

# 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: Server Patching

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

© Copyright 2001-2011 Hewlett-Packard Development Company, L.P.

### 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

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

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

## Support

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

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](http://h20230.www2.hp.com/new_access_levels.jsp)**



# Contents

1	Quick Start to Patch Management	11
2	Patch Management for Windows	13
	Overview	13
	Features	14
	Types of Patch Browsing	14
	Scheduling and Notifications	14
	Patch Policies and Exceptions	14
	Patch Installation Preview	15
	Patch Uninstallation Preview	15
	Exporting Patch Data	15
	SA Client Library	16
	Prerequisites	17
	Patch & Patch Policy Search	17
	Windows Server 2008 Patch Management Support	17
	Microsoft Patch Database	19
	SA Integration	20
	Support for Windows Patch Testing and Installation Standardization	20
	Supported Technologies for Patch Management	20
	Windows Hotfixes—qchain.exe and Reboot	21
	Roles for Windows Patch Management	22
	Predefined Patch User Groups	23
	Patch Management Process	24
	Patch Management Tasks	26
	Viewing Patch Information	26
	Patch Dependencies and Supersedence	26
	Viewing Windows Patches	27
	Editing Windows Patch Properties	27
	Importing Custom Documentation for a Patch	28
	Deleting Custom Documentation for a Patch	28
	Finding Vendor-Recommended Windows Patches	28
	Finding Servers That Have a Windows Patch Installed	29
	Finding Servers That Do Not Have a Windows Patch Installed	29
	Importing a Patch	29
	Importing Windows Patches	30
	Exporting a Windows Patch	32
	Exporting Windows Patch Information	32
	Policy Management	34
	Patch Policy	34

Patch Policy Exception . . . . .	35
Precedence Rules for Applying Policies . . . . .	36
Remediation Process . . . . .	36
Remediating Patch Policies . . . . .	37
Setting Remediate Options . . . . .	38
Setting Reboot Options for Remediation . . . . .	38
Specifying Pre and Post Install Scripts for Remediation . . . . .	39
Scheduling a Patch Installation for Remediation . . . . .	40
Setting Up Email Notifications for Remediation . . . . .	40
Previewing and Starting a Remediation . . . . .	41
Verifying Patch Policy Compliance . . . . .	42
Creating a Patch Policy . . . . .	43
Deleting a Patch Policy . . . . .	43
Adding a Patch to a Patch Policy . . . . .	43
Removing a Patch from a Patch Policy . . . . .	44
Attaching a Patch Policy to a Server . . . . .	44
Detaching a Patch Policy from a Server . . . . .	45
Setting a Patch Policy Exception . . . . .	45
Finding an Existing Patch Policy Exception . . . . .	46
Copying a Patch Policy Exception . . . . .	46
Removing a Patch Policy Exception . . . . .	47
Patch Compliance . . . . .	47
Patch Compliance Scans . . . . .	47
Ways to Start a Patch Compliance Scan . . . . .	47
Starting a Patch Compliance Scan Immediately . . . . .	48
Refreshing the Compliance Status of Selected Servers . . . . .	48
Viewing Scan Failure Details . . . . .	48
Patch Compliance Icons . . . . .	49
Patch Compliance Levels . . . . .	49
Patch Compliance Rules . . . . .	50
Patch Administration . . . . .	51
Prerequisite for Importing the Patch Database & Utilities . . . . .	51
Setting Patch Availability . . . . .	51
Importing the Microsoft Patch Database . . . . .	52
Selecting Windows Products to Track for Patching . . . . .	53
Scheduling a Patch Compliance Scan . . . . .	53
Setting a Patch Compliance Level . . . . .	54
Importing Windows Patch Utilities . . . . .	54
Exporting Windows Patch Utilities . . . . .	55
Finding Servers that Require a Reboot . . . . .	55
Patch Locales . . . . .	57
Supported Locales . . . . .	57
Locale Configuration Tasks . . . . .	57
Patch Installation . . . . .	59
Installation Flags . . . . .	60
Application Patches . . . . .	61
Service Packs, Update Rollups, & Hotfixes . . . . .	61

Installing a Windows Patch .....	62
Setting Windows Install Options .....	63
Setting Reboot Options for a Windows Patch Installation .....	63
Specifying Install Scripts for a Windows Patch Installation .....	64
Scheduling a Windows Patch Installation .....	65
Setting Up Email Notifications for a Windows Patch Installation .....	66
Previewing a Windows Patch Installation .....	66
Viewing Job Progress of a Windows Patch Installation .....	67
Patch Uninstallation .....	68
Uninstallation Flags .....	69
Uninstalling a Windows Patch .....	69
Setting Uninstall Options .....	70
Setting Reboot Options for a Windows Patch Uninstallation .....	71
Specifying Install Scripts for a Windows Patch Uninstallation .....	72
Scheduling a Windows Patch Uninstallation .....	73
Setting Up Email Notifications for a Windows Patch Uninstallation .....	73
Previewing and Starting a Windows Patch Uninstallation .....	74
Viewing Job Progress of a Patch Uninstallation .....	74
<b>3 Patch Management for HP-UX .....</b>	<b>75</b>
Overview .....	75
Features .....	75
Prerequisites .....	76
Supported Operating Systems .....	76
HP-UX Depots .....	76
HP-UX Software Catalog File .....	78
Software Policy Management .....	79
Creating an HP-UX Software Policy .....	79
Viewing an HP-UX Software Policy .....	81
Editing an HP-UX Software Policy .....	83
Adding an HP-UX Patch to a Software Policy .....	83
Removing Software from a Software Policy .....	84
Viewing Software Policy History .....	84
Viewing Servers Attached to a Software Policy .....	85
Finding a Software Policy in Folders .....	85
Custom Attributes .....	86
Patch Compliance .....	87
Patch Installation .....	89
Installation Flags .....	89
Installing an HP-UX Patch .....	90
Setting HP-UX Install Options .....	90
Setting Reboot Options .....	91
Specifying Install Scripts .....	92
Scheduling a Patch Installation .....	92
Setting Up Email Notifications .....	93
Previewing a Patch Installation .....	93
Viewing Job Progress .....	94

Patch Uninstallation .....	95
<b>4 Patch Management for Solaris .....</b>	<b>97</b>
Overview .....	97
Features .....	97
Policy-based Patch Management .....	98
Solaris Patch Bundles .....	99
Fujitsu Clusters .....	100
Quick Start .....	101
Patch Management Process .....	102
Patching Servers .....	102
Installing Patches .....	104
Patch Compliance .....	105
Running a Patch Compliance Scan .....	107
Patch Policy Management .....	107
Creating a Solaris Patch Policy .....	108
Viewing a Solaris Patch Policy .....	110
Editing a Solaris Patch Policy .....	111
Adding a Solaris Patch to a Patch Policy .....	111
Removing a Patch from a Solaris Patch Policy .....	112
Resolving Patch Dependencies .....	113
Custom Attributes .....	116
Viewing Patch Policy History .....	117
Viewing Software Policies Associated with a Patch Policy .....	117
Viewing OS Sequences Associated with a Patch Policy .....	117
Viewing Servers Attached to a Patch Policy .....	118
Finding a Solaris Patch Policy in Folders .....	118
Patch Management Tasks .....	119
Running solpatch_import .....	119
Initializing the Solaris Patch Database .....	120
Maintaining the Solaris Patch Database .....	121
Finding Solaris Patches .....	122
Importing a Patch or Patch Cluster .....	125
Exporting a Patch or Patch Cluster .....	126
Opening a Solaris Patch .....	127
Managing Properties .....	127
Importing Custom Documentation .....	132
Patches and Patch Clusters .....	132
Solaris Zones .....	134
Installing a Patch .....	135
Installing a Patch Cluster .....	135
Installing Manual Patches—patchadd .....	135
Detecting Benign Error Codes .....	136
Installing Patches Using a Patch Policy .....	136
Remediating a Server Against a Patch Policy .....	138
Troubleshooting Patch Installation .....	140
Installing Patches Using Offline Volumes .....	141



Uninstalling a Patch .....	142
<b>5 Patch Management for Unix .....</b>	<b>143</b>
Overview .....	143
Tracking Patches on Managed Servers .....	145
Support for Unix Patch Testing and Installation Standardization .....	145
Viewing Patches in the SA Client .....	146
Searching for Patches .....	146
Patch Management Roles for Unix .....	147
Patch Management for Specific Unix Operating Systems .....	148
Supported Unix Versions and Patch Types .....	148
Underlying Technologies for Patch Management on Unix .....	148
AIX Patches .....	149
Solaris Patches .....	150
HP-UX Patches .....	150
Uploading Unix Patches into the SA Library .....	150
Unix Patch Information .....	151
Patch Properties View .....	152
Contents View .....	152
Depots View—HP-UX Only .....	152
Patch Products View—HP-UX Only .....	153
Patch Clusters View—Solaris Only .....	153
LPPs/APARs View—AIX Only .....	153
Software Policies View .....	153
Patch Policies View .....	153
Servers View .....	153
Viewing and Editing Unix Patch Properties .....	153
Finding Servers That Have a Unix Patch Installed .....	154
Exporting a Patch .....	154
Deleting a Patch .....	154
Using Software Policies to Manage Patches .....	155
Patch Compliance Reports .....	155
Patch Administration for Unix .....	156
Setting the Default Patch Availability .....	156
Patch Installation .....	156
Installation Flags .....	157
Application Patches .....	157
Installing a Patch .....	158
Setting Install Options .....	159
Setting Reboot Options .....	159
Specifying Install Scripts .....	160
Scheduling a Patch Installation .....	161
Setting Up Email Notifications .....	161
Previewing a Patch Installation .....	162
Viewing Job Progress for a Patch Installation .....	162
Patch Uninstallation .....	163
Uninstallation Flags .....	163

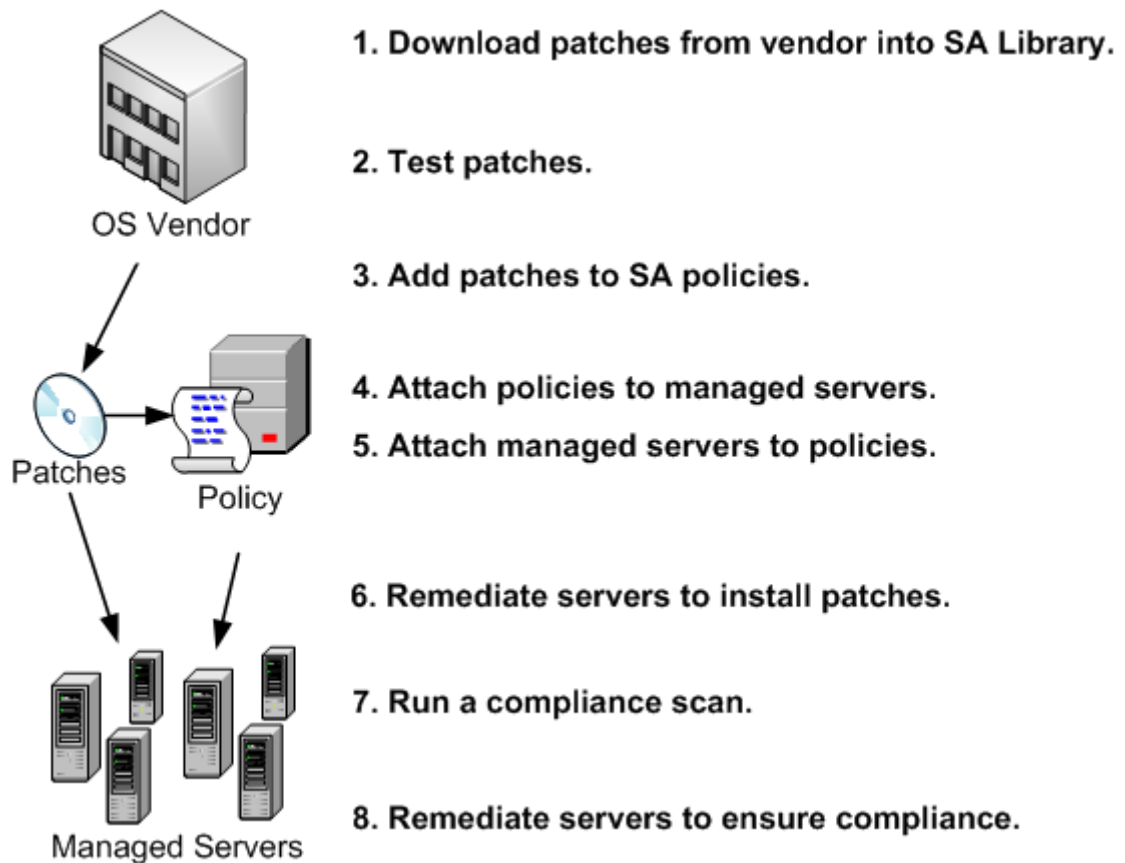
Uninstalling a Patch .....	164
Setting Uninstall Options .....	165
Setting Reboot Options .....	165
Specifying Pre and Post Install Scripts .....	166
Scheduling a Patch Uninstallation .....	166
Setting Up Email Notifications .....	167
Previewing a Patch Uninstallation .....	167
Viewing Job Progress for a Patch Uninstallation .....	167

# 1 Quick Start to Patch Management

This quick start is an overview of how to download, install, and maintain patches on SA managed servers in your IT environment. This section identifies the steps required to set up and manage patches for all supported operating systems.

Figure 1 shows the general workflow for downloading patches, testing them, adding them to SA policies, attaching policies to servers, attaching servers to policies, remediating servers to install patches, running compliance scans to determine which servers are out of compliance, and remediating servers to bring them back into compliance. SA policies are either patch policies or software policies, and are used according to the operating system you are patching.

**Figure 1 Patch Management Workflow**



For detailed information about SA patch management for a certain operating system, see the following sections:

- [Patch Management for Windows](#) on page 13
- [Patch Management for HP-UX](#) on page 75
- [Patch Management for Solaris](#) on page 97
- [Patch Management for Unix](#) on page 143

## 2 Patch Management for Windows



### Overview

In Server Automation (SA), patch management for Windows enables you to identify, install, and remove Microsoft® Windows patches, and maintain a high level of security across managed servers in your organization. You can identify and install patches that protect against security vulnerabilities for the following Windows operating systems:

- Windows 2000, Service Pack 4
- Windows Server 2003
- Windows Server 2003 x64
- Windows Server 2008
- Windows Server 2008 x64
- Windows Server 2008 R2 x64
- Windows XP x86, Service Pack 2 and higher

See the *Server Automation Compatibility Matrix* for more information.

SA automates the key aspects of patch management, while offering a fine degree of control over how and under what conditions patches are installed. By automating the patching process, patch management can reduce the amount of downtime required for patching. SA also allows you to schedule patch activity, so that patching occurs during off-peak hours.

Because Windows patches are often released to address serious security threats, an organization must be able to roll out patches quickly, before systems are compromised. However, at the same time, patches themselves can cause serious problems, from performance degradation to server failures.

While patch management allows you to react quickly to newly discovered threats, it also provides support for strict testing and standardization of patch installation. And, if patches cause problems, even after being tested and approved, Windows patching also allows you to uninstall the patches in a safe and standardized way.

This documentation contains information about how to install Windows patches using patch policies and how to uninstall patches using a sequence of tasks. It also contains information about running patch compliance scans and generating patch policy compliance reports.

# Features

SA automates Windows patching by providing the following features and capabilities:

- A **central repository** where patches are stored and organized in their native formats
- A **database** that stores information about every patch that has been applied
- **Customized scripts** that can be run before and after a patch is installed
- **Advanced search** abilities that identify servers that require patching
- **Auditing abilities** for tracking the deployment of important patches

These features and capabilities enable you to browse patches by a certain operating system, schedule patch downloads and installations, set up email notifications, preview a patch installation, use policies and remediation to install patches, and export patch information to a reusable file format.

## Types of Patch Browsing

The SA Client interface organizes Windows patches by operating systems and displays detailed vendor security information about each patch, such as *Microsoft Security Bulletins*. You can browse patches by the date Microsoft released the patch, by the severity level, Security Bulletin ID, QNumber, and so on. You can also browse all patches that are installed on a server, and view and edit patch metadata.

## Scheduling and Notifications

In the SA Client, you can separately schedule when you want patches to be imported from Microsoft into Server Automation, either by a schedule or on demand, and when you want these patches to be downloaded to managed servers.



**Best Practice:** Schedule patch installations for a day and time that minimize disruption to your business operation.

Windows patching also allows you to set up email notifications that alert you when the download and installation operations completed, succeeded, or failed. When you schedule a patch installation, you can also specify reboot preferences to adopt, override, postpone, or suppress the vendor's reboot options.

## Patch Policies and Exceptions

To provide flexibility in how you identify and distribute patches on managed servers or groups of servers, Windows patching allows you to create patch policies that define groups of patches you need to install.

By creating a patch policy and attaching it to a server or a group of servers, you can effectively manage which patches get installed where in your organization. If you want to *include* or *exclude* a patch from a patch installation, patch management allows you to deviate from a patch policy by specifying that a certain patch is a *patch policy exception*.

An additional patch is one that is not already specified in the patch policy and is one that you want to *include* in (add to) the patch installation. A patch that you want to *exclude* from a patch installation is one that is already specified in a patch policy and is identified in the patch policy exception as one you do not want installed.



**Best Practice:** In cases where it is already known that a certain Windows patch may cause a server or application to malfunction, you should create a patch policy exception to exclude it from being installed on that server or on all servers that have that application.

## Patch Installation Preview

While patch management allows you to react quickly to newly discovered security vulnerabilities, it also provides support for strict testing and standardization of patch installation.

After you have identified patches to install, patch management allows you to simulate (preview) the installation before you actually install a patch. Use the preview process to identify whether the servers that you selected for the patch installation already have that patch installed. In some cases, a server could already have a patch installed if a system administrator had manually installed it.

After this type of patch installation, if a compliance scan has not been run or the installed patch has not been registered, SA does not know about it. The preview process for an up-to-date report of the patch state of servers. The preview process also reports on patch dependency and supersedence information, such as patches that require certain Windows products, and patches that supersede other patches or are superseded by other patches.

## Patch Uninstallation Preview

Patch management also provides a solution for remediating servers that are not operating properly due to installed patches. If installed patches cause problems, even after being tested and approved, Windows patching allows you to uninstall patches in a safe and standardized way. You can specify uninstall options that control server reboots and the execution of uninstall commands, and pre-uninstall and post-uninstall scripts. Similar to previewing a patch installation, you can also preview a patch uninstallation.

## Exporting Patch Data

To help you track the patch state of servers or groups of servers, patch management allows you to export this information. This information can be exported in a comma-separated value (.csv) file and includes details about when a patch was last detected as being installed, when a patch was installed by Server Automation, the patch compliance level, what patch policy exceptions exist, and so on. You can then import this information into a spreadsheet or database to perform a variety of patch analysis tasks.

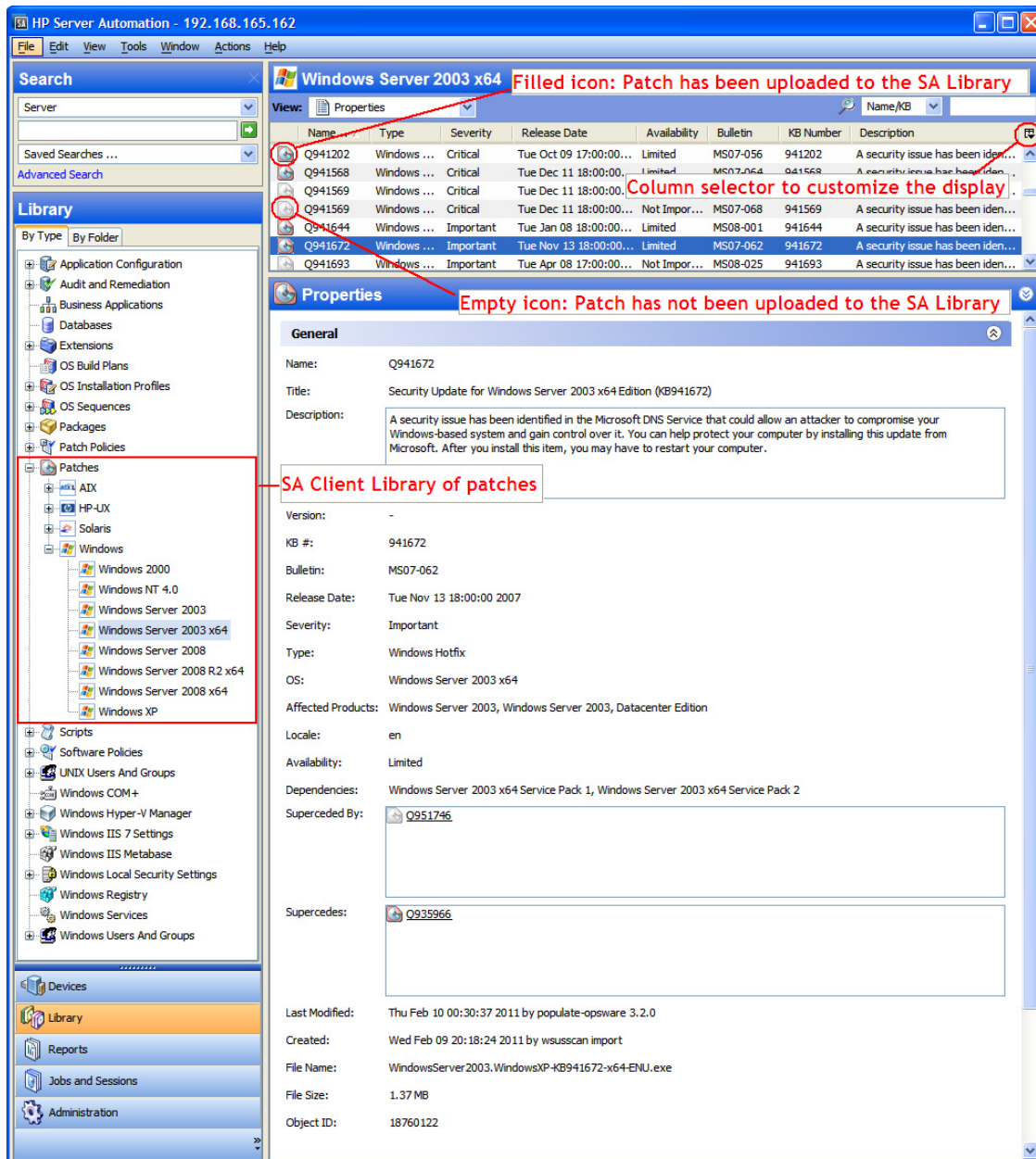
# SA Client Library

The SA Client Library provides flexibility in searching for and displaying Microsoft patches by bulletin ID, release date, severity level, operating system, and so on. See [Figure 2](#).

In the content pane, a dimmed patch icon indicates that the patch has not been uploaded to the Library. Use the column selector to control the columns of patch metadata data that you want to display.

Since the Library is integrated with Microsoft patch metadata, you can review vendor information *in real-time* in the preview pane.

**Figure 2 Windows Patches in the SA Client Library**





## Prerequisites

The managed servers that will be patched have the following requirements:

- Either Microsoft Core XML Services (MSXML) 3.0 (or later), or Internet Explorer (IE) 6.0 (or later) must be installed on the managed servers. These versions of MSXML and IE support the Microsoft XML parser and related DLL files.
- Windows Installer 3.1 must be installed on managed servers that are running Windows 2000, Windows 2003, or Windows XP. This installer is available at the following URL:  
<http://support.microsoft.com/kb/893803/>
- On the managed servers, the Windows Update service must be set to either Automatic or Manual. To set a Windows service, from the Windows Control Panel select **Administration Tools ► Services**.
- For Windows Server 2008, the Add and Remove Programs dialogue must be closed when you run Windows patch management tasks.
- For Windows XP managed servers, SP2 or higher must be installed.
- To install and uninstall patches, and to perform remediation, the SA Agent must be version 5.5 or later.
- To use patch management on managed servers with SA Agent versions earlier than 6.1, the language (locale) of the managed server must be either English, Japanese, or Korean. To set the language, on the managed server, open the Control Panel, open the Regional and Language Options window, select the Regional Options tab, and then select a language from the drop-down list in the “Standards and formats” section. Click **OK** to save your changes.

See the *Server Automation Compatibility Matrix* for more information.

## Patch & Patch Policy Search

In the SA Client, you can search for information about your operational environment by using the SA Client Search feature. The Search feature enables you to search for patches, patch policies, servers, and so on. See “SA Client Search” in the *SA User Guide: Server Automation*.

## Windows Server 2008 Patch Management Support

As of Server Automation 9.0, Windows Server 2008 x86, Windows Server 2008 x64, and Windows Server 2008 R2 Patch Management are supported. SA patch management for Windows enables you to identify, install, and remove Microsoft® Windows patches and maintain a high level of security across managed servers in your organization.

SA Windows Server 2008 patch management support is compatible with a mixed-version multimaster mesh (where both patched and unpatched cores co-exist) with the following caveats:

- Install, uninstall, and remediation of Windows Server 2008 patches work correctly only if invoked from an SA 9.0 core.
- Managed servers that register to a pre-SA 9.0 core can have an incorrect compliance status and server patch list. However, after the core is patched, the data is corrected after the next patch compliance scan.
- The Windows Update patch database must be imported from a patched core.

SA patch management for Windows Server 2008 is similar to that for Windows Server 2003. In addition to the Windows platform patch management functions, after Server Automation 9.0 is installed the following will apply:

- Windows Server 2008 patches will appear under Library after the patch database is imported.

- You can select `Windows Server 2008` under **Administration** ► **Patch Settings** ► **Windows Patch Downloads** ► **Patch Products** to specify whether to import Windows Server 2008 patch metadata.
- Windows Server 2008 patches can be managed just like patches for other Windows platforms. You can:
  - Invoke a patch browser to edit patch properties, descriptions, and reboot/install/uninstall flags.
  - See the following patch views when a Windows Server 2008 server is selected.
    - Patches Needed
    - Patches Recommended By Vendor
    - Patches with Policies or Exceptions
    - Patches Installed
    - Patches with Exceptions
    - All Patches
- You can import patch binaries from the vendor using the SA Client or from a file.
- You can attach Windows Server 2008 patch policies to servers and server groups.
- You can define patch policy exceptions for Windows Server 2008 patches on servers and server groups.

## The `populate-opsware-update-library` Script

This script has been updated to include the following command line arguments:

- `no_w2k8`  
specifies Windows Server 2008 x86 patch binaries should not be uploaded.
- `no_w2k8x64`  
specifies Windows Server 2008 x64 patch binaries should not be uploaded.

## Policies and Exceptions for Windows Server 2008 Patches

SA provides a recommended patch policy for Windows Server 2008 x86 and patch policy for Windows Server 2008 x64. You can also define additional custom patch policies in the same way as described in the *SA User Guide: Application Automation*.

## Remediate and Ad-hoc Install/Uninstall

Similar to Windows Server 2003, you can remediate Windows Server 2008 patch policies and perform ad-hoc Windows Server 2008 patch installations and uninstallations. Windows Server 2008 patches can be remediated in software policies and ad-hoc installations using install/uninstall software. However, software compliance does not account for applicability. This is consistent with other Windows Server platform patches contained in software policies.

## Patch Compliance

You can perform patch compliance scans on Windows Server 2008 servers to determine compliance relative to attached 2008 policies and exceptions. Patch compliance is based on patch applicability on the selected server(s).

The Compliance view in the SA Client displays compliance details for Windows Server 2008 servers, just as it does for other Windows servers.

## Known limitations

- The Install/Uninstall Patch window typically allows you to specify install/uninstall flags when a patch is selected for installation/uninstallation. The patch must be in an .EXE file format. Microsoft delivers Windows Server 2008 patches in both .EXE and .CAB format. In SA, if a patch is in .CAB file format, you cannot specify install/uninstall flags in the Patch, Install Patch, and/or Uninstall Patch windows because command-line arguments are not supported for .CAB format patches.
- If you add install or uninstall flags using the Windows patch browser, any flags that SA would otherwise have used are overwritten.

**Note:** Overriding the `-q` flag (if the patch supports `-q`) will cause the patch installation to fail. This type of installation failure can take as long as one hour to time out.

Therefore, if you must use additional flags in a Windows patch browser, you must specify the `-q` flag with your additional flags. For example, if you want to log the install/uninstall process and do not want to override the default flags, specify the following:

```
/log:c:\mylog.txt /q /z
```

- Prior to the introduction of Windows Server 2008 .CAB patches, each Windows patch identified specific applicable locales, such as `en` for English servers, `ja` for Japanese servers, and so on.
  - The locale of CAB patches can be `ALL`, which means the patch can be applicable for servers of all locales.
  - When you view vendor documentation for a .CAB patch, only the English version is displayed.

## Microsoft Patch Database

The Microsoft patch database contains information about released patches and how they should be applied. Patch Management compares all Windows servers to the Microsoft patch database to identify which patches must be applied.

Microsoft posts patches on its web site on the second Tuesday of each month, unless a special circumstance requires an immediate release. Windows patches released on *patch Tuesday* are available immediately to import into Server Automation. Before patch management can install a patch on a managed server, the patch must be downloaded from the Microsoft web site and imported into the Software Repository. You can download and import patches by using the SA Client or by running a script.

Once every 24 hours, the SA Agent on a Windows server compares the server's current state against the Microsoft patch database (based on the latest version of `wsusscn2.cab`) that has been imported into SA by the patch administrator. The Agent reports the results of that comparison and then stores the data in the Model Repository. When you request a compliance scan, it can take several minutes. When you look up compliance for a server, the status information is derived from the Web Services Data Access Engine.

If you perform a patch analysis of a Windows server immediately after importing a new version of the Microsoft patch database, the analysis does not yet include the data from the new patch database. Instead, SA reports on data from when the Agent last recorded the results of its comparison.

**Scenario A:** The SA 5.5 Agent on a Windows server uses Microsoft's latest detection engine (MBSA 2.0.1) to identify installed patches.

**Scenario B:** You used a previous version of the Agent to create a package of installed patches (from a server snapshot), where a previous version of Microsoft's detection engine (MBSA 1.2.1, 2.0.1) was used.

**Analysis:** In scenarios A and B, because different versions of MBSA were used to identify patches installed on a Windows server, you should expect to see a difference between the list of installed patches that the SA Client displays and the installed patches in the package that was created from a snapshot.



---

While MBSA 2.1 can include programs that are not patches in the Microsoft patch database, such as Malicious Software Removal Tool entries, these programs are excluded from patch management.

---

## SA Integration

When a server is managed by Server Automation, the SA Agent installed on the server registers the server's configuration, including its installed patches, with SA. The SA Agent repeats this registration every 24 hours. This information is immediately recorded in the Model Repository, such as data about the operating system version, hardware type, and installed software and patches. When you first provision a server with SA, the same data is immediately recorded.

When a new patch is issued, you can use the SA Client to immediately identify which servers require patching. SA provides a Software Repository where you upload patches and other software to. Using the SA Client, you access this software to install patches on the appropriate servers.



**Best Practice:** After a server is brought under SA management, you should install all Windows patches by using SA Windows patch management. If you install a patch manually, SA does not have data about that patch until the next software registration. If you install a patch manually, it can take as long as 24 hours until data about that server in the Model Repository is up-to-date. However, when you install patches using SA Windows patch management, the Agent immediately updates the information about the server in the Model Repository.



---

You cannot use Server Automation to uninstall a patch that was not installed by using SA Windows patch management.

---

## Support for Windows Patch Testing and Installation Standardization

Server Automation minimizes the risks of rolling out patches. When a patch is initially imported into SA, its status is marked as **Limited** and only administrators with the required permissions can install it.

The patch administrator then defines patch installation and uninstallation options and tests the patch. Only after the patch is tested and the patch administrator marks it as available for use (**Available**) can other administrators install the patch.

In Server Automation, Windows patch management allows you to standardize the way patches are installed and uninstalled, thereby preventing ad-hoc installation procedures. Patch administrators standardize patch installation by providing pre-install and post-install scripts, install and uninstall flags, reboot instructions, and error handling options.

## Supported Technologies for Patch Management

In Server Automation, Windows patch management consolidates many tools that allow you to perform server patching using a single interface.

The following patch management and installation tools are used for supported Windows operating systems:

- **msiexec.exe:** Installs and uninstalls MSI packages.
- **pkgmgr.exe:** Installs and uninstalls CAB patches.
- **qchain.exe:** Enables a single reboot when you are installing more than one hotfix.
- **unzip.exe:** Extracts info-zip compatible zip archives.

- **Windows Update Agent (WUA):** Enables access to the Microsoft framework for patch installations and updates.

See [Importing Windows Patch Utilities](#) on page 54 for instructions on how to import these utilities into Server Automation.

## Windows Hotfixes—`qchain.exe` and Reboot

After a Microsoft Windows hotfix is imported into Server Automation, you can specify options to reboot the server when a hotfix is installed or uninstalled. A Windows hotfix typically requires a reboot if it updates system files. This reboot enables SA to use the newly updated system files.

When a hotfix is installed along with other hotfixes, this process is called *hotfix chaining*. If one or more hotfixes require that the server must be rebooted, the reboot can sometimes be postponed until after all hotfixes have been installed. The user performing the installation must first run `qchain.exe` before performing the reboot. This ensures that the Pending File Rename Queue is correctly ordered.

Postponing reboots is not always possible, due to a defect in `qchain.exe` that was resolved in December 2002. All Windows hotfixes created after May 2001 included the Pending File Rename Queue manipulation logic in `qchain.exe`. Therefore, all hotfixes created between May 2001 and December 2002 are vulnerable to the same `qchain.exe` defect. See the Microsoft Article for Q815062.



---

If a Windows Service Pack or Security Rollup Package is being installed in the same hotfix chaining process, a reboot is required. This reboot cannot be postponed. Before the reboot that is associated with this package occurs, `qchain.exe` must be run.

---

When multiple hotfixes are chained by Server Automation, the setting that specifies that a reboot on install is required for each hotfix is honored. Server Automation analyzes the set of hotfixes being installed to determine whether one or more reboots can be postponed until the end of the chaining operation.



---

If you are installing a Windows hotfix that does not support the `-z` flag, remember to use the `/-z` option to prevent Server Automation from passing in the `-z` flag.

---

Server Automation conforms to the following criteria for running `qchain.exe` and rebooting:

- SA examines the date each hotfix was created to determine whether any associated reboot can be safely postponed until the end of the chained installation.
- SA will *not* change the installation order of the chained hotfixes (as an attempt to further reduce the number of reboots), whether or not Service Pack or Security Rollup Packages are being installed in the chained operation.
- When SA Windows patch management installs a hotfix *in isolation* (when the hotfix is not as part of a chained installation operation), SA honors the value of the reboot on the installation operation.
- Windows patch management runs `qchain.exe` on the managed server after the installation of each Windows hotfix and before any associated reboot. This guards against problems associated with an incorrectly ordered Pending File Rename Queue. This problem might occur if another hotfix was installed on the managed server outside of Server Automation actions.

## Roles for Windows Patch Management

Server Automation provides support for rigorous change management by assigning the functions of patch management to several types of users in an organization. These users include a policy setter, a patch administrator, and a system administrator.



---

These responsibilities are controlled by assigning permissions for managing patches in SA. To obtain these permissions, contact your SA Administrator. See the *SA Administration Guide*.

---

- **Policy Setter:** The policy setter is a member of a security standards group that reviews patch releases and identifies the vendor patches that will be included in the organization's patch policies. A policy setter is responsible for reviewing the latest security threats and the patches that vendors have released to address these problems. A policy setter is generally known as an expert in the operating systems and applications that they manage, and is able to assess the necessity of applying patches issued by vendors. A policy setter is also able to diagnose common problems that arise after patches are installed, allowing for a thorough test of the patch application process.
- **Patch Administrator:** The patch administrator has the authority to import, test, and edit patch options. The patch administrator is often referred to as the security administrator in an organization. A patch administrator is granted specific permissions to import patches into Server Automation to test the patches and then mark them as available for use. Basic users can import patches, but they cannot install them or mark them as available. Patch administrators are also able to edit patch options (such as installation scripts) through patch management. Other types of users are not allowed to import or edit patches. Typically, a patch administrator imports the Microsoft patch database and tests patches on non-production reference hardware. After testing the patches and determining that the patches are safe to apply to production systems, a patch administrator marks the patches available in the Library and then advises the system administrators that they must apply the approved patches.
- **System Administrator:** The system administrator installs patches (that have been approved for use) uniformly and automatically, according to the options that the patch administrator specifies. The system administrator is an SA user who is responsible for the day-to-day maintenance of the servers in a deployment. These users are not required to have the same level of expertise in low-level system details as the policy setter and patch administrator. Because the patch administrator has set up the patch installation, the system administrator can attach policies to servers, set an exception for a patch, and install patches on a large number of managed servers. They are responsible for searching for servers that require the approved patch, installing the patches, and verifying that the patches were successfully installed. The system administrator can import patches but cannot install a patch until the patch administrator has marked it as available. The system administrator can also uninstall patches.



---

Server Automation also provides predefined patch user groups for patch deployers and patch policy setters. See [Predefined Patch User Groups](#) on page 23.

---

## Predefined Patch User Groups

During an SA installation or upgrade, certain predefined user groups are created, such as patch deployers and patch policy setters.

- **Patch Deployers**—Access to install patches.
- **Patch Policy Setters**—Access to set patching policy.

You must grant read and/or write permissions to the first facility and other appropriate permissions to these user groups. Use of these predefined user groups is optional. You can modify the permissions of the predefined user groups and you can also delete or copy these groups to create new groups. Changes to or deletions of these predefined user groups are not affected by SA upgrades. See the *SA User Guide: Server Automation* for more information.

# Patch Management Process

The Windows patching process consists of the following phases:

- **Setup:** This phase includes getting the Microsoft database (patches and metadata) into Server Automation, identifying products you want to track patches for, and configuring patch compliance.
- **Policy Management:** This phase includes investigating released patches, creating and updating patch policies or exceptions, marking patches available to use, and attaching policies or exceptions to servers or groups of servers.
- **Patch Compliance:** This phase includes running compliance scans to determine whether a server is out of compliance, remediating policies, setting up installation options, and installing applicable patches.
- **Deployment:** To deploy patches on demand, you can import the required patches, test them, update policies, create new policies, mark them as available to use, specify install options, and install the required patches. [Figure 3](#) and [Figure 4](#) illustrate these phases and their required steps.

**Figure 3 Windows Patching Process: Part A and Part B**

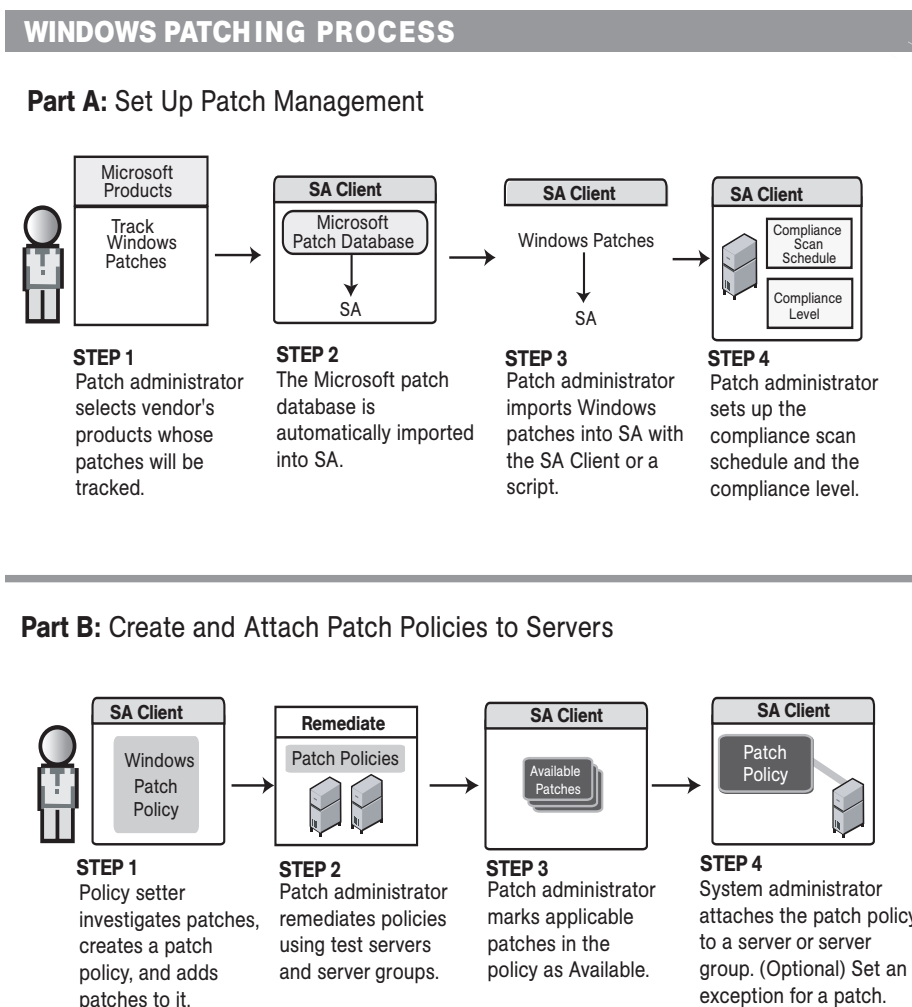
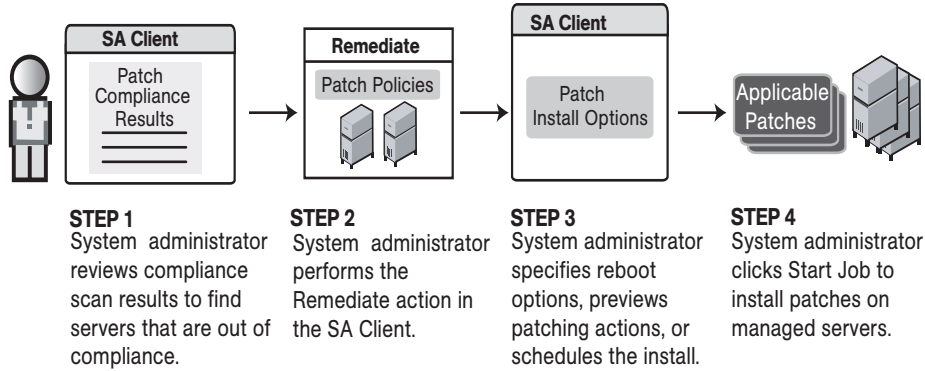




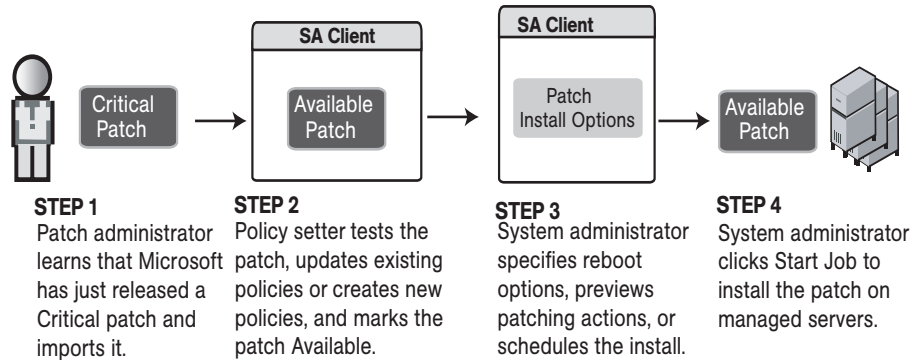
Figure 4 Windows Patching Process: Part C and Part D

## WINDOWS PATCHING PROCESS

### Part C: Install Patches By Remediating Policies



### Part D: Install Patches on Demand



# Patch Management Tasks

This section describes how to find and manage information about a Windows patch.

