsware\sm\com.opsware.server.module.discovered_software.ext
```

   For details, see Viewing Package Properties on page 41 and Editing Package Properties on page 44.

8 In the same folder (from step 5 above), create a software policy named com.opsware.server.module.discovered_software.ext. Right click and select **New software policy...** or select the **Actions ➤ New software policy...** menu item. For details, see Creating Software Policies and Software Templates on page 21.

9 Add your imported zip file to the software policy. Open the software policy, select the Policy Items view, and select the "+" button. For details, see Adding Software Resources to a Software Policy on page 26.

10 On the core server, run the smtool command with the `--upgrade` and `--force_upgrade` options. Specify the user name and password of an SA user with the "Manage Server Module: Read & Write" permission. Specify the Software Discovery zip package that you downloaded from BSA Essentials as described in Downloading the Software Discovery Package on page 91. For example:

```
smtool --username=<user name> --password=<password> --upgrade
--force-upgrade OPSWsmo_discovered_software-<version>.zip
```

This command adds your custom software discovery package to the Discovered software policy. `OPSWsmo_discovered_software-<version>.zip` is the Software Discovery package downloaded from the BSA Essentials Network as described in Downloading the Software Discovery Package on page 91.

For more information on the smtool, run `smtool --help`. The smtool command is located on the SA core server in the directory `/opt/opsware/smtool`. For more information on SA permissions, see Software Discovery Permissions on page 92 and the *SA Administration Guide*.

11 Run your custom software discovery code as described in Deploying Software Discovery Using Inventory Snapshots on page 93.

Writing Custom Software Discovery Code

This section describes how to write custom Python code to discover software that is not already discoverable by the SA Software Discovery feature. For instructions on how to integrate your custom code into SA, see Extending Software Discovery on page 106.

- The Python script must contain a `discover()` function that takes a list argument named objects, and returns a tuple of `(objects, merge_flag)` where `objects` is a list and `merge_flag` is an integer.
- The `objects` argument contains all the software objects Software Discovery has found. The returned list contains either the list of objects passed into the `discover()` function merged with the software objects discovered by your extension, or only the software objects discovered by your extension, depending on the integer value returned in the second parameter. See below for an example.
- The integer value, `merge_flag`, returned by the `discover()` function must be 0, 1 or 2 as described in the following table.

Table 5 Integer Value Returned by the discover() Function

Value Returned	Meaning
0	Your extension has merged the software objects passed in to the `discover()` function with the software objects it has found and returns the union of these two sets.

Table 5 Integer Value Returned by the discover() Function (cont'd)

Value Returned	Meaning
1	Your extension returns only the software objects it has found. The Software Discovery server module will merge the returned objects with its list of software objects. If there is a conflict, the software objects discovered by your extension will take precedence.
2	Your extension returns only the software objects it has found. The Software Discovery server module will merge the returned objects with its list of software objects. If there is a conflict, the software objects discovered by the Software Discovery server module will take precedence.

- The file name of your Python script must be in the following format:

  `ds_ext_<unique name>.py.`

  The <unique name> must be unique in all extensions in both the HP Software Discovery directory and the software discovery extensions directory.

  Best Practice: As a best practice, use your company name in the <unique name> to avoid conflicts. For example, the following could be a script from the "abc company": `ds_ext_abcco_app.py`.

- The `discover()` function will be called after the Software Discovery server module runs and before it returns the result to the caller.

- Below is a sample implementation of the `discover()` function that returns a list containing one simulated software object:

```
def discover(objects):
    obj = {
        'opswType': 'software',
        'FILENAME': '/usr/local/bin/,
        'FILEPATH': 'my_util',
        'primaryKey': '/usr/local/bin/my_util',
        'VERSION': '1.3.0.1',
        'DISPLAY_VERSION': '1.3',
        'PRODUCT': 'My Util',
        'DISPLAY_PRODUCT': 'My Util',
        'VENDOR': 'abc co',
        'DISPLAY_VENDOR': 'abc co',
        'VOLUME': '',
        'FILESIZE': 32656,
        'FILEVER': '1.3.0.1',
        'FILEDATE': '2008-12-02 01:03:38'
    }
    return ([obj], 1)
```

- After writing your software discovery code, integrate it into SA as described in Extending Software Discovery on page 106.

B ISM Controls Reference

About Running ISM Controls

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 on page 112.

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. Adding Software Resources to a Software Policy on page 26 and Attach a Software Policy to a Server or Device Group on page 62.

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.

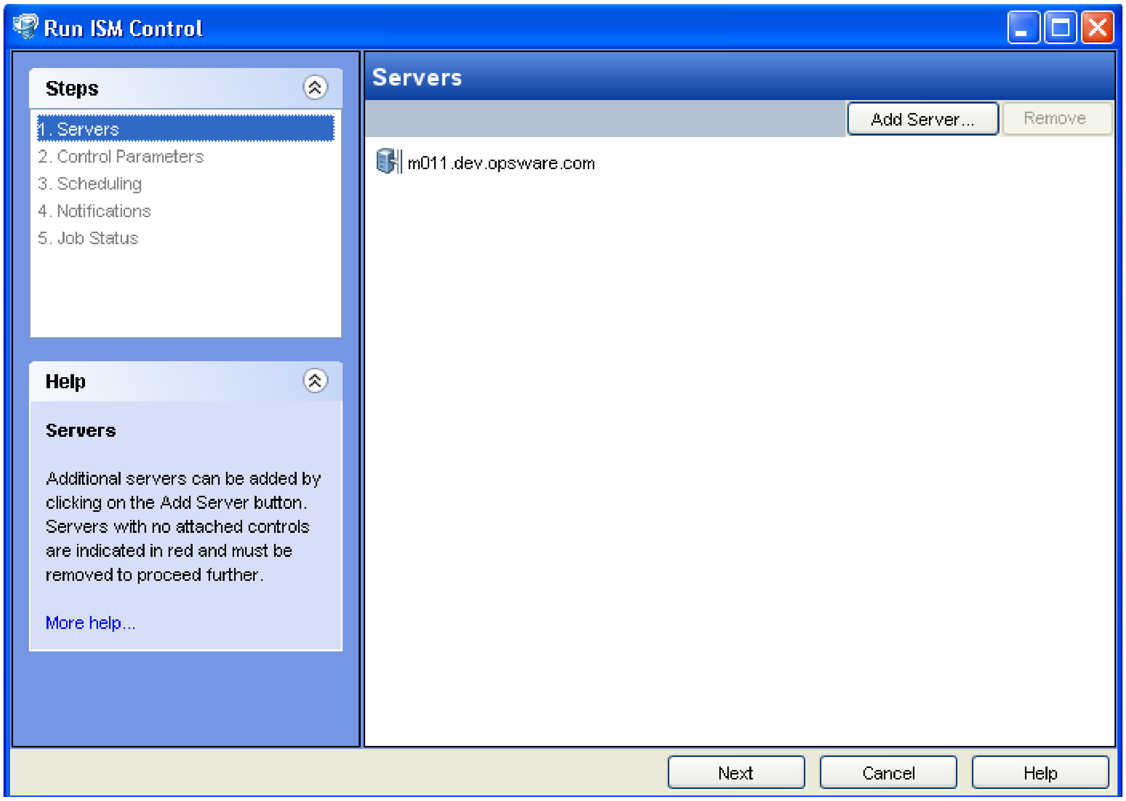
c From the **View** drop-down list, select **Server Usage**. A list of the servers attached to this policy appears in the lower pain. Select a server, and then select **ISM Control** from the **Actions** menu. The Run ISM Control window appears.

Running ISM Controls

Use the Run ISM Control window (Figure 16) 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

Figure 16 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 on page 109.
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.

➤ 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 on page 26 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 on page 109 for more information about running ISM controls.

The name of a parameter matches the name of its corresponding custom attribute. 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.

C Package Type Reference

This appendix describes the SA supported software packages, including:

- Supported Operating Systems and Package Types
- AIX Packages
- HP-UX Packages
- Linux Packages
- Solaris 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 Table 6.

Table 6 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 Installation Media	.zip	N/A
	Executable	.exe, .sh	N/A
HP-UX	Depot (contains products and filesets)	.tar, .depot	N/A
	ZIP	.zip	N/A
	Application Installation Media	.zip	N/A
	Executable	.exe, .sh	N/A

Table 6 Supported Operating Systems and Package Types (cont'd)

Operating System	Package Type	File Formats	Additional Metadata
Linux	RPM	.rpm	N/A
	ZIP	.zip	N/A
	Application Installation Media	.zip	N/A
	Executable	.exe, .sh	N/A
Solaris	Patch	.jar, .tar, tar.gz, .tar.Z, t.gz, .zip	N/A
	Patch Cluster (contains patches)	.tar, .tar.gz, tar.Z, .tgz, .zip	N/A
	Solaris package (contains package instances)	.pkg, .tar	N/A
	RPM	.rpm	N/A
	ZIP	.zip	N/A
	Application Installation Media	.zip	N/A
	Executable	.exe, .sh	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 (Microsoft Security Baseline Analyzer and qchain)	.exe	N/A
	Microsoft Patch Database (contains a description of available patches) See the *SA User Guide: Server Patching* for more information.	.xml, .cab	N/A
	ZIP	.zip	N/A

Table 6 Supported Operating Systems and Package Types (cont'd)

Operating System	Package Type	File Formats	Additional Metadata
	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.

AIX 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

➤ 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.

➤ 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.

➤ 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.

➤ 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.

➤ For more information on creating a script to automate this step, see Example: File – Script to Split a Depot by Product on page 118 and Example: File – Script to Split a Depot by Bundle on page 118.

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
```

Linux 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 an RPM Package on page 28 for more information.

Solaris 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.
- 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 on page 61 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 Package 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
```

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 operating systems:

- Windows
- Unix

ZIP Packaging

Use ZIP packages primarily to deliver code that can be run on a server. You can also use them to deliver application files for installing applications.

When a user installs a ZIP package on a server, the files are automatically extracted and saved to a directory that the user selects; 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 standalone 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 files on SA. You can download the.zip 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.

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 (OCLI).

  When the encoding is specified, the SAS 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 SAS 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)