- Viewing Patch Information
- Patch Dependencies and Supersedence
- Viewing Windows Patches
- Editing Windows Patch Properties
- Importing Custom Documentation for a Patch
- Deleting Custom Documentation for a Patch
- Finding Vendor-Recommended Windows Patches
- Finding Servers That Have a Windows Patch Installed
- Finding Servers That Do Not Have a Windows Patch Installed
- Importing a Patch
- Importing Windows Patches
- Exporting a Windows Patch
- Exporting Windows Patch Information

## Viewing Patch Information

To view detailed information (properties) about a patch:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**.
- 2 Expand Patches and select a specific operating system.  
The content pane displays all patches associated with that operating system.
- 3 In the content pane, open a patch to view its properties in the Patch window.



---

Press **F1** to display descriptions of the fields displayed in the Patch Properties window.

---

## Patch Dependencies and Supersedence

Patch metadata identifies all known dependency and supersedence relationships between patches and Windows products, and between patches and other patches.

In Server Automation:

- **Dependency** relationships identify Windows products that must already exist on a server before you can install a certain patch.
- **Supersedence** relationships identify patches that supersede or are superseded by other patches. In Windows patch management, *supersedes* means that one patch replaces another and *superseded by* means that the patch you are installing is replaced by another patch.



---

In Server Automation, Windows patch management does not detect whether two patches are *mutually exclusive*—which is when either one can be installed but not both. Subsequently, patch management does not prevent you from installing both patches on a server. This means that you may be able to install both a superseded patch and a superseding patch on a server.

---

## Viewing Windows Patches

The SA Client displays information about Microsoft Windows patches that have been imported into Server Automation.

To view information about a patch:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**.
- 2 Expand Patches and select a specific Windows operating system.  
The content pane displays all patches listed in the Microsoft Patch Database for the Windows operating system that you selected.
- 3 (*Optional*) Use the column selector to sort the patches according to Name, Type, Severity, Availability, Release Date, and Bulletin Number.
- 4 In the content pane, open a patch to view its properties in the Patch window.

## Editing Windows Patch Properties

You can edit a patch's Description, Availability, Install Parameters, and Uninstall parameters.

The Availability property indicates the status of the patch in Server Automation. If the Availability is Not Imported, you cannot change this property.

You can set the install and uninstall parameters on either the patch properties page or in the Patch Actions only when you are installing or uninstalling one patch at a time. The parameters on the properties page are saved in the Model Repository, but the parameters in Patch Actions are used only for that action. The parameters in Patch Actions override those on the patch properties page.

To edit the patch properties:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**.
- 2 Expand Patches and select a specific Windows operating system.  
The content pane displays all patches associated with that operating system.
- 3 In the content pane, open a patch to view its properties in the Patch window.
- 4 Edit any of the following fields: Description, Availability, and the Install and Uninstall parameters.
- 5 From the **File** menu, select **Save** to save your changes.

## Importing Custom Documentation for a Patch

The Custom Documentation view of a patch displays text files that have been imported from the local file system. Non-plain text file types, such as .html or .doc, are not supported.

To import your own documentation for a patch:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**.
- 2 Expand Patches and select a specific Windows operating system.  
The content pane displays all patches associated with that operating system.
- 3 In the content pane, open a patch to view its properties in the Patch window.
- 4 In the Views pane, select **Custom Documentation**.
- 5 From the **Actions** menu, select **Import**.
- 6 In the Import Custom Documentation window, locate a text file and specify encoding.
- 7 Click **Import**.

## Deleting Custom Documentation for a Patch

The Custom Documentation view of a patch displays text files that have been imported from the local file system. Non-plain text file types, such as .html or .doc, are not supported.

To delete custom documentation for a patch:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**.
- 2 Expand Patches and select a specific Windows operating system.  
The content pane displays all patches associated with that operating system.
- 3 In the content pane, open a patch to view its properties in the Patch window.
- 4 In the Views pane, select **Custom Documentation**.
- 5 From the **Actions** menu, select **Delete**.
- 6 In the Delete Custom Documentation window, click **Delete**.

## Finding Vendor-Recommended Windows Patches

To find patches that Microsoft recommends for a particular server, based on Windows Update Agent (WUA):

- 1 In the navigation pane, select **Devices** ► **Servers** ► **All Managed Servers**.
- 2 From the View drop-down list, select **Patches**.
- 3 In the content pane, select a server that is running SA Agent 5.5 and Windows Server 2000 Service Pack 4, Windows Server 2003, Windows XP, or Windows Server 2008.
- 4 In the preview pane, select **Patches Recommended By Vendor** from the drop-down list to display the types of patches for the selected server.

## Finding Servers That Have a Windows Patch Installed

To find servers that have a particular patch installed:

- 1 In the navigation pane, select **Library ► By Type ► Patches**.
- 2 Expand Patches and select a specific Windows operating system.  
The content pane displays all patches associated with that operating system.
- 3 In the content pane, select a patch.
- 4 From the View drop-down list in the content pane, select **Servers**.
- 5 From the Show drop-down list for the selected patch, select **Servers with Patch Installed**.

You can browse a server in this list to view a list of all installed patches. Notice that this list might display a more complete list of installed patches than the list you will find in the Windows Add or Remove Programs utility.

## Finding Servers That Do Not Have a Windows Patch Installed

To find servers that do not have a particular patch installed:

- 1 In the navigation pane, select **Library ► Patches**.
- 2 Expand Patches and select a specific Windows operating system.  
The content pane displays all patches associated with that operating system.
- 3 In the content pane, select a patch.
- 4 In the View drop-down list, select **Servers**.
- 5 In the Show drop-down list, select **Servers without Patch Installed**.

## Importing a Patch

Windows patches are downloaded from the Microsoft web site and then imported (uploaded) into Server Automation. To verify whether a patch has been imported, view the patch's Availability property. The Availability of an imported patch is either Limited, Available, or Deprecated. A patch can be imported with the SA Client or with a script. For information about the script, see [Importing Windows Patches](#) on page 30.

To import a patch with the SA Client:

- 1 In the navigation pane, select **Library ► By Type ► Patches**.
- 2 Expand the Package Repository and select a specific Windows operating system.  
The content pane displays all patches associated with that operating system.
- 3 In the content pane, select a patch.
- 4 To import a patch directly from the Microsoft web site, from the **Actions** menu, select **Import Contents ► Import from Vendor**.

The Import from Vendor window displays the URL of the patch's location on the Microsoft web site. *(Optional)* You can override this URL.

Or

To import a patch that has already been downloaded to your local file system, from the **Actions** menu, select **Import** ► **Import from File**.

In the file browser window, locate the patch.

- 5 Click **Import**.

## Importing Windows Patches

The `populate-opsware-update-library` shell script downloads the Microsoft Patch Database and patches from the Microsoft site. This script also imports the database and patches into Server Automation. (



To be imported, a patch must be in the Microsoft Patch Database that has been imported into the Software Repository.)

Optionally, this shell script sets the initial status (Available or Limited) of newly imported patches. The script can also filter the patches imported according to operating system, such as Windows Server 2003 and Windows Server 2008. The functionality of the script is also available in the SA Client, as described in [Importing the Microsoft Patch Database](#) on page 52.

To run the `populate-opsware-update-library` script, you need to log on to the Software Repository server as `root`. Typically, you schedule the script to run periodically as a `cron` job on the Software Repository server. To end users of the SA Client, the patches imported with the script appear to have been automatically imported. Do not run concurrent instances of the script.

The `populate-opsware-update-library` script is located in the following directory:

```
/opt/opsware/mm_wordbot/util/
```

Table 1 describes the script's options.

**Table 1** Options of `populate-opsware-update-library`

Option	Description
<code>--spin hostname-or-IP</code>	Hostname or IP address of the Data Access Engine (spin) host. Default: spin
<code>--theword hostname-or-IP</code>	Hostname or IP address of the Software Repository (theword) host. Default: theword
<code>--cert_path file-path</code>	File specification of the cert file to be used for the spin connection. Default: <code>/var/opt/opsware/crypto/wordbot/wordbot.srv</code>
<code>--ca_path file-path</code>	File specification of CA file to be used for Spin connection. Default value: <code>/var/opt/opsware/crypto/wordbot/opsware-ca.crt</code>
<code>--verbose</code>	Display comprehensive output, including patches that were skipped during the upload.

**Table 1 Options of populate-opsware-update-library (cont'd)**

<b>Option</b>	<b>Description</b>
<code>--no_w2k</code>	Do not process W2K patches.
<code>--no_w2k3</code>	Do not process W2K3 patches.
<code>--no_w2k3x64</code>	Do not process W2K3 (64-bit) patches.
<code>--no_w2k8</code>	Do not process W2K8 patches.
<code>--no_w2k8x64</code>	Do not process Windows 2008 (64-bit) patches.
<code>--no_xp</code>	Do not process Windows XP (32-bit) patches.
<code>--use_proxy_url url</code>	When downloading binaries, connect via this proxy URL.
<code>--proxy_userid userid</code>	Basic-auth userid to provide to proxy server.
<code>--proxy_passwd passwd</code>	Basic-auth passwd to provide to proxy server.
<code>--set_available</code>	Set availability status to Available when uploading patches. The <code>--set_available</code> and <code>--set_limited</code> options cannot be specified at the same time.
<code>--set_limited</code>	Set availability status to Limited when uploading patches.
<code>--no_hotfixes</code>	Do not upload hotfixes.
<code>--no_servicepacks</code>	Do not upload servicepacks.
<code>--no_updaterollups</code>	Do not upload updaterollups.
<code>--no_wsusscan_upload</code>	Do not upload the MBSA 2.1x patch database.
<code>--wsusscan_url_override url</code>	Download the MBSA 2.1x patch database from this URL.
<code>--update_all</code>	Refresh the patches already uploaded into SA.
<code>--download_only path</code>	Download files from the vendor's web site to the specified path (directory), but do not upload them into SA. The files are downloaded into the <code>platform_ver/locale</code> subdirectory beneath the specified path.
<code>--upload_from_update_root path</code>	Upload files from the specified path (directory), not from the vendor's web site. The script looks for patches in the <code>platform_ver/locale</code> subdirectory beneath the specified path. If it cannot find the patch in the that subdirectory, the script looks for the patch in the specified path. If a patch is not found, the script skips the patch and does not upload it. This option is ignored if <code>--download_only</code> is also specified.

**Table 1** Options of populate-opsware-update-library (cont'd)

Option	Description
--help	Display the syntax of this script.  --wget_path <file-path>  Use wget for the proxy downloads versus built-in proxy support.  File specification of the wget utility must also specify:  --proxy_userid --proxy_passwd --wget_http_proxy --wget_ftp_proxy  --wget_http_proxy <server:port>  Specify the wget HTTP proxy server in the format: proxyserver:httpport  --wget_ftp_proxy <server:port>  Specify the wget FTP proxy server in the format: proxyserver:ftpport  --use_temp_download_path <path>  Tip: Download files to a temporary download directory (/var/tmp), instead of a subdirectory.

## Exporting a Windows Patch

To export a patch from Server Automation to a local file system:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**.
- 2 Expand Patches and select a specific Windows operating system.  
The content pane displays all patches associated with that operating system.
- 3 In the content pane, select a patch.
- 4 From the **Actions** menu, select **Export**.
- 5 In the Export Patch window, enter the folder name that will contain the patch file in the File Name field.
- 6 Click **Export**.

## Exporting Windows Patch Information

You can export information about patches installed on an SA managed server and patches recommended by the vendor. You can also export information from patches recommended by the vendor along with model information on the selected server, such as patch policies or patch policy exceptions. The following information is exported into a .csv file:

- **Server Name:** The name of the managed server.
- **OS:** The operating system of the server.



- **Service Pack:** The service pack level of the server being reported, such as Service Pack 3, Service Pack 4, and so on.
- **KB#:** The Microsoft Knowledge Base Article number for the patch.
- **Bulletin:** The MSYY-XXX ID associated with a hotfix, such as MS05-012, MS06-012, and so on. If the MSYY-XXX ID is unknown, this column will be blank.
- **Description:** A brief description of the purpose of the patch.
- **Time Queried:** The last software registration by the Agent.
- **Time Installed:** The time that the patch was installed.
- **Type:** The patch type.
- **Compliance Level:** An integer that represents the compliance level.
- **Compliance:** Text that displays when you place your cursor over the Compliance column in the Patch preview pane.
- **Exception Type:** The type of exception, such as Always Install or Never Install.
- **Exception Reason:** A description that explains the purpose of the exception.

Windows patch management will display all of the text, including commas, from the Description field displayed in the Patch Properties window in the Description column in the .csv file. To ensure that all of the text about a patch displays in the Description field in the .csv file, patch management surrounds the entire description (that you see in the Patch Properties window) with double quotes.

To export the patch information to a .csv file:

- 1 In the navigation pane, select **Devices ► All Managed Servers**.
- 2 In the content pane, select one or more managed servers.
- 3 From the Show drop-down list, select an option.
- 4 From the **Actions** menu, select **Export Patch Info to CSV**.
- 5 In the Export to CSV window, navigate to a folder and enter the file name.
- 6 Verify that the file type is Comma Separated Value Files (.csv).

If you did not include the .csv extension in the file name field, SA will append it only if you have the .csv file type selected.

- 7 Click **Export** to save the patch information in a .csv file or click **Cancel** if you do not want to export the patch information.

# Policy Management

In Windows patch management, patch policies and patch policy exceptions enable you to customize patch distribution in your environment. Policies and exceptions define the Windows patches that should be installed or not installed on your managed servers.

You can choose to have patching in your server environment comply to the model that these policies and exceptions define or you can choose to deviate from this model. If you choose to deviate from the patch policies and exceptions and perform ad hoc patch installs, then you need to remediate. The remediation process ensures that the applicable patches get installed on servers.

## Patch Policy

A *patch policy* is a group of patches that you want to install on SA managed servers. All patches in a patch policy must apply to the same Windows operating system.

A patch policy provides broad flexibility for distributing patches. For example, you can create a patch policy that contains security patches that you want to distribute only to servers used by your sales force. You can also create a patch policy that contains security patches that are applicable to specific software that is already installed on a server, such as Exchange Server, Internet Information Services (IIS), SQL Server, and so on. Or, you can create a patch policy that includes all patches ranked as critical by Microsoft and then installs them on all servers that are used by everyone in your organization.



---

If you do not want to create a patch policy, you can use the vendor-recommended set of patches (by operating system) as a default patch policy, such as the patches provided by `wsusscn2.cab`.

---

You can attach as many patch policies as you want to servers or groups of servers. If several policies are attached to one server, the installation logic is cumulative—all patches listed in all attached policies will be installed on the server. The Remediate window allows you to select an individual patch policy to remediate. You do not have to remediate all policies attached to a server. You cannot nest patch policies.

If a description of the patch policy is defined, it is recorded in the server's patched state in the Model Repository. This information enables patch management to report on patch policies for patch compliance purposes. The patch compliance process compares patch policies with corresponding patch policy exceptions.

Windows patch management supports the following types of patch policies:

- **User-defined patch policy:** This type of patch policy allows you to specify the patches you want in the policy. A user-defined patch policy can be edited or deleted by a user who has the required permissions.  
This type of patch policy allows a policy setter to opt out of patches. The policy setter can create a user-defined patch policy that is a subset of all available patches that are in a vendor-recommended patch policy. This enables the policy setter to apply only those patches that their environment needs.
- **Vendor-recommended patch policy:** Membership of patches is defined by `wsusscn2.cab` recommendations on a server-by-server basis. Vendor-recommended patch policies are system defined and cannot be edited or deleted by a user.



---

You can only export user-defined patch policies. You cannot export vendor-recommended patch policies.

---

Patch policies have the following characteristics:

- All patches in a patch policy must apply to the same operating system, such as Windows 2003.
- A patch policy is associated with an operating system version, such as Windows Server 2003 or Windows 2008.
- A patch policy has a name and can (optionally) include a description that explains its purpose.
- A patch policy can be either user-defined or vendor-defined.
- A patch policy does not have sub-policies. There is no inheritance.
- A patch policy is Customer Independent, which means that patches in the policy can be installed on any managed server, no matter what customer is associated with it. See the *SA User Guide: Server Automation*.
- A patch policy is always public.
- A patch policy can be attached to zero or more servers or public device groups.
- More than one patch policy can be attached to a server or public device group.
- Only user-defined patch policies can be created, edited, and deleted by a user who has permissions.

## Patch Policy Exception

A *patch policy exception* identifies a single patch that you want to explicitly include or exclude from a specific managed server, along with an optional reason for why the exception exists. The patch in a patch policy exception must apply to the same Windows operating system that the established patch policy is attached to.

A patch policy exception allows you to deviate from an established patch policy—one that is already attached to a server or a group of servers. You can do this by deselecting or adding individual patches to a server. Since patch policy exceptions override all patch policies attached to a server, you can use them to intentionally deviate from a patch policy on a server-by-server basis.

If a reason for a patch policy exception is defined, the description is recorded in the server's patched state in the Model Repository. This information enables SA to report on patch policy exceptions for patch compliance purposes. The patch compliance results explain how patch policy exceptions compare with corresponding established patch policies. All users who have access to the managed server can view its attached patch policy exceptions.

Windows patch management supports the following types of patch policy exceptions:

- **Always Installed:** The patch should be installed on the server, even if the patch is not in the policy.
- **Never Installed:** The patch should not be installed on the server, even if the patch is in the policy.



---

If you ever need to override a patch policy exception, you can manually install a patch.

---

The following information summarizes characteristics of a patch policy exception:

- A patch policy exception can (optionally) include a description that explains its purpose.
- A patch policy exception can have a rule value of Never Installed or Always Installed.

- A patch policy exception can be set for one patch and one server of the same operating system version. If a patch policy exception is set for a public device group and a server in that group does *not* match the operating system version specified in the patch policy exception, the patch policy exception is *not* applied.
- A patch policy exception can be set, copied, and removed by users who have permissions.

## Precedence Rules for Applying Policies

By creating multiple patch policies and patch policy exceptions that are either directly attached to a server or attached to a group of servers, you control the patches that should be installed or not installed on a server. A precedence hierarchy in patch management delineates how a patch policy or a patch policy exception is applied to a patch installation. This hierarchy is based on whether the patch policy or patch policy exception is attached at the server or device group level.

The following precedence rules apply to policies and exceptions:

- Patch policy exceptions that are directly attached to a server always take precedence over patch policies that are directly attached to a server.
- Patch policies that are directly attached to a server take precedence over patch policies and patch policy exceptions that are attached to a public device group.
- Patch policy exceptions that are attached to a public device group take precedence over patch policies that are attached to a public device group.
- If a server is in multiple public device groups, a Never Installed patch policy exception type always take precedence over an Always Installed patch policy exception type for the same patch.

## Remediation Process

See [Remediating and Installing Software](#) on page 53 for information about the fundamentals of SA remediation.

To ensure patch compliance, Windows patch management identifies vulnerable managed servers and simultaneously deploys patches to many servers when a remediation process is performed. The remediation process examines and applies an entire patch policy, including multiple policies, to the managed servers that it is attached to. A policy must be attached to a server or a group of servers before you can remediate the policy with that server or group.



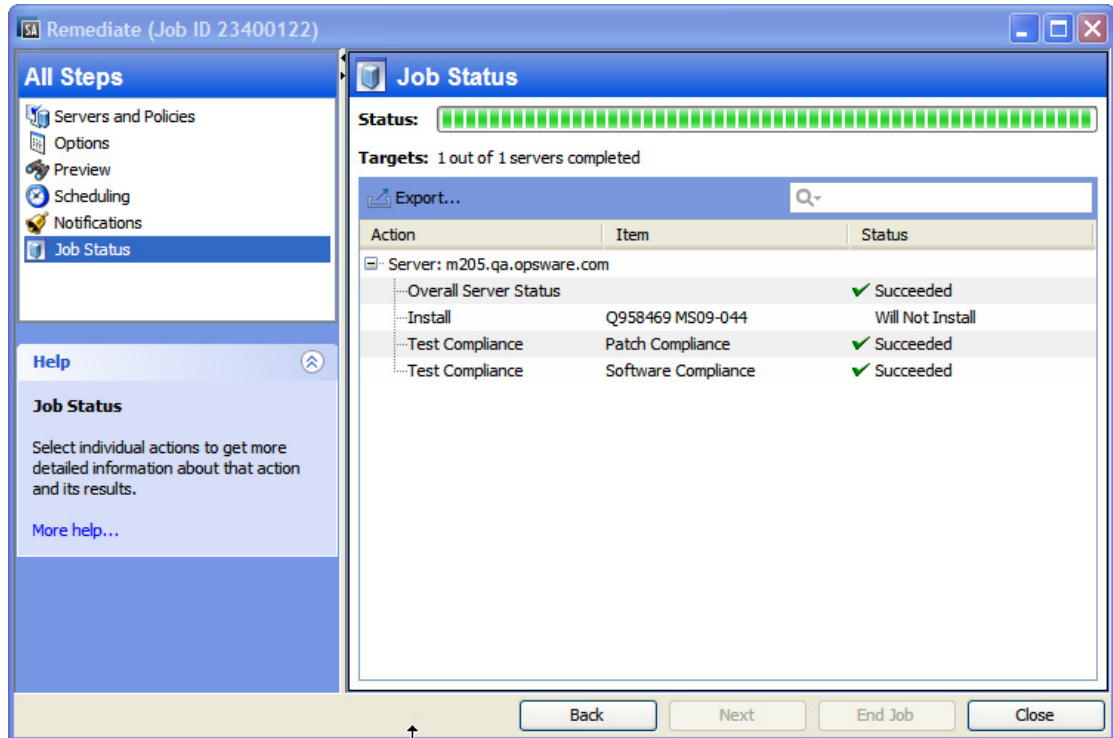
**Best Practice:** Each time you review the latest Microsoft patch releases and subsequently update a patch policy, by adding new patches to a policy, you should perform remediation. In these situations, a remediation process provides demand forecasting information. This allows you to determine how patch policy changes will impact servers that this policy is attached to.

If the remediation process discovers any applicable, missing patches, these patches will be installed on the servers.

After SA determines which patches need to be installed to complete the remediation process, remediation uses a set of standard system utilities to complete the operation. See [Supported Technologies for Patch Management](#) on page 20.

To help you optimally manage the remediation conditions, SA allows you to specify remediate options and pre and post actions, and set up ticket IDs and email notifications that alert you about the status of the remediate process. The Remediate wizard guides you through setting up these conditions.

**Figure 5 Remediate Wizard**



## Remediating Patch Policies

This action installs the patches in a policy that has been attached to managed servers. This action does not uninstall patches. A patch policy can be overridden by an exception, which indicates that a patch is either always or never installed on a particular server.

To remediate a patch policy:

- 1 In the navigation pane, select **Library > By Type > Patch Policies**.
- 2 Expand Patch Policies and select a specific Windows operating system.  
The content pane displays all patch policies associated with that operating system.
- 3 In the content pane, open a patch policy.
- 4 In the View drop-down list, select **Servers**.
- 5 In the Show drop-down list in the content pane, select **Servers with Policy Attached**.
- 6 In the preview pane, select one or more servers.
- 7 From the **Actions** menu, select **Remediate**.

The first step of the Remediate window appears: Servers and Device Groups.

For instructions on each step, see the following sections:

- [Setting Remediate Options](#)
- [Setting Reboot Options for Remediation](#)
- [Specifying Pre and Post Install Scripts for Remediation](#)
- [Scheduling a Patch Installation for Remediation](#)
- [Setting Up Email Notifications for Remediation](#)
- [Previewing and Starting a Remediation](#)

After you have completed a step, click **Next** to advance to the next step. Before you click **Start Job**, you can return to a completed step to make changes by clicking on it in the list of steps.

- 8 Click **Start Job** to launch the remediation job.

After you launch the job, you cannot change its parameters, even if the job is scheduled to run at a later time.

## Setting Remediate Options

You can specify the following remediate policy option:

**Do not interrupt the remediate process even when an error occurs with one of the policies.**

To set this option:

- 1 In the Remediate window, click **Next** to advance to the Options step.
- 2 Select a rebooting option. See [Setting Reboot Options for Remediation](#) on page 38.
- 3 Select the Error Handling check box if you want the remediation process to continue even when an error occurs with any of the patches or scripts. As a default, this check box is not selected.
- 4 Click **Next** to go to the next step or click **Close** to close the Remediate window.

## Setting Reboot Options for Remediation

To minimize the downtime that server reboots can cause, you can control when servers reboot during a patch installation.

You can specify the reboot options in the following SA Client windows:

- Patch Properties window—Install Parameters tab
- Remediate window—Pre & Post Actions step



**Best Practice:** When you are selecting reboot options in the Remediate window, Hewlett Packard recommends that you use Microsoft's reboot recommendations, which is the **Reboot servers as specified by individual software items** option. If it is not possible to use the Microsoft reboot setting, select the single reboot option, which is the **Hold all server reboots until after all packages are installed and/or uninstalled** option. Failure to do this can result in the Windows Update Agent (WUA) incorrectly reporting which patches are installed on the server until the next reboot occurs (outside of SA control).

The following options in the Remediate window determine whether the servers are rebooted after the patch is installed. These options apply only to the job launched by the Remediate window. They do not change the Reboot Required option, which is in the Install Parameters tab of the Patch Properties window. Except for the first option, the following options override the Reboot Required option.

- **Reboot servers as specified by individual software items (Default):** By default, the decision to reboot depends on the Reboot Required option of the patch or package properties.
- **Reboot servers after each installation or uninstallation:** As a best practice, reboot the server after *every* patch or package installation or uninstallation, regardless of the vendor reboot setting on the individual patch or package.
- **Hold all server reboots until after all packages are installed and/or uninstalled:** If the Reboot Required option is set for some selected patches but not for others, the server is rebooted one time after all patches are installed. If the Reboot Required option is not set for any of the selected patches, the server is not rebooted.
- **Suppress all server reboots:** Even if the Reboot Required option of the patch properties is set, do not reboot the server. (Because of vendor settings, some patches ignore the suppress option and force a reboot.

To set reboot options:

- 1 From the Remediate window, click **Next** to advance to the Options step.
- 2 Select one of the Rebooting options.
- 3 Click **Next** to go to the next step or click **Close** to close the Remediate window.

## Specifying Pre and Post Install Scripts for Remediation

For each patch remediation, you can specify a command or script to run before or after remediation. A pre-install script, for example, could check a certain condition on the managed server. If the condition is not met or if the pre-install script fails, the patches would not be installed. A pre-install script could also be used to shut down a service or application before it is patched. A post-install script could be used to perform a certain cleanup process on the managed server.

You can specify the following types of scripts to run on the managed server before or after a remediation process:

- **Pre-Download:** A script that runs before patches are downloaded from SA to the managed server. This is available only if you select Staged in the Remediate Options step.
- **Post-Download:** A script that runs after patches are downloaded from SA to the managed server and before the patch is installed. This is available only if you select Staged in the Remediate Options step.
- **Pre-Install:** A script that runs before patches are installed on the managed server.
- **Post-Install:** A script that runs after patches are installed on the managed server.

To specify a pre-install script:

- 1 From the Remediate window, click **Next** to advance to the Pre & Post Actions step.
- 2 Select the Pre-Install tab.  
You may specify different scripts and options on each of the tabs.
- 3 Select the Enable Script check box. This option enables the remainder of the fields on the tab. If Enable Script is not selected, the script will not run.

- 4 Select either Saved Script or Ad-Hoc Script from the drop-down list.

A Saved Script has been previously stored in Server Automation with the SA Web Client. To specify the script, click **Select**.

An Ad-Hoc script runs only for this operation and is not saved in SA. Select the Type, such as .bat. In the Script box, enter the contents of the script, including the drive letter of where the script is located, such as `echo dir>> C:\temp\preinstall11.log`. If you do not enter a drive letter, the default is %SYSTEMDRIVE%, which is where the system folder of Windows is installed.

- 5 If the script requires command-line flags, enter the flags in the Command text box.
- 6 In the User section, if the system is not Local System, select Name.
- 7 Enter the system name, your password, and the Domain name.
- 8 To stop the installation if the script returns an error, select the Error check box.
- 9 Click **Next** to go to the next step or click **Cancel** to close the Remediate window

## Scheduling a Patch Installation for Remediation

You can schedule when you want patches installed and when you want patches downloaded.

To schedule a patch installation:

- 1 In the Remediate window, select the Scheduling step.

By default, the Scheduling step displays only the scheduling options for the installation phase. If you selected Staged in the Remediate Options step, the scheduling options for the download phase will also be displayed.
- 2 Select one of the following Scheduling options:
  - **Schedule Analysis:** This enables you to specify a date and time that you want the analysis to run.
  - **Schedule Download:** This enables you to specify a date and time that you want the download or installation performed.
  - **Schedule Remediate:** This enables you to specify a data and time that you want the remediate process to run.
- 3 Click **Next** to go to the next step or click **Cancel** to close the Remediate window.



## Setting Up Email Notifications for Remediation

You can set up email notifications to alert users when the download and installation operations complete successfully or with errors.

To set up email notifications:

- 1 From the Remediate window, click **Next** to advance to the Notifications step.
- 2 To add email addresses, click **Add Notifier** and enter the email addresses in the Notification Email Address field.



- 3 To set the notification status on the success of a Job, select the  icon. To set the notification status on the failure of a Job, select the  icon. By default, the Notification step displays only the notification status for the installation phase. If you selected Staged in the Remediate Options step, the notification status for the download phase is also displayed.
- 4 Enter a Ticket ID to be associated with a Job in the Ticket ID field.
- 5 Click **Next** to go to the next step or click **Cancel** to close the Remediate window.



---

If you previously selected Staged in the Remediate Options step, the Notifications pane displays notification options for both the download and installation phases.

---

## Previewing and Starting a Remediation

The remediate preview process provides an up-to-date report about the patch state of servers. The Preview is an optional step that lets you see the patches that will be installed on managed servers. This preview process verifies whether the servers you selected for the patch installation already have that patch installed (based on `wsusscn2.cab`). In some cases, a server could already have the patch installed if a system administrator had manually installed it, which means that patch management does not know about it.

In the Preview, the servers, device groups, and patches that are listed in the Summary Step window will be submitted to remediation when you click **Start Job**. Patches that are not recommended by the vendor will be excluded from this list. If there are other patches in the policy with the same QNumber, only the vendor-recommended patch is displayed.

This list shows patches and their associated servers, regardless of any patch policy and server group membership changes that may have occurred. If you preview a remediation, this same list of servers, device groups, and patches will be used, even if changes have occurred to the patch policy or server group memberships.

If you modify parameters in the Remediate window after you have already clicked **Preview**, the preview process will produce an invalid summary of simulated patching actions. For example, if you have already clicked **Preview** and you add patches, patch policies, servers, or device groups, you must click **Preview** again for results that include your changes.



---

The remediation preview does not report on the behavior of the server as though the patches have been applied.

---

### To preview a remediation:

- 1 In the Remediate window, in the Servers and Policies step, select a server or policy.
- 2 Click **Next** or select the Options step to specify your rebooting, error handling, and script preferences.
- 3 Click **Next** or select the Preview step to see the separate actions that will be performed when the patch is installed.
- 4 In the Preview step, click **Preview** to view the details of a previewed action.
- 5 To launch the installation job, click **Start Job**.

If you selected **Run Immediately After Analysis** in the Scheduling step, the job will run now. If you selected a specific time, the job will run then.

- 6 The Job Status displays in the Remediate window.

The Status bar and text indicate how many of the actions listed in the table have been completed. For each server, the following actions can be performed:

- **Overall Server Status:** The overall status of all servers included in this remediation job.
- **Analyze:** SA examines the patches needed for the installation, checks the managed servers for the most recent patches installed, and determines other actions that must be performed, such as download, install, or reboot.
- **Download:** The patch is downloaded from Server Automation to the managed server.
- **Install:** After it is downloaded, the patch is installed.
- **Reboot:** If this action is specified in the Options step, the server is rebooted.
- **Registration:** Software registration is performed to retrieve currently installed packages and patches on the managed server.
- **Test Compliance:** A compliance scan is performed to report the current compliance status of the managed server.
- **Run Script:** If scripts are specified in the Options step, the scripts are run before or/and after the download or/and installation.
- **Install & Reboot:** If you specify to reboot the server according to each patch or package setting in the Options step, the server will be rebooted immediately after each individual patch or package is installed.

- 7 To view additional details about a specific action, select the row in the table to display this information in the bottom pane.

Or

- 8 In the navigation pane, select Jobs and Sessions to review detailed information about the job. See [Browsing Job Logs](#) on page 48.
- 9 Click **End Job** to prevent the job from running or click **Close** to close the Remediate window. You can end a job only if it is scheduled.

*(Optional)* See [Cancelling or Terminating Installation, Uninstallation or Remediation Jobs](#) on page 66.

## Verifying Patch Policy Compliance

To determine whether a managed server complies with patch policies and exceptions:

- 1 In the navigation pane, select **Devices ► All Managed Servers**.
- 2 From the View drop-down list, select Compliance to display patch compliance status.
- 3 Select a specific server or check **Check All Rows** to view detailed Patch compliance information in the details pane. At any time, select **Uncheck All Rows** to modify your server selection.
- 4 In the details pane, expand the Patch row to see status and compliance summary details. Use the status filter to narrow your compliance display preferences. By default, this is set to **No Status Filter**.

## Creating a Patch Policy

A patch policy is a set of patches that should be installed on a managed server. When it is first created, a patch policy contains no patches and is not attached to servers.

To create a patch policy:

- 1 In the navigation pane, select **Library ► By Type ► Patch Policies**.
- 2 Select a specific Windows operating system.
- 3 From the **Actions** menu, select **Create Patch Policy**.  
The name of the policy you just created is New Patch Policy n, where n is a number based on the number of New Patch Policies already in existence.
- 4 In the content pane, open the New Patch Policy.
- 5 (*Optional*) In the Name field of the Properties, enter a name that describes the purpose or contents of the policy.

## Deleting a Patch Policy

This action removes a patch policy from SA but does not remove or uninstall patches from managed servers. You cannot delete a patch policy if it is attached to servers or groups of servers. You must first detach the policy from the servers or groups of servers before removing it from SA.

To delete a patch policy from SA:

- 1 In the navigation pane, select **Library ► By Type ► Patch Policies**.
- 2 Select a specific Windows operating system.
- 3 In the content pane of the main window, select a policy.
- 4 From the **Actions** menu, select **Delete Patch Policy**.

## Adding a Patch to a Patch Policy

This action adds a patch to a patch policy, but does not install the patch on a managed server. The patch will be installed when the policy is remediated.

To add a patch to a patch policy to SA:

- 1 In the navigation pane, select **Library ► By Type ► Patch Policies**.
- 2 Select a specific Windows operating system and view the list of Windows patches.
- 3 In the content pane, select the patch.
- 4 From the View drop-down list, select Patch Policies.
- 5 From the Show drop-down list, select **Policies without Patch Added**.
- 6 Select a policy.

- 7 From the **Actions** menu, select **Add to Patch Policy**.
- 8 In the Add to Patch Policy window, click **Add**.

## Removing a Patch from a Patch Policy

This action only removes a patch from a patch policy. This action does not uninstall the patch from a managed server and does not remove the patch from SA.

To remove a patch from a patch policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**.
- 2 Select a specific Windows operating system and view the list of Windows patches.
- 3 From the content pane, select a patch.
- 4 From the View drop-down list, select **Patch Policies**.
- 5 From the Show drop-down list, select **Policies with Patch Added**.
- 6 Select a patch. From the **Actions** menu, select **Remove from Patch Policy**.
- 7 In the Remove Patch from Policy window, select the policy and click **Remove**.

## Attaching a Patch Policy to a Server

This action associates a patch policy with a server or a group of servers). You must perform this action before you remediate a policy with a server or a group of servers.

To attach the policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patch Policies**.
- 2 Select a specific Windows operating system and view the list of Windows patch policies.
- 3 In the content pane, select a patch policy.
- 4 From the View drop-down list, select **Server Usage** or **Device Group Usage**.
- 5 From the Show drop-down list, select **Servers with Policy Not Attached** or **Server Groups with Policy Not Attached**.
- 6 In the preview pane, select one or more servers.
- 7 From the **Actions** menu, select **Attach Server**.
- 8 Click **Attach**.

## Detaching a Patch Policy from a Server

This action does not delete the patch policy and does not uninstall patches from a managed server.

To detach the policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patch Policies**.
- 2 Select a specific Windows operating system and view the list of Windows patch policies.
- 3 In the content pane, select a patch policy.
- 4 From the View drop-down list, select Server Usage (or Device Group Usage).
- 5 From the Show drop-down list, select **Servers with Policy Attached** or **Server Groups with Policy Attached**.
- 6 In the preview pane, select one or more servers.
- 7 From the **Actions** menu, select **Detach Server**.
- 8 Click **Detach**.

## Setting a Patch Policy Exception

A patch policy exception indicates whether the patch is installed during the remediation process. The Install Patch and Uninstall Patch actions ignore patch policy exceptions. A patch policy exception overrides the policy. You can specify an exception for a particular patch and server or a group of servers, but not for a patch policy.

To set a patch policy exception:


- 1 In the navigation pane, select **Devices** ► **All Managed Servers**.
- 2 Select a server.
- 3 In the content pane, select a server.
- 4 From the View drop-down list, select **Patches**.
- 5 In the preview pane, select a patch.
- 6 From the **Actions** menu, select **Set Exception**.
- 7 In the Set Policy Exception window, select the Exception Type:
  - **Never Install**: The patch should not be installed on the server, even if the patch is in the policy.
  - **Always Install**: The patch should be installed on the server even if the patch is not in the policy.
- 8 *(Optional)* In the Reason field, enter an explanation. This explanation is displayed when you move the cursor over the Exception column in the preview pane. The Patches with Exceptions option must be selected. When you are finished, click **OK**.


## Finding an Existing Patch Policy Exception


You can search for managed servers that already have patch policy exceptions attached to them and you can search for patches that have exceptions.


To find an existing patch policy exception:

- 1 In the navigation pane, select **Devices** ► **All Managed Servers**.
- 2 From the View drop-down list, select **Patches**.
- 3 In the content pane, select a server.
- 4 From the Show drop-down list, select **Patches with Policies or Exceptions** or **Patches with Exceptions**.
- 5 In the Exception column, move the cursor over the icon to display the reason for this exception. The following icons indicate the type of patch policy exception:

 An always install exception on a patch/server association.

 An always install exception inherited to a server from a group of servers/patch association.

 A never install exception on a patch/server association.

 A never install exception inherited to a server from a group of servers/patch association.

## Copying a Patch Policy Exception

To copy an exception between servers or groups of servers:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**.
- 2 Expand the Patches and select a specific Windows operating system.
- 3 In the content pane, select a patch.
- 4 From the View drop-down list, select **Server Usage** or **Device Group Usage**.
- 5 From the Show drop-down list, select **Servers with Exception** or **Server Groups with Exception**.
- 6 In the preview pane, select a server. This server is the source of the copied exception.
- 7 From the **Actions** menu, select **Copy Exception**.
- 8 In the Copy Policy Exception window, select the target servers or device groups.

These servers are the destinations of the copied exception. If this operation would result in replacing an existing exception, a message displays asking you to confirm whether this is the preferred action.

- 9 Click **Copy**.

## Removing a Patch Policy Exception

To remove a patch policy exception:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**.
- 2 Expand the Patches and select a specific Windows operating system.
- 3 In the content pane, select a patch.
- 4 From the View drop-down list, select **Servers**.
- 5 From the Show drop-down list, select **Servers with Exception**.
- 6 In the preview pane, select a server.
- 7 From the **Actions** menu, select **Remove Exception**.

## Patch Compliance

Server Automation performs conformance tests (compliance checks) against managed servers and public device groups to determine whether all patches in a policy and a policy exception were installed successfully. To optimize patch compliance information for your organization, you can set the patch compliance levels and edit the rules of the customized patch compliance level.

### Patch Compliance Scans

A patch compliance scan compares patches that are installed on a server with patch policies and patch policy exceptions that are attached to that server. The results of this scan show you the servers that are *in compliance* (have all required patches installed) and the servers that are *out of compliance* (do not have all required patches installed).

You should run or schedule patch compliance scans based on the dynamics of your patching environment. For example, if you updated a patch policy or installed a patch outside of (by not using) Server Automation, a compliance scan is required because the SA model has been changed and the compliance information must now be recalculated. SA indicates these types of conditions by displaying Scan Needed. In this case, instead of waiting for the scan schedule to iterate, you can start compliance scan on one or more servers.

### Ways to Start a Patch Compliance Scan

You can start a patch compliance scan in the following ways:

- **Immediately**, by selecting servers or groups and then selecting a menu item.  
See [Starting a Patch Compliance Scan Immediately](#) on page 48.
- **Periodically**, by setting up a schedule.  
See [Scheduling a Patch Compliance Scan](#) on page 53. By default, the scans are not scheduled.
- **As a result of another task**.

SA performs a patch compliance scan on a managed server at the end of the tasks described in the following sections:

- [Installing a Windows Patch](#) on page 62
- [Uninstalling a Windows Patch](#) on page 69
- [Remediating Patch Policies](#) on page 37

## Starting a Patch Compliance Scan Immediately

To start a scan on selected servers:

- 1 In the navigation pane, select **Devices**.
- 2 Select an entry from the Servers or Device Groups list.
- 3 Right-click and then select **Scan ► Patch Compliance** to display the Patch Compliance Scan Status window.


## Refreshing the Compliance Status of Selected Servers

When you refresh the compliance status of a Windows server, the SA Client retrieves the latest data from the Web Services Data Access Engine. A refresh action does not re-scan Windows servers for compliance information.

To refresh the compliance status for one or more servers:

- 1 In the navigation pane, select **Devices**.
- 2 From the View drop-down list, select Compliance.
- 3 In the content pane, select one or more servers.
- 4 Right-click and select **Refresh Server**.
- 5 Review the Status column for any changed compliance information.

## Viewing Scan Failure Details

If the scan operation fails, you cannot determine whether a server is in compliance. A scan failure is indicated by the Scan Failed  icon. To find out why a patch compliance scan failed:

In the navigation pane, select **Devices**.





- 6 Drill down to the server you want to check.
- 7 In the contents pane, select a server.
- 8 Right-click and then select **Scan ► Show Patch Compliance Scan Failure Details**.
- 9 In the Patch Compliance Scan Failure Details window, select a server and examine the detailed error message that appears in the lower part of the window.



## Patch Compliance Icons

Server Automation displays the following icons in [Table 2](#).

**Table 2 Patch Compliance Status Icons**

Status/Icon	Description
 <b>Compliant</b>	The server is compliant for all patches. Patches in policies attached to the server are all installed on the target server.
 <b>Partial</b>	The server is partially compliant for patches. An exception has been set for these patches.
 <b>Non-Compliant</b>	The installed patches on the server do not match the conditions defined in the patch policy.
 <b>Scan Failed</b>	The scan operation failed. Patch Management is unable to check the compliance of the server.

### About Patch Non-Compliance

A Patch non-compliant status for a server or group of servers can be caused by different factors, such as the existence of applicable patches that need to be installed as defined in a patch policy attached to the servers. Or, there could be exceptions that affect a server patch compliance level.

For example, a server will be considered non-compliant if the patch policy has a patch marked as a “Never Install” exception but the target server does have that patch installed.

Also, if superseded patches are recommended and included in policies or exception, they are counted in the compliance calculations, and if they are missing on the target server, then the server's patch compliance status will be non-compliant.

## Patch Compliance Levels

Patch compliance levels define your patch compliance rules. Results of a patch compliance scan can include only policies, both policies and exceptions, or your own customized level.

Windows patch management supports the following compliance levels:

- **Policy Only:** Verifies whether the patches installed on a server comply with the patch policies.
- **Policy and Exception:** Verifies whether the patches installed on a server comply with the patch policies and any exceptions. The Partial icon is displayed if the policy and exception do not agree and the exception does not have data in the Reason field.
- **Customized:** Verifies the rules that you edited for this compliance level.

## Patch Compliance Rules

Patch compliance rules are the conditions that determine the compliance icons that are displayed in the Managed Server window.

Windows patch management supports the following compliance rules:

- **Patch Added to Policy:** The patch has been added to the patch policy.
- **Patch Installed on Server:** The patch has been installed on the managed server.
- **Exception Type:** The Exception Type can have the following values:
  - **Always Installed:** The patch should be installed on the server, even if the patch is not in the policy.
  - **Never Installed:** The patch should not be installed on the server, even if the patch is in the policy.
  - **None:** An exception has not been specified for the patch and server.
- **Exception Reason:** A description entered in the Exception Reason of the Set Policy Exception window. In the Patch Compliance Rules window, the Exception Reason can have the following values.
  - **Yes:** The Exception Reason has data.
  - **No:** The Exception Reason is empty.
  - **N/A:** An exception has not been specified for the patch and server.
- **Compliance Result:** The icon that indicates the result of the patch compliance scan. These icons are displayed in the Managed Server window.

# Patch Administration

As a best practice in your data center environment, you should customize patch administration for Windows so that you can:

- Specify whether you want patches immediately available for installation by using a command-line script or the SA Client.
- Import the Microsoft patch database on demand by using a command-line script or the SA Client.
- Customize the icon display of policy compliance scan results.
- Easily find servers that require a reboot.
- Track and import only patches that apply to certain Microsoft products or particular locales.
- Import and export Windows patch utilities.
- Manually launch on demand or schedule periodic policy compliance scans to determine the patch state of your managed servers.

## Prerequisite for Importing the Patch Database & Utilities

Before you can import the Microsoft patch database or Windows patch utilities, you must configure your browser to *not* use the web proxy when communicating with your SA core.

To configure your browser:

- 1 In the Log in to HP Server Automation Client window, click **More** to expand the window.
- 2 Click **Advanced Settings** to open the Advanced Settings window.
- 3 In the Proxies section, if the Use Browser is selected, configure your browser to *not* use the web proxy when communicating with your SA core.  
Or
- 4 In the Proxies section, if Manual is selected (which means that the proxy is set manually), enter the core's IP or hostname in the No Proxy Hosts text box. This will ensure that the SA Client communicates directly with the SA core

## Setting Patch Availability

You can set the default patch availability by using the SA Client or a command-line script. The default used by the script overrides the default set by the SA Client. For information about the script, see [Importing Windows Patches](#) on page 30.

To set the default value for the availability of a newly imported patch by using the SA Client:

- 1 In the navigation pane, select **Administration** ► **Patch Settings**.
- 2 From the **Default Availability for Imported Patches** drop-down list, select either **Limited Availability** or **Available**.

**Limited Availability (Default)**—A patch marked Limited Availability has been imported into Server Automation and can be installed only by a patch administrator who has the required permissions. To obtain these permissions, contact your system administrator. See the *SA Administration Guide* for an explanation of these permissions.

**Available**—A patch marked Available can be installed on managed servers.

## Importing the Microsoft Patch Database

You can import the Microsoft Patch Database by using the SA Client or a command-line script. For information about the script, see [Importing Windows Patches](#) on page 30.



Before you can import the Microsoft patch database, you must configure your browser to *not* use the web proxy when communicating with your SA core. See [Prerequisite for Importing the Patch Database & Utilities](#) on page 51 for instructions.

---

To import the database by using the SA Client:

- 1 In the navigation pane, select **Administration ► Patch Settings**.
- 2 In the Windows MBSA tab, select **Patch Database**.
- 3 To import the database from the Microsoft web site, click **Import from Vendor**.

The Import from Vendor window displays the default URL for the location of the database on the Microsoft web site. Click **Import**. To re-import a new version of the Microsoft database that is released monthly, you must use the default URL.

- 4 To import the database from the local file system, click **Import from File**.

In the Import Microsoft Patch Database window, verify that the file name is `wsusscn2.cab` and then click **Import**. This file must have been previously downloaded from the Microsoft web site and copied to the local file system.



To be imported, a patch must be in the Microsoft Patch Database that has already been imported into the SA Software Repository.

---

## Selecting Windows Products to Track for Patching

You can limit the patches tracked by Server Automation to specific Windows products. When you import the Microsoft Patch Database, any new patches listed by SA are limited to the products that you selected. Patches that were previously listed by SA are still tracked. You can also track patches for Windows Update Agent (WUA).

To limit the patches tracked to specific Windows operating systems, run the command-line script that automatically imports patches. See [Importing Windows Patches](#) on page 30 for more information about the script.

To select Windows products to track for patching by using the SA Client:

- 1 In the navigation pane, select **Administration** ► **Patch Settings**.
- 2 In the Windows MBSA tab, select Patch Products and then click **Edit**.
- 3 In the Edit Patch Products window, use the include (+) and exclude (-) arrows to select the products whose patches you want to import.
- 4 Click **OK** to save your settings.

## Scheduling a Patch Compliance Scan

To schedule a patch compliance scan on all Windows managed servers:

- 1 In the navigation pane, select **Administration** ► **Compliance Settings**.
- 2 In the Compliance Settings content pane, in the Patch Compliance Schedule section, click **Edit Settings**.
- 3 In the Schedule Compliance Scan window, select **Enable Compliance Scan**.
- 4 From the Schedule drop-down list, select the frequency of the scans.

If you select Custom, specify the `crontab` string with the following values:

- Minute (0-59)
- Hour (0-23)
- Day of the month (1-31)
- Month of the year (1-12)
- Day of the week (0-6 with 0=Sunday)
- Any of these fields can contain an asterisk to indicate all possible values. For example, the following `crontab` string runs the job at midnight every weekday:

```
0 0 * * 1-5
```

The `crontab` string can also handle serial (1,2,3,4) as well as range (1-5) values. For more information, consult the `crontab` man pages on a Unix computer.

- 5 In the Start Time field, specify the time you want the job to begin.

- 6 From the Time Zone drop-down list, select a default time zone for the job execution time or accept the default time zone. The default time shown converts the scheduled time to the time zone set in your user preferences. If you do not set a preferred time zone, the time zone is derived from the Server Automation core server, which is typically UTC.
- 7 Click **OK** to save your settings.

## Setting a Patch Compliance Level

The patch policy compliance level defines your patch compliance level.

To set the patch compliance level:

- 1 In the navigation pane, select **Administration** ► **Compliance Settings**.
- 2 From the Compliance Rules drop-down list, select one of the following compliance levels: Policy Only, Policy and Exception, or Customized.

If you select Customized, click **Edit Custom** to open the Edit Customized Policy Compliance Level window. To edit the compliance level, click the icon in the Compliance Result column. Click **Apply** to save your changes.

## Importing Windows Patch Utilities

To enable patch management for Windows servers, you must import the Windows patch utilities.



---

If you do not plan to use SA to manage your Windows servers, you can optionally choose not to install these files and still successfully complete the installation process. However, if these files are not installed, no operations against Windows servers should be performed. These files are required for many Windows-based operations other than Windows patching.

---



---

During an SA core installation, the `windows_util_loc` parameter is not changed. If you change this parameter to `none`, the Windows utilities will not be imported during a core installation and operations on Windows servers will not be supported. See the *SA Simple/Advanced Installation Guide* for more information.

---



---

Before you can import the Windows utilities, you must configure your browser to *not* use the web proxy when communicating with your SA core. See [Prerequisite for Importing the Patch Database & Utilities](#) on page 51 for instructions.

---

After you install an SA core, you can import (download) the following Windows utilities from the vendor:

- `qchain.exe`
- `WindowsUpdateAgent-ia64.exe`
- `WindowsUpdateAgent-x64.exe`
- `WindowsUpdateAgent-x86.exe`

To import Windows patch utilities:

- 1 In the navigation pane, select **Administration** ► **Patch Settings**.
- 2 Click **Import from Vendor**.
- 3 In the Import from Vendor window, select one or more utilities and then click **Import**.  
The Importing Utility Update window displays the status of the process. If the Status indicates that the job failed, double-click the error icon **✖** to display the error message.
- 4 After the process completes, click **Close**.

## Exporting Windows Patch Utilities

You can export the following Windows utilities from Server Automation to your local file system:

- qchain.exe
- WindowsUpdateAgent-ia64.exe
- WindowsUpdateAgent-x64.exe
- WindowsUpdateAgent-x86.exe

To export a Windows patch utility:

- 1 In the navigation pane, select **Administration** ► **Patch Settings**.
- 2 In the Windows Patch Utilities section, select one or more utilities.
- 3 Click **Export Utility**.
- 4 In the Export Patch Utility window, specify a location in your file system.
- 5 Click **Export**.

## Finding Servers that Require a Reboot

The following are typical use cases where a Reboot Pending server state occurs:

- When a Windows patch or package is installed or uninstalled and a reboot is not performed, the server is marked as needing a reboot.
- When a Windows package is installed or uninstalled and the SA metadata for the package indicates that a reboot is required, but no reboot is performed, the server is marked as needing a reboot.



---

When a server has a state of Reboot Pending, a subsequent install or uninstall patch action might fail. Before performing any subsequent patch install or uninstall actions on the server or group of servers (device group), you must first reboot the server.

---

In SA, you can easily determine whether an individual managed server requires a reboot by reviewing its properties or by filtering the list of managed servers. You can also use the SA Client Search feature to find all managed servers and device groups in your data center that require a reboot.

## Reboot Required for a Single Managed Server

Review the managed server's properties to determine whether it requires a reboot.



To find this information:

- 1 In the All Managed Servers pane, select a server and then select Properties in the View drop-down list.
- 2 In the bottom Properties pane, review the Reboot Required field. A "Yes" value means that this server requires a reboot.
- 3 With the server selected, right-click and then select Reboot Server to manually reboot or schedule a reboot for the server, using the Reboot Server wizard. See [Rebooting a Server](#) on page 90.

## Reboot Required for All Managed Servers

You can easily filter the All Managed Servers pane to determine which servers require a reboot.

To find this information:

- 1 In the All Managed Servers pane, use the search tool  to select Reboot Required.
- 2 A "Yes" value in the Reboot Required column means that this server requires a reboot.  
  
Use the column selector  to make sure you have this column set to show.
- 3 With one or more servers selected, right-click and then select Reboot Server to manually reboot or schedule a reboot for the server(s), using the Reboot Server wizard. See [Rebooting a Server](#) on page 90.

## Reboot Required for Multiple Servers & Device Groups

Use the SA Client Search feature to find all servers that have had a patch or package installed, that require a reboot. This information allows you to schedule reboots for these servers and device groups.

To find servers and device groups that require a reboot:

- 1 In the Advanced Search window, in the Where field, select Reboot Required.
- 2 Keep Equals as the default operator.
- 3 In the Select Values dialog, in Available, select Yes and click the plus (+) arrow to move this setting to Selected.
- 4 Click **OK** to save your Select Values settings.
- 5 In the Advanced Search window, click **Search** to display a list of servers that require a reboot. For each server in this list, the Reboot Required column displays Yes.
- 6 Select one or more servers in this list.
- 7 Right-click and then select Reboot Server to manually reboot or schedule a reboot for one or more servers or device groups, using the Reboot Server wizard. See [Rebooting a Server](#) on page 90.



## Patch Locales

The locale of a patch identifies the language of the Windows servers that should receive the patch. A patch with the same name might be available for different locales. For example, a patch named Q123456 might be available for servers running the English and Japanese versions of Windows. Although they have the same name, the patches installed on the English and Japanese servers are different binaries.

Windows patch management supports multiple locales in the same SA multimaster mesh. To install a patch on Windows servers with different locales, you specify the patch by name. During the installation (or policy remediation), SA matches the locale of the patch with the locale of each managed server. You do not need to repeat the installation for each locale.

## Supported Locales

Windows patch management supports Microsoft patches for the following locales:

- English (en)
- French (fr)
- German (de)
- Italian (it)
- Japanese (ja)
- Korean (ko)

## Locale Configuration Tasks

By default, Windows patch management supports only the English locale. To set up Windows patching for non-English locales, complete the instructions in the following sections:

- [Configuring the SA Core for Non-English Locales](#) on page 57
- [Selecting the Locales of Patches to Import](#) on page 58
- [End User Requirements for Non-English Locales](#) on page 59

### Configuring the SA Core for Non-English Locales



---

This task requires `root` access to core servers and a restart of the SA Web Client.

---

To configure the core for non-English locales, complete the following steps on each core server that is running the SA Web Client:

- 1 Log on to the server as `root`.
- 2 In `/etc/opt/opsware/occ/psrvr.properties`, change the line for `pref.user.locales` to `pref.user.localesAllowed=en;ja;ko`

- 3 Restart the SA Web Client on the core:

```
/etc/init.d/opsware-sas restart occ.server
```

- 4 In a text editor, open the following file:

```
/opt/opsware/occclient/jnlp.tpl
```

- 5 For the Japanese language, in the <resources> section of the jnlp.tpl file, add the following XML element:

```
<property name="com.opsware.ngui.font.japanese" value="Arial Unicode MS"/>
```

- 6 For the Korean language, in the <resources> section of the jnlp.tpl file, add the following XML element:

```
<property name="com.opsware.ngui.font.korean" value="Arial Unicode MS"/>
```

- 7 In the /opt/opsware/occclient directory, if the following files exist, delete them:

```
$HOST_ja.jnlp
```

```
$IP_ja.jnlp
```

```
$HOST_ko.jnlp
```

```
$IP_ko.jnlp
```

- 8 Complete the steps in [Selecting the Locales of Patches to Import](#) on page 58.

## Selecting the Locales of Patches to Import



---

Complete the instructions in [Configuring the SA Core for Non-English Locales](#) on page 57 before performing the steps in this section.

---

This operation selects the locales of the Windows patches to import into Server Automation. The selections take effect the next time patches are imported into SA. After the patches have been imported, they can be installed on managed servers. If you remove locales from the list with this operation, patches with those locales that have already been imported are not removed from SA.

To select the locales of the Windows patches to import into SA:

- 1 In the navigation pane, select **Administration**.
- 2 Select **Patch Settings**.
- 3 In the Windows MBSA tab, select Patch Locales.
- 4 Click **Edit**.
- 5 In the Edit Patch Locales window, use the include (+) and exclude (-) arrows to select the locales whose patches you want to import.

If you want to select a locale that is not listed in [Supported Locales](#) on page 57, contact Support.

- 6 Click **OK** to save your settings.
- 7 Complete the steps in [End User Requirements for Non-English Locales](#) on page 59.

## End User Requirements for Non-English Locales

To view non-English fonts in the SA Client:

- 1 Verify that the Windows desktop running the SA Client uses the Arial Unicode MS font.
- 2 After the system administrator performs the steps in [Configuring the SA Core for Non-English Locales](#) on page 57, the end user logs on to the SAS Web Client and goes to the My Profile page,
- 3 On the My Profile page, the end user updates the Locale field on the User Identification tab. For example, if the system administrator configured the core for Japanese, then the end user sets the Locale field to Japanese.

## Patch Installation

patch management provides the following two phases in the patch installation process:

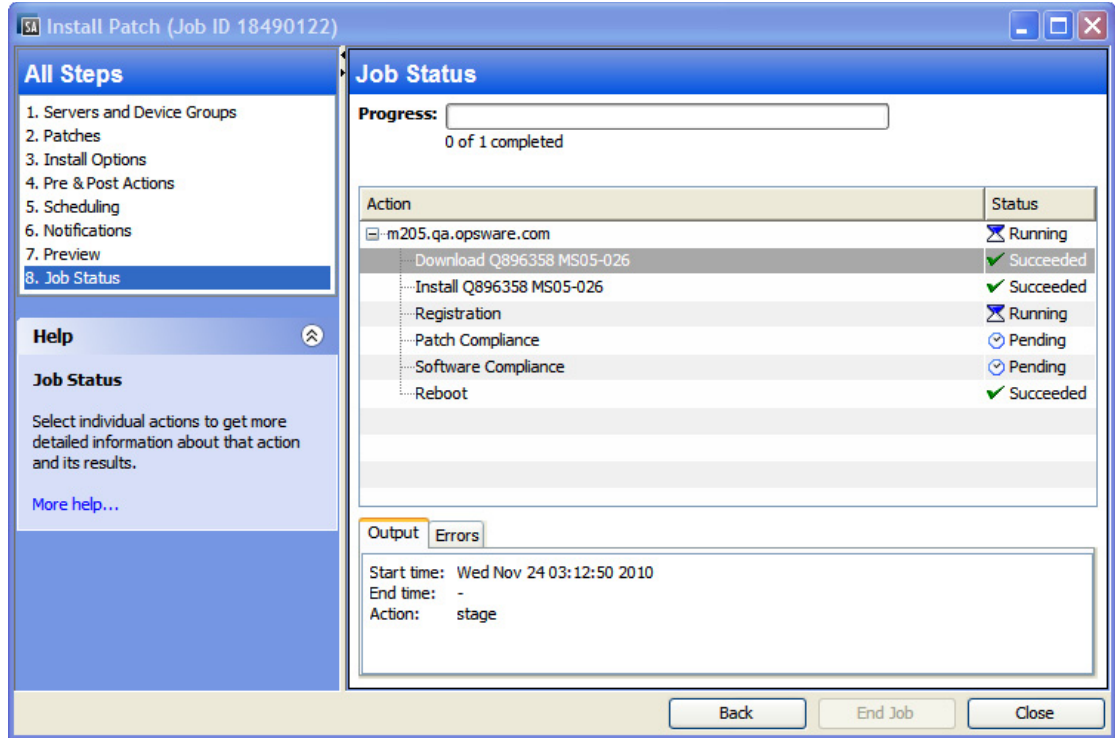
- **Phase 1—Download/Staging:** This is when the patch is downloaded from Server Automation to the managed server. This phase is commonly referred to as *staging*.
- **Phase 2—Installation/Deployment:** This is when the patch is installed on a managed server. This phase is commonly referred to as *deployment*.

You can specify whether you want the installation to occur immediately after the patch is downloaded (staged) or you can schedule the installation to occur at a later date and time. Windows patch management also supports the need for best-effort installations of multiple patches by allowing you to specify that the patch installation process will continue even when an error occurs with one of the patches.

Windows patch management displays the name of the command, such as an .exe file and any predefined command-line arguments, that the SA Agent runs on the managed server to install the patch. You can override these default command-line arguments.

To help you optimally manage Windows patch installation, patch management allows you to manage server reboot options, specify pre and post installation scripts, simulate (preview) a patch installation, and set up email notifications to alert you about the status of the installation process. The Install Patch wizard guides you through setting up these conditions. See [Figure](#) .

## Install Patch Wizard



## Installation Flags

You can specify installation flags that are applied whenever a Windows patch is installed. However, Server Automation also uses default installation flags and requires that patches are installed with these flags. Therefore, you must be sure that you do not specify any installation flags that override or contradict the default flags passed by Server Automation. See [Setting Windows Install Options](#) on page 63 for information about how to specify commands and flags.



Some Windows hotfixes do not support the `-z` flag, some do not support the `-q` flag, and some do not support either. In such cases, you must use a special expression: `/-z` or `/-q` or `/-z -q` respectively. This prevents Windows patch management from passing in the `-z` or `-q` or `-z -q` flag. By default, SA adds `/z /q` to the command line arguments when installing patches. To override this, specify `/-z /-q`. For example, if you prefer to not suppress the reboot, specify `/-z`.

The following table lists the default installation flags that Server Automation uses.

**Table 3** Default Installation Flags

Windows Patch Type	Flags
Windows Hotfix	<code>-q -z</code>
Windows Security Rollup Package (treated identically like a Hotfix by WIndows patch management)	<code>-q -z</code>
Windows OS Service Pack	<code>-u -n -o -q -z</code>

## Application Patches

Windows patch management does not allow you to apply a patch to an operating system for which the patch is not intended. When you are installing an application patch, ad hoc installation does not automatically filter out servers that do not have the corresponding application installed. Although Windows patch management does not prevent you from doing so, you should not attempt to apply application patches to servers that do not have the necessary applications installed. If a patch is for an application that is not installed on the server, the patch will not be applied and an error message will display, such as “There was an error with package <name of the package>”.

If an application patch is intended for an application that is running on more than one version of the same operating system, you cannot apply the patch to all of the servers at the same time. An application patch is associated with only one operating system version. You must first select the patch for one operating system, select the servers where the application is installed, and apply the patch. You must repeat this process for each version of the operating system where the application is installed.

Similarly, when uninstalling application patches that are installed on multiple versions of the same operating system, you cannot uninstall all of the patches at the same time. You must repeat the uninstallation process for each version of the operating system where the patch is installed.

## Service Packs, Update Rollups, & Hotfixes

When you try to install a Service Pack, Update Rollup, or a Hotfix, there is a known delay when a confirmation dialog displays. Since the SA Agent is installing or uninstalling the patch, it cannot respond to the confirmation dialog. The Agent will time out an installation or uninstallation process if you do not click **OK** in the confirmation dialog.

- For Hotfixes, the Agent will time out if five minutes have lapsed and you have not clicked **OK** in the confirmation dialog.
- For Service Packs and Update Rollups, the Agent will time out if 60 minutes have lapsed and you have not clicked **OK** in the confirmation dialog.

To prevent this from happening, patch install and uninstall commands should have arguments that invoke silent mode installs and uninstalls. By default, the `-q` flag is set.

## Installing a Windows Patch

Before a patch can be installed on a managed server, it must be imported into Server Automation and its status must be Available. Administrators who have the required permissions can install patches that are marked Limited.



---

You must have permissions to manage patches. To obtain these permissions, contact your system administrator. See the *SA Administration Guide*.

---

You can perform the installation by explicitly selecting patches and servers, and you can install a patch even if the patch policy exception is Never Install.

To install a patch on a managed server:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**.
- 2 Expand the Patches and select a specific Windows operating system.
- 3 In the content pane, select a patch.
- 4 From the View drop-down list, select Servers (or Device Groups).
- 5 From the Show drop-down list, select **Servers without Patch Installed** or **Device Groups without Patch Installed**.
- 6 In the preview pane, select one or more servers.
- 7 From the **Actions** menu, select **Install Patch**.

The first step of the Install Patch window appears: 1. Servers and Device Groups. For instructions on each step, see the following sections:

- [Setting Windows Install Options](#)
- [Setting Reboot Options for a Windows Patch Installation](#)
- [Specifying Install Scripts for a Windows Patch Installation](#)
- [Scheduling a Windows Patch Installation](#)
- [Setting Up Email Notifications for a Windows Patch Installation](#)
- [Previewing a Windows Patch Installation](#)
- [Viewing Job Progress of a Windows Patch Installation](#)

After you have completed a step, click **Next** to advance to the next step. Before you click **Start Job**, you can return to a completed step to make changes by clicking on it in the list of steps.

- 8 When you are ready to launch the installation job, click **Start Job**.

After you launch the job, you cannot change its parameters, even if the job is scheduled to run at a later time.

If the Install Patch window remains open until the job completes, Windows patch management updates the Patch Compliance column in the All Managed Servers window with the revised compliance count (in parenthesis) for affected servers. Press **F5** or select **Refresh** from the View menu to update information in the Patch Preview pane.

See [Remediating Patch Policies](#) on page 37 for another method of installing a patch.

## Setting Windows Install Options

You can specify the following types of patch installation options:

- Perform the patch installation immediately after the patch is downloaded or at a later date and time.
- Do not interrupt the patch installation process, even when an error occurs with only one of the patches.
- Use different command-line options to perform the installation.

To set these options:

- 1 In the Install Patch window, click **Next** to advance to the Install Options step.
- 2 Select one of the following Staged Install Options:
  - **Continuous**: This allows you to run all phases as an uninterrupted operation.
  - **Staged**: This allows you to schedule the download and installation to run separately.
- 3 Select the Error Options check box if you want the patch installation process to continue even when an error occurs with one of the patches. As a default, this check box is not selected.
- 4 In the Install Command text box, enter command-line arguments for the command (.exe file) that is displayed. By default, Server Automation adds `/z /q`. If you want to override these install flags, enter `/-z /-q` in the text box.
- 5 Click **Next** to go to the next step or click **Cancel** to close the Install Patch window.

## Setting Reboot Options for a Windows Patch Installation

To minimize the downtime that server reboots can cause, you can control when servers will and will not be rebooted. You can adopt the vendor's reboot assignments, reboot a server each time a patch is installed on it, completely suppress all server reboots, or postpone reboots until all patches have been installed.



When you are selecting reboot options in the Install Patch window, HP recommends that you use Microsoft's reboot recommendations, which is the **Reboot servers as specified by individual software items** option. If it is not possible to use the Microsoft reboot setting, select *the single reboot option*, which is the **Hold all server reboots until after all packages are installed and/or uninstalled** option. Failure to do this can result in WUA incorrectly reporting the patches that are installed on the server until the next reboot occurs (outside of SA control).

The following options determine whether the servers are rebooted after the patch is installed. These options apply only to the job launched by the Install Patch window; they do not change the Reboot Required that is in the Install Parameters tab of the Patch Properties window.



If a server has a state of Reboot Pending, a subsequent install patch action may fail. Before performing any subsequent patch installation actions on the server, you must first reboot the server. See [Finding Servers that Require a Reboot](#) on page 55.

Except for the first option, the following options override the Reboot Required option.

- **Reboot servers as specified by individual software items (Default)**: By default, the decision to reboot depends on the Reboot Required option of the patch properties.
- **Reboot servers after each patch install**: Even if the Reboot Required option of the patch properties is not set, reboot the server. If multiple patches are installed, the server reboots multiple times.

- **Suppress all server reboots:** Even if the Reboot Required option of the patch properties is set, do not reboot the server. Because of vendor settings, some patches ignore the suppress option and force a reboot. For a service pack, if a reboot is suppressed, then the action is incomplete—the service pack is not installed until after the reboot. The system does not have the software installed. The status is “Not Installed/Uninstalled”. If you manually check the system (look at the registry or server properties), this is not the same information that displays in the SA Client. After the reboot, the SA Client will not reflect the correct software or patch installed information until after the next software registration.

*Note:* When you suppress reboot during a Windows patch installation (such as for a service pack), the system's software state might not accurately display. Accurate state information will display after the managed server is rebooted and software registration has completed.

- **Hold all server reboots until after all packages are installed and/or uninstalled:** If the Reboot Required option is set for some selected patches but not for others, the server is rebooted one time after all patches are installed. This option is commonly known as *the single reboot option*. If the Reboot Required option is not set for any of the selected patches, the server is not rebooted.

To set reboot options:

- 1 From the Install Patch window, click **Next** to advance to the Pre & Post Actions step.
- 2 Select one of the Rebooting Options.
- 3 Click **Next** to go to the next step or click **Cancel** to close the Install Patch window.

## Specifying Install Scripts for a Windows Patch Installation

For each patch, you can specify a command or script to run before installation or after installation. A pre-install script, for example, could check a certain condition on the managed server. If the condition is not met or if the pre-install script fails, the patch would not be installed. A pre-install script could also be used to shut down a service or application before it is patched. A post-install script could be used to perform a certain cleanup process on the managed server.

You can also specify the following types of scripts to run on the managed server before or after an installation or download phase:

- **Pre-Download:** A script that runs before patches are downloaded from SA to the managed server. This is available only if you select Staged in the Install Options step.
- **Post-Download:** A script that runs after patches are downloaded from SA to the managed server and before the patch is installed. This is available only if you select Staged in the Install Options step.
- **Pre-Install:** A script that runs before patches are installed on the managed server.
- **Post-Install:** A script that runs after patches are installed on the managed server.

To specify a pre-install script:

- 1 From the Install Patch window, click **Next** to advance to the Pre & Post Actions step.
- 2 Select the Pre-Install tab. You may specify different scripts and options on each of the tabs.
- 3 Select Enable Script. This option enables the remainder of the fields on the tab. If Enable Script is not selected, the script will not run.



- 4 Select either Saved Script or Ad-Hoc Script.

A Saved Script has been previously stored in Server Automation with the SA Web Client. To specify the script, click **Select**.

An Ad-Hoc script runs only for this operation and is not saved in Server Automation. Select the Type, such as .bat. In the Script box, enter the contents of the script, including the drive letter of where the script is located, such as echo dir>> C:\temp\preinstall1.log. If you do not enter a drive letter, the default is %SYSTEMDRIVE%, which is where the system folder of Windows is installed.

- 5 If the script requires command-line flags, enter the flags in the Command text box.
- 6 Specify the information in the User section. If you choose a system other than Local System, enter the User Name, Password, and Domain. The script will be run by this user on the managed server.
- 7 To stop the installation if the script returns an error, select the Error check box.
- 8 Click **Next** to go to the next step or click **Cancel** to close the Install Patch window.

## Scheduling a Windows Patch Installation

Since the two phases of Windows patching can be decoupled, you can schedule when you want patches installed independently of when you want patches downloaded.

To schedule a patch installation:

- 1 From the Install Patch window, click **Next** to advance to the Scheduling step.

By default, the Scheduling step displays only the scheduling options for the installation phase. If you selected Staged in the Install Options step, the scheduling options for the download phase will also be displayed.

- 2 Select one of the following Install Phase options:
  - **Run Task Immediately:** This enables the system to perform a preview analysis in the Summary Review step. The scheduling option for the download phase is **Run Immediately Following Download**.
  - **Run Task At:** This enables you to specify a later date and time that you want the installation or download performed.
- 3 Click **Next** to go to the next step or click **Cancel** to close the Install Patch window.



---



A scheduled patch installation can be cancelled prior to its execution, even if the patch download has already completed.

---

## Setting Up Email Notifications for a Windows Patch Installation

You can set up email notifications to alert users when the download and installation operations complete successfully or with errors.

To set up email notifications:

- 1 From the Install Patch window, click **Next** to advance to the Notifications step.
- 2 To add email addresses, click **Add Notifier** and enter the email addresses in the Notification Email Address field.
- 3 To set the notification status on the success of a Job, select the  icon. To set the notification status on the failure of a Job, select the  icon. By default, the Notification step displays only the notification status for the installation phase.
- 4 Enter a Ticket ID to be associated with a Job in the Ticket ID field.
- 5 Click **Next** to go to the next step or click **Cancel** to close the Install Patch window.



---

If you previously selected Staged in the Install Options step, the Notifications pane displays notification options for both the download and installation phases.

---

## Previewing a Windows Patch Installation

The installation preview process provides an up-to-date report about the patch state of servers. The installation preview is an optional step that lets you see the patches that will be installed on managed servers and the type of server reboots that are required. This preview process verifies whether the servers that you selected for the patch installation already have that patch installed, based on WUA. In some cases, a server could already have the patch installed if a system administrator had manually installed it, which means that Windows patch management does not know about it.

The preview process also reports on dependency and supersedence information, such as patches that require certain Windows products, and patches that supersede other patches or are superseded by other patches. If a dependency is not met, patch management will display an error message indicating this condition.

For example, if a managed server is not running Windows Server 2003 x86/x64 or Windows Server 2008 x86/x64, and an Server Automation 5.5 Agent, patch management will report that a dependency has not been fulfilled. If you try to install a patch for Service Pack 4 and your server is using Service Pack 3, the remediate preview will display a “Will Not Install” error message to indicate this discrepancy. The Install Patch window allows superseded patches to be installed.

The following list explains user cases in which a patch will not be installed, as displayed in the Preview step of the Install Patch or Remediate Patch Window:

- This patch has a Never Install patch policy exception, so it will not be installed.
- This patch is superseded by another patch in the same job, so it will not be installed. This means that another patch in the current job is more up to date than the marked patch.
- This patch is superseded by another patch, so it will not be installed. This means that the patch installed on the server is more recent than the patch in the policy, so it will not be installed.

- This patch is not applicable because it is not recommended by WUA, so it will not be installed.
- This patch is for a different locale, so it will not be installed.

This information is also displayed in the Job results window and in an email, if email notification has been configured for the patch install job.



The installation preview does not report on the behavior of the server as though the patches have been applied.

#### To preview a patch installation:

- 1 From the Install Patch window, click **Next** to advance to the Summary Review step.
- 2 (Optional) Click **Preview** to see the separate actions that will be performed when the patch is installed. To view the details of a previewed action, select a row in the table.
- 3 Click **Start Job** to launch the installation job or click **Cancel** to close the Install Patch window without launching the installation.

If you selected **Run Task Immediately** in the Scheduling step, the job begins now. If you selected **Run Task At**, the job will be launched at the specified time and date.

## Viewing Job Progress of a Windows Patch Installation

You can review progress information about a patch installation job, such as whether actions have completed or failed.

#### To display job progress information:

- 1 From the Install Patch window, click **Next** to advance to the Job Progress step. This will start the installation job.

The Progress bar and text indicate how many of the actions listed in the table have been completed. For each server, the following actions can be performed:

- **Analyze:** Server Automation examines the patches needed for the installation, checks the managed servers for the most recent patches installed, and determines other actions that it must perform.
  - **Download:** The patch is downloaded from Server Automation to the managed server.
  - **Install:** After it is downloaded, the patch is installed.
  - **Final Reboot:** If this action is specified in the Pre & Post Actions step, the server is rebooted.
  - **Pre/Post Install/Download Script:** If this action is specified in the Pre & Post Actions step, a script is run before or after the installation.
  - **Install & Reboot:** When a patch is installed, the server is also rebooted.
  - **Verify:** Installed patches will be included in the software registration.
- 2 To view additional details about a specific action, select the row in the table to display the start and completion times of the job. In the navigation pane, select Jobs and Sessions to review detailed information about the job. See the *SA User Guide: Server Automation* for more information about browsing job logs.
  - 3 Click **End Job** to prevent the job from running or click **Close** to close the Install Patch window. (Optional) See [Cancelling or Terminating Installation, Uninstallation or Remediation Jobs](#) on page 66.

# Patch Uninstallation

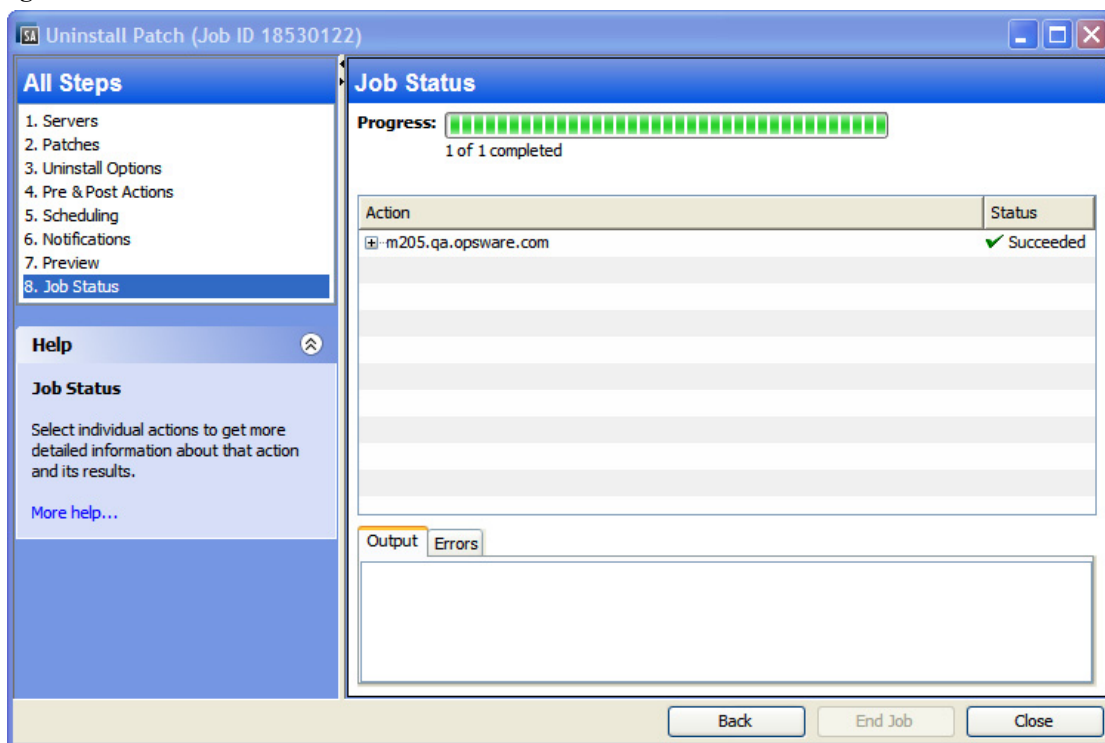
Windows patch management provides granular control over how and under what conditions Microsoft patches are uninstalled (removed) from managed servers. To minimize problems, you can only uninstall one patch at a time. You cannot use Server Automation to uninstall a patch that was not originally installed using Server Automation.

To help you optimally manage these conditions, patch management allows you to do the following:

- Manage server reboot options, and pre and post installation scripts.
- Simulate (preview) a patch uninstallation.
- Set up email notifications to alert you about the status of the uninstallation process.

The Uninstall Patch wizard steps you through setting up these conditions. See [Figure 6](#).

**Figure 6 Uninstall Patch Wizard**



## Uninstallation Flags

You can specify uninstallation flags that are applied whenever a Windows patch is uninstalled. However, SA also uses default uninstallation flags and requires that patches are uninstalled with these flags. You must therefore be certain that you do not specify any uninstallation flags that override or contradict the default flags passed by Server Automation.



Some Windows hotfixes do not support the `-z` flag, some do not support the `-q` flag, and some do not support either. In such cases, you must use a special expression: `/-z` or `/-q` or `/-z -q` respectively, to prevent Server Automation from passing in the `-z` or `-q` or `-z -q` flag. By default, Server Automation adds `/z /q` to the command line arguments when uninstalling patches. To override this, specify `/-z /-q`. For example, if you prefer to not suppress the reboot, specify `/-z`.

Table 4 lists the default uninstallation flags used in SA.

**Table 4** Default Uninstallation Flags

Windows Patch Types	Flags
Windows Hotfix	<code>-q -z</code>
Security Rollup Package	<code>-q -z</code>
Windows OS Service Pack	Not uninstallable

## Uninstalling a Windows Patch

You can uninstall a Service Pack if it was originally installed by SA and can be uninstalled the from the control panel, directly from the server. If the Service Pack cannot be uninstalled by the control panel, then SA cannot uninstall it either.

To remove a patch from a managed server:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**.
- 2 Expand the Patches and select a specific Windows operating system.
- 3 In the content pane, select a patch.
- 4 From the View drop-down list, select Servers.
- 5 From the Show drop-down list, select Servers with Patch Installed.
- 6 In the preview pane, select one or more servers.
- 7 From the **Actions** menu, select **Uninstall Patch**. The first step (Servers) in the Uninstall Patch window appears.  
For instructions on each step, see the following sections:
  - [Setting Uninstall Options](#)
  - [Setting Reboot Options for a Windows Patch Uninstallation](#)
  - [Specifying Install Scripts for a Windows Patch Uninstallation](#)
  - [Scheduling a Windows Patch Uninstallation](#)

- [Setting Up Email Notifications for a Windows Patch Uninstallation](#)
- [Viewing Job Progress of a Patch Uninstallation](#)

After you have completed a step, click **Next** to advance to the next step. Before you click **Start Job**, you can return to a completed step to make changes by clicking on it in the list of steps.

- 8 When you are ready to launch the uninstallation job, click **Start Job**.

After you launch the job, you cannot change its parameters, even if the job is scheduled to run at a later time.

If the Uninstall Patch window remains open until the job completes, patch management updates the Patch Compliance column in the All Managed Servers window with the revised compliance count (in parenthesis) for affected servers. Press **F5** or select Refresh from the View menu to update information in the Patch preview pane.

## Setting Uninstall Options

You can specify the following types of patch uninstallation options:

- Do not interrupt the patch uninstallation process even when an error occurs with one of the patches.
- Use different command-line options to perform the uninstallation.

To set these options:

- 1 From the Uninstall Patch window, click **Next** to advance to the Uninstall Options step.
- 2 Select the Error Options check box if you want the patch installation process to continue even when an error occurs with one of the patches. As a default, this check box is not selected.
- 3 In the Uninstall Command text box, enter command-line arguments for the command (.exe file) that is displayed. By default, Server Automation adds `/z /q`. If you want to override these uninstall flags, enter `/-z /-q` in the text box.
- 4 Click **Next** to go to the next step or click **Cancel** to close the Uninstall Patch window.

## Setting Reboot Options for a Windows Patch Uninstallation

To minimize the downtime that server reboots can cause, you can control when servers will and will not be rebooted. You can adopt the vendor's reboot assignments, reboot a server each time a patch is removed from it, completely suppress all server reboots, or postpone reboots until all patches have been uninstalled.



When you are selecting reboot options in the Uninstall Patch window, HP recommends that you use Microsoft's reboot recommendation. This is the **Reboot servers as specified by individual software items** option. If it is not possible to use the Microsoft reboot setting, select *single reboot option*, which is the **Hold all server reboots until after all packages are installed and/or uninstalled** option. Failure to do this can result in WUA incorrectly reporting which patches are installed on the server until the next reboot occurs (outside of SA control).

The following options determine whether the servers are rebooted after the patch is installed. These options apply only to the job launched by the Uninstall Patch window; they do not change the Reboot Required option, which is on the Uninstall Parameters tab of the patch Properties window.



If a server has a state of Reboot Pending, a subsequent uninstall patch action may fail. Before performing any subsequent patch uninstallation actions on the server, you must first reboot the server. See [Finding Servers that Require a Reboot](#) on page 55.

Except for the first option, the following options override the Reboot Required option.

- **Reboot servers as specified by individual software items** (*Default*): By default, the decision to reboot depends on the Reboot Required option of the patch properties.
- **Reboot servers after each patch install**: Even if the Reboot Required option of the patch properties is not set, reboot the server. If multiple patches are installed, the server reboots multiple times.
- **Suppress all server reboots**: Even if the Reboot Required option of the patch properties is set, do not reboot the server. Because of vendor settings, some patches ignore the suppress option and force a reboot. For a service pack, if a reboot is suppressed, then the action is incomplete—the service pack is not uninstalled until after the reboot. The software has not been uninstalled from the system. The status is “Not Installed/Uninstalled”. If you manually check the system (look at the registry or server properties), this is not the same information that displays in the SA Client. After the reboot, the SA Client will not reflect the correct software or patch removed information until after the next software registration.

*Note:* When you suppress reboot during a Windows patch uninstallation (such as for a service pack), the system's software state might not accurately display. Accurate state information will display after the managed server is rebooted and software registration has completed.

- **Hold all server reboots until after all packages are installed and/or uninstalled**: If the Reboot Required option is set for some selected patches but not for others, the server is rebooted one time after all patches are installed. This is commonly known as the *single reboot option*. If the Reboot Required option is not set for any of the selected patches, the server is not rebooted.

### To set reboot options:

- 1 From the Uninstall Patch window, click **Next** to advance to the Pre & Post Actions step.
- 2 Select one of the Rebooting Options.
- 3 Click **Next** to go to the next step or click **Cancel** to close the Uninstall Patch window.

## Specifying Install Scripts for a Windows Patch Uninstallation

For each patch, you can specify a command or script to run before uninstallation or after uninstallation. A pre-uninstall script, for example, could check a certain condition on the managed server. If the condition is not met or if the pre-uninstall script fails, the patch would not be removed from a server. A pre-uninstall script could also be used to shut down a service or application before it is removed from a server. A post-uninstall script could be used to perform a certain cleanup process on the managed server.

You can specify the following types of scripts to run on the managed server before or after a patch uninstallation:

- **Pre-Uninstall:** A script that runs before the patch is removed from a managed server.
- **Post-Uninstall:** A script that runs after the patch is removed from a managed server.

### To specify a script:

- 1 From the Uninstall Patch window, click **Next** to advance to the Pre & Post Actions step.
- 2 Select the Pre-Uninstall or Post-Uninstall tab.  
You may specify different scripts and options on each of the tabs.
- 3 Select Enable Script.  
This option enables the remainder of the fields on the tab. If Enable Script is not selected, the script will not run.
- 4 Select either Saved Script or Ad-Hoc Script.  
A Saved Script has been previously stored in Server Automation with the SAS Web Client. To specify the script, click **Select**.  
An Ad-Hoc script runs only for this operation and is not saved in Server Automation. Select the Type, such as .bat. In the Script box, enter the contents of the script, including the drive letter of where the script is located, such as `echo dir>> C:\temp\preinstall11.log`. If you do not enter a drive letter, the default is %SYSTEMDRIVE%, which is where the system folder of Windows is installed.
- 5 If the script requires command-line flags, enter the flags in Commands.
- 6 Specify the information in the User section. The script will be run by this user on the managed server.
- 7 To stop the uninstallation if the script returns an error, select Error.



## Scheduling a Windows Patch Uninstallation

You can remove a patch from a server immediately, or at a later date and time.



To schedule a patch uninstallation:

- 1 From the Uninstall Patch window, click **Next** to advance to the Scheduling step.
- 2 Select one of the following Install Phase options:
  - **Run Task Immediately**: This enables you to perform the uninstallation in the Summary Review step.
  - **Run Task At**: This enables you to specify a later date and time that you want the uninstallation performed.
- 3 Click **Next** to go to the next step or click **Cancel** to close the Uninstall Patch window.

## Setting Up Email Notifications for a Windows Patch Uninstallation

You can set up email notifications to alert users when the patch uninstallation operation completes successfully or with errors.

To set up email notifications:

- 1 From the Uninstall Patch window, click **Next** to advance to the Notifications step.
- 2 To add email addresses, click **Add Notifier** and enter the email addresses in the Notification Email Address field.
- 3 To set the notification status on the success of a Job, select the  icon. To set the notification status on the failure of a Job, select the  icon. By default, the Notification step displays only the notification status for the uninstallation phase.
- 4 Enter a Ticket ID to be associated with a Job in the Ticket ID field.
- 5 Click **Next** to go to the next step or click **Cancel** to close the Uninstall Patch window.

## Previewing and Starting a Windows Patch Uninstallation

The uninstallation preview process provides an up-to-date report about the patch state of servers. The uninstallation preview is an optional step that lets you see the patches that will be removed from managed servers. This preview process verifies whether the servers you selected for the patch uninstallation have that patch installed, based on `wsusscn2.cab`.



---

The uninstallation preview process does not report or simulate the behavior of a system with patches removed from the server.

---

### To preview a patch uninstallation:

- 1 From the Uninstall Patch window, click **Next** to advance to the Summary Review step.
- 2 Verify the information displayed for the Servers, Device Groups, and Patches at the top of the window.
- 3 (Optional) Click **Preview** to see the separate actions that will be performed when the patch is uninstalled. To view the details of a previewed action, select a row in the table.
- 4 Click **Start Job** to launch the job or click **Cancel** to close the Uninstall Patch window without launching the uninstallation.

If you selected **Run Task Immediately** in the Scheduling step, the job begins now. If you selected **Run Task At**, the job will be launched at the specified time and date.

## Viewing Job Progress of a Patch Uninstallation

You can review progress information about a patch uninstallation job, such as whether actions have completed or failed.

### To display job progress information:

- 1 From the Uninstall Patch window, click **Next** to advance to the Job Progress step. The Progress bar and text indicate how many of the actions listed in the table have been completed. For each server, the following actions can be performed:
  - **Analyze:** Server Automation examines the patches needed for the uninstallation, checks the managed servers for the most recent patches installed, and determines other actions it must perform.
  - **Uninstall:** The patch is uninstalled.
  - **Final Reboot:** If this action is specified in the Pre & Post Actions step, the server is rebooted.
  - **Pre/Post Uninstall Script:** If this action is specified in the Pre & Post Actions step, a script is run before or after the uninstallation.
  - **Uninstall & Reboot:** When a patch is installed, the server is also rebooted.
  - **Verify:** Installed patches will be included in the software registration.
- 2 To view additional details about a specific action, select the row in the table to display the start and completion times of the job. In the navigation pane, select Jobs and Sessions to review detailed information about the job. See the *SA User Guide: Server Automation* for more information on browsing job logs.
- 3 Click **End Job** to prevent the job from running or click **Close** to close the Uninstall Patch window.  
(Optional) See [Cancelling or Terminating Installation, Uninstallation or Remediation Jobs](#) on page 66.

# 3 Patch Management for HP-UX



## Overview

In Server Automation (SA), patches for the HP-UX operating system are delivered exclusively by HP as *depots*. Depots contain multiple patch products and each patch product contains multiple patch file sets. These depots can be uploaded into Server Automation.

In patch management for HP-UX, you can:

- Create HP-UX software policies from HP-UX patches or patch bundles.
- Identify, install, and remove HP-UX patches from the server.
- Install software and patches by remediating software policies.
- Download metadata information associated with each patch.
- Support multi-platform patches, patch dependencies, and automatic reboots.
- Run compliance scans.

## Features

SA automates HP-UX patch management by enabling you to:

- Define HP-UX software policies that provide a model-based approach to managing your HP-UX servers. Server Automation enables you to create a model of your IT environment using HP-UX software policies. These software policies specify patches and scripts that can be installed on the managed servers.
- Install HP-UX patches and patch bundles on your managed servers.
- Establish a patch installation process.
- Schedule the stages of patch management: analysis, download, and installation. You can also set up email notification for each stage and associate a ticket ID for each job.
- Verify the compliance status of servers, based on software policies.
- Display the Compliance view to see whether servers are configured according to the software policy and to remediate non-compliant servers.
- Search for software resources and servers.
- Use the Library to search for HP-UX packages, patches, and software policies using powerful and flexible search criteria, such as availability, architecture, operating system, reboot options, version, and so on. You can also search for HP-UX software policies by name, folder name, availability, and operating system.
- View patch dependencies and patch applicability analysis while previewing patch installation.

## Prerequisites

You must complete the following tasks to use the patch management for HP-UX:

- Download the HP-UX Software Catalog file.  
You must have a service level contract to download the HP-UX Software Catalog file. Use the `import_hpux_metadata` script to download this file. For more information, review the `-h` option that is provided with this script. See `/opt/opsware/mm_wordbot/util/import_hpux_depots` on page 76.
- Upload the new patches and re-upload the existing HP-UX patches, depots, and bundles to the SA.
- Update the HP-UX agent on all existing managed servers. The agent version must be equal to or higher than `opsware-agent-37.0.0.2.130`.

## Supported Operating Systems

See the *Server Automation Compatibility Matrix* for detailed information about supported HP-UX operating systems for patch management.

## HP-UX Depots

The `import_hpux_depot` script imports HP-UX patches, bundles, and depots into the SA Library. For each source depot, this tool creates a `<depot name>` Depot policy in the SA Library that contains the depot's products.

The `import_hpux_depot` script requires the `.depot` extension to script input:

- By default, standard HP-UX bundles that are downloaded from `http://itrc.hp.com` already have a `.depot` extension.
- By default, HP-UX patches that are downloaded from `http://itrc.hp.com` do not include the `.depot` extension. These patches must be manually downloaded to an HP-UX server, unshared to create a `.depot` file, and then uploaded to the SA Library using the `import_hpux_depot` script.

The `import_hpux_depot` script is located in the following directory:

```
/opt/opsware/mm_wordbot/util/import_hpux_depots
```



Importing patches and depots using the SA Client instead of scripts will not create software policies and patch dependency will not work.

---



After HP-UX patches have been uploaded to the SA Library, you cannot delete them. The delete option is disabled when you select an "HP-UX Patch Product" or an "HP-UX Patch Fileset".

---

Table 5 describes the script's options.

**Table 5 Options of import\_hpux\_depot**

Option	Description
<code>import_hpux_depots [options]</code>	All *.depot files in the current working directory are imported into the Library.
<code>import_hpux_depots [options] &lt;source-directory&gt;</code>	All *.depot files in the specified directory are imported into the Library.
<code>import_hpux_depots [options] &lt;*.depot</code>	The specified depots are imported into the Library.
<code>import_hpux_depots -h</code>	Show additional options.
<code>-b, --bundle-policies create a policy for each depot bundle</code>	For each bundle that appears in a source depot, this tool creates a <bundle name> Bundle policy in the SA Library that contains the bundle's products using the <code>--bundle-policies</code> option.
<code>-f, --force</code>	Force depot products to be imported even if already in the SA Library.
<code>-h, --help</code>	Displays the help message.
<code>-n, --silent</code>	Display errors only.
<code>-o OS, --os=OS</code>	HP-UX release of depot products 10.20, 11.00, 11.11, 11.23, and 11.31. Some patches are common to both 11.23 and 11.31 operating system versions. Use <code>-o=11.23</code> or <code>-o=11.31</code> to upload these patches into the SA Library.
<code>-p POLICY_FOLDER, --policy_folder=POLICY_FOLDER</code>	Path to Library folder in which to create policies.
<code>-s SPLIT, --split=SPLIT How to split each depot (default: product): 'product', 'instance', 'none'</code>	<p>Products that are already in the SA Library are not re-imported unless <code>--force</code> is specified.</p> <p>By default, depots containing multiple products are split by product so that each product is kept in the SA Library as its own self-contained depot. The split behavior is controlled by the <code>--split</code> option:</p> <ul style="list-style-type: none"> <li><code>none</code>—Source depots are not split but are imported as is.</li> <li><code>product</code>—Source depots are split by product. If a depot contains multiple instances of the same product (by name), the instances are kept together. This is the default.</li> <li><code>instance</code>—Source depots are split by product instance. If a depot contains multiple instances of the same product (by name), each instance is split into its own depot.</li> </ul>
<code>-u USERNAME, --username=USERNAME</code>	Upload packages as specified user (default: opsware).
<code>-v, --verbose</code>	Display verbose output

**Table 5 Options of import\_hpux\_depot (cont'd)**

Option	Description
--manual	Show manual page and exit.
--version	Show version and exit.

## HP-UX Software Catalog File

The HP-UX Software Catalog file is the HP-UX Patch Database in XML format. The catalog file is `swa_catalog.xml` and can be downloaded from <ftp://ftp.itrc.hp.com/export/patches>.

The HP-UX Metadata script is used to import the HP-UX Software Catalog file into the SA Library. This script can list dependent patches for any patch that exists in the software catalog file and indicate the dependent patches that are missing in the package repository.

The HP-UX Metadata script is located in the following directory:

```
/opt/opsware/mm_wordbot/util/import_hpux_metadata
```

Table 6 describes the script's options.

**Table 6 Options of the HP-UX Metadata Script**

Option	Description
-a HPUX_ANALYZE_PATCHES, --analyze_patches=HPUX_ANALYZE_PATCHES	Specifies the HP-UX patches that will be analyzed for any dependent patches missing in the package repository. Multiple HP-UX patches can be specified by separating them with a comma (.). To analyze all HP-UX patches in the package repository, include the keyword <code>all</code> .
-c HPUX_SW_CATALOG_FILE, --catalog_file=HPUX_SW_CATALOG_FILE	Specifies the source location of the HP-UX software catalog file. The <code>swa_catalog.xml</code> catalog file can be downloaded from <a href="ftp://ftp.itrc.hp.com/export/patches">ftp://ftp.itrc.hp.com/export/patches</a> . This option does not apply when the user ID and password are specified.
-d DISPLAY_DEPENDENCIES,--display_dependencies=DISPLAY_DEPENDENCIES	Specifies HP-UX patches for which the dependencies should be displayed. To display the dependencies for all patches in the software catalog file, include the keyword <code>all</code> .
-h, --help	Displays the help message.
-n, --no_supersedence	Flag is used with the <code>-a</code> option indicating whether to use the superseded dependence tree or the basic dependence tree for reporting missing patches. The superseded dependence tree is the default behavior for HP-UX patching. It performs the most recent dependency check. The basic dependency tree performs the least recent dependence check.

**Table 6 Options of the HP-UX Metadata Script (cont'd)**

Option	Description
-p PASSWORD --password=PASSWORD	The password that is required to access the <i>itrc.hp.com</i> website to automatically download the <i>swa_catalog.xml</i> file. Both user ID and password must be specified.
-u USERID, --user=USERID	The user ID that is required to access the <i>itrc.hp.com</i> website to automatically download the <i>swa_catalog.xml</i> file. Both user ID and password must be specified.

## Software Policy Management

In Server Automation, HP-UX software policies enable you to install HP-UX software and patches on servers and groups of servers. When you create a software policy, you attach it to servers or groups of servers. When you remediate a server or a group of servers, the patches specified in the attached software policy are automatically installed. The remediation process compares what is actually installed on a server with the software policy that specifies the patches that should be installed on the server. SA then determines what operations are required to modify the server to bring it *in compliance* with the policy. The following sections describe how to manage HP-UX software policies.

### Creating an HP-UX Software Policy

In the SA Client, you create a software policy by using either one of the following Library features:

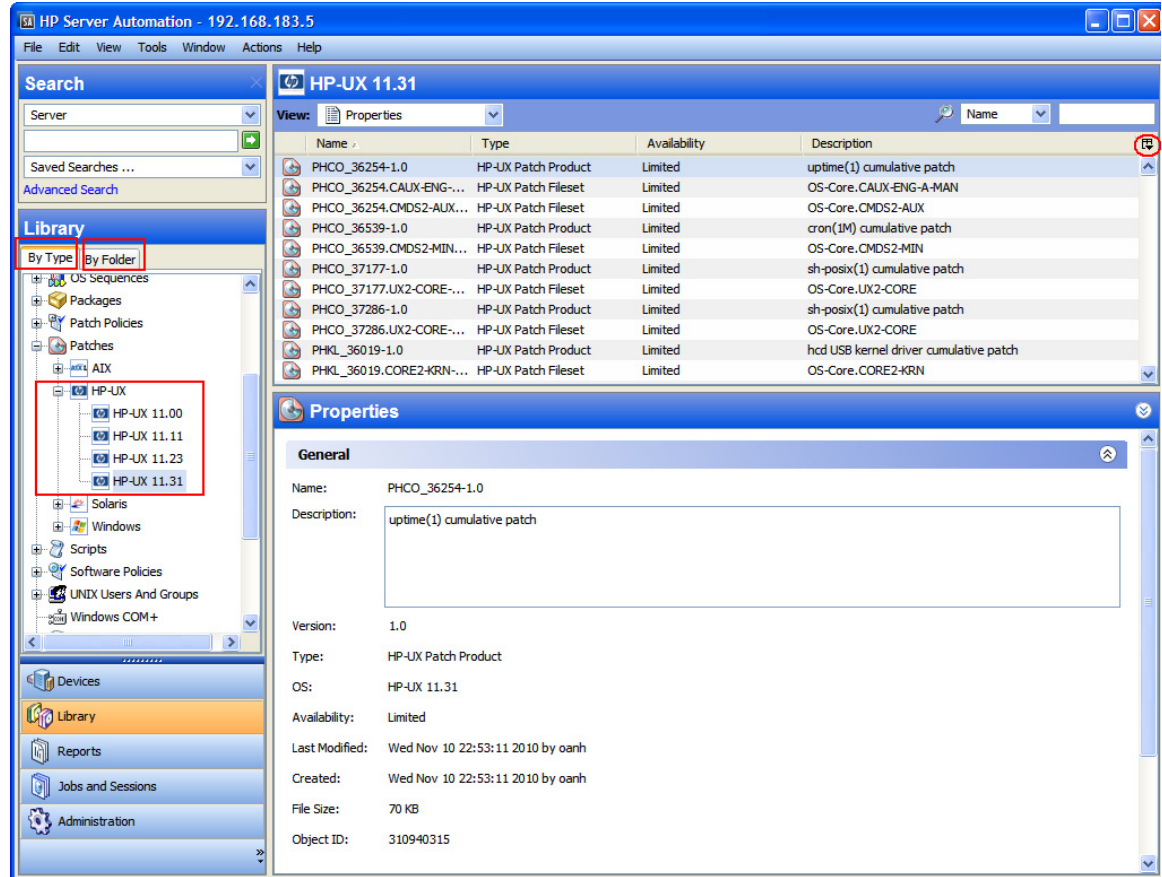
- Library—By Type
- Library—By Folder



You must have permissions to create and manage an HP-UX software policy. To obtain these permissions, contact your system administrator. See the *SA Administration Guide* for more information about software management permissions.

In the content pane, a dimmed patch icon indicates that the patch has not been uploaded to the Library. Use the column selector to control the columns of patch metadata data that you want to display. See [Table 7](#).

Figure 7 HP-UX Patches in the SA Client Library



## Library—By Type

To use the By Type feature to create a software policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Software Policies** ► **HP-UX**. The content pane displays a list of software policies. By default, the software policies are organized by operating system families.
- 2 Double-click to select an operating system.
- 3 From the Actions menu, select **New** to open the New Software Policy window.
- 4 In the Name field, enter the name of the HP-UX software policy.
- 5 (Optional) In the Description field, enter text that describes the purpose or contents of the policy.
- 6 Next to the Location field, click **Select** to specify the location for the software policy in the folder hierarchy.
- 7 In the Select Folder window, select a folder in the Library to specify the location of the software policy and then click **Select** to save your setting.
- 8 From the Availability drop-down list, select an SA server life cycle value (Available or Deprecated) for the software policy.
- 9 From the OS drop-down list, select the operating system family or specific operating systems in that family.



- 10 Keep the Template value set to No, which is the default.
- 11 From the File menu, select Save.

## Library—By Folder

To use the By Folder feature to create a software policy:

- 1 In the navigation pane, select **Library ► By Folder**. The content pane displays the folder hierarchy in the library.
- 2 In the content pane, select the folder that you want to contain the software policy.
- 3 From the Actions menu, select **New ► Software Policy** to open the New Software Policy window.
- 4 In the Name field, enter the name of the HP-UX software policy.
- 5 (*Optional*) In the Description field, enter text that describes the purpose or contents of the policy.
- 6 Next to the Location field, click **Select** to change the location for the software policy in the folder hierarchy.
- 7 In the Select Folder window, select a folder in the Library to specify the location of the software policy and then **Select** to save your setting.
- 8 In the Availability drop-down list, select an SA server life cycle value (Available or Deprecated) for the software policy.
- 9 In the OS drop-down list, select the operating system family or specific operating systems in that family.
- 10 Keep the Template value set to No, which is the default.
- 11 From the File menu, select Save.


## Viewing an HP-UX Software Policy

In the SA Client, you view a software policy by using any of the following navigation features:

- Search
- Devices
- Library—By Type
- Library—By Folder

### Search

To use the Search feature to view a software policy:

- 1 In the navigation pane, select Search.
- 2 In the drop-down list, select Software Policy and then enter the name of the policy in the text field.
- 3 Click  to display the search results in the content pane.  
See [SA Client Search](#) on page 35 for more information about the search feature.
- 4 In the content pane, select the software policy and then right-click to open the Software Policy window.

## Devices

To use the Devices feature to view a software policy:

- 1 In the navigation pane, select **Devices** ► **Servers** ► **All Managed Servers** to display a list of servers in the content pane.  
Or  
In the navigation pane, select **Devices** ► **Device Groups** to display a list of servers in the content pane
- 2 In the content pane, select a server.
- 3 Right-click the selected server to open the Server window.
- 4 In the Information pane, select **Management Policies**.
- 5 In the Management Policies pane, select Software Policies to display the software policies attached to the server in the content pane.
- 6 In the content pane, select the software policy and then right-click to open the Software Policy window.

## Library—By Type

To use the By Type feature to view a software policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Software Policies** ► **HP-UX** and an operating system version. The content pane displays a list of software policies. By default, the software policies are organized by operating system families.
- 2 In the content pane, select the software policy and then right-click to open the Software Policy window.

## Library—By Folder

To use the By Folder feature to view a software policy:

- 1 In the navigation pane, select **Library** ► **By Folder**. The content pane displays the folder hierarchy in the library.
- 2 In the content pane, select the folder that contains the software policy.
- 3 Right-click to open the folder.
- 4 Select the software policy and then right-click to open the Software Policy window.

## Editing an HP-UX Software Policy

After you create an HP-UX 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 (edit) the name, description, availability, location of the software policy in the Library, and the operating systems of the software policy.



---

You must have permissions to manage an HP-UX software policy. To obtain these permissions, contact your system administrator. See the *SA Administration Guide* for more information about software management permissions.

---

To edit the properties of a software policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Software Policies** ► **HP-UX** and an operating system version.
- 2 In the content pane, select the software policy and then right-click to open the Software Policy window.
- 3 In the Software Policy window, in the Views pane, select Properties.
- 4 In the Properties content pane, you can edit the Name, Description, Location, Availability, and OS for the software policy. See [Creating an HP-UX Software Policy](#) on page 79 for guidelines about information in these fields.
- 5 After you have made your changes, from the File menu, select Save.

## Adding an HP-UX Patch to a Software Policy

After you create an HP-UX software policy, you can add HP-UX patches, HP-UX software, and server scripts to it. Adding these does not install them on a managed server. You must attach the software policy to a managed server and then remediate the server.







---

You must have permissions to add an HP-UX patch, HP-UX software, and server scripts to an HP-UX software policy. To obtain these permissions, contact your system administrator. See the *SA Administration Guide* for more information about software management permissions.

---

To add software resources to a software policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Software Policies** ► **HP-UX** and an operating system version.
- 2 In the content pane, select a software policy.
- 3 Right-click the selected software policy to open the Software Policy window.
- 4 In the Views pane, select Policy Items.
- 5 Click  or, from the Actions menu, select Add to display the Select Library Item window.
- 6 Select the Browse Types tab to display items that can be added to the software policy.

- 7 Select one or more items you want to add to the policy and then click **Select**. The items are added to the policy.  
Or  
Select the Browse Folders tab to display the folder hierarchy in the Library and the list of items contained in the folders. Select one or more items you want to add to the policy and then click **Select**. The items are added to the policy.
- 8 To change the order in which the software is installed, use the   arrows.
- 9 To remove an item from the policy, select it and then click . See [Removing Software from a Software Policy](#) on page 84 for more information about this action.
- 10 From the File menu, select Save to save the changes you made to the policy.

## Removing Software from a Software Policy

When you remove software from an HP-UX software policy, the software is not uninstalled from the managed server. This action only removes the software from the policy. To uninstall the HP-UX software from a managed server, you must directly uninstall the software from the managed server.




---

You must have permissions to remove HP-UX software from an HP-UX software policy. To obtain these permissions, contact your system administrator. For more information, see the *SA Administration Guide*.

---

To remove HP-UX software from a software policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Software Policies** ► **HP-UX** and an operating system version.
- 2 In the content pane, select the software policy and then right-click to open the Software Policy window.
- 3 In 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 Click  or, from the Actions menu, select Remove.
- 6 From the File menu, select Save to save the changes you made to the policy.

## Viewing Software Policy History

To view the events associated with an HP-UX software policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Software Policies** ► **HP-UX** and an operating system version.
- 2 In the content pane, select the software policy and then right-click to open the Software Policy window.
- 3 In the Views pane, select History. The events associated with the software policy display in the content pane. You can view the action performed on the policy, the user who performed the action, and the time when the action was performed.
- 4 From the Show drop-down list, select a meaningful time period narrows or widens the volume of events.

## Viewing Servers Attached to a Software Policy

In the SA Client, you can view a list of all servers and device groups that have a selected HP-UX software policy attached to them.

To view a list of all servers that have a selected HP-UX software policy attached to them:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Software Policies** ► **HP-UX** and an operating system version.
- 2 In the content pane, select the software policy and then right-click to open the Software Policy window.
- 3 In the Views pane, select Server Usage. A list of servers that have the selected software policy attached to them displays in the content pane.

## Finding a Software Policy in Folders

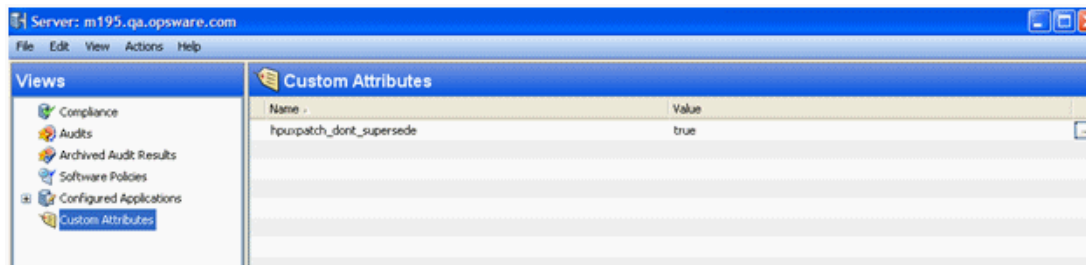
To find an HP-UX software policy in the folder hierarchy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Software Policies** ► **HP-UX** and an operating system version.
- 2 In the content pane, select a software policy.
- 3 Right-click and then select **Locate in Folders** to display the folder hierarchy for the software policy in the content pane.

## Custom Attributes

Patch management for HP-UX enables you to set a `hpuxpatch_dont_supersede` custom attribute to any managed server, as shown in [Figure 8](#).

**Figure 8** Custom Attribute: `hpuxpatch_dont_supersede`



Server Automation requires that the latest patches are included in the software policy, with the custom attribute *not* set. This default behavior is designed to resolve dependency by looking for the latest patches in the software policy. If the latest patches are not available, SA will display an error message that reminds you to download the latest patches from HP.






# Patch Compliance

An HP-UX patch compliance scan compares the patches that are installed on a managed server with the patch policies that are attached to the server. If the actual server configuration does not match the patch policies attached to the server, the server is *out of compliance* with the patch policies. In addition, if a patch in the patch policy has been superseded by a newer patch and the newer patch is installed on a server, that server will be marked as *compliant*.

In the SA Client, when you perform a patch compliance scan, the scan indicates the server's overall compliance with all HP-UX patch policies that are attached to the server. Even if only one HP-UX patch policy attached to the server is not compliant, the server is considered *non-compliant*. You can then view the non-compliant server and remediate the server against the applicable patch policy.

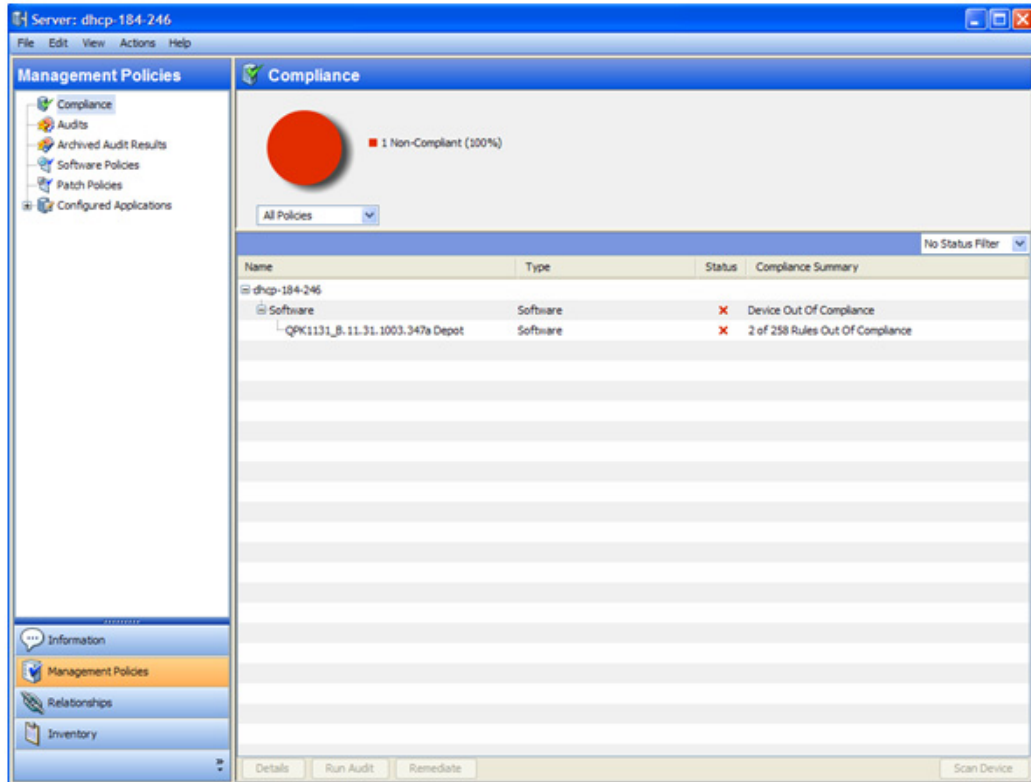
The SA Client displays the following compliance information for a patch policy:

**Table 7 Compliance Status for a Managed Server**

Icon	Status	Description
	<b>Compliant</b>	All patch policies attached to a server are <i>compliant</i> —all patches specified in all patch policies are installed on the server.
	<b>Non-compliant</b>	At least one of the patch policies attached to the server is <i>not compliant</i> —at least one patch in the policy is not installed on the server.
	<b>Scan Started</b>	The patch compliance information is currently being collected.
	<b>Scan Failed</b>	The patch compliance scan was unable to run.
	<b>Scan Needed</b>	The patch compliance information needs to be collected or the compliance information may be inaccurate.
—	<b>Not Applicable</b>	The patch compliance information does not apply.

See [Figure 9](#) for an example of patch compliance status for the Standard HP-UX bundle.

Figure 9 Patch Compliance Status



In this example, Server Automation reports that the compliance status for the Standard HP-UX QPK bundle is “2 of 258 rules out of compliance.” The total number of patches within QPK bundle is 259. SA determined that one patch in this bundle is not applicable to this managed server. Therefore, it reports compliance status only for 258 patches instead of 259 patches.

SA also determined that two patches have superseded patches and that these superseded patches are installed on the server but not uploaded in the repository. Therefore, they are reported as *out of compliance*.



# Patch Installation

The patch installation process consists of two phases:

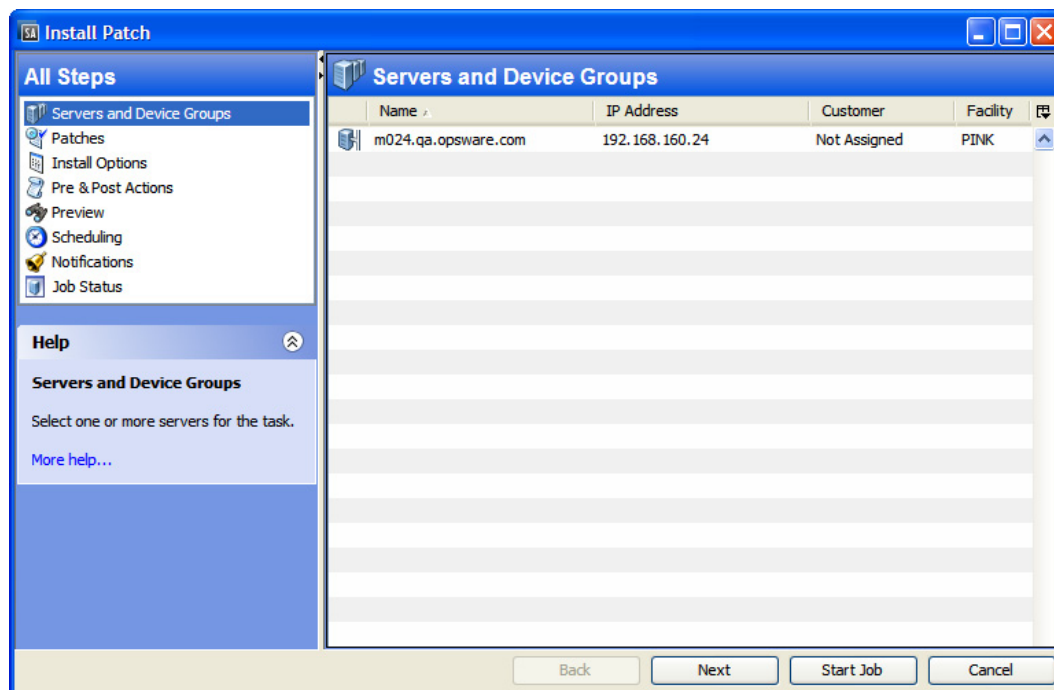
- **Download Phase**—This is when the patch is downloaded from Server Automation to the managed server. This phase is commonly referred to as *staging*.
- **Installation Phase**: This is when the patch is installed on the managed server. This phase is commonly referred to as *deployment*.

You can specify whether you want the installation to occur immediately after the patch is downloaded (*staged*) or you can schedule it to occur at a later date and time. Patch management also supports the need for best-effort installations of multiple patches by allowing you to specify that the patch installation process will continue even when an error occurs with one of the patches.

SA displays the name of the command that installs the patch. The SA Agent runs this command on the managed server. You can override the default command-line arguments that you want to perform the installation.

To optimally manage HP-UX patch installations, patch management enables you to manage server reboot options and pre- and post-installation scripts, simulate (preview) a patch installation, and set up email notifications to alert you about the status of the installation process. The Install Patch wizard guides you through the setup. See [Figure 10](#).

**Figure 10** Install Patch Wizard



## Installation Flags

You can specify installation flags that are applied when an HP-UX patch is installed. However, Server Automation also uses default installation flags and requires that patches be installed with these flags. make sure that you do not specify any installation flags that override or contradict the default flags passed in by SA.

## Installing an HP-UX Patch

Before a patch can be installed on a managed server, it must be imported into SA and its status must be Available. Only system administrators who have the required permissions can install patches that are marked Limited.



---

You must have permissions to manage patches. To obtain these permissions, contact your system administrator. For more information, see the *SA Administration Guide*.

---

You can perform the installation by explicitly selecting patches and servers.

To install a patch on a managed server:

- 1 In the navigation pane, select **Devices > Servers > All Managed Servers**
- 2 In the content pane, select an HP-UX server.
- 3 From the Actions menu, select Install Patch. The first step of the Install Patch window, Servers and Server Groups, opens.
- 4 Click **Next** to advance to the next step in the Install Patch wizard.
- 5 From the list of patches, select the patch you want to install.
- 6 After you complete a step, click **Next** to advance to the next step. Before you click Start Job, you can return to a completed step to make changes by clicking on it in the list of steps.
- 7 When you are ready to launch the installation job, click **Start Job**.

After you launch the job, you cannot change its parameters, even if the job is scheduled to run at a later time.

## Setting HP-UX Install Options

You can specify the following types of patch installation options:

- Perform the patch installation immediately after the patch is downloaded or at a later date and time.
- Do not interrupt the patch installation process, even when an error occurs with one of the patches.
- Use different command-line options to perform the installation.

To set these install options:

- 1 In the Install Patch window, click **Next** to advance to the Options step.
- 2 Select one of the following Staged Install Options:
  - **Continuous**: Enables you to run all phases as an uninterrupted operation.
  - **Staged**: Enables you to schedule the download and installation to run separately.
- 3 Select the Error Options check box if you want the patch installation process to continue even when an error occurs with one of the patches. By default, this check box is not selected.
- 4 In the Install Command text box, enter command-line arguments for the command that is displayed.
- 5 Click **Next** to go to the next step or click **Cancel** to close the Install Patch window.

## Setting Reboot Options

To minimize the downtime that server reboots can cause, you can control when servers will and will not be rebooted. You can adopt the vendor's reboot assignments, reboot a server each time a patch is installed on it, completely suppress all server reboots, or postpone reboots until all patches are installed.

When you are selecting reboot options in the Install Patch window, HP recommends that you use the HP-UX reboot recommendations, which is the “Reboot servers as specified by patch properties” option. If you cannot use the HP-UX reboot setting, select the single reboot option, which is the “Do not reboot servers until all patches are installed” option.

The following options determine whether the servers are rebooted after the patch is installed. These options apply only to the job launched by the Install Patch window. They do not change the Reboot Required option, which is on the Install Parameters tab of the patch properties window. Except for the first option, the following options override the Reboot Required option.

- Reboot servers as specified by patch properties
- By default, the decision to reboot depends on the Reboot Required option of the patch properties. The server is rebooted only once at the end. This is done to satisfy the patch dependency. In effect, the option works as the third option which is to not reboot servers until all patches are installed
- Reboot servers after each patch install
- Even if the Reboot Required option of the patch properties is not set, reboot the server. If multiple patches are installed, the server will be rebooted only once after all patches are installed.
- Do not reboot servers until all patches are installed
- If the Reboot Required option is set for some selected patches but not for others, the server is rebooted one time after all patches are installed. If the Reboot Required option is not set for any of the selected patches, the server is not rebooted.
- Suppress all server reboots
- Even if the Reboot Required option of the patch properties is set, do not reboot the server. (Because of vendor settings, some patches ignore the suppress option and force a reboot.)

### To set reboot options:

- 1 In the Install Patch window, click **Next** to advance to the Pre & Post Actions step.
- 2 Select one of the Rebooting Options.
- 3 Click **Next** to go to the next step or click **Cancel** to close the Install Patch window.

## Specifying Install Scripts

For each patch, you can specify a command or script to run before installation or after installation. A pre-install script, for example, could check a certain condition on the managed server. If the condition is not met or if the pre-install script fails, the patch is not installed. A pre-install script could also be used to shut down a service or application before it is patched. A post-install script could be used to perform a certain cleanup process on the managed server. You can also specify the following types of scripts to run on the managed server before or after an installation or download phase:

- **Pre-Install:** A script that runs before patches are installed on the managed server.
- **Post-Install:** A script that runs after patches are installed on the managed server.

To specify a pre-install script:

- 1 In the Install Patch window, click **Next** to advance to the Pre & Post Actions step.
- 2 Select the Pre-Install tab. You may specify different scripts and options on each of the tabs.
- 3 Select **Enable Script**. This option enables the remainder of the fields on the tab. If Enable Script is not selected, the script will not run.
- 4 Select either **Saved Script** or **Ad-Hoc Script**.
- 5 A Saved Script was previously stored in SA with the SAS Web Client. To specify the script, click **Select**.
- 6 If the script requires command-line flags, enter the flags in the Command text box.
- 7 Specify the information in the User section. If you choose a system other than Local, enter the User Name, Password, and Domain. The script will be run by this user on the managed server.
- 8 To stop the installation if the script returns an error, select the **Error** check box.
- 9 Click **Next** to go to the next step or click **Cancel** to close the Install Patch window.

## Scheduling a Patch Installation

Because the two phases of patching can be decoupled, you can schedule when you want patches installed (*deployed*) to occur independently of when patches are downloaded (*staged*).

To schedule a patch installation:

- 1 In the Install Patch window, click **Next** to advance to the Scheduling step.  
By default, the Scheduling step displays only the scheduling options for the install phase. If you selected Staged in the Install Options step, the scheduling options for the download phase are also displayed.
- 2 Select one of the following Install Phase options:
  - **Run Task Immediately:** This enables the system to perform a preview analysis in the Summary Review step. The scheduling option for the download phase is Run Immediately Following Download.
  - **Run Task At:** This enables you to specify a later date and time that you want the installation or download performed.
- 3 Click **Next** to go to the next step or click **Cancel** to close the Install Patch window. A scheduled patch installation can be cancelled (prior to its execution), even if the patch download has already completed.

## Setting Up Email Notifications

You can set up email notifications to alert users when the download and installation operations complete successfully or with errors.

To set up email notifications:

- 1 In the Install Patch window, click **Next** to advance to the Notifications step.
- 2 To set the notification status on the success of a Job, select the icon. To set the notification status on the failure of a Job, select the icon. By default, the Notification step displays only the notification status for the installation phase.
- 3 Enter a Ticket ID to be associated with a Job in the Ticket ID field.
- 4 Click **Next** to go to the next step or click **Cancel** to close the Install Patch window.



---

If you previously selected Staged in the Install Options step, the Notifications pane displays notification options for both the download and installation phase

---

## Previewing a Patch Installation

The installation preview process provides an up-to-date report about the patch state of servers. The installation preview is an optional step that lets you see what patches, either single patch or patches part of standard HP-UX bundle, will be installed on managed servers and what type of server reboots are required. This preview process verifies whether the servers you selected for the patch installation already have that patch installed. In some cases, a server could already have the patch installed if a system administrator manually installed it, which means that SA does not know about it.

The preview process also reports on dependency information, such as patches that require certain HP-UX products, and patches that obsolete other patches or are obsoleted by other patches. If a dependency is not met, SA displays an error message indicating this condition.

To preview a patch installation:

- 1 From the Install Patch window, click **Next** to advance to the Summary Review step.
- 2 Verify the information displayed for the Servers, Server Groups, and Patches at the top of the window.
- 3 *(Optional)* Click **Preview** to see the separate actions that will be performed when the patch is installed. To view the details of a previewed action, select a row in the table. See [Figure 11](#).
- 4 Click **Start Job** to launch the installation job or click **Cancel** to close the Install Patch window without launching the installation.

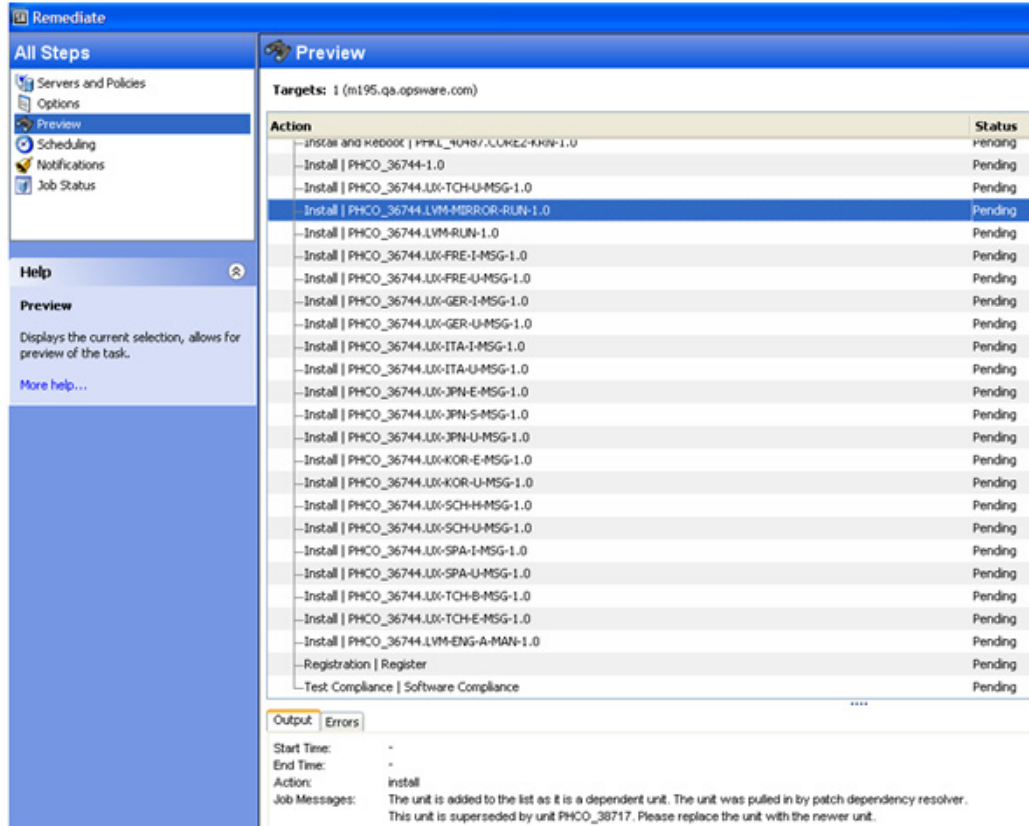


---

If you selected Run Task Immediately in the Scheduling step, the job begins now. If you selected Run Task At, the job will be launched at the specified time and date.

---

Figure 11 Patch Installation Preview



## Viewing Job Progress

You can review progress information about a patch installation (job), such as whether actions completed or failed.

To display job progress information:

- 1 From the Install Patch window, click **Next** to advance to the Job Progress step. This starts the installation job.

The Progress bar and text indicate how many of the actions listed in the table were completed. For each server, the following actions can be performed:

- **Analyze:** SA examines the patches needed for the installation, checks the managed servers for the most recent patches installed, and determines other actions it must perform.
- **Download:** The patch is downloaded from SA to the managed server.
- **Install:** After being downloaded, the patch is installed.
- **Final Reboot:** If this action is specified in the Pre & Post Actions step, the server is rebooted.
- **Pre/Post Install/Download Script:** If this action is specified in the Pre & Post Actions step, a script is run before or after the uninstallation.
- **Install & Reboot:** When a patch will be installed is also when the server will be rebooted.
- **Verify:** Installed patches will be included in the software registration.

- 2 To view additional details about a specific action, select the row in the table to display the start and completion times of the job. In the navigation pane, select Jobs and Sessions to review detailed information about the job.
- 3 Click **End Job** to prevent the job from running or click **Close** to close the Install Patch window.

## Patch Uninstallation

Uninstalling HP-UX patches and bundles is not supported in this release. To uninstall an HP-UX patch and bundle from a managed server, you must directly uninstall the HP-UX patch and bundles from the managed server.





# 4 Patch Management for Solaris



## Overview

In Server Automation (SA), patch management for Solaris enables you to identify, install, and remove Solaris patches, and maintain a high level of security across managed servers in your organization. You can identify and install patches that protect against security vulnerabilities for the following Solaris operating systems:

**Table 8 Supported Operating System Version**

OS Version	Architecture
Solaris 6, 7, 8, 9	Sun SPARC
Solaris 10 (Update 1 through Update 9)	Sun SPARC, 64bit x86, 32 bit x86, and Niagara

See the *Server Automation Compatibility Matrix* for more information.

## Features

SA automates Solaris patching by enabling you to:

- **Determine which patches your managed servers need.**

SA can determine the patches your managed Solaris servers need by examining the OS version, the applications installed on your servers, and the patches already installed on your servers. SA examines all available Solaris patches and then determines which patches your servers need, the required installation order, and the reboot requirements.

- **Create Solaris patch policies.**

This is a model-based approach to managing your Solaris servers. SA enables a policy setter to create a model of their IT environment by creating a Solaris patch policy. A Solaris patch policy specifies patches, patch clusters, and scripts that must be installed on your managed servers. A system administrator can then apply the patch policies to the Solaris servers in their environment. Create Solaris patch policies from downloaded Solaris patches and patch clusters.

- **Download Solaris patches, patch clusters, and patch bundles, and then store them, and related vendor information, in the SA Library.**

SA can import Solaris patches, patch clusters, Fujitsu clusters, and related vendor information from My Oracle website and add them to Solaris patch policies. Vendor information can include reboot specifications, platform settings (such as support for multi-platform patches), patch dependencies, and a Readme file. Your patch policies are stored in the SA Library and accessible from the SA Client.

- **Resolve all dependent patches for Solaris patches.**

SA can examine all Solaris patch metadata and identify obsolete patches, superseded patches, incompatible patches, required dependent patches and withdrawn patches, and then update your patch policy. SA also places the patches in the correct install order.

- **Install Solaris patches and patch clusters on managed servers.**

SA allows you to directly install Solaris patches and patch clusters on managed servers or to install by using Solaris patch policies. In the SA Client, you can set the installation order for the patches and patch clusters in the patch policy. SA includes the reboot settings from the Solaris patches in the policy.

SA installs patches, patch clusters, Fujitsu clusters, and patch bundles by remediating patch policies on managed Solaris servers. The remediate process offers various patch reboot settings, such as single-user mode, reconfiguration reboot, and reboot immediate.

SA ensures that each patch is applicable to each server. For example, if the package or application the patch applies to is not installed on the server or if a newer patch is already installed on the server, SA will not install that patch on the server.

- **Install Solaris patches in single-user mode.**

SA will install Solaris patches in single-user mode if it is required by the patch metadata published by Oracle. After the patch installation is completed, SA will return to multi-user mode.

- **Install patches by Solaris zones.**

The SA Client lets you can install patches on Solaris global and non-global zones by using Solaris patch policies.

- **Establish a patch installation process.**

In SA, you can separate and independently schedule the various stages of Solaris patch management, such as by analysis, download, and installation. You can set up email notification for the job status of each completed stage and associate a ticket ID with each job.

- **Verify the compliance status of servers with patch policies.**

The Compliance view allows you to determine if servers are configured according to the patch policy and to remediate non-compliant servers. You can perform compliance scans, including server platform, patch supersedence, and package applicability checks.

- **Search for software resources and servers.**

In the SA Client, the Library provides a way to search for Solaris patches, clusters and patch policies using powerful and flexible search criteria such as by availability, architecture, operating system, reboot options, version, and many other parameters. You can also search for Solaris patch policies by name, folder name, availability, operating system, and so on. See [SA Client Search](#) on page 35 for information on the search feature.

## Policy-based Patch Management

With Solaris patch policies, you can ensure your Solaris servers have the right patches installed by creating a patch policy. A patch policy is a model of your desired IT environment. A Solaris patch policy defines a server baseline to ensure that all servers are provisioned with standard contents. Using SA, you can automatically download Solaris patches, organize them into polices, define installation order among patches in the policy, automatically resolve all dependencies for the patches and set reboot settings for all patches in the policy.

System administrators can then manage the servers in their environment by applying the Solaris patch policy to the servers. SA applies the changes to the managed servers when you remediate the managed servers with the patch policy. When a change needs to be made to a patch policy, a policy setter simply changes the baseline defined in the policy and the incremental differences are applied across the target servers.

## Solaris Patch Bundles

You can import and install Solaris patch bundles.

- You can download Solaris patch bundles and import them into the SA library using the `solpatch_import` command.
- You can install Solaris patch bundles directly on managed servers or on all servers in a device group or you can add Solaris patch bundles to a Solaris patch policy (or to a software policy), attach the policy to managed servers or device groups and then remediate the servers against those policies. When you remediate the servers or device groups, the Solaris patches specified in the attached policy are automatically installed on the managed servers.
- All `solpatch_import` actions, except the policy action, now can be performed with patch bundles.
- When you import a bundle, SA updates the metadata in the SA Library with all the patches contained in the bundle. Depending on the number of patches in your SA Library, the bundle import may take some time.
- Deleting a patch bundle from the SA Library or by using the `solpatch_import` command deletes all the parts of the bundle.
- The default reboot settings for patch bundles are listed below. You can change these settings by opening the patch bundle in the SA Client, selecting the Properties view and editing the Install Parameters.
  - Reboot Required: Yes – This setting indicates the managed server will be rebooted when the patch bundle is successfully installed.
  - Install Mode: Single-user Mode – This setting indicates that the patch bundle will be installed in single user mode. Note that the Solaris system is rebooted to single user mode, then the patch bundle is installed, then the system is rebooted to multiuser mode.
  - Reboot Type: Reconfiguration – This setting indicates that a reconfiguration reboot will be performed after installing the patch bundle.
  - Reboot Time: Immediate – This setting indicates that the server will be rebooted immediately after installing the patch bundle.
- A Solaris patch compliance scan will indicate that the server is out of compliance even though the patch bundle installed successfully if one or more patches in the bundle were not installed because a required prerequisite patch was not installed. For details on what patches in the patch bundle were not installed, see the log file for the patch bundle installation job.

A software compliance scan will similarly indicate the server is out of compliance if the patch bundle is included in the software policy and the same scenario occurs.

To bring the server into compliance, place the relevant patches into a patch policy, resolve the dependencies on the policy to place all required patches in the policy and remediate the policy on the server.

- You must set the “Manage Packages” permission to “Read and Write” to use the `solpatch_import` command. For details on permissions, see the *SA Administration Guide*.
- If you encounter errors when importing Solaris patch bundles, perform the following troubleshooting steps.
  - a Log in as root to the SA core where the SA 9.10 patch has been installed.
  - b Locate the log file from the 9.10 patch install, which is typically located at:  

```
/var/log/opsware/install_opsware/patch_opsware.<time stamp>.log
```

- c Search this log file for a message with “update\_supplements.” For example, you could use the following `grep` command:
 

```
grep update_supp patch_opsware*
```
- d The result should be a log message with “update\_supplements successfully completed”. However, if the message indicates the update\_supplements failed, update the Solaris patch supplement file manually as follows.
- e Log in as root to an SA core system where the `solpatch_import` command is installed.
- f Change to the directory where the `solpatch_import` command is:
 

```
/opt/opsware/solpatch_import/bin.
```
- g Run the following command:
 

```
./solpatch_import -a update_supplements
```
- h Try importing Solaris patch bundles again.

## Fujitsu Clusters

A Fujitsu cluster is a cluster designed for a Solaris operating system that runs on Fujitsu hardware. SA supports Fujitsu clusters.

### SA Commands

You can use the same cluster commands for Fujitsu clusters as you do for standard Solaris clusters.

Use the following command to display additional information about cluster commands:

```
/opt/opsware/solpatch_import -manual
```




---

Fujitsu clusters can only be imported using the `solpatch_import` command.

---

### Cluster Downloads

If you use a single `solpatch_import` command to download both a Fujitsu cluster and a Solaris recommended cluster file, both files will be downloaded to the same location but will not be imported into the SA core. The first downloaded cluster will be overwritten by the second downloaded cluster, because both clusters have the same file names (such as: `10_Recommended.zip`). To avoid overwriting one file with the other, do not use a single `solpatch_import` command to download the two clusters. Instead, download the first cluster, move it to a different location, and then download the second one.




---

You can still use a single `solpatch_import` command to import Fujitsu clusters and standard Solaris recommended clusters for the same operating system because when SA imports a file, it downloads and then immediately imports it to the core. No file overwriting can occur.

---

### Patch Policies

You can create patch policies for any cluster from the command line or by using the SA Client.

When you create a patch policy for a Fujitsu cluster by using the `-policy` option from a command line, *all* applicable patches included in the cluster are applied—regardless of whether Fujitsu intended them to be installed on your hardware model, using the cluster install. These extra patches do not cause harm.

If you want to apply *only* the patches that Fujitsu has designated for your hardware model, use the SA Client to create a new policy and include the Fujitsu cluster. When you remediate the policy, SA will correctly apply *only* the relevant patches.

## Quick Start

To set up and initialize Solaris patching in SA:

- 1 Create an SA user that has the following permissions:
  - Read and write permissions for the `/Opware/Tools/Solaris Patching` folder
  - Read and write permission for the “Manage Patch” feature permission
  - Feature permissions set to “Yes” for:
    - “Allow Install Patch”
    - “Allow Uninstall Patch”
    - “Manage Patch Compliance Rules”

See the *SA Administration Guide* for more information on creating users and setting permissions.

- 2 Log in as `root` to an SA slice core server or a master core server.

- 3 Update the configuration file located at `/etc/opt/opsware/solpatch_import/solpatch_import.conf` as follows:

Add your SA user name and password to the lines that begin with `hpsa_user` and `hpsa_pass`.

Example:

```
hpsa_user=my_sa_username
hpsa_pass=<password>
```

- Add your My Oracle account user name and password to the lines that begin with `download_user` and `download_pass`.

Example:

```
download_user=my_oracle_username
download_pass=<password>
```

This configuration file is used by the `solpatch_import` command.



You can create a separate, private copy of the configuration file and use the `-c` option or the `--conf` option for `solpatch_import` to specify your configuration file.

- 4 (Optional) Run the following command to encrypt your passwords in the configuration file:

```
solpatch_import --hide_passwords
```

The `solpatch_import` command is located in `/opt/opsware/solpatch_import/bin`.



If this is the first time you are using Solaris patch management in SA, you must create a new Solaris patch database. The `solpatch_import -a create_db` command creates the Solaris patch database, downloads patch information from Oracle (in the `patchdiag.xref` file), and then uploads the patch information into the database:

```
solpatch_import -a create_db
```

If you already have a `patchdiag.xref` file, use the following command to create the Solaris patch database and upload the patch information from your `patchdiag.xref` file into the database:

```
solpatch_import -a create_db -x <local patchdiag.xref file>
```

This command can take a few hours to run, depending on how many Solaris patches are already in your SA Library.

SA is now ready for you to download Solaris patches and install them on your servers as described in the following sections.

- 5 Make sure your Solaris patch database contains the latest patch information. See [Maintaining the Solaris Patch Database](#) on page 121.

## Patch Management Process

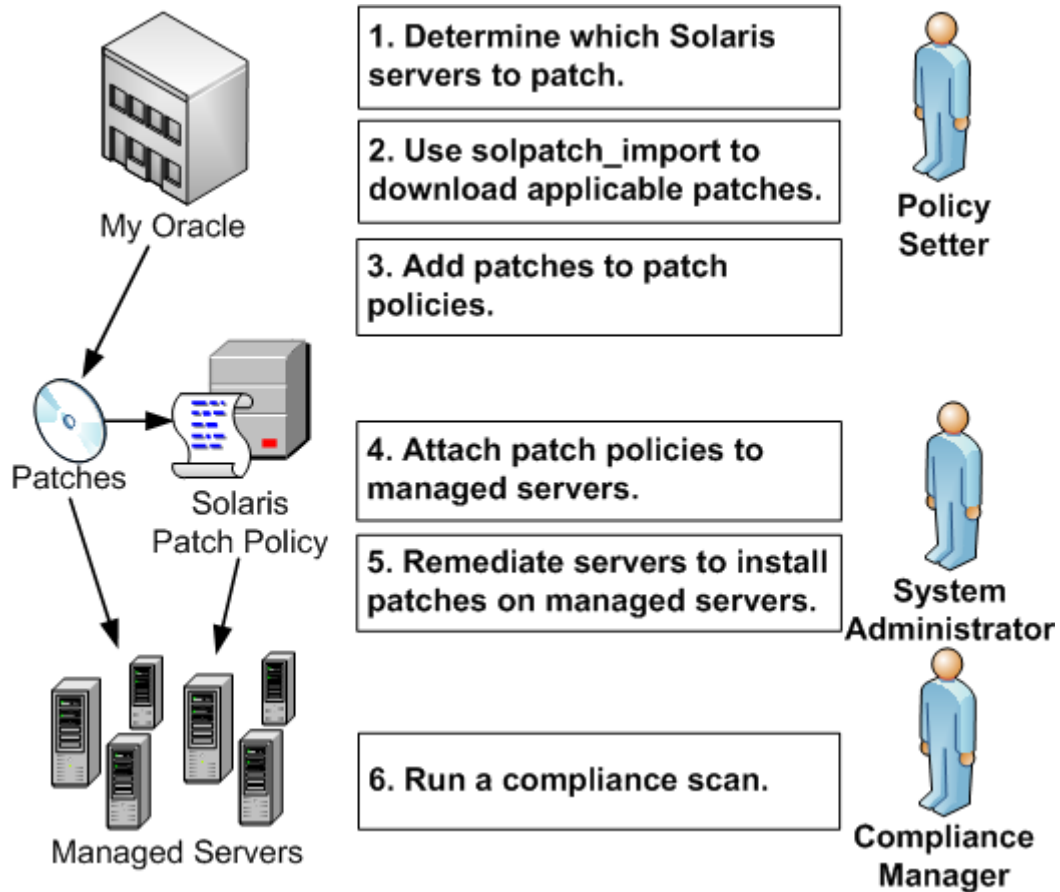
The Solaris patching process consists of the following phases:

- [Patching Servers](#) on page 102
- [Installing Patches](#) on page 104

### Patching Servers

[Figure 12](#) shows the steps required when you know which Solaris servers you want to patch and how you identify which patches those servers need. These steps include downloading and installing patches on your Solaris managed servers.

Figure 12 Patching Selected Servers

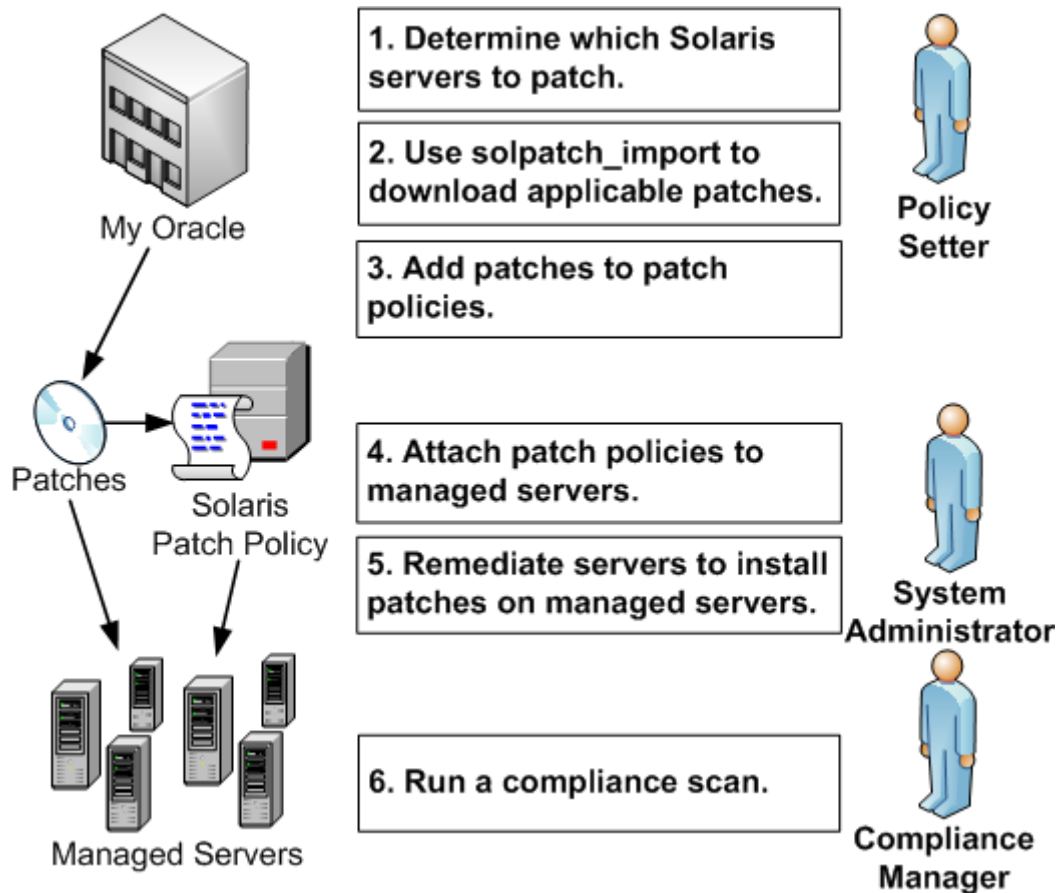


- 1 A policy setter determines which Solaris servers need to be patched. For example, you may want to patch one specific Solaris server, all your servers running 5.10, all servers used by a particular department, or some other subset of your Solaris servers.
- 2 A policy setter uses the `solpatch_import` command to download the patches from Oracle that are required by the selected Solaris servers. The `solpatch_import` command determines which patches are required by the selected servers, resolves all patch dependencies, and includes all applicable patches.
- 3 A policy setter adds the patches to a Solaris patch policy.  
This step can be completed by running the `solpatch_import` command as part of [step 2](#) (excluding patch bundles) or you can manually place the Solaris patches into a patch policy by using the SA Client.
- 4 A system administrator attaches the patch policies to managed servers.  
Your system administrator can test the patches by attaching the patch policy to one or more test servers, to make sure they behave as expected. If problems occur, you can add or remove patches from the patch policy and then test the patches again. After testing is complete, your system administrator can attach the patch policy to all other Solaris servers.
- 5 A system administrator remediates patch policies. The remediate process installs the patches on your managed servers.
- 6 A compliance manager performs a compliance scan to determine which servers do not have the required patches installed.

## Installing Patches

Figure 13 shows the steps required when you know which Solaris patches you want to install and how you identify all dependent patches. These steps include downloading and installing one or more Solaris patches.

Figure 13 Installing Selected Patches



- 1 A policy setter determines which Solaris patches need to be installed. You might be required to install one specific Solaris security patch or one specific patch that fixes a known problem on your managed servers.
- 2 A policy setter uses the `solpatch_import` command to download specific patches, patch clusters, or patch bundles from Oracle.
- 3 A policy setter adds the patches to a Solaris patch policy.  
This step can be completed by running the `solpatch_import` command as part of [step 2](#) (excluding patch bundles) or you can manually add the Solaris patches to a patch policy by using the SA Client.
- 4 A policy setter uses the [Resolve Dependencies](#) button in the SA Client to resolve all dependencies for patches in the patch policy, including determining dependent patches, superseding patches, obsolete patches, incompatible patches, and withdrawn patches.
- 5 A system administrator attaches the patch policies to managed servers.  
Your system administrator can test the patches by attaching the patch policy to one or more test servers, to make sure they behave as expected. If problems occur, you can add or remove patches from the patch policy and then test the patches again. After testing is complete, your system administrator can attach the patch policy to all other Solaris servers.



- 6 A system administrator remediates patch policies. The remediate process installs the patches on your managed servers.
- 7 A compliance manager performs a compliance scan to determine which servers do not have the required patches installed.

## Patch Compliance

A Solaris Patch compliance scan compares the Solaris patches that are installed on a managed server with the patches listed in the Solaris patch policies that are attached to the server and reports the results. If the actual server configuration does not match the Solaris patch policies attached to the server, then the server is out of compliance with the Solaris patch policies.

Patches that are not applicable to a particular Solaris server will not impact the compliance status of the server. For example:

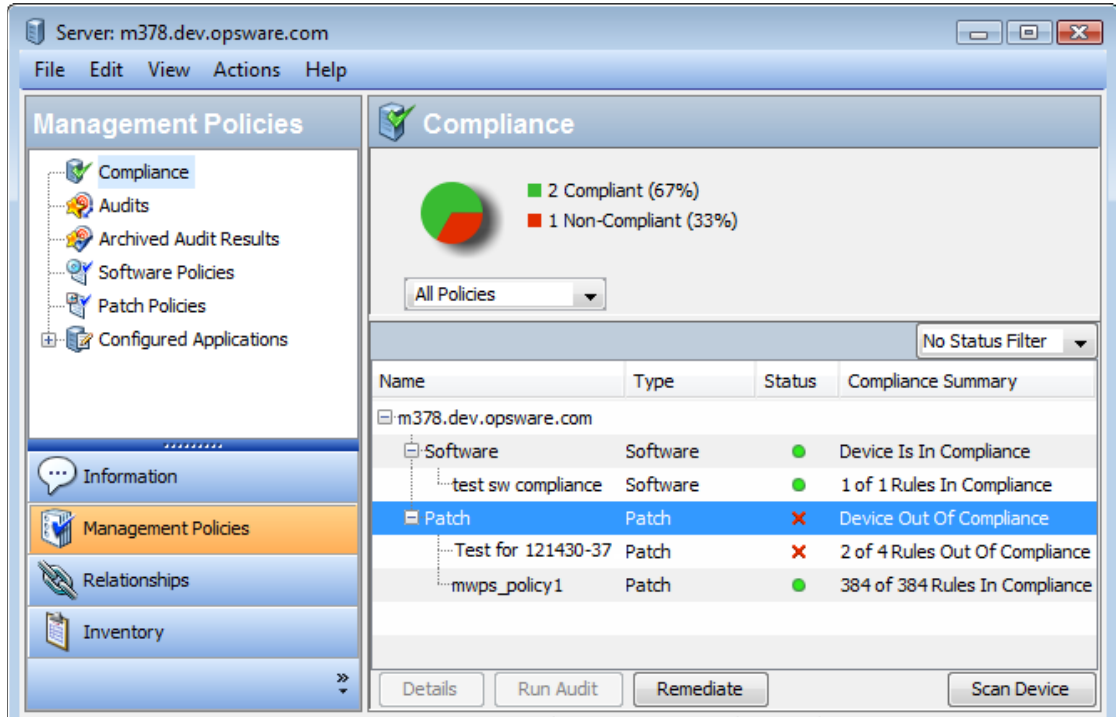
- If a policy contains a patch for the package “SUNWpkgg”, but “SUNWpkgg” is not installed on a particular server, the patch is not applicable to that server and that patch will not impact the results of the compliance scan for that server. The Compliance Summary does not include non-applicable patches. For example, if a policy contained 5 patches but only 3 were applicable to a given server and those 3 were installed on that server, the Compliance Summary would report “3 of 3 Rules In Compliance”, ignoring the 2 non-applicable patches.
- If a particular patch in the patch policy has been superseded by a newer patch and the newer patch is installed on a server, that server will be marked as compliant. (In essence, the patch policy is out of date. You can update the policy as described in [Resolving Patch Dependencies](#) on page 113.)
- Manual patches are always shown as out of compliance because SA cannot determine if manual patches are installed on Solaris servers. For more information, see [Installing Manual Patches—patchadd](#) on page 135.

In the SA Client, when you perform a patch compliance scan, the results indicate the server’s overall compliance with all the Solaris patch policies attached to the server. Even if only one Solaris patch policy attached to the server is not compliant, the server is considered non-compliant. You can then view the non-compliant server and remediate the server against the applicable patch policy.

[Figure 14](#) shows the compliance view for a Solaris server. Notice that the server is *out of compliance* because some patches are not installed on the server:

- Patch policy “Test for 121430-37” contains 4 applicable patches, but only 2 are installed on the server.
- Patch policy “mwps\_policy1” contains 384 applicable patches and all are installed on the server.

**Figure 14 Compliance Results for a Solaris Server**



The values for the Status column are described in the table below.

**Table 9 Compliance Status for a Managed Server**

Compliance Icon	Compliance Status	Description
	<b>Compliant</b>	All the patch policies attached to a server are compliant. That is, all the patches specified in all the patch policies are installed on the server.
	<b>Non-compliant</b>	At least one of the patch policies attached to the server is not compliant, which means at least one patch in the policy is not installed on the server.
	<b>Scan Started</b>	The patch compliance information is currently being gathered.
	<b>Scan Failed</b>	The patch compliance scan was unable to run.
	<b>Scan Needed</b>	The patch compliance information needs to be gathered or the compliance information may be inaccurate.
—	<b>Not Applicable</b>	The patch compliance information does not apply.

In the SA Client, you can check for patch compliance on an individual server or view overall compliance levels for all servers and groups of servers in your facility.

See the *SA User Guide: Application Automation* for information about compliance scans for all the servers in your data center.

## Running a Patch Compliance Scan



You must have a set of permissions to perform a patch compliance scan. To obtain these permissions, contact your SA Administrator. See the *SA Administration Guide* for more information.

---

To scan a server for Solaris patch compliance:

- 1 In the navigation pane, select **Devices** ► **Servers** ► **All Managed Servers**. The server list appears in the content pane.
- 2 In the content pane, select a Solaris server.
- 3 Right-click or from the **Actions** menu, select **Scan** ► **Patch Compliance**. The Patch Compliance Scan Status window appears and begins the patch compliance scan.
- 4 Click on the status icon in the Status column for more information on the current status.
- 5 When the scan finishes, view the results in the Status column of the Patch Compliance Scan Status window. See also [Figure 13](#).
- 6 (*Optional*) In the content pane, select Compliance from the View drop down list to view the patch policies that are not compliant. This displays all the patch policies attached to the server and the compliance status of each policy.

## Patch Policy Management

In Server Automation, Solaris patch policies allow you to install patches and patch clusters on managed servers and groups of managed servers in your environment. After creating a patch policy, you can attach it to servers or groups of servers. When you remediate a server or group of servers, the patches specified in the attached policy are installed. The remediate process compares what is actually installed on a server to the patches that should be installed on the server, based on the policy. SA then determines what operations are required to configure the server so that it complies with the policy.

After you add Solaris patches and patch clusters to a patch policy, you can specify the order in which you want them to be installed. When you attach the patch policy to a server and remediate the server, SA installs the patches and patch clusters in the patch policy in the specified order.

You can also use software policies to manage and install patches. A Solaris patch policy cannot include other patch policies; however, a software policy can include Solaris patch policies. See the *SA Software Management Guide* for more information.

Using the SA Client, you can also attach a Solaris patch policy to an OS sequence. When you run the OS sequence, if the remediate option is enabled (in the Remediate Policy window), all the patches in the patch policy will be installed on the server where the OS sequence is being installed. If the remediate option is disabled, none of the patches will be installed on the server. See the *SA OS Provisioning Guide* for more information.

Solaris patch policy management includes the following tasks:

- [Creating a Solaris Patch Policy](#) on page 108
- [Viewing a Solaris Patch Policy](#) on page 110
- [Editing a Solaris Patch Policy](#) on page 111
- [Adding a Solaris Patch to a Patch Policy](#) on page 111
- [Removing a Patch from a Solaris Patch Policy](#) on page 112

- [Resolving Patch Dependencies](#) on page 113
- [Adding a Custom Attribute to a Patch Policy](#) on page 116
- [Deleting a Custom Attribute from a Patch Policy](#) on page 116
- [Viewing Patch Policy History](#) on page 117
- [Viewing Software Policies Associated with a Patch Policy](#) on page 117
- [Viewing OS Sequences Associated with a Patch Policy](#) on page 117
- [Viewing Servers Attached to a Patch Policy](#) on page 118
- [Finding a Solaris Patch Policy in Folders](#) on page 118
- [Installing Patches Using a Patch Policy](#) on page 136.

## Creating a Solaris Patch Policy

In the SA Client, you create a Solaris patch policy by using either one of the following Library features:

- [Library—By Type](#) on page 108
- [Library—By Folder](#) on page 109
- [solpatch\\_import](#) on page 109




---

You must have permissions to create and manage a Solaris patch policy. To obtain these permissions, contact your system administrator. See the *SA Administration Guide* for more information about patch management permissions.

---

### Library—By Type

To use the **By Type** feature to create a patch policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patch Policies** ► **Solaris**. The content pane displays a list of patch policies. By default, the patch policies are organized by operating system families.
- 2 Double-click to select an operating system.
- 3 From the Actions menu, select **New** to open the Solaris Patch Policy window.
- 4 In the Name field, enter the name of the Solaris patch policy.
- 5 *(Optional)* In the Description field, enter text that describes the purpose or contents of the policy.
- 6 Click **Browse** to specify the location for the Solaris patch policy in the folder hierarchy. The Select Folder window appears.
- 7 In the Select Folder window, select a folder in the Library to specify the location of the Solaris patch policy and then click **Select** to save your setting.
- 8 From the Availability drop-down list, select an SA server life cycle value for the Solaris patch policy.
- 9 From the OS drop-down list, select the operating system family or specific operating systems in that family.
- 10 To save your changes, select **Save** from the **File** menu.

## Library—By Folder

To use the **By Folder** feature to create a patch policy:

- 1 In the navigation pane, select **Library ► By Folder**. The content pane displays the folder hierarchy in the library.
- 2 Select the folder that should contain the Solaris patch policy.
- 3 From the **Actions** menu, select **New ► Solaris Patch Policy** to open the Solaris Patch Policy window.
- 4 In the Name field, enter the name of the Solaris patch policy.
- 5 (*Optional*) In the Description field, enter text that describes the purpose or contents of the policy.
- 6 Click **Browse** to change the location for the Solaris patch policy in the folder hierarchy. The Select Folder window appears.
- 7 Select a folder in the Library to specify the location of the Solaris patch policy and then click **Select**.
- 8 From the Availability drop-down list, select an SA server life cycle value for the Solaris patch policy.
- 9 From the OS drop-down list, select the operating system family or specific operating systems in that family.
- 10 From the File menu, select **Save**.

## solpatch\_import

You can create a Solaris patch policy using the `solpatch_import` command and then add patches to the policy.

### Example A: Show Vendor-recommended Patches

The following command displays all vendor-recommended Solaris patches for all managed servers running Solaris 5.8:

```
solpatch_import --action=show --filter="rec,OS=5.8"
```

### Example B: Vendor Recommended Patches and Security Patches in a Policy

The following command downloads all vendor-recommended patches and security patches for all managed servers running Solaris 5.8, uploads these patches to the SA library, and then adds them to the `Sol/SolPatches` patch policy in the SA library:

```
solpatch_import --action=policy --policy_path=/Sol/Solpatches \  
--filter="rec,sec,OS=5.8"
```

### Example C: Patch Cluster in a Policy

The following command downloads the Solaris 10 SPARC Sun Alert Patch Cluster and adds all patches in that cluster to the `SolClusterPatches` policy. The cluster is not added to the policy; however, all patches in the cluster are added to the policy.

```
echo "Solaris 10 SPARC Sun Alert Patch Cluster" | solpatch_import \  
-a policy --policy_path="/Sol/SolClusterPatches"
```


## Viewing a Solaris Patch Policy

In the SA Client, you view a patch policy by using any of the following navigation features:

- [Search](#) on page 110
- [Devices](#) on page 110
- [Library—By Type](#) on page 110
- [Library—By Folder](#) on page 111

### Search

To use the Search feature to view a patch policy:

- 1 In the navigation pane, select Search.
- 2 From the drop-down list, select Solaris Patch Policy and then enter the name of the policy in the text field.
- 3 Click  to display the results in the content pane.
- 4 In the content pane, select the patch policy and then right-click to open the Solaris Patch Policy window.

### Devices

To use the Devices feature to view a patch policy:

- 1 In the navigation pane, select **Devices** ► **Servers** ► **All Managed Servers** to display a list of servers in the content pane.  
Or  
In the navigation pane, select **Devices** ► **Device Groups** to display a list of device groups in the content pane.
- 2 In the content pane, select a server and then right-click to open the Server Explorer window.
- 3 In the Views pane, select **Management Policies** ► **Patch Policies** to display the patch policies attached to the server appear in the content pane.
- 4 In the content pane, select the patch policy and then right-click to open the Solaris Patch Policy window.

### Library—By Type

To use the By Type feature to view a patch policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patch Policies** ► **Solaris** to display the Solaris patch policies in the content pane.
- 2 In the content pane, select the Solaris patch policy and then right-click to open the Solaris Patch Policy window.

### Library—By Folder

To use the By Folder feature to view a patch policy:

- 1 In the navigation pane, select **Library** ► **By Folder**. The content pane displays the folder hierarchy in the library.
- 2 In the content pane, select the folder that contains the patch policy.

- 3 Right-click to open the folder.
- 4 Select the patch policy and then right-click to open the Solaris Patch Policy window.

## Editing a Solaris Patch Policy

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



---

You must have permissions to edit Solaris patch policy properties. To obtain these permissions, contact your system administrator. See the *SA Administration Guide* for more information about these permissions.

---

To edit the properties of a patch policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patch Policies** ► **Solaris**.
- 2 In the content pane, select the Solaris patch policy and then right-click to open the Solaris Patch Policy window.
- 3 In the Views pane, select Properties.
- 4 In the Properties content pane, you can edit the Name, Description, Location, Availability, and OS for the software policy.
- 5 You can edit the name, description, location, life cycle, and operating systems for the Solaris patch policy in the content pane. See [Creating a Solaris Patch Policy](#) on page 108 for guidelines about information in these fields.
- 6 After you have made your changes, from the File menu, select Save.

## Adding a Solaris Patch to a Patch Policy

After you create a Solaris patch policy, you can add a Solaris patches, patch clusters and bundles, and server scripts to it. Adding these does not install them on a managed server. After you add these to a Solaris patch policy, you must attach the patch policy to a managed server and then remediate the server.

You can also use the `solpatch_import` command to place patches in a patch policy.







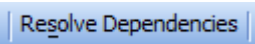
---

You must have permissions to add Solaris patches, Solaris patch clusters, and server scripts to a Solaris patch policy. To obtain these permissions, contact your system administrator. See the *SA Administration Guide* for more information about these permissions.

---

To add patch resources to a patch policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patch Policies** ► **Solaris**.
- 2 In the content pane, select the Solaris patch policy and then right-click to open the Solaris Patch Policy window.
- 3 In the Views pane, select Policy Items.
- 4 Click , or, from the **Actions** menu, select **Add** to display the Select Library Item window.
- 5 Select the Browse Types tab to display items that can be added to the Solaris patch policy.

- 6 Select one or more items you want to add to the policy and then click **Select**. The items are added to the policy.  
Or  
Select the Browse Folders tab to display the folder hierarchy in the Library and the list of items contained in the folders. Select one or more items you want to add to the policy and then click **Select**. The items are added to the policy.
- 7 To change the order in which the patches are installed, use the   arrows.
- 8 To remove a patch from the policy, select the patch and then click .
- 9 To determine all dependent, obsolete, superseding, incompatible and withdrawn patches, select **Actions** ► **Resolve Dependencies** or select .
- 10 From the File menu, select Save to save the changes you made to the policy.
- 11 To save the changes to the policy, select **Save** from the **File** menu.


## Removing a Patch from a Solaris Patch Policy

When you remove a patch or patch clusters from a Solaris patch policy, they are not uninstalled from the managed server. This action only removes the patch or patch cluster from the policy. To uninstall the Solaris patch or patch cluster from a managed server, you must directly uninstall the Solaris patch or patch cluster from the managed server.



You must have permissions to remove Solaris patches or patch clusters from a Solaris patch policy. To obtain these permissions, contact your system administrator. See the *SA Administration Guide* for more information.

To remove a Solaris patch or patch cluster from a Solaris patch policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patch Policies** ► **Solaris** and then select a version of Solaris.
- 2 In the content pane, select the Solaris patch policy and then right-click to open the Solaris Patch Policy window.
- 3 In 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 Click , or, from the Actions menu, select Remove.
- 6 From the File menu, select Save to save the changes you made to the policy.

## Resolving Patch Dependencies

When you use the `solpatch_import` command with the filter option, the command resolves all patch dependencies, resulting in a complete set of installable patches.

When you add patches manually to a patch policy, SA can determine the dependencies for all patches in the patch policy.

For each patch in the Solaris patch policy, SA determines the following conditions:

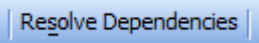
- Patches that supersede or obsolete a given patch and should be installed instead of the patch.



- Patches that are a prerequisite to a given patch and must be installed before the patch.
- Patches that are incompatible with each other and cannot be installed together. You must specify which incompatible patches you want to install.
- Patches that have been withdrawn by the vendor.
- The valid installation order of all patches, preserving the installation order of the original patches that were in the policy, unless a change is required.

To determine patch dependencies, you must place the patches in a Solaris patch policy.

To resolve dependent patches in a patch policy:

- 1 Select **Library** ► **By Type** ► **Patch Policies** ► **Solaris**.
- 2 Select a version of SunOS and then select a patch policy.)
- 3 Double-click a Solaris patch to open the Patch Policy window.
- 4 In the Patch Policy window, select Policy Items in the View pane. This displays the list of Solaris patches in the patch policy.
- 5 In the Patch Policy window, select **Actions** ► **Resolve Dependencies** or click . This action examines the Solaris patch database in SA and identifies all dependencies and displays the result, showing the resulting list of patches that need to be installed.

## Example: Resolving Solaris Patch Dependencies

Figure 15 shows a Solaris patch policy that contains 2 scripts and 3 patches. The order shown is the order in which the scripts will be executed and the order in which the patches will be installed

**Figure 15 Solaris Patch Policy: Resolve Dependencies**

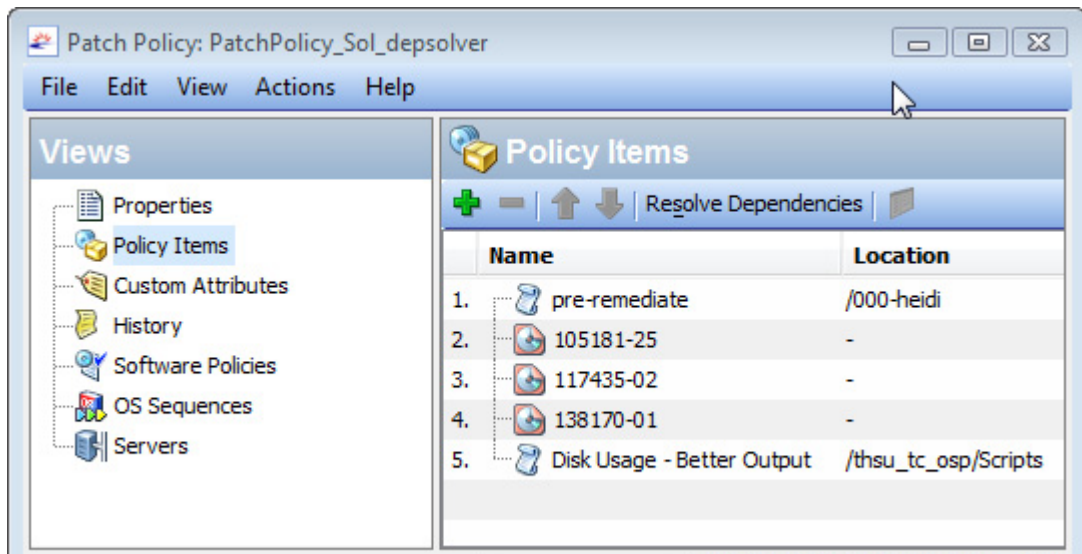


Figure 16 shows the results of selecting **Resolve Dependencies** for this patch policy. The following changes have been made to this patch policy:

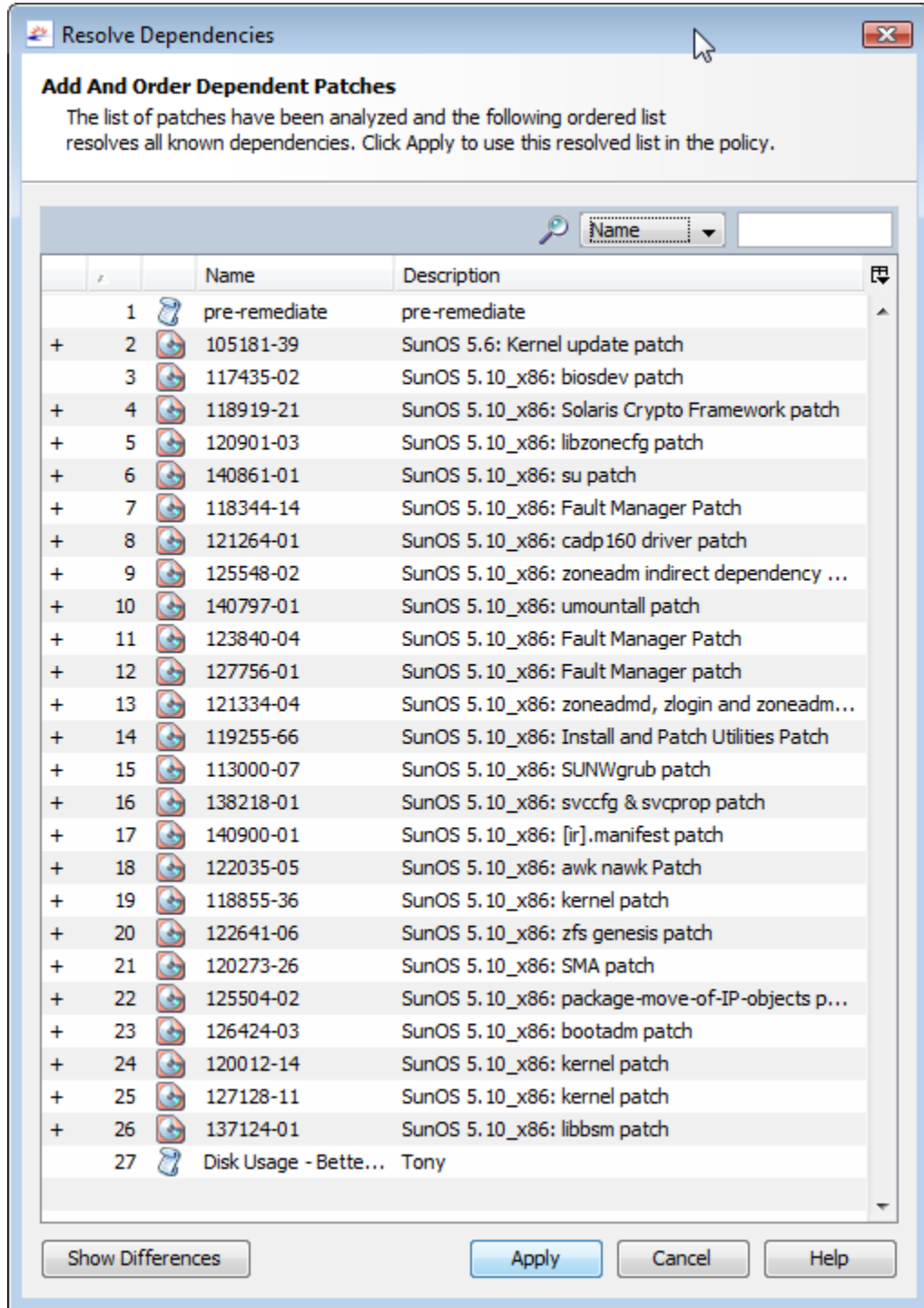
- Patch 105181-25 has been replaced with a newer version, 105181-39.
- Patch 117435-02 remains in the policy.
- Patch 137124-01 replaces patch 138170-01.
- 23 additional patches have been added because they are required by 137124-01.

- The two scripts remain in the policy, in their respective positions in the policy.



Because of the iterative nature of resolving dependencies for a set of patches, it is not always obvious how the changes to a patch policy were made.

**Figure 16 Dependencies for all Patches in a Patch Policy**



Click **Show Differences** to display more details about the differences between the original patch policy and the proposed new set of patches. In the Show Differences window, click **Export** to save the differences between the policies to a file. You can use this information with the `solpatch_import` command to import the new patches into SA.

## Custom Attributes

Custom attributes are named data values that you can create and set for patch policies. They provide a way for you can save additional information about patch policies. You can use custom attributes in a variety of ways including in scripts, network and server configuration, notifications, and CRON script configurations. When you set a custom attribute for a patch policy, it is available to all servers attached to the policy. For more information on custom attributes, see the *SA User Guide: Server Automation*.

### Adding a Custom Attribute to a Patch Policy

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





---

You must have a set of permissions to add custom attributes to a Solaris patch policy. To obtain these permissions, contact your SA administrator. See the *SA Administration Guide* for more information.


---

To add a custom attribute to a patch policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patch Policies** ► **Solaris** and select a version of Solaris.
- 2 In the content pane, select the Solaris patch policy and open it. The Solaris Patch Policy window appears.
- 3 In the Views pane, select Custom Attributes.
- 4 Either select , or from the **Actions** menu, select **Add...** A new custom attribute is added named “New Attribute”.
- 5 Enter the name of the custom attribute and select Enter.
- 6 To give a value to the custom attribute, either double click on the row under the Value column and enter the value, or click  and enter the value in the Input Dialog.
- 7 Select **Save** from the **File** menu.

### Deleting a Custom Attribute from a Patch Policy

To delete a custom attribute from a patch policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patch Policies** ► **Solaris** and select a version of Solaris.
- 2 In the content pane, select the Solaris patch policy and open it. The Solaris Patch Policy window appears.
- 3 In the Views pane, select Custom Attributes. This displays the custom attributes defined for the policy.
- 4 In the content pane, select the custom attribute that you want to delete and then click , or from the **Actions** menu, select **Remove**.

- 5 Select **Save** from the **File** menu.

## Viewing Patch Policy History

To view the events associated with a Solaris patch policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patch Policies** ► **Solaris** and select a version of Solaris.
- 2 In the content pane, select the Solaris patch policy.
- 3 Right-click to open the Solaris Patch Policy window.
- 4 In the Views pane, select History. The content pane displays the events associated with the Solaris patch policy. You can view the action performed on the policy, the user who performed the action, and the time when the action was performed.
- 5 From the Show drop-down list, select the time period you want to see the events from.

## Viewing Software Policies Associated with a Patch Policy

A software policy can contain Solaris patch policies. In the Solaris patch policy window, you can view all software policies that include the selected Solaris patch policy as one of the items to be installed.

To view software policies that contain the selected Solaris patch policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patch Policies** ► **Solaris** and select a version of Solaris.
- 2 In the content pane, select the Solaris patch policy.
- 3 Right-click to open the Solaris Patch Policy window.
- 4 In the Views pane, select Software Policies. The content pane displays a list of software policies that contain the selected Solaris patch policy as one of the items to be installed.

## Viewing OS Sequences Associated with a Patch Policy

In the Solaris Patch Policy window, you can view all the OS Sequences that contain the selected patch policy as one of the items to be installed.

To view OS sequences associated with a Solaris patch policy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patch Policies** ► **Solaris** and select a version of Solaris.
- 2 In the content pane, select the Solaris patch policy.
- 3 Right-click to open the Solaris Patch Policy window.
- 4 In the Views pane, select OS Sequences. The content pane displays a list of OS Sequences that contain the selected patch policy as one of the items to be installed.

## Viewing Servers Attached to a Patch Policy

In the SA Client, you can view a list of all servers and device groups that have a selected Solaris patch policy attached to them.

To view a list of all servers that have a selected Solaris patch policy attached to them:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Software Policies** ► **Solaris** and an operating system version.
- 2 In the content pane, select the Solaris patch policy and then right-click to open the Solaris Patch Policy window.
- 3 In the Views pane, select Servers. A list of servers that have the selected Solaris patch policy attached to them displays in the content pane.

## Finding a Solaris Patch Policy in Folders

To find a Solaris patch policy in the folder hierarchy:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patch Policies** ► **Solaris** and select a version of Solaris.
- 2 In the content pane, select a Solaris patch policy.
- 3 Right-click and then select **Locate in Folders** to display the folder hierarchy for the Solaris patch policy in the content pane.

# Patch Management Tasks

Patch management for Solaris consists of the following tasks:

- [Initializing the Solaris Patch Database](#) on page 120
- [Finding Solaris Patches](#) on page 122
- [Importing a Patch or Patch Cluster](#) on page 125
- [SA Client Import](#) on page 125
- [Exporting a Patch or Patch Cluster](#) on page 126
- [Opening a Solaris Patch](#) on page 127
- [Managing Properties](#) on page 127
- [Editing Properties](#) on page 131
- [Viewing the Vendor Readme](#) on page 131
- [Importing Custom Documentation](#) on page 132
- [Viewing Patch Cluster Contents](#) on page 132
- [Viewing Patch Clusters Associated with a Patch](#) on page 132
- [Viewing Software Policies Associated with a Patch or Patch Cluster](#) on page 133
- [Viewing Patch Policies Associated with a Patch or Patch Cluster](#) on page 133
- [Viewing Servers Associated with a Patch or Patch Cluster](#) on page 133
- [Deleting a Patch or Patch Cluster](#) on page 134
- [Installing a Patch](#) on page 135
- [Uninstalling a Patch](#) on page 142
- [Detecting Benign Error Codes](#) on page 136

## Running `solpatch_import`



In a multimaster mesh environment, do not simultaneously run the `solpatch_import` command on more than one core system. This action could result in lost data. It is recommended that you run `solpatch_import` on your core servers, one at a time.

Some Solaris patch management tasks use the `solpatch_import` command. You must have the following permissions to run the `solpatch_import` command:

**Table 10** Permissions Required for Using `solpatch_import`

Type of Permission	Permission Setting
Permissions on the folders <code>/Opware</code> , <code>/Opware/Tools</code> and <code>/Opware/Tools/Solaris Patching</code> in the SA library	You must have full permissions on these folders. This is where SA stores Solaris patch information.
“Manage Patch” feature permission	You must have “Read & Write” permission.

**Table 10 Permissions Required for Using solpatch\_import**

Type of Permission	Permission Setting
“Allow Install Patch” feature permission	This must be set to “Yes”.
“Allow Uninstall Patch” feature permission	This must be set to “Yes”.
“Manage Patch Compliance Rules” feature permission	This must be set to “Yes”.

See the *SA Administration Guide* for more information on folder permissions and Solaris patching permissions.

To use the `solpatch_import` command, you must log in to the SA core server as `root`.

To run the command, log into the core server running the Software Repository component (part of the Slice Component bundle) and, as `root`, run the `solpatch_import` command that is located in the following directory:

```
/opt/opsware/solpatch_import/bin/
```

The complete documentation for the `solpatch_import` command is available by running the command with the following option:

```
solpatch_import --manual
```

## Initializing the Solaris Patch Database



Before you download patches and patch data from Oracle, you must set up and initialize the Solaris patch database in SA.

### To set up and initialize the Solaris patch database:

- 1 Create a configuration file that specifies information needed by the `solpatch_import` command.

The default location for this file is `/etc/opt/opsware/solpatch_import/solpatch_import.conf`.

If you do not use the default location, you must use the `-c` or `--conf` option. If you use the default location, you do not need the `-c` or `--conf` option.

For details on the contents of this configuration file, see the `solpatch_import` man page by running `solpatch_import --manual`. The following example shows partial contents of a configuration file.

```
[main]
hpsa_user=<SA user name>
hpsa_pass=<SA user password>
download_user=<My Oracle account user name>
download_pass=<My Oracle account password>
```

- 2 Run the following command to initialize SA for Solaris patch information:

```
solpatch_import -a create_db
```

This command downloads the `patchdiag.xref` file from Oracle (or you can specify a local copy of this file if you previously downloaded it), examines the patch information and places the data in SA.



---

You only need to use the `-a create_db` option once to initialize the Solaris patch information in SA.

---

- 3 Make sure your Solaris patch database contains the latest patch information. See [Maintaining the Solaris Patch Database](#) on page 121.

## Maintaining the Solaris Patch Database

Complete the following tasks to make sure your Solaris patch database contains the latest patch information:

- [Retrieving the Latest Patch Data from Oracle](#)
- [Retrieving the Solaris Patch Supplementary Data File](#)
- [Manually Downloading the Solaris Patch Supplementary Data File](#)



**Best Practice:** Whichever method you use, it is recommended that you regularly check for updates and install them to the SA patch database.

### Retrieving the Latest Patch Data from Oracle

Oracle typically updates their patch information daily Monday through Friday. To obtain the latest Solaris patch information from Oracle (in the `patchdiag.xref` file) and upload it to the SA patch database, you should routinely run the command below, based on your company policy. For example you could place the following command in a cron job:

```
solpatch_import -a update_db
```

### Retrieving the Solaris Patch Supplementary Data File

SA retrieves information about Solaris patches from Oracle (from the `patchdiag.xref` file). However, SA provides valuable supplementary data about Solaris patches that you can obtain automatically from the HP BSA Essentials Network. When HP updates this supplementary data, you can configure the HP BSA Network to automatically upload it to the SA Solaris patch database.

**To obtain the supplementary data file when it is updated and upload it into the SA Library:**

- 1 Obtain a BSA Essentials Network account from <http://www.hp.com/go/bsanetwork>.
- 2 Install and configure the HP Live Network connector (LNC) on the core server where the SA Software Repository component is installed.

See the *HP Live Network connector Installation and Configuration Guide*. This document is available on the BSA Essentials Web site at <http://www.hp.com/go/bsanetwork>.

- 3 On the system where the LNC is installed, run the following command to enable the Solaris patching service:

```
live-network-connector write-config --setting=content.solaris_patching=1
```

- 4 (Optional) To disable the Solaris patching service, run the same command with the value set to 0:

```
live-network-connector write-config --setting=content.solaris_patching=0
```

Alternatively, you can manually download the supplementary Solaris patch data file from the HP BSA Essentials Network and upload it to the SA database. See [Manually Downloading the Solaris Patch Supplementary Data File](#) on page 122.



## Manually Downloading the Solaris Patch Supplementary Data File

This section describes how to manually download the supplementary Solaris patch data file from the HP BSA Essentials Network and upload it into the SA patch database. It is recommended that you set up the LNC to automatically upload this file whenever it changes as described in [Retrieving the Solaris Patch Supplementary Data File](#) on page 121. However, if you download the file manually, you should regularly check for updates and install them into the SA patch database as described here.

To obtain the supplementary data file:

- 1 Obtain a BSA Essentials Network account from <http://www.hp.com/go/bsanetwork>.
- 2 Log in to the BSA Essentials Network Web site at <http://www.hp.com/go/bsanetwork>.
- 3 Locate the package “Solaris Patching for Server Automation” under the Standard Content, under Server Automation Community”.
- 4 Download the Solaris patching package, named `solpatchdb_supplement.zip`.
- 5 Place the `solpatchdb_supplement.zip` file on a core slice server in any temporary directory such as `/tmp`.
- 6 Unzip the `solpatchdb_supplement.zip` file.
- 7 Run the file `install.sh` which was in the `solpatchdb_supplement.zip` file. This uploads the Solaris patch supplementary data into the SA patch database.
- 8 Since HP updates the Solaris patch supplementary data file, it is recommended that you periodically check this file for updates and when this file changes, follow these steps again to download the latest supplementary patch information into your SA patch database.

## Finding Solaris Patches

With SA you can quickly and easily determine which patches your Solaris servers need.

Using the `solpatch_import` command, you can:

- Display Solaris patches required by your Solaris servers, including all dependent patches and patches listed in the correct install order.
- Download those patches and import them to the SA Library.
- Add those patches to a Solaris patch policy.

The following table lists options for the `solpatch_import` command to display patch information, download patches, import them to the SA Library, and add them to a Solaris patch policy.

**Table 11 Specifying Actions for the `solpatch_import` Command**

Option to <code>solpatch_import</code> Command	Description
<code>-a show</code> or <code>--action show</code>	Displays information about the specified patches.
<code>-a import</code> or <code>--action import</code>	Downloads the specified patches and imports them into the SA Library.
<code>-a policy</code> or <code>--action policy</code>	Downloads the specified patches, imports them into the SA Library, and places them in the specified Solaris patch policy. This action requires you to specify a Solaris patch policy using the <code>--policy_path</code> option.

The `solpatch_import` command finds all patches that are applicable to your managed servers, excluding patches that are not applicable. For example, if you do not have certain software applications or dependent patches installed, SA considers certain patches as not applicable. The resulting set of patches are complete and in the required install order.

Table 12 lists the `solpatch_import` command filters that specify which Solaris patches you want:

**Table 12 Specifying Desired Patches with the Filter Option to `solpatch_import`**

Desired Set of Patches	Filter Options to Use	Example Filter Option	Description of Example Filter Option
All patches recommended by Oracle for a particular server	<code>rec server</code>	<code>-f "rec,server=sys01.hp.com"</code>	Specifies all patches recommended by Oracle for the <code>sys01.hp.com</code> managed server.
All patches recommended by Oracle for a set of servers	<code>rec platform</code>	<code>-f "rec,OS=5.10"</code>	Specifies all patches recommended by Oracle for all managed servers running Solaris 5.10.
All Oracle security patches for a particular server	<code>sec server</code>	<code>-f "sec,server=sys01.hp.com"</code>	Specifies all Oracle security patches for the <code>sys01.hp.com</code> managed server.
All Oracle security patches for a set of servers	<code>sec OS</code>	<code>-f "sec, OS=5.9"</code>	Specifies all Oracle security patches for all managed servers running Solaris 5.9.
All Oracle security patches and all Oracle recommended patches for a server.	<code>rec sec server</code>	<code>-f "rec, sec, OS=5.8"</code>	Specifies all Oracle security patches and all the Oracle recommended patches for all managed servers running Solaris 5.8.

The following examples show ways you can use the `solpatch_import` command to determine which patches are needed by your Solaris servers:

- [Finding All Patches Required by a Selected Server](#) on page 124
- [Finding Oracle Recommended Patches for Your Servers](#) on page 124
- [Finding Oracle Security Patches for Your Servers](#) on page 124
- [Finding a Specific Set of Patches](#) on page 124

For complete information, run `solpatch_import --manual` as described in [Running solpatch\\_import](#) on page 119.

## Finding All Patches Required by a Selected Server

The following example command finds all the patches needed by the server named “sys01.hp.com”. The first command just displays the list of patches. The second command downloads the patches and places them into the SA Library. The third command places them into the Solaris patch policy names “SolPatches/MyPolicy”.

```
solpatch_import --action=show --filter="server=sys01.hp.com"
solpatch_import --action=import --filter="server=sys01.hp.com"
solpatch_import --action=policy --policy_path="SolPatches/MyPolicy" \
  --filter="server=sys01.hp.com"
```

## Finding Oracle Recommended Patches for Your Servers

The following example command finds the Oracle recommended patches for all managed servers running Solaris 10. The first command just displays the list of patches. The second command downloads the patches and places them into the SA Library. The third command places them into the Solaris patch policy named MySolPolicy.

```
solpatch_import --action=show --filter="rec,OS=5.10"
solpatch_import --action=import --filter="rec,OS=5.10"
solpatch_import --action=policy --policy_path="MySolPolicy" \
  --filter="rec,OS=5.10"
```

## Finding Oracle Security Patches for Your Servers

The following example command displays the Oracle security patches for all your managed servers running Solaris 9:

```
solpatch_import --action=show --filter="sec,OS=5.9"
```

## Finding a Specific Set of Patches

You can display information about one or more patches by providing the patch names to the `solpatch_import` command or in a text file. This example assumes the file `my_sol_patches.txt` contains the following lines:

```
120900-04 121133-02 119254-67
119317-01 121296-01 127884-01
```

The following example command displays the set of patches listed in the file `my_sol_patches.txt`:

```
solpatch_import --action=show my_sol_patches.txt
```

The following command downloads the set of patches listed in the file `my_sol_patches.txt` and places the patches into the SA Library:

```
solpatch_import --action=import my_sol_patches.txt
```

The following example command downloads the set of patches listed in the file `my_sol_patches.txt`, places the patches into the SA Library, and places the patches into a Solaris patch policy named “/SolPatches/SolPatchPolicy”:

```
solpatch_import --action=policy --policy_path=/SolPatches/SolPatchPolicy \
  my_sol_patches.txt
```

For more information on the `solpatch_import` command, see [Running solpatch\\_import](#) on page 119.

## Importing a Patch or Patch Cluster

You can import a patch or patch cluster by using `solpatch_import` command or you can import a patch or patch cluster by using the SA Client.

### `solpatch_import`



**Best Practice:** HP recommends that you use the `solpatch_import` command to import Solaris patches and patch clusters from Oracle.

With the `solpatch_import` command you can automatically download Solaris patches and patch clusters from Oracle, import them into SA, place them into Solaris patch policies, and store the patch policies in a folder in the SA Library. The `solpatch_import` command also downloads reboot settings and patch dependencies and saves them with the patch.

### SA Client Import

You can also import Solaris patches by using the SA Client.

Solaris patches are downloaded from Oracle and stored in SA.

To see if a patch has been imported, view the patch’s Availability property in the SA Client. The Availability property of an imported patch can be set to one of the values listed in [Table 13](#).

**Table 13 Patch Availability Property Settings**

Patch Availability Setting	Description
<b>Available</b>	The patch has been imported into SA, has been tested, and can be installed on managed servers.
<b>Limited</b>	The patch has been imported into SA but requires additional permissions (Manage Patch: Read & Write) to be installed. This is the default patch availability. For more information on permissions, see the <i>SA Administration Guide</i> .
<b>Deprecated</b>	The patch cannot be added to patch policies but can still be installed.
<b>Not Imported</b>	The patch is not stored in the SA library.



---

You must have permissions to import Solaris patches or patch clusters. To obtain these permissions, contact your SA administrator. See the *SA Administration Guide* for more information.

---

#### To import a Solaris patch or patch cluster from a file into SA:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**. The patches are organized by operating system.
- 2 From the **Actions** menu, select **Import Software** to open the Import Software window.
- 3 Click **Browse** to locate and select the patch or patch cluster to import.

Before you click **Open** in the Open window, select the character encoding to be used by the patch or patch cluster from the Encoding drop-down list.

You must specify the character encoding so that SA can extract the metadata contained in the patch or patch cluster and then correctly display the information in non-ASCII characters in the SA Client, such as in the Patch Properties window. Patch metadata includes comments, READMEs, scripts, descriptions, and content lists.

- 4 Click **Open**.
- 5 In the Import Software window, from the Type drop-down list, select either Solaris Patch or Solaris Patch Cluster.

This action grays out the Folder edit field because Solaris patches and patch clusters are not stored in folders.

- 6 From the Platform drop-down list, select the applicable Solaris operating system.
- 7 Click **Import** to import the Solaris patch or patch cluster into SA.
- 8 Run the following command to update the Solaris patch information in SA:

```
solpatch_import -a update_db
```

## Exporting a Patch or Patch Cluster

You can export a Solaris patch or patch cluster to your local computer so that you can check the installation of the patch or patch cluster on a test or staging machine.

#### To export a patch or patch cluster to your local drive:


- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**. The patches are organized by operating system in the content pane. Navigate to the desired operating system version.
- 2 In the content pane, select a patch or patch cluster to export.
- 3 Right click or from the **Actions** menu, select **Export** to open the Export Patch window.
- 4 Specify the location for the package to be exported to.
- 5 Click **Export**.

## Opening a Solaris Patch

In the SA Client, you open a Solaris patch by using any of the following navigation features:

- [Search](#) on page 127
- [Library—By Type](#) on page 127

### Search

- 1 In the navigation pane, select Search.
- 2 Select Patch from the drop-down list and then enter the name of the Solaris patch or patch cluster in the text field.
- 3 Select . The search results appear in the content pane.
- 4 In the content pane, select the patch or patch cluster.
- 5 From the **Actions** menu, select **Open** to open the Patch or Patch Cluster window.

### Library—By Type

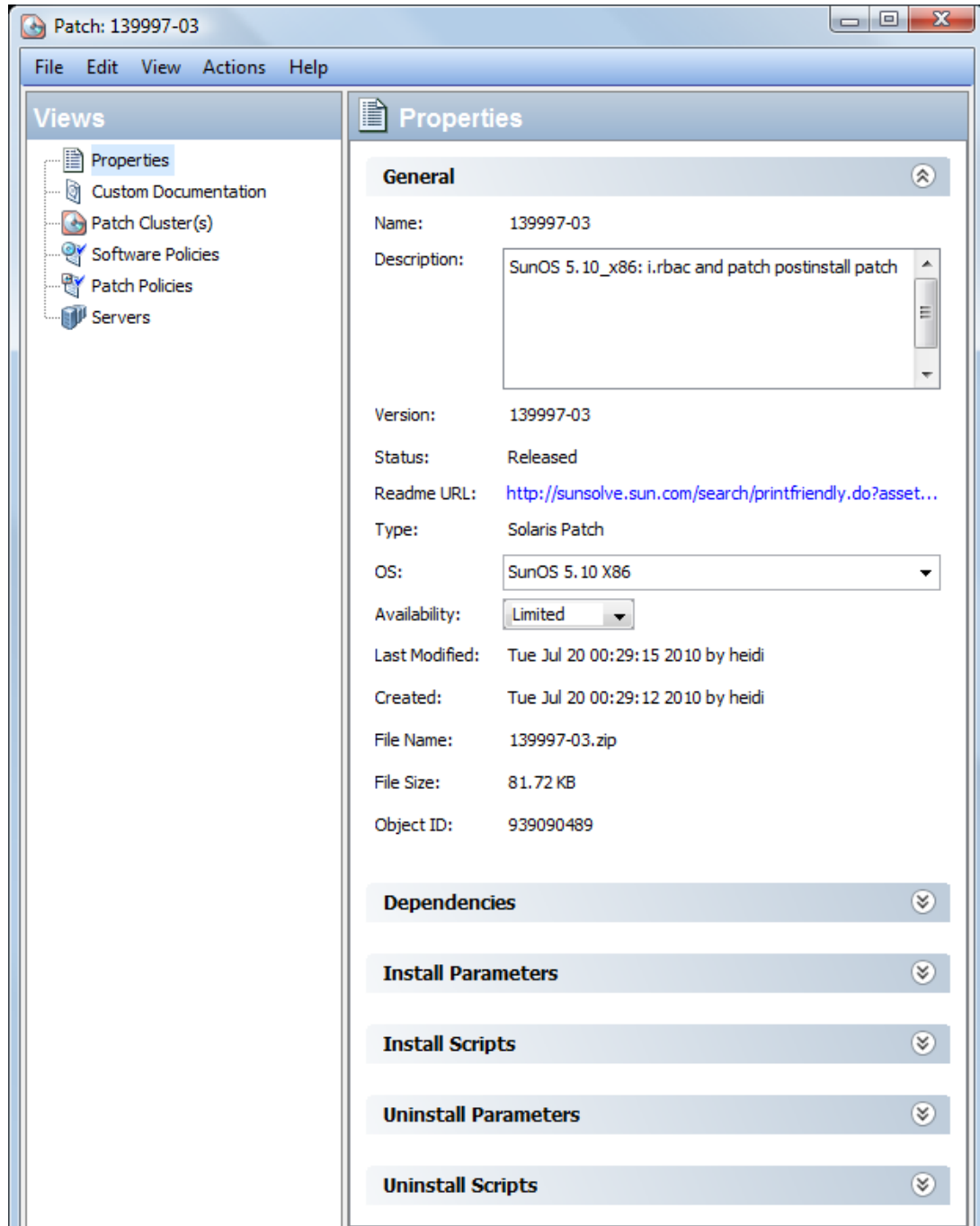
- 1 In the navigation pane, select **Library ► By Type ► Patches**. The patches appear in the content pane.
- 2 In the content pane, select the patch or patch cluster.
- 3 From the **Actions** menu, select **Open** to open the Patch or Patch Cluster window.

## Managing Properties

To view the properties of a Solaris patch, patch cluster, or patch bundle:

- 1 In the navigation pane, select **Library ► By Type ► Patches**. The patches are organized by operating system appear in the content pane. Navigate to the desired OS version.
- 2 In the content pane, select the Solaris patch, patch cluster or patch bundle to view.
- 3 Right-click and select **Open** to display the Patch window.
- 4 In the Views pane, select Properties to display the patch properties as shown in [Figure 17](#).

Figure 17 Patch Properties Window



## General Properties

**Name:** The name of the patch, patch cluster or bundle, as defined by Oracle.

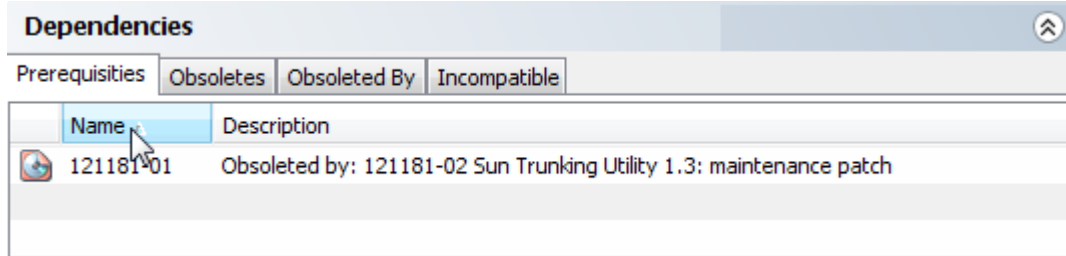
- **Description:** The description of the patch, cluster, or bundle's contents.
- **Version:** The version number, as defined by Oracle.
- **Status:** The status as defined, by Oracle.
- **Readme URL:** A link to documentation about the patch. You must provide your My Oracle credentials to view this information.

- **Type:** Specifies whether the item is a patch, a patch cluster, or a patch bundle.
- **OS:** The operating systems associated with the patch, cluster, or bundle.
- **Availability:** The availability of the patch to SA users. You can set this to Limited, Available or Deprecated.
- **Last Modified:** The date and time when the patch was last modified and the SA user who last modified the patch.
- **Created:** The date and time when the patch or patch cluster was created by an SA user.
- **File Name:** The file name of the package.
- **File Size:** The file size of the package.
- **Object ID:** The unique SA identifier for the package.

## Dependencies

Figure 18 shows the dependencies for a patch in the Patch Properties window.

**Figure 18 Patch Dependencies**



- **Prerequisites:** The patches that must be installed before this patch can be installed.
- **Obsoletes:** The older patches that are made obsolete by this patch.
- **Obsoleted by:** The newer patches that make this patch obsolete.
- **Incompatible:** The patches that cannot be installed with this patch.

## Install Parameters

Figure 19 shows a list of the actual settings for the patch and the settings that Oracle specifies for the patch. The selected radio buttons are the actual settings that will be used when the patch is installed. Settings that Oracle recommends are labeled “Oracle default”. The Oracle default settings are the values that were downloaded with the patch.

The settings specified by the selected radio buttons will be used when the patch is installed. However, when you remediate a server against a patch policy or install a patch, you can override these settings. For more information, see [Rebooting Options](#) on page 139.



Figure 19 Install Parameters in the Patch Properties Window

**Install Parameters**

Install Flags:

Reboot Required:  Yes  No (Oracle default)

Install Mode:  Single User Mode  Multi User Mode (Oracle default)

Reboot Type:  Standard (Oracle default)  Reconfiguration

Reboot Time:  Normal (Oracle default)  Immediate

- **Install Flags:** (*Optional*) Arguments that are used when the patch or patch cluster is installed on a managed server.
- **Reboot Required:** Specifies whether the managed server will be rebooted when the patch or patch cluster is successfully installed. Oracle’s recommendation is labeled “Oracle default”.
- **Install Mode:** Specifies whether the patch or patch cluster will be installed in single user mode or multi-user mode. Oracle’s recommendation is labeled “Oracle default”. The Solaris system is rebooted to get into single user mode, then the patch is installed, and then the system is rebooted to get to multi-user mode.
- **Reboot Type:** Specifies whether a standard reboot or a reconfiguration reboot will be performed after installing the patch or patch cluster. Oracle’s recommendation is labeled “Oracle default”.
- **Reboot Time:** Specifies whether the server will be rebooted immediately after installing the patch or at some later time after the patch or patch cluster is installed. Oracle’s recommendation is labeled “Oracle default”.

When installing a patch with the setting **Reboot Time: Normal**, the reboot will occur at the end of the job, unless another patch in the job requires an immediate reboot before the end of the job. However, the Job Preview and the Job Status windows will display the **Install and Reboot** message for the patch. This indicates that the reboot will occur *sometime* after the patch is installed, not *immediately* after the patch is installed.

## Install Scripts

- **Pre-Install Script:** A script that is required to run on a managed server *before* the patch or patch cluster is installed.
- **Post-Install Script:** A script that is required to run on a managed server *after* the patch or patch cluster is installed.
- **If script returns an error:** Specifies whether or not to stop the installation of the patch or patch cluster if the script fails.

## Uninstall Parameters

- **Uninstall Flags:** (*Optional*) Arguments that are used when the patch or patch cluster is uninstalled from a managed server.
- **Reboot Required:** Specifies whether the managed server will be rebooted when the patch or patch cluster is successfully uninstalled. Oracle’s recommendation is labeled “Oracle default”.

- **Uninstall Mode:** Specifies whether the patch or patch cluster will be uninstalled in single user mode or multi-user mode. Oracle’s recommendation is labeled “Oracle default”. The Solaris system is rebooted to get into single user mode, then the patch is uninstalled, and then the system is rebooted to get to multi-user mode.
- **Reboot Type:** Specifies whether a standard reboot or a reconfiguration reboot will be performed after uninstalling the patch or patch cluster. Oracle’s recommendation is labeled “Oracle default”.
- **Reboot Time:** Specifies whether the server will be rebooted immediately or at some later time after the patch or patch cluster is uninstalled. Oracle’s recommendation is labeled “Oracle default”.

## Uninstall Scripts

- **Pre-Uninstall Script:** A script that is required to run on a managed server before the patch or patch cluster is uninstalled.
- **Post-Uninstall Script:** A script that is required to run on a managed server after the patch or patch cluster is uninstalled.
- **If script returns an error:** Specifies whether or not to stop the uninstallation of the patch or patch cluster if the script fails.

## Editing Properties

After you upload a new Solaris patch, patch cluster, or patch bundle, or select an existing one, you can add or edit many of its properties in the SA Client.



You must have a set of permissions to edit the properties of a patch or patch cluster. To obtain these permissions, contact your SA administrator. See the *SA Administration Guide* for more information.

To edit the properties of a Solaris patch, patch cluster, or patch bundle:

- 1 In the Patch window, select a patch.
- 2 Right-click to open the Patch Properties.
- 3 Edit any of the properties that are editable in the SA Client.

## Viewing the Vendor Readme

The SA Client gives you access to patch information from Oracle, using the URL provided with the downloaded patch, cluster, or bundle.

To view the readme:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**. The patches are organized by operating system. Navigate to an OS version.
- 2 In the content pane, select a Solaris patch, patch cluster, or patch bundle to view.
- 3 From the **Actions** menu, select **Open**. This displays the patch information window.
- 4 In the Views pane, select Properties. This displays information about the patch, including a URL link to the patch information.
- 5 Select the Readme URL and enter your My Oracle credentials to view the vendor information.

## Importing Custom Documentation

To import custom documentation for a Solaris patch or patch cluster using the SA Client:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**. The patches are organized by operating system. Navigate to the desired OS version.
- 2 In the content pane, select the Solaris patch or patch cluster to view.
- 3 Right-click and then select **Open**. The Patch or Patch Cluster window appears.
- 4 In the Views pane, select Custom Documentation. The contents of the Custom Documentation for the patch or patch cluster appear in the content pane.
- 5 From the **Actions** menu, select **Import**. The Import Custom Documentation window appears.
- 6 In the Import Custom Documentation window, locate the text file and specify the encoding.
- 7 Click **Import**.

## Patches and Patch Clusters

The SA Client provides the following capabilities that help you manage Solaris patches and patch clusters:

- [Viewing Patch Cluster Contents](#) on page 132
- [Viewing Patch Clusters Associated with a Patch](#) on page 132
- [Viewing Software Policies Associated with a Patch or Patch Cluster](#) on page 133
- [Viewing Patch Policies Associated with a Patch or Patch Cluster](#) on page 133
- [Viewing Servers Associated with a Patch or Patch Cluster](#) on page 133
- [Deleting a Patch or Patch Cluster](#) on page 134

### Viewing Patch Cluster Contents

To view the contents of a Solaris patch cluster:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**. The patches organized by operating systems appear in the content pane. Navigate to the desired OS version.
- 2 In the content pane, select the Solaris patch cluster.
- 3 From the **Actions** menu, select **Open**. The Patch Cluster window appears.
- 4 In the Views pane, select Contents. The list of patches included in the patch cluster appears in the content pane.
- 5 Select a patch in the content pane.
- 6 From the **Actions** menu, select Open to view the patch properties.

### Viewing Patch Clusters Associated with a Patch

To view the patch clusters that contain the Solaris patch:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**. The patches organized by operating systems appear in the content pane. Navigate to the desired OS version.
- 2 In the content pane, select the Solaris patch.

- 3 From the **Actions** menu, select **Open**. The Patch window appears.
- 4 In the Views pane, select Patch Clusters. The list of patch clusters that contain the patch appears in the content pane.
- 5 Select a patch cluster in the content pane, and from the **Actions** menu, select Open to view the properties of the patch cluster.

## Viewing Software Policies Associated with a Patch or Patch Cluster

To view the software policies that contain the Solaris patch or patch cluster:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**. The patches organized by operating systems appear in the content pane. Navigate to the desired OS version.
- 2 In the content pane, select the Solaris patch or patch cluster.
- 3 From the **Actions** menu, select **Open**. The Patch or Patch Cluster window appears.
- 4 In the Views pane, select Software Policies. The list of software policies that contain the patch or patch cluster as one of the policy items appear in the content pane.
- 5 Select a software policy in the content pane, and from the **Actions** menu, select Open to view the properties of the software policy.

## Viewing Patch Policies Associated with a Patch or Patch Cluster

To view patch policies that contain the Solaris patch or patch cluster:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**. The patches organized by operating systems appear in the content pane. Navigate to the desired OS version.
- 2 In the content pane, select the Solaris patch.
- 3 From the **Actions** menu, select **Open**. The Patch or Patch Cluster window appears.
- 4 In the Views pane, select Patch Policies. The list of patch policies that contain the patch or patch cluster as one of the policy items appear in the content pane.
- 5 Select a software policy in the content pane, and from the **Actions** menu, select Open to view the properties of the patch policy.

## Viewing Servers Associated with a Patch or Patch Cluster

To view the servers that have the Solaris patch or patch cluster installed by SA:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**. The patches organized by operating systems appear in the content pane. Navigate to the desired OS version.
- 2 In the content pane, select the Solaris patch.
- 3 From the **Actions** menu, select **Open**. The Patch or Patch Cluster window appears.
- 4 In the Views pane, select Servers. The list of servers that have the patch or patch cluster installed appear in the content pane.
- 5 Select a server in the content pane, and from the **Actions** menu, select Open to view the properties of the server.

## Deleting a Patch or Patch Cluster

When you delete a Solaris patch or patch cluster, it is removed from SA; however, it is not uninstalled from your managed servers. A patch or patch cluster cannot be deleted if it is attached to a patch policy or a software policy.



You must have a set of permissions to delete a patch or patch cluster. To obtain these permissions, contact your SA administrator. See the *SA Administration Guide* for more information.

To delete a Solaris patch or patch cluster:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**. The patches organized by operating system appear in the content pane. Navigate to the desired OS version.
- 2 In the content pane, select a patch or patch cluster to delete.
- 3 From the **Actions** menu, select **Delete**.

## Solaris Zones

The SA Client provides the following capabilities that help you manage Solaris zones:

- [Patching Solaris Zones](#) on page 134
- [Viewing Solaris Zones](#) on page 134

### Patching Solaris Zones

SA virtual server management enables you to perform the same operations on virtual servers that you can perform on physical servers, including audit, remediation, application configuration, software management, patch management, and so on.

You can install patches on Solaris global and non-global zones by using Solaris patch policies or by installing patches directly on a virtual server. In the SA Client, you can view the Solaris zones from either the Managed Servers lists or the Virtual Servers list.

### Viewing Solaris Zones

To view Solaris zones:

- 1 In the navigation pane, select **Devices**.
- 2 Expand **Servers**.
- 3 Select Virtual Servers to display a list of virtual servers in the content pane.

Or

Select Managed Servers. To identify whether a server is a hypervisor or a virtual server in the **All Managed Servers** list, select **Virtualization** from the column selector.

- 4 From the View drop-down list, select **Virtualization** to display the configuration properties of the virtual server.

## Installing a Patch

You can install a Solaris patch directly on managed a server or on all servers in a device group, or you can add a Solaris patch to a Solaris patch policy (or to a software policy), attach the policy to a managed server or device group and then remediate the server against the policy. When you remediate a server or device group, the Solaris patch specified in the attached policy is installed on the managed server.

SA provides the following ways to install a Solaris patch on a managed server:

- Install a Solaris patch directly on a managed server by using the Install Patch wizard.
- Install a Solaris patch directly on a managed server by using the Install Software wizard.
- Install a Solaris patch or a patch cluster on a managed server by using a Solaris patch policy.
- Install a Solaris patch or a patch cluster on a managed server by using a software policy.



---

If you install or remove a Solaris patch without using SA, you must perform a software registration and a compliance scan to make sure that SA has complete and up-to-date information about the managed server. See [Patch Compliance](#) on page 105.

---

## Installing a Patch Cluster



---

Before you install the Solaris patch cluster, review the Readme file for each cluster. For clusters that require a passcode, SA does not require that you to manually enter the passcode that is in the Readme file.

---

SA can install all Solaris patch clusters, including clusters that require passcodes. Some clusters may need to reboot the server multiple times during the install process. SA will automatically perform the reboots when the cluster Install Parameters has **Reboot Required** set to **Yes** and the remediate job options for rebooting are set to either **Reboot servers as specified by individual software items** (*Default*) or **Reboot servers after each installation or uninstallation**.

If any of these reboot options are not set, the cluster will install up to the point where a reboot is required, if one is required. At the completion of the remediation job, the cluster status will display **Not installed**, the job status will show **Failed**, and the output of the job will contain a message indicating that the server must be rebooted before any more patches can be installed. After rebooting the server, the rest of the cluster can be installed by running the job again. If the cluster requires a reboot, no other patches can be installed until the server is rebooted.

## Installing Manual Patches—`patchadd`

SA uses the `patchadd` utility to install Solaris patches. However, some patches, such as firmware updates, cannot be installed with `patchadd`. These *manual patches* have special installation instructions in their Readme files and must be installed manually on your Solaris servers.

While you can import these patches into the SA software repository and install them manually on servers, if you attempt to remediate a manual patch, the job will result in a Warning status. The patch status display **Will Not Install** and the output will indicate that the patch requires a special installation procedure and must be installed manually.

SA cannot determine if these manual patches have been installed. A compliance scan on a patch policy that contains a manual patch will report that the policy is non-compliant. In this case, you should install the patch manually and remove the patch from the policy.

## Detecting Benign Error Codes

Installing Solaris patches sometimes results in benign error codes. A benign error code is an error code that does not reflect a true error situation. For example, a patch installation may fail because the patch is already installed or because a superseding patch is already installed, resulting in a benign error code. The exit code from the Solaris `patchadd` command would indicate an error, when in reality the patch was not installed for a valid reason.

When a patch does not install because of a true error situation such as the server being out of disk space, SA reports the error and the valid error code.

SA detects benign error codes and reports success in most cases. In the following two cases, however, Solaris cannot detect benign error codes:

- Solaris Deferred-Activation Patches
- Any patches installed on Solaris Global Zones, where Local Zones are defined

To configure SA so that it will detect benign error codes:

- 1 Install the following patches on all your servers that are running Solaris 10:
  - 119254-36 (sparc)
  - 119255-36 (i386)
- 2 Run the SAS Web Client and log in as a user with the **Configure Opware** permission.  
By default, the **Configure Opware** permission is assigned to the **SA/Opware System Administrators** group. To locate and set it in the SAS Web Client:
  - a Select **Administration** ► **Users & Groups**.
  - b Select the Groups tab.
  - c Select the **SA/Opware System Administrators** group.
  - d Select the Features tab.
- 3 Under **Administration**, select **System Configuration**.
- 4 Select Command Engine.
- 5 In the configuration parameters table, locate the line:  
`way.remediate.sol_parse_patchadd_output`
- 6 Select **Use value:**.
- 7 Enter the number **1** in the edit field.
- 8 Click **Save**.

## Installing Patches Using a Patch Policy

Using a patch policy to install a Solaris patch consists of the following phases:

- [Attaching a Patch Policy to a Server](#) on page 137
- [Attaching a Server to a Patch Policy](#) on page 137.

## Attaching a Patch Policy to a Server

When you attach a Solaris patch policy to a server or a group of servers, the Solaris patch policy is associated with that server or group of servers. This action does not install the patches and patch clusters contained in the Solaris patch policy. To install the patches and patch clusters, you must remediate the server with the Solaris patch policies.



---

You must have permissions to attach a Solaris patch policy to a server. To obtain these permissions, contact your SA Administrator. See the *SA Administration Guide* for more information.

---

### To attach a Solaris patch policy to a server:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patch Policies** ► **Solaris**.
- 2 Select a Solaris version to display the patch policies in the content pane.
- 3 (*Optional*) In the content pane, select the Solaris patch policy.
  - a Right-click to open the patch policy in the Solaris Patch Policy window.
  - b From the View drop-down list, select Servers.
  - c In the content pane, select a server.
- 4 From the **Actions** menu, select **Attach Server**.
- 5 In the Attach Server window, select servers or device groups and then click **Attach**.

You can only select servers that are not in italics. Servers in italics indicate that you do not have the permission to attach a Solaris patch policy to the server.

- 6 (*Optional*) Select **Remediate Servers Immediately** to remediate the servers against the Solaris patch policy. Selecting this option displays the Remediate window. This option is only available if you have the Remediate Servers permission.

## Attaching a Server to a Patch Policy

When you attach a server or a group of servers to a Solaris patch policy, the policy is associated with that server or group of servers. This action does not install the patches or patch clusters contained in the Solaris patch policy. To install the patch and patch clusters, you must remediate the server with the Solaris patch policy.



---

You must have permissions to attach a server to a Solaris patch policy. To obtain these permissions, contact your SA Administrator. See the *SA Administration Guide* for more information.

---

### To attach a server to a Solaris patch policy:

- 1 In the navigation pane, select **Devices** ► **Servers** ► **All Managed Servers** to display a list of managed servers in the content pane.

Or

In the navigation pane, select **Devices** ► **Device Groups**. Navigate to a device group to display a list of device groups list in the content pane.
- 2 In the content pane, select a server or a device group.
- 3 From the **Actions** menu, select **Attach** ► **Patch Policy** to open the Attach Solaris Patch Policy window.



- 4 Click **Browse Solaris Patch Policies** and then select one or more policies in the list.  
Or  
Click **Browse Folders** and then select one or more policies in the folder hierarchy.
- 5 Click **Attach**.
- 6 (Optional) Select **Remediate Servers Immediately** to remediate the servers against the Solaris patch policy. Selecting this option displays the Remediate window. This option is only available if you have the Remediate Servers permission.

## Remediating a Server Against a Patch Policy

To install a Solaris patch in a patch policy on a Solaris server, you remediate the server against the policy. To remediate Solaris servers against a Solaris patch policy, perform the steps described in the *SA Software Management Guide*.

### Analyzing Patch Applicability

Before patches are downloaded and installed on each managed Solaris server, SA verifies that the patch is required on the server. This applicability analysis verifies that the:

- 1 Server platform matches the supported platform listed for the patch.
- 2 Patch or a superseding patch is not already installed on the server.
- 3 Package the patch applies to is already installed on the server.

If any of these conditions do not exist, the patch is non-applicable and will not be downloaded to or installed on a managed server. Non-applicable patches do not impact the overall job status—the job can still complete successfully.

### Install Parameters

Each Solaris patch has reboot settings specified by Oracle. These reboot settings are in the Install Parameters display in the SA Client. See [Figure 20](#). The Oracle settings are marked with “Oracle default”. The actual settings that will be used are the selected radio buttons.

[Figure 20](#) shows a patch for which Oracle does not require a reboot after installing the patch; however, the server will actually be rebooted. The policy setter has changed the **Reboot Required** setting to **Yes** to override Oracle’s recommendation and reboot the system after this patch is installed.

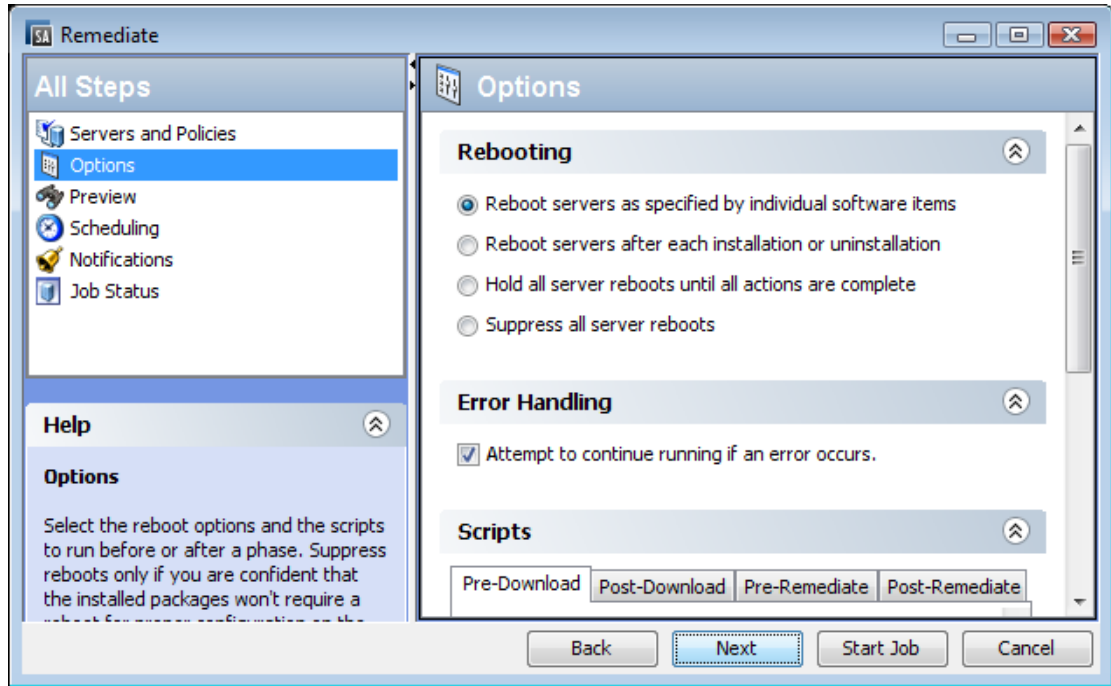
**Figure 20** Install Parameters

Install Parameters	
Install Flags:	<input type="text"/>
Reboot Required:	<input checked="" type="radio"/> <b>Yes</b> (Oracle default) <input type="radio"/> No (Oracle default)
Install Mode:	<input type="radio"/> Single User Mode <input checked="" type="radio"/> Multi User Mode (Oracle default)
Reboot Type:	<input checked="" type="radio"/> Standard (Oracle default) <input type="radio"/> Reconfiguration
Reboot Time:	<input checked="" type="radio"/> Normal (Oracle default) <input type="radio"/> Immediate

## Rebooting Options

When you remediate a Solaris server against a Solaris patch policy, SA installs the patches and uses the reboot settings specified for each patch. However, you can override these settings when starting the remediate job. Figure 21 shows the Options settings for the Remediate patch policy job.

**Figure 21 Rebooting Options**



The following options in the Remediate wizard determine whether the servers are rebooted after the patch is installed. These options apply only to the job launched by the Remediate window. They do not change the Reboot Required option, which is in the Install Parameters tab of the Patch Properties window. Except for the first option, the following options override the Reboot Required option.

- **Reboot servers as specified by individual software items (Default):** By default, the decision to reboot depends on the Reboot Required option of the patch or package properties.
- **Reboot servers after each installation or uninstallation:** As a best practice, reboot the server after *every* patch or package installation or uninstallation, regardless of the vendor reboot setting on the individual patch or package.
- **Hold all server reboots until after all packages are installed and/or uninstalled:** If the Reboot Required option is set for some selected patches but not for others, the server is rebooted one time after all patches are installed. If the Reboot Required option is not set for any of the selected patches, the server is not rebooted.
- **Suppress all server reboots:** Even if the Reboot Required option of the patch properties is set, do not reboot the server. (Because of vendor settings, some patches ignore the suppress option and force a reboot.

## Troubleshooting Patch Installation

When you remediate a Solaris patch that has the Install Mode (under Install Parameters in the Properties view) set to **Single User Mode**, the server will be rebooted into single user mode before installing the patch. If the remediation fails for some reason (such as when there is a network outage or a hardware failure), the system will remain in single-user mode.

To return the system to multi-user mode:

- 1 Log in to the Solaris server console.
- 2 Depending on the Solaris version, change to the directory by entering one of the following commands:

```
cd /etc/rcS.d/      # On Solaris 5.10
cd /etc/rc1.d      # On Solaris 5.6 - 5.9
```

- 3 Enter the following command.

```
./S99zOpswPatching exit_single_user_mode
```

- 4 Reboot the server by entering the following command or another method. This will reboot the server into multi-user mode.

```
shutdown -y -g 0 -i 6
```

If you do not have access to a server console on your Solaris server, use the SA Global Shell (OGSH) rosh utility:

- 1 Using an SA user who has the OGFS permission “Log in to Server”, open an OGSH session. For example, you could enter an `ssh` command such as:

```
ssh -p 2222 <user-name>@<ogfs-host>
```

- 2 Navigate to your Solaris server using a command such as:

```
cd /opsw/Server/@/<server name>/files/root
```

- 3 Launch the `rosh` utility.

- 4 Depending on the Solaris version, change to the directory by entering one of the following commands:

```
cd /etc/rcS.d/      # On Solaris 5.10
cd /etc/rc1.d      # On Solaris 5.6 - 5.9
```

- 5 Enter the following command:

```
./S99zOpswPatching exit_single_user_mode
```

- 6 Reboot the server entering the following command or another method. This will reboot the server into multi-user mode.

```
shutdown -y -g 0 -i 6
```

When you reboot the server, your `rosh` process will be terminated. Make sure the server is configured to auto-reboot.

If a patch requires single-user mode and fails to install for some other reason, such as a dependent patch is not installed, the Solaris host will be rebooted to single-user mode, the patch installation will be attempted, and the host will be rebooted to multi-user mode. These two reboots occur even if the patch installation fails.

## Installing Patches Using Offline Volumes

You can install Solaris patches using offline volumes. This section assumes you are familiar with Solaris Volume Manager.



---

A sample script is available so that you can modify it and use it to install Solaris patches using offline volumes.

---

To install Solaris patches using offline volumes:

- 1 Create a Solaris patch policy that contains the patches you want to install on the server. See [Creating a Solaris Patch Policy](#) on page 108.
- 2 Create a disk mirror on the server being patched.
- 3 Split the mirror.
- 4 Mount the offline disk.
- 5 Create a text file on the server named `/etc/opt/opsware/agent/offline_disk`.
- 6 Edit this file and enter the mount point of the offline disk, such as `/alt`.
- 7 Remediate the server against the patch policy to install the patches on the server.  
SA installs the patches to the offline disk at the offline disk mount point listed in the file `/etc/opt/opsware/agent/offline_disk`.
- 8 Reboot the server to the newly patched offline disk.
- 9 Verify that the patches are installed on the patched disk and that the server is running properly.
- 10 If the patched disk is behaving as expected, sync the mirror.

If the patched disk is not behaving as expected, reboot the system to the original disk and sync the mirrors.

## Uninstalling a Patch

When you remove a Solaris patch or patch cluster from a Solaris patch policy, this action does not uninstall it from a managed server. This action only removes the Solaris patch or patch cluster from the Solaris patch policy. To uninstall a Solaris patch from a managed server, you must directly uninstall the Solaris patch from the managed server. To remove a patch cluster, you must remove each of the patches in the patch cluster from the managed server.

SA provides the following ways to uninstall Solaris patches from managed servers or device groups:

- Uninstall a Solaris patch directly from a managed server by using the Uninstall Patch wizard.
- Uninstall a Solaris patch directly from a managed servers by using the Uninstall Software wizard.

In the SA Client, you can check for patch compliance on an individual server or view overall compliance levels for all servers and groups of servers in your facility.



# 5 Patch Management for Unix



## Overview

In Server Automation (SA), patch management for Unix enables you to identify, install, and remove patches, to maintain a high level of security across managed servers in your organization. Using the SA Client, you can identify and install patches that protect against security vulnerabilities for AIX operating systems.

This section contains information about how to install and uninstall Unix patches using software policies.

SA automates the key aspects of patch management, while offering a fine degree of control over how and under what conditions patches are installed.

Because patches are often released to address grave security threats, an organization needs to be able to roll out patches quickly, *before* systems are compromised. At the same time, however, patches can cause serious problems, from performance degradation to server failures.

SA allows you to react quickly to newly discovered threats and also provides support for strict testing and standardization of patch installation. If patches cause problems after being tested and approved, SA allows you to uninstall the patches in a safe and standardized way.

SA stores patch information in the SA Library that includes detailed information about every server under management, the patches and software installed on the servers, and the patches and software available for installation. You can use this data to determine the severity of your exposure to a newly discovered threats, and to help assess the benefits of rolling out a patch versus the costs in downtime and testing requirements.

By automating the patching procedure, SA can reduce the amount of downtime required for patching. SA also allows you to schedule patch activity, so that patching occurs during off-peak hours.

Server Automation automates patch management by providing the following features:

- The SA Library where patches are stored and organized in their formats
- A database that includes information on every patch that has been applied
- Customized scripts that can be run before and after a patch is installed
- Advanced search abilities that identify servers that require patching
- Auditing abilities that enable security personnel to track the deployment of important patches

These features enable you to browse patches by a certain operating system, schedule patch downloads and installations, set up email notifications, preview a patch installation, use software policies and remediation to install and uninstall patches, and export patch information to a reusable file format.

## Types of Patch Browsing

The HP Server Automation Client interface organizes Unix patches by operating systems and displays detailed vendor security information about each patch. You can browse patches by patch type, availability, platform version, and so on. You can also browse all patches that are installed on a server, and view and edit patch metadata.

## Scheduling and Notifications

You can schedule when patches are uploaded into the SA Library and when they are downloaded to managed servers. As a best practice, patch installations are typically scheduled for a time that causes minimal disruption to an organization's business operation. If you are installing one patch on one server, the installation operation will start only after the download operation has completed.

You can set up email notifications that alert you whether the download and installation operations completed, succeeded, or failed. When you schedule a patch installation, you can also specify reboot preferences to adopt, override, postpone, or suppress the vendor's reboot options.

## Using Software Policies to Manage Patches

Software policies enable you to customize patch distribution in your environment. They define the Unix patches that should be installed or not installed on certain managed servers. See the *SA Software Management Guide* for more information about creating software policies to install Unix patches.

## Previewing Patch Installation

While SA allows you to react quickly to newly discovered security vulnerabilities, it also provides support for strict testing and standardization of patch installation. After you have identified patches to install, SA allows you to simulate or preview the installation before you actually install a patch. This preview process tells you whether the servers that you selected for the patch installation already have that patch installed. In some cases, a server could already have a patch installed if a system administrator had manually installed it. The preview process provides an up-to-date report of the patch state of servers.

## Software Policy Remediation

SA also provides a solution for remediating servers that are not operating properly due to installed patches. If installed patches cause problems, even after being tested and approved, SA allows you to uninstall the patches in a safe and standardized way. SA allows you to specify uninstall options that control server reboots and the execution of uninstall commands, and pre-uninstall and post-uninstall scripts. Similar to previewing a patch installation, you can also preview a patch uninstall. See the *SA Software Management Guide* for more information.

## Exporting Patch Data

To help you track the patch state of servers or groups of servers, SA allows you to export this information. This information can be exported in a comma-separated value (.csv) file and includes details about when a patch was last detected as being installed, when a patch was installed by HP Server Automation, the patch compliance level, what patch policy exceptions exist, and so on. You can then import this information into a spreadsheet or database to perform a variety of patch analysis tasks. For more information, see [Exporting a Patch](#) on page 154.



## Tracking Patches on Managed Servers

When a server is brought under management by SA, the SA Agent installed on the server registers the server's hardware and software configuration with SA. This information includes installed software and patches, is recorded in the SA Library. The SA Agent repeats this registration every 24 hours.

When a new patch is issued, you can use HP Server Automation to immediately identify the servers that require patching. The SA Library stores patches and other software. You can access the SA Library from the SA Client to install patches on the appropriate servers.

After a server is brought under management, you should install all required patches. If you install a patch manually, HP Server Automation does not have data about that patch until the next SA Agent registration. If you install a patch manually, it can take up to 24 hours until the data about that server in the SA Library is up-to-date.

Whenever you install or uninstall software or patches with HP Server Automation, however, SA immediately updates the information about the server in the SA Library.

## Support for Unix Patch Testing and Installation Standardization

With SA you can minimize the risk of rolling out patches. First, when a patch is uploaded into the SA Library, its status is marked as untested and only administrators with special privileges can install it.

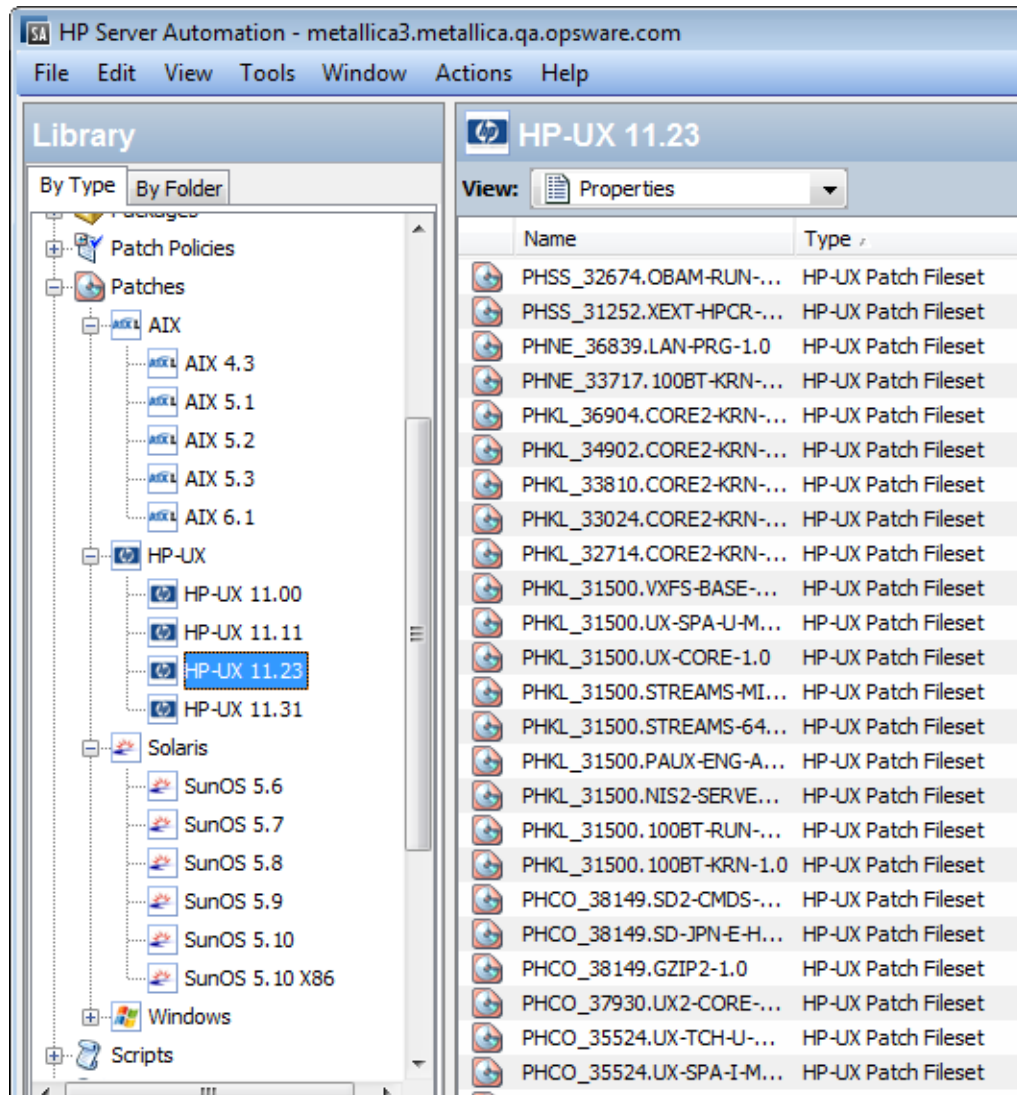
The patch administrator then defines patch installation and uninstallation options and tests the patch. Only after the patch is tested and the patch administrator marks it as available for use can other administrators install the patch.

SA allows you to standardize the way that patches are installed and uninstalled, thereby preventing ad-hoc installation procedures. Patch administrators standardize patch installation by providing pre-install and post-install scripts, install and uninstall flags, reboot instructions, and how to handle error codes from the pre-install and post-install scripts.

## Viewing Patches in the SA Client

The SA Client lets you search for and display Unix patches by name, type of patch, operating system, relationship to other packages, and so on. Figure 22 below shows a list of patches for HP-UX 11.23. Use the column selector to right of the column headers to control which columns of patch data to display. For more information, see [Unix Patch Information](#) on page 151 and [Viewing and Editing Unix Patch Properties](#) on page 153.

**Figure 22** HP-UX Patches in the SA Library



## Searching for Patches

In the SA Client, you can search for any information about your operational environment that is available in HP Server Automation using the SA Client. The SA Client enables you to search for patches, software policies, servers, and so on. See “SA Client Search” in the *SA User Guide: Server Automation*.

# Patch Management Roles for Unix

HP Server Automation provides support for rigorous change management by assigning the functions of patch management to the patch administrator and the system administrator:

- The patch administrator (often referred to as the security administrator) has the authority to upload, test, and edit patch options.
- The system administrator applies the patches (that have been approved for use) uniformly, according to the options that the patch administrator specifies.



---

Only the patch administrator should have the Patches permission, which gives access to advanced features. To obtain these permissions, contact your SA Administrator. See the Permissions Reference appendix in the *SA Administration Guide*.

---

## Patch Administrator

In most organizations, patch administrators are responsible for reviewing the latest security threats and the patches that vendors have released to address these problems. The patch administrators are generally experts in the operating systems and applications that they manage, and are able to assess the necessity of applying patches issued by vendors. They are able to diagnose common problems that arise after patches are installed, allowing them to thoroughly test the patch application process.

In HP Server Automation, patch administrators are granted specific permissions that allow them to upload patches into HP Server Automation to test the patches and then mark them as available for use. Basic users can upload patches, but they cannot install them or mark them as available. Patch administrators are also able to edit patch options (such as installation scripts) through patch management. Other types of users are not allowed to upload or edit patches.

Typically, the patch administrator uploads patches and then tests them on non-production reference hardware. After testing the patches and determining that the patches are safe to apply to production systems, they mark the patches as available in the HP Server Automation Client, and then advise the system administrators that they must apply the approved patches.

## System Administrator

System administrators are responsible for the day-to-day maintenance of the servers in a deployment. These users are not required to have the same level of expertise in low-level system details as the patch administrator.

Because the patch administrator has set up the patch installation, the system administrators can apply the patches to a large number of servers with a few mouse clicks. They are responsible for searching for the servers that require the approved patch, installing the patch, and verifying that the patches are installed successfully.

# Patch Management for Specific Unix Operating Systems

The types of patches and their underlying technologies can vary according to the vendor of the operating system. This section discusses the vendor-specific details for Unix patch management in HP Server Automation.

## Supported Unix Versions and Patch Types

SA supports all of the operating system versions that HP Server Automation supports, except for Linux.

Linux does not support patches in the ordinary sense. The packages are not patchable. Instead, new versions of the RPM are delivered. Linux systems that HP Server Automation manages are therefore not viewable through the patch interfaces. New Linux packages and updates should be managed and applied through the software policy. See the *SA Software Management Guide* for information about importing and installing RPMs using a software policy.

To see the Unix versions and patch types that SA supports.

- 1 In the SA Client, select the Library tab.
- 2 Select the By Type tab.
- 3 Locate and open the Patches node. This displays all the operating systems on which SA supports patches.
- 4 Select an operating system and open the node for that operating system. This displays all the versions of that operating system that SA supports. For an example, see [Figure 22 HP-UX Patches in the SA Library on page 146](#).

## Underlying Technologies for Patch Management on Unix

Although the utilities vary, HP Server Automation enables you to perform patching tasks by using a single interface. HP Server Automation models the way it treats patches by the way the underlying utility treats patches. For example, if the Solaris patchadd utility is not able to install one patch contained in a patch cluster, the Solaris utility continues to install the remaining patches in the patch cluster. HP Server Automation respects this behavior and allows that patch installation operation to continue. Any patches that are not installed are reported at the end of the installation operation.

The following table shows the patch management and installation tools that are used for each of the supported Unix systems.

**Table 14 Supporting Technologies for Patch Management on Unix**

Solaris	AIX	HP-UX
Patchadd installs Solaris patches	Installp installs and uninstalls filesets	Swlist lists patch products, files, products, and filesets
Patchrm uninstalls Solaris patches	Lslpp lists installed LPPs	Swinstall installs a depot

**Table 14 Supporting Technologies for Patch Management on Unix (cont'd)**

Solaris	AIX	HP-UX
Showrev lists installed Solaris patches	Instfix lists installed APARs	Swremove removes a depot
Pkgadd installs Solaris packages		
Pkginfo lists installed Solaris packages		

## AIX Patches

AIX periodically releases Authorized Program Analysis Reports (APARs), which specify what update filesets (contained in LPPs) are necessary to fix an identified problem. An APAR only specifies the minimum version of an update fileset required to fix a problem; an APAR can therefore be satisfied with later versions of the same filesets. To maintain compatibility, however, HP Server Automation always adopts the fileset with the lowest version number that meets the minimum version that APAR specifies. If a later version of the update fileset is uploaded, HP Server Automation still associates the earlier version of the fileset with the APAR.

When uploading an LPP, HP Server Automation recognizes which APARs the filesets contained in the LPP belong to. An entry is created for the APAR in the SA Library when the first fileset associated with an APAR is uploaded. (In some cases, a fileset is associated with more than one APAR. An entry is created for each APAR the fileset is associated with, if the entry does not already exist.)

If you want to install all LPPs that APAR specifies, you must make certain to upload all of the specified LPPs into the SA Library.

If you do not upload all of the LPPs that APAR specifies, it is still possible for the system administrator to browse for an APAR and install the partial set of LPPs that are uploaded. In such cases, the administrator receives a warning that the filesets for the APAR are not all installed.



The Patch Administrator must first upload and test an LPP before it is generally available in HP Server Automation. The new fileset is integrated into the APAR only after the LPP is tested and approved. Even though the APAR is updated automatically, you still maintain control over the exact filesets that are allowed to be installed on your managed servers.



APAR update filesets cannot be installed on a server if the server does not already have the base filesets for which the update filesets are intended.

If, however, a server has a partial set of the base filesets, the APAR can be applied and only the applicable filesets for the base filesets are installed. For example, if an APAR specifies four update filesets to update four base filesets, and you attempt to apply the APAR to a server that has only three of the base filesets, three of the four update filesets from the APAR are installed.

When installing an AIX update fileset, the SA normally applies the fileset, which allows it to be rejected (uninstalled.) If you want to commit the fileset instead (so that it cannot be removed), use the `-c` option here.



Since update filesets can be included in folders, global read permissions are required to view and edit AIX update filesets. See the *SA User Guide: Server Automation* for information about how to use folders.

## Solaris Patches

A Solaris patch cluster contains a set of selected patches for a specific Solaris release level. Ordinarily, after a patch cluster is installed, it is not possible to search for a particular patch cluster. The patches do not contain any metadata that relate them to the patch cluster in which they were originally bundled. You can only search for the individual patches.

If you install a Solaris patch cluster, however, HP Server Automation keeps track of the patch cluster in the SA Library. You can therefore search for a patch cluster to determine if a full patch cluster is installed. If you installed the patch cluster, you can uninstall individual patches in the cluster. You cannot uninstall a patch cluster.

See [Patch Management for Solaris](#) on page 97 for more information.

## HP-UX Patches

HP-UX patches are delivered exclusively as depots, which are patch products that contain patch filesets. The depot is uploaded directly into HP Server Automation.

If a depot is already uploaded and attached to a node, it cannot be uploaded by SA. If you want to upload the depot with SA, you must detach a depot from any nodes that it is attached to, and then delete it from the SA Library.

See [Patch Management for HP-UX](#) on page 75 for more information.

## Uploading Unix Patches into the SA Library

Before a Unix patch can be installed on a managed server, the patch must be downloaded from the server vendor and uploaded into the SA Library. For more information, see the *SA Administration Guide*.

To upload Unix patches to the SA Library.

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**. The patches are organized by operating system.
- 2 Navigate to the desired operating system version.
- 3 From the **Actions** menu, select **Import Software** to open the Import Software window.
- 4 In the Import Software window, click **Browse** to locate and select the patch to import.

Before clicking **Open** in the Open window, select the character encoding to be used by the patch from the Encoding drop-down list.

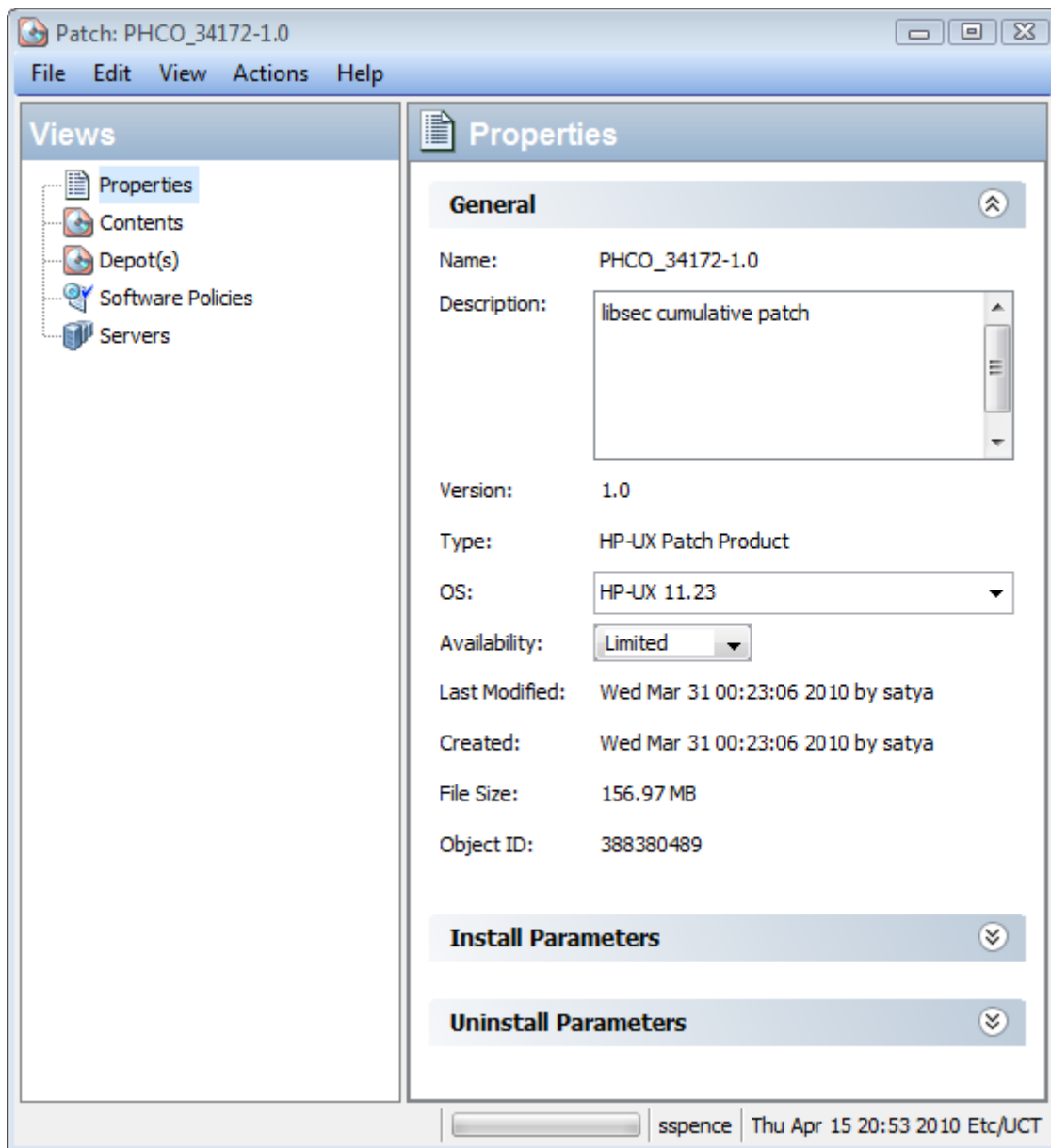
You need to specify the character encoding so that SA can extract the metadata contained in the patch and correctly display the information in non-ASCII characters in the SA Client (for example, in the Patch Properties pages). Patch metadata includes comments, READMEs, scripts, descriptions, and content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

- 5 Click **Open**.
- 6 In the Import Software window, select the appropriate type from the Type drop-down list.
- 7 In the Folder field, enter the path in the SA Library where you want to store the patch or click **Browse**.
- 8 From the Platform drop-down list, select all the operating system versions that the patch applies to. You can only install the patch on servers that are running those versions of the operating system.
- 9 Click **Import** to import the patch into the SA Library.

# Unix Patch Information

The SA Client displays detailed information about a patch in several different views. For example, [Figure 23](#) below shows the Properties view of an HP-UX patch. Note that the details about each patch vary depending on the type and OS of patch. To view or edit patch properties, see [Viewing and Editing Unix Patch Properties](#) on page 153.

**Figure 23** Unix Patch Properties in the SA Client



## Patch Properties View

Patch properties include the following information. Note that some information is only displayed for certain operating systems and not others.

- **Version:** The version number of the patch.
- **Status:** The vendor's status for the patch.
- **Type:** The type of Unix patch. Some examples are HP-UX Patch Product, HP-UX Patch Fileset, Solaris Patch, Solaris Cluster, AIX APAR and AIX Update Fileset.
- **OS:** The Unix operating systems that are known to be affected by this patch.
- **Availability:** The status of a patch within HP Server Automation, which can be one of the following:
  - **Limited:** The patch has been imported into SA but requires additional permissions (Manage Patch: Read & Write) to be installed. This is the default patch availability. For more information on permissions, see the *SA Administration Guide*.
  - **Available:** The patch has been imported into HP Server Automation, tested, and has been marked available to be installed on managed servers.
  - **Deprecated:** The patch cannot be added to patch policies or set as a patch policy exception but can still be installed.
- **Object ID:** The HP Server Automation unique ID for the patch.
- **Dependencies:** When present, lists the dependencies on the selected patch. This is only provided for some patch types and some platforms. For more information, see [Managing Properties](#) on page 127.
- **Install Parameters:** When present, lists the actual install settings for the patch and the settings that the patch vendor specifies for the patch. This is only provided for some patch types and some platforms.
- **Install Scripts:** When present, lists scripts that will run on a managed server before or after the patch is installed. This is only provided for some patch types and some platforms.
- **Uninstall Parameters:** When present, lists the actual uninstall settings for the patch and the settings that the patch vendor specifies for the patch. This is only provided for some patch types and some platforms.
- **Uninstall Scripts:** When present, lists scripts that will run on a managed server before or after the patch is uninstalled. This is only provided for some patch types and some platforms.

## Contents View

Patch Contents are displayed only for certain types of patch containers such as HP-UX Patch Products, AIX APARs and Solaris Clusters. The Contents view lists all the patches included in the selected patch container.

## Depots View—HP-UX Only

Patch Depots are only displayed for HP-UX Patch Products. The Depots view displays the HP-UX depots that contain the selected patch product. SA displays HP-UX depots as SA packages. See [Patch Management for HP-UX](#) on page 75 for more information.



## Patch Products View—HP-UX Only

Patch Products are only displayed for HP-UX Patch Filesets. The Patch Products view displays the HP-UX patch products that contain the selected HP-UX patch fileset. See [Patch Management for HP-UX](#) on page 75 for more information.

## Patch Clusters View—Solaris Only

Patch Clusters are only displayed for Solaris patches. The Patch Clusters view displays the Solaris patch clusters that contain the selected Solaris patch. For more information on Solaris patches, see [Patch Management for Solaris](#) on page 97.

## LPPs/APARs View—AIX Only

The LPPs/APARs view is only displayed for AIX patches. This view displays the LPPs and APARs that contain the selected patch.

## Software Policies View

The Software Policies view displays all the software policies that include the selected patch.

## Patch Policies View

The Patch Policies view displays all the patch policies that include the selected patch. The Patch Policies view is only displayed for some platforms.

## Servers View

The Servers view displays all the servers where the selected patch is installed.

## Viewing and Editing Unix Patch Properties

The SA Client displays information about Unix patches that have been imported into HP Server Automation as described in [Unix Patch Information](#) on page 151. You can edit some of a patch's properties in the properties view. Some properties are not editable.

You can set the install and uninstall parameters on either the patch properties page or when you are install or uninstall the patch. The parameters on the Properties view are saved in the SA Library, but the parameters specified during a patch install or uninstall are used only for that action. The parameters specified during an install or uninstall override those on the patch Properties view.

To view or edit information about a patch:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**.
- 2 Expand Patches and select a specific Unix operating system.
- 3 (*Optional*) Use the column selector to sort the patches according to Name, Type, Availability, and Description.
- 4 In the content pane, select a patch.

- 5 Right-click the patch or, from the Actions menu, select the Open menu. This displays the patch in a separate screen.
- 6 If you have modified any properties, select **File** ► **Save** to save your changes.

## Finding Servers That Have a Unix Patch Installed

To find out which servers have a particular patch installed:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**.
- 2 Expand Patches and select a specific Unix operating system. The content pane will display all patches associated with that operating system.
- 3 In the content pane, select a patch.
- 4 From the View drop-down list in the content pane, select Servers. This shows all the servers where the selected patch is installed.

## Exporting a Patch

You can export patches to the local file system. However, not all patch types can be exported. If you attempt to export a patch and find that the Export menu is grayed out, that patch cannot be exported.

To export a patch from the SA Library to the local file system:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**.
- 2 Expand Patches and select a specific Unix operating system. The content pane will display all patches associated with that operating system.
- 3 In the content pane, select a patch.
- 4 From the **Actions** menu, select **Export**. If the Export menu is grayed out, that patch cannot be exported.
- 5 In the Export Patch window, enter the folder name that will contain the patch file in the File Name field.
- 6 Click **Export**.

## Deleting a Patch

This action removes a patch from the SA Library; however, it does *not* uninstall the patch from managed servers. A patch cannot be deleted if it is attached to a policy.



---

Do *not* delete all of the patches from the SA Library. If you accidentally do so, contact your support representative for assistance in uploading all of the patches back into SA.

---

To delete a patch:

- 1 In the navigation pane, select **Library** ► **By Type** ► **Patches**.
- 2 Expand Patches.
- 3 Select a Unix operating system. The content pane displays all patches associated with that operating system.
- 4 In the content pane, select a patch.

- 5 From the **Actions** menu, select **Delete Patch**.
- 6 In the Delete Patches window, click **Delete**.

## Using Software Policies to Manage Patches

Patch Policies for Windows and Solaris are the best way to manage patches for the Windows and Solaris platforms. For more information see [Patch Management for Windows](#) on page 13 and [Patch Management for Solaris](#) on page 97.

For other platforms, software policies enable you to customize patch distribution in your environment. Software policies define which Unix patches should be installed or not installed on certain managed servers.

If you use software policies and you also perform ad hoc patch installs, you must run the remediate process to install all applicable patches on servers. See the *SA Software Managment Guide* for more information about creating and remediating software policies to install Unix patches.

### Patch Compliance Reports

To troubleshoot and resolve patch compliance problems, you can run and examine several patch compliance reports in the SA Client. The following patch compliance reports identify whether all patches in a software policy were installed successfully on managed servers in your environment.

#### Patch Policy Compliance (All Servers)

This report groups all managed servers by their patch policy compliance level to show compliant and non-compliant servers.

#### Patch Policy Compliance by Customer

This report lists all servers by the customer they belong to and then by the patch policy compliance level.

#### Patch Policy Compliance by Facility

This report groups all managed servers by the facility they belong to and then by the patch software policy compliance level.



---

See the *SA Reports Guide* for information about how to run, export, and print these reports.

---

# Patch Administration for Unix

You can customize patch administration for Unix to best support your environment by setting the availability flag.

## Setting the Default Patch Availability

You can set the default patch availability with the SA Client. The default used by the script overrides the default set by the SA Client. See the *SA Administration Guide* for information about the script.

To set the default value for the Availability of a newly imported patch:

- 1 In the navigation pane, select **Administration**.
- 2 Select **Patch Configuration**.
- 3 For the **Default Availability** for Imported Patches, select either Available or Limited. The default is Limited.

If the patch is Available, it can be installed on managed servers. If the patch is Limited, it has been imported into HP Server Automation and can be installed only by a patch administrator who has the required permissions (Manage Patch: Read & Write). To obtain these permissions, contact your SA Administrator. See also the *SA Administration Guide*.

## Patch Installation

The patch installation process consists of the following two phases:

- **Download Phase:** This is when the patch is downloaded from HP Server Automation to the managed server. This phase is commonly referred to as the staging phase.
- **Installation Phase:** This is when the patch is installed on the managed server. This phase is commonly referred to as the deployment phase.

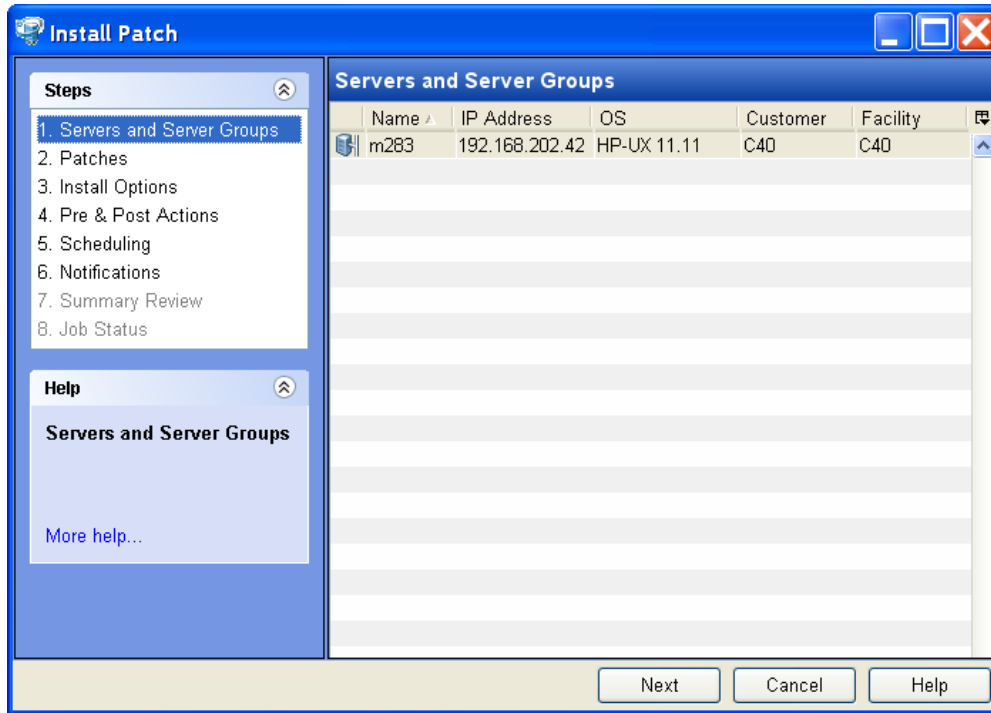
You can specify whether you want the installation to occur immediately after the patch is downloaded (staged) or you can schedule the installation to occur at a later date and time. SA also supports best-effort installations of multiple patches by allowing you to specify that the patch installation process will continue even when an error occurs with one of the patches.

SA displays the name of the command that installs the patch. The SA Agent runs this command on the managed server. You can override the default command-line arguments that you want to perform the installation.

To optimally manage Unix patch installations, SA allows you to manage server reboot options, and pre and post installation scripts, simulate (preview) a patch installation, and set up email notifications to alert you about the status of the installation process.

The Install Patch window guides you through setting up these conditions.

**Figure 24 Install Patch Window**



## Installation Flags

You can specify installation flags that are applied whenever a Unix patch is installed. However, HP Server Automation also uses default installation flags and requires that patches are installed with these flags. You must therefore be certain that you do not specify any installation flags that override or contradict the default flags passed in by HP Server Automation. See [Setting Install Options](#) on page 159 for information about how to specify commands.

The following table lists the default installation flags that HP Server Automation uses.

**Table 15 Default Installation Flags**

Unix Patch Type	Flags
AIX	-a -Q -g -X -w
HP-UX	None

## Application Patches

SA does not allow you to apply a patch to an operating system for which the patch is not intended. When you are installing an application patch, SA does not automatically filter out servers that do not have the corresponding application installed. Although SA does not prevent you from doing so, you should not attempt to apply application patches to servers that do not have the necessary applications installed. If a patch is for an application that is not installed on the server, the patch will not be applied and an error message will display, such as “There was an error with package <name of the package>”.

If an application patch is intended for an application that is running on more than one version of the same operating system, you cannot apply the patch to all of the servers at the same time. An application patch is associated with only one operating system version. You must first select the patch for one operating system, select the servers where the application is installed, and apply the patch. You must repeat this process for each version of the operating system where the application is installed.

Similarly, when uninstalling application patches that are installed on multiple versions of the same operating system, you cannot uninstall all of the patches at the same time. You must repeat the uninstallation process for each version of the operating system where the patch is installed.

## Installing a Patch

Before a patch can be installed on a managed server, it must be imported into HP Server Automation and its status must be Available. Administrators who have the required permissions can install patches that are marked Limited.



---

You must have a set of permissions to manage patches. To obtain these permissions, contact your SA Administrator. See the *SA Administration Guide*.

---

You can perform the installation by explicitly selecting patches and servers.

To install a patch on a managed server:

- 1 In the navigation pane, select **Library** and then select **Patches**.
- 2 Expand the Patches and select a specific Unix operating system.
- 3 In the content pane, select a patch.
- 4 From the View drop-down list, select Servers (or Server Groups).
- 5 From the Show drop-down list, select Servers without Patch Installed (or Server Groups without Patch Installed).
- 6 In the preview pane, select one or more servers.
- 7 From the **Actions** menu, select **Install Patch**.

The first step of the Install Patch window appears: Servers and Server Groups. For instructions on each step, see the following sections:

- [Setting Install Options](#)
- [Setting Reboot Options](#)
- [Specifying Install Scripts](#)
- [Scheduling a Patch Installation](#)
- [Setting Up Email Notifications](#)
- [Previewing a Patch Installation](#)
- [Viewing Job Progress for a Patch Installation](#)

After you have completed a step, click **Next** to advance to the next step. Before you click **Start Job**, you can return to a completed step to make changes by clicking on it in the list of steps.

- 8 When you are ready to launch the installation job, click **Start Job**.

After you launch the job, you cannot change its parameters, even if the job is scheduled to run at a later time.

If the Install Patch window remains open until the job completes, SA updates the Patch Compliance column in the All Managed Servers window with the revised compliance count (in parenthesis) for affected servers. Press F5 or select **Refresh** from the **View** menu to update information in the patch preview pane.

## Setting Install Options

You can specify the following types of patch installation options:

- Perform the patch installation immediately after the patch is downloaded or at a later date and time.
- Do not interrupt the patch installation process even when an error occurs with one of the patches.
- Use different command-line options to perform the installation.

To set these options:

- 1 In the Install Patch window, click **Next** to advance to the Install Options step.
- 2 Select one of the following Staged Install Options:  
**Continuous:** This allows you to run all phases as an uninterrupted operation.  
**Staged:** This allows you to schedule the download and installation to run separately.
- 3 Select the Error Options check box if you want the patch installation process to continue even when an error occurs with one of the patches. As a default, this check box is not selected.
- 4 In the Install Command text box, enter command-line arguments for the command that is displayed.
- 5 Click **Next** to go to the next step or click **Cancel** to close the Install Patch window.

## Setting Reboot Options

To minimize the downtime that server reboots can cause, you can control when servers will and will not be rebooted. You can adopt the vendor's reboot assignments, reboot a server each time a patch is installed on it, completely suppress all server reboots, or postpone reboots until all patches have been installed.



---

When you are selecting reboot options in the Install Patch window, Hewlett Packard recommends that you use the Unix reboot recommendations, which is the “Reboot servers as specified by patch properties” option. If you cannot use the Unix reboot setting, select the single reboot option, which is the “Do not reboot servers until all patches are installed” option.

---

The following options determine whether the servers are rebooted after the patch is installed. These options apply only to the job launched by the Install Patch window; they do not change the Reboot Required option, which is on the Install Parameters tab of the patch properties window. Except for the first option, the following options override the Reboot Required option.

- **Reboot servers as specified by patch properties:** By default, the decision to reboot depends on the Reboot Required option of the patch properties.
- **Reboot servers after each patch install:** Even if the Reboot Required option of the patch properties is not set, reboot the server. If multiple patches are installed, the server reboots multiple times.
- **Suppress all server reboots:** Even if the Reboot Required option of the patch properties is set, do not reboot the server. (Because of vendor settings, some patches ignore the suppress option and force a reboot.)

- **Do not reboot servers until all patches are installed:** If the Reboot Required option is set for some selected patches but not for others, the server is rebooted one time after all patches are installed. If the Reboot Required option is not set for any of the selected patches, the server is not rebooted.

To set reboot options:

- 1 In the Install Patch window, click **Next** to advance to the Pre & Post Actions step.
- 2 Select one of the Rebooting Options.
- 3 Click **Next** to go to the next step or click **Cancel** to close the Install Patch window.

## Specifying Install Scripts

For each patch, you can specify a command or script to run before installation or after installation. A pre-install script, for example, could check a certain condition on the managed server. If the condition is not met or if the pre-install script fails, the patch would not be installed. A pre-install script could also be used to shut down a service or application before it is patched. A post-install script could be used to perform a certain cleanup process on the managed server.

You can also specify the following types of scripts to run on the managed server before or after an installation or download phase:

- **Pre-Download:** A script that runs before patches are downloaded from SA to the managed server. This is available only if you select Staged in the Install Options step.
- **Post-Download:** A script that runs after patches are downloaded from SA to the managed server and before the patch is installed. This is available only if you select Staged in the Install Options step.
- **Pre-Install:** A script that runs before patches are installed on the managed server.
- **Post-Install:** A script that runs after patches are installed on the managed server.

To specify a pre-install script:

- 1 In the Install Patch window, click **Next** to advance to the Pre & Post Actions step.
- 2 Select the Pre-Install tab. You may specify different scripts and options on each of the tabs.
- 3 Select Enable Script. This option enables the remainder of the fields on the tab. If Enable Script is not selected, the script will not run.
- 4 Select either Saved Script or Ad-Hoc Script.

A Saved Script has been previously stored in HP Server Automation with the SAS Web Client. To specify the script, click **Select**.

- 5 If the script requires command-line flags, enter the flags in the Command text box.
- 6 Specify the information in the User section. If you choose a system other than Local, enter the User Name, Password, and Domain. The script will be run by this user on the managed server.
- 7 To stop the installation if the script returns an error, select the Error check box.
- 8 Click **Next** to go to the next step or click **Cancel** to close the Install Patch window.



## Scheduling a Patch Installation

Since the two phases of patching can be decoupled, you can schedule when you want patches installed (deployed) to occur independently of when patches are downloaded (staged).

To schedule a patch installation:

- 1 In the Install Patch window, click **Next** to advance to the Scheduling step.  
By default, the Scheduling step displays only the scheduling options for the install phase. If you selected Staged in the Install Options step, the scheduling options for the download phase will also be displayed.
- 2 Select one of the following Install Phase options:
  - **Run Task Immediately**: This enables the system to perform a preview analysis in the Summary Review step. The scheduling option for the download phase is **Run Immediately Following Download**.
  - **Run Task At**: This enables you to specify a later date and time that you want the installation or download performed.
- 3 Click **Next** to go to the next step or click **Cancel** to close the Install Patch window.



---



A scheduled patch installation can be cancelled (prior to its execution), even if the patch download has already completed.

---

## Setting Up Email Notifications

You can set up email notifications to alert users when the download and installation operations complete successfully or with errors.

To set up email notifications:

- 1 In the Install Patch window, click **Next** to advance to the Notifications step.
- 2 To set the notification status on the success of a Job, select the  icon. To set the notification status on the failure of a Job, select the  icon. By default, the Notification step displays only the notification status for the installation phase.
- 3 Enter a Ticket ID to be associated with a Job in the Ticket ID field.
- 4 Click **Next** to go to the next step or click **Cancel** to close the Install Patch window.



---

If you previously selected Staged in the Install Options step, the Notifications pane displays notification options for both the download and installation phases.

---

## Previewing a Patch Installation

The installation preview process provides an up-to-date report about the patch state of servers. The installation preview is an optional step that lets you see what patches will be installed on managed servers and what type of server reboots are required. This preview process verifies whether the servers you selected for the patch installation already have that patch installed. In some cases, a server could already have the patch installed if a system administrator had manually installed it, which means that SA does not know about it.

The preview process also reports on dependency information, such as patches that require certain Unix products, and patches that obsolete other patches or are obsoleted by other patches. If a dependency is not met, SA will display an error message indicating this condition.



---

The installation preview does not report on the behavior of the server as though the patches have been applied.

---

### To preview a patch installation:

- 1 In the Install Patch window, click **Next** to advance to the Summary Review step.
- 2 Verify the information displayed for the Servers, Server Groups, and Patches at the top of the window.
- 3 *(Optional)* Click **Preview** to see the separate actions that will be performed when the patch is installed. To view the details of a previewed action, select a row in the table.
- 4 Click **Start Job** to launch the installation job or click **Cancel** to close the Install Patch window without launching the installation.

If you selected Run Task Immediately in the Scheduling step, the job begins now. If you selected Run Task At, the job will be launched at the specified time and date.

## Viewing Job Progress for a Patch Installation

You can review progress information about a patch installation (job), such as whether actions have completed or failed.

### To display job progress information:

- 1 In the Install Patch window, click **Next** to advance to the Job Progress step. This will start the installation job.

The Progress bar and text indicate how many of the actions listed in the table have been completed. For each server, the following actions can be performed:

- **Analyze:** HP Server Automation examines the patches needed for the installation, checks the managed servers for the most recent patches installed, and determines other actions that it must perform.
- **Download:** The patch is downloaded from HP Server Automation to the managed server.
- **Install:** After it is downloaded, the patch is installed.
- **Final Reboot:** If this action is specified in the Pre & Post Actions step, the server is rebooted.
- **Pre/Post Install/Download Script:** If this action is specified in the Pre & Post Actions step, a script is run before or after the uninstallation.
- **Install & Reboot:** When a patch will be installed is also when the server will be rebooted.
- **Verify:** Installed patches will be included in the software registration.

- 2 To view additional details about a specific action, select the row in the table to display the start and completion times of the job. In the navigation pane, select Jobs and Sessions to review detailed information about the job. See the *SA User Guide: Server Automation* for more information about browsing job logs.
- 3 Click **End Job** to prevent the job from running or click **Close** to close the Install Patch window.

## Patch Uninstallation

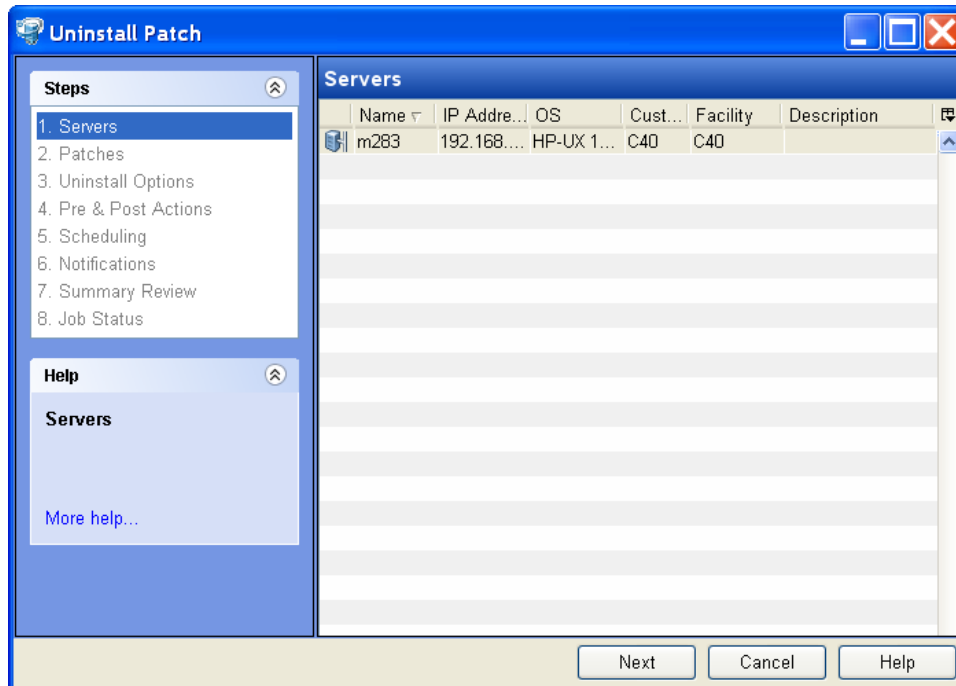
SA provides granular control over how and under what conditions Unix patches are uninstalled (removed) from managed servers. To minimize problems, you can only uninstall one patch at a time. You cannot use SA to uninstall a patch that was not installed using SA.

To help you optimally manage these conditions, SA allows you to do the following:

- Manage server reboot options, and pre and post installation scripts.
- Simulate (preview) a patch uninstallation.
- Set up email notifications to alert you about the status of the uninstallation process.

The Uninstall Patch window guides you through setting up these conditions.

**Figure 25 Uninstall Patch Window**



## Uninstallation Flags

You can specify uninstallation flags that are applied whenever a Unix patch is uninstalled. However, HP Server Automation also uses default uninstallation flags and requires that patches are uninstalled with these flags. You must therefore be certain that you do not specify any uninstallation flags that override or contradict the default flags passed by HP Server Automation.

The following table lists the default uninstallation flags that HP Server Automation uses.

**Table 16 Default Uninstallation Flags**

Operating System/Patch Types	Flags
AIX	-u -g -X
AIX Reject Options	-r -g -X
HP-UX	None

## Uninstalling a Patch

To remove a patch from a managed server:

- 1 In the navigation pane, select **Library** and then select **Patches**.
- 2 Expand the Patches and select a specific Unix operating system.
- 3 In the content pane, select a patch.
- 4 From the View drop-down list, select Servers.
- 5 From the Show drop-down list, select Servers with Patch Installed.
- 6 In the preview pane, select one or more servers.
- 7 From the **Actions** menu, select **Uninstall Patch**.

The first step of the Uninstall Patch window appears: Servers.

For instructions on each step, see the following sections:

- [Setting Reboot Options](#)
- [Specifying Pre and Post Install Scripts](#)
- [Scheduling a Patch Uninstallation](#)
- [Setting Up Email Notifications](#)
- [Viewing Job Progress for a Patch Uninstallation](#)

After you have completed a step, select **Next** to advance to the next step. Before you click **Start Job**, you can return to a completed step to make changes by clicking on it in the list of steps.

- 8 When you are ready to launch the uninstallation job, select **Start Job**.

After you launch the job, you cannot change its parameters, even if the job is scheduled to run at a later time.

If the Uninstall Patch window remains open until the job completes, SA updates the Patch Compliance column in the All Managed Servers window with the revised compliance count (in parenthesis) for affected servers. Press F5 or select Refresh from the View menu to update information in the patch preview pane

## Setting Uninstall Options

You can specify the following types of patch uninstallation options:

- Do not interrupt the patch uninstallation process even when an error occurs with one of the patches.
- Use different command-line options to perform the uninstallation.

To set these options:

- 1 In the Uninstall Patch window, click **Next** to advance to the Uninstall Options step.
- 2 Select the Error Options check box if you want the patch installation process to continue even when an error occurs with one of the patches. As a default, this check box is not selected.
- 3 In the Uninstall Command text box, enter command-line arguments for the command that is displayed.
- 4 Click **Next** to go to the next step or click **Cancel** to close the Uninstall Patch window.

## Setting Reboot Options

To minimize the downtime that server reboots can cause, you can control when servers will and will not be rebooted. You can adopt the vendor's reboot assignments, reboot a server each time a patch is removed from it, completely suppress all server reboots, or postpone reboots until all patches have been uninstalled.



---

When you are selecting reboot options in the Uninstall Patch window, Hewlett Packard recommends that you use the Unix reboot recommendations, which is the “Reboot servers as specified by patch properties” option in the window. If it is not possible to use the Unix reboot setting, select the single reboot option, which is the “Do not reboot servers until all patches are installed” option in the window.

---

The following options determine whether the servers are rebooted after the patch is uninstalled. These options apply only to the job launched by the Uninstall Patch window; they do not change the Reboot Required option, which is on the Uninstall Parameters tab of the patch properties window. Except for the first option, the following options override the Reboot Required option.

- **Reboot servers as specified by patch properties:** By default, the decision to reboot depends on the Reboot Required option of the patch properties.
- **Reboot servers after each patch install:** Even if the Reboot Required option of the patch properties is not set, reboot the server. If multiple patches are installed, the server reboots multiple times.
- **Suppress all server reboots:** Even if the Reboot Required option of the patch properties is set, do not reboot the server. (Because of vendor settings, some patches ignore the suppress option and force a reboot.)
- **Do not reboot servers until all patches are installed:** If the Reboot Required option is set for some selected patches but not for others, the server is rebooted one time after all patches are installed. If the Reboot Required option is not set for any of the selected patches, the server is not rebooted.

To set reboot options:

- 1 In the Uninstall Patch window, click **Next** to advance to the Pre & Post Actions step.
- 2 Select one of the Rebooting Options.
- 3 Click **Next** to go to the next step or click **Cancel** to close the Uninstall Patch window.

## Specifying Pre and Post Install Scripts

For each patch, you can specify a command or script to run before uninstallation or after uninstallation. A pre-uninstall script, for example, could check a certain condition on the managed server. If the condition is not met or if the pre-uninstall script fails, the patch would not be removed from a server. A pre-uninstall script could also be used to shut down a service or application before it is removed from a server. A post-uninstall script could be used to perform a certain cleanup process on the managed server.

You can specify the following types of scripts to run on the managed server before or after a patch uninstallation:

- **Pre-Uninstall:** A script that runs before the patch is removed from a managed server.
- **Post-Uninstall:** A script that runs after the patch is removed from a managed server.

### To specify a script:

- 1 In the Uninstall Patch window, click **Next** to advance to the Pre & Post Actions step.
- 2 Select the Pre-Uninstall or Post-Uninstall tab.  
You may specify different scripts and options on each of the tabs.
- 3 Select Enable Script.  
This option enables the remainder of the fields on the tab. If Enable Script is not selected, the script will not run.
- 4 Select either Saved Script or Ad-Hoc Script.  
A Saved Script has been previously stored in HP Server Automation with the SAS Web Client. To specify the script, click **Select**.
- 5 If the script requires command-line flags, enter the flags in Commands.
- 6 Specify the information in the User section. The script will be run by this user on the managed server.
- 7 To stop the uninstallation if the script returns an error, select Error.

## Scheduling a Patch Uninstallation

You can schedule that a patch will be removed from a server immediately, or at a later date and time.



### To schedule a patch uninstallation:

- 1 In the Uninstall Patch window, click **Next** to advance to the Scheduling step.
- 2 Select one of the following Install Phase options:
  - **Run Task Immediately:** This enables you to perform the uninstallation in the Summary Review step.
  - **Run Task At:** This enables you to specify a later date and time that you want the uninstallation performed.
- 3 Click **Next** to go to the next step or click **Cancel** to close the Uninstall Patch window.

## Setting Up Email Notifications

You can set up email notifications to alert users when the patch uninstallation operation completes successfully or with errors.

To set up email notifications:

- 1 In the Uninstall Patch window, click **Next** to advance to the Notifications step.
- 2 To set the notification status on the success of a Job, select the  icon. To set the notification status on the failure of a Job, select the  icon. By default, the Notification step displays only the notification status for the uninstallation phase.
- 3 Enter a Ticket ID to be associated with a Job in the Ticket ID field.
- 4 Click **Next** to go to the next step or click **Cancel** to close the Uninstall Patch window.

## Previewing a Patch Uninstallation

The uninstallation preview process provides an up-to-date report about the patch state of servers. The uninstallation preview is an optional step that lets you see what patches will be removed from managed servers. This preview process verifies whether the servers you selected for the patch uninstallation have that patch installed.



---

The uninstallation preview process does not report or simulate the behavior of a system with patches removed from the server.

---

To preview a patch uninstallation:

- 1 In the Uninstall Patch window, click **Next** to advance to the Summary Review step.
- 2 Verify the information displayed for the Servers, Server Groups, and Patches at the top of the window.
- 3 (*Optional*) Click **Preview** to see the separate actions that will be performed when the patch is uninstalled. To view the details of a previewed action, select a row in the table.
- 4 Click **Start Job** to launch the job or click **Cancel** to close the Uninstall Patch window without launching the uninstallation.

If you selected Run Task Immediately in the Scheduling step, the job begins now. If you selected Run Task At, the job will be launched at the specified time and date.

## Viewing Job Progress for a Patch Uninstallation

You can review progress information about a patch uninstallation (job), such as whether actions have completed or failed.

To display job progress information:

- 1 In the Uninstall Patch window, click **Next** to advance to the Job Progress step. The Progress bar and text indicate how many of the actions listed in the table have been completed. For each server, the following actions can be performed:

- **Analyze:** HP Server Automation examines the patches needed for the uninstallation, checks the managed servers for the most recent patches installed, and determines other actions that it must perform.
  - **Uninstall:** The patch is uninstalled.
  - **Final Reboot:** If this action is specified in the Pre & Post Actions step, the server is rebooted.
  - **Pre/Post Uninstall Script:** If this action is specified in the Pre & Post Actions step, a script is run before or after the uninstallation.
  - **Uninstall & Reboot:** When a patch will be installed is also when the server will be rebooted.
  - **Verify:** Installed patches will be included in the software registration.
- 2 To view additional details about a specific action, select the row in the table to display the start and completion times of the job. In the navigation pane, select Jobs and Sessions to review detailed information about the job. See the *SA User Guide: Server Automation* for more information on browsing job logs.
  - 3 Click **End Job** to prevent the job from running or click **Close** to close the Uninstall Patch window.



# Index

## A

Ad-Hoc script, 40  
AIX  
    APARs  
        about, 149  
        uploading, 149  
    LPPs, about, 149  
AIX operating system, 143  
APARs. *See* AIX APARs.  
Arial Unicode MS font, 59

## B

benign error codes, 136  
best practice  
    patch policies and exceptions, 15  
    reboot options, 38  
    remediation process, 36, 38  
    SA integration with patch management, 20, 36, 38  
    scheduling and notifications, 14  
BSA Essentials Network, 121

## C

compliance  
    performing software compliance scan, 107  
Configure Opsware permission, 136  
crontab, 53

## D

depots  
    HP-UX, 75

## E

e-mail notifications, 40, 66, 73, 161, 167  
error codes, 136

## F

font, 59  
Fujitsu cluster, 100

## G

Global Shell rosh utility, 140

## H

hotfix chaining, 21  
HP Live Network connector, 121  
HP-UX Depot importer script, 76  
HP-UX Patch Database, 78  
HP-UX Software Catalog file, 76, 78

## I

import\_hpux\_depot script, 76  
import\_hpux\_metadata script, 76  
installation  
    flags, overview, 60, 69, 157  
Install Patch wizard, 59, 135, 157, 158, 163  
install scripts, specifying, 39, 166  
Install Software wizard, 135

## L

LNC. *See* HP Live Network connector., 121  
locales, 57

## M

Malicious Software Removal Tool, 20  
MBSA 1.2.1, 19  
MBSA 2.0.1, 19  
Microsoft Patch Database, importing, 52  
Microsoft patch management prerequisites, 17  
Microsoft Security Bulletins, 14  
Model Repository, 20, 34, 35  
msiexec.exe, 20  
multi-user mode, 140  
My Oracle account, 101  
My Oracle website, 97

## O

offline volumes, 141

## P

package types

AIX APAR, 149

HP-UX depots, 150

LPP, 149

RPM, 148

Windows Hotfix, 60

passcodes, Solaris patch cluster, 135

patchadd utility, 135

patch compliance, 34, 35, 36

Patch Deployers, 23

patches

installation flags, 60, 157

uninstallation flags, 69

patch installation, previewing, 66, 162

patch installation, scheduling, 40, 65

patch management

Microsoft patch releases, 19

patch information from Agent, 145

patch testing, support for, 145

roles, 147

uploading automatically, 30

patch policy, 34

patch policy exception, 14, 35

Patch Policy Setters, 23

patch reboot options, 63, 159

patch uninstallation, previewing, 74, 167

patch uninstallation, scheduling, 73, 166

Pending File Rename Queue, 21

pkgmgr.exe, 20

policy setter, 22

populate-opsware-update-library, 30

## Q

qchain.exe, 20, 21, 54, 55

QNumber, 14, 41

## R

reboot options for remediation, 38

Reboot Pending state, 63, 71

Reboot Required option, 63, 71

Remediate wizard, 37

## RPM

patching, 148

## S

SAS Web Client

patch administration in, 156

Saved Script, 40

scan

patch compliance, 47

software compliance, 107

Security Rollup Package, 21

Server Agent, 20

registration, 145

service pack

suppress server reboot, 64

single-user mode, 140

Software Catalog file, HP-UX, 76

software policy

performing software compliance scan, 107

Software Repository, 20

Solaris Volume Manager, 141

solpatch\_import, 111

solpatch\_import command, 100, 115, 123

best practice, 125

Summary Review, 67, 74, 162, 167

## T

troubleshooting, detecting benign error codes, 136

troubleshooting, patch installation, 140

## U

uninstallation

flags, overview, 60, 69, 157

Uninstall Patch wizard, 68, 142, 163

Uninstall Software wizard, 142

unzip.exe, 20

## W

windows\_util\_loc parameter, 54

Windows Hotfix

installation flags, 60

uploading, 60

Windows Service Pack, 21

Windows Update Agent, 21, 28, 38, 53

WindowsUpdateAgent-ia64.exe, 54, 55

WindowsUpdateAgent-x64.exe, 54, 55

WindowsUpdateAgent-x86.exe, 54, 55

wizard. See Install Patch wizard., 59

wsusscn2.cab, 19, 34, 41, 52, 66, 74

WUA. See Windows Update Agent., 21, 28, 53, 63, 71

