

# Server Automation

Software Version: 10.23.007

## User Guide: Server Patching

Document Release Date: July, 2017  
Software Release Date: July, 2017



## Legal Notices

### Warranty

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

The information contained herein is subject to change without notice.

### Restricted Rights Legend

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

### Copyright Notice

© Copyright 2000-2017 Hewlett-Packard Development Company, L.P.

### Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

UNIX® is a registered trademark of The Open Group.

## Documentation Updates

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

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

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

**<https://softwaresupport.hp.com>**

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:

**<https://hpp12.passport.hp.com/hppcf/createuser.do>**

Or click the **Register** link at the top of the HP Software Support 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: **<https://softwaresupport.hp.com>**

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:

**<https://hpp12.passport.hp.com/hppcf/createuser.do>**

To find more information about access levels, go to:

**<https://softwaresupport.hp.com/web/softwaresupport/access-levels>**

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

**<http://h20230.www2.hp.com/sc/solutions/index.jsp>**

# Contents

Server patching overview .....	13
Quick start to patch management .....	13
Patch management for Windows .....	14
SA integration .....	15
Features .....	15
Support for Windows patch testing and installation standardization .....	17
Windows patch database conflict report .....	18
Supported technologies for patch management .....	18
Roles for Windows patch management .....	18
Requirements for managed servers .....	20
Supported Windows versions .....	20
Supported products in the Microsoft patch database .....	20
About the SA Client patch library .....	21
Windows server patch management support .....	22
SA patching modes .....	23
Patch Settings window .....	24
Windows Patch Settings .....	24
Ubuntu Patch Settings .....	26
Patch management process .....	26
Configure patch settings .....	26
Access the Microsoft patch database .....	27
Importing Windows patch database from the MS offline catalog .....	27
Prerequisites for importing the MS offline catalog .....	28
Configuring your browser for importing the MS offline catalog .....	28
Importing Windows patch utilities for the offline patch catalog .....	29
Manually importing the Windows patching utilities .....	30
Retrieving Microsoft patch supplements from HPLN .....	31
Manually downloading the Microsoft patch supplements from HPLN .....	32
Downloading the Microsoft Offline patch catalog from the command line .....	33
Exporting Windows patch utilities .....	37
Importing the Windows patch database from WSUS .....	37
Workflow diagram - Importing WSUS patches into SA .....	38
Connecting SA to a WSUS server .....	39
Deploying the WSUS Web service .....	40
Connecting SA managed servers to WSUS .....	44
Parameters for the Configure Server With WSUS script .....	46
Changing configuration settings for the WSUS Web service .....	46
Select Windows patch products and locales for import .....	47
Patch locales .....	48
Supported locales .....	48
Locale configuration tasks .....	49

- Import metadata for Windows patches ..... 51
  - Filtering metadata for import ..... 51
  - Check the list of imported MS patch metadata ..... 51
- Set patch availability ..... 52
  - From the SA Client ..... 52
  - From the command-line script ..... 52
- Configure patch policies ..... 52
  - Patch policy ..... 52
  - Patch policy exception ..... 54
  - Precedence rules for applying policies ..... 54
- Add items to a Windows patch policy using the Object ID ..... 55
  - Set remediate options ..... 55
    - Windows patch policy remediation job option—Windows Patch Installation Order ..... 55
  - Set reboot options for remediation ..... 57
  - Specify pre-installation and post-installation scripts for remediation ..... 58
  - Schedule a patch installation for remediation ..... 59
  - Set up email notifications for remediation ..... 59
  - Preview and start a remediation ..... 60
  - Verify patch policy compliance ..... 61
  - Create a patch policy ..... 62
  - Delete a patch policy ..... 62
  - Add a patch to a patch policy ..... 62
  - Remove a patch from a patch policy ..... 63
  - Attach a patch policy to a server ..... 63
  - Detach a patch policy from a server ..... 63
  - Set a patch policy exception ..... 64
  - Find an existing patch policy exception ..... 64
  - Copy a patch policy exception ..... 65
  - Remove a patch policy exception ..... 65
- Run compliance scans ..... 65
  - Patch compliance ..... 66
    - Patch compliance scans ..... 66
    - Ways to start a patch compliance scan ..... 66
    - Start a patch compliance scan immediately ..... 67
    - Refresh the compliance status of selected servers ..... 67
    - View scan failure details ..... 67
    - Patch compliance icons ..... 67
    - Patch non-compliance ..... 68
    - Patch compliance levels ..... 68
    - Patch compliance rules ..... 68
  - Schedule a patch compliance scan ..... 69
  - Set a patch compliance level ..... 70
- Import applicable Windows patch binaries ..... 70
  - Importing binaries in Offline Catalog patching mode ..... 70
  - Importing binaries in WSUS patching mode ..... 71

Deploy patches/Remediate servers .....	71
Patch installation for Windows .....	72
Installation flags Windows .....	73
Application patches .....	74
Install a patch .....	74
Set install options .....	75
Set reboot options for a Windows patch installation .....	75
Specify install scripts .....	76
Schedule a Windows patch installation .....	77
Set up email notifications for a Windows patch installation .....	78
Preview a Windows patch installation .....	78
View job progress of a Windows patch installation .....	79
Check for patch updates .....	80
Patch management administration .....	80
View patch information .....	80
Patch dependencies and supersedence .....	81
Supersedence relationships in WSUS patching mode .....	81
Skipping superseded patches .....	81
View Windows patches .....	81
Edit Windows patch properties .....	82
Import custom documentation for a patch .....	82
Delete custom documentation for a patch .....	83
Find vendor-recommended Windows patches .....	83
Find servers that have Windows patch installed .....	83
Find servers that do not have Windows patch installed .....	83
Export a Windows patch .....	84
Enable/disable Windows Server 2008 Itanium (IA64) patches .....	84
Export Windows patch information .....	85
Patch uninstallation .....	86
Uninstallation flags .....	86
Uninstall a Windows patch .....	87
Set uninstall options .....	87
Set reboot options for a Windows patch installation .....	88
Specify install scripts for a Windows patch uninstallation .....	89
Schedule a Windows patch uninstallation .....	90
Set up email notifications for a Windows patch uninstallation .....	90
Preview and starting a Windows patch uninstallation .....	90
View job progress of a patch uninstallation .....	91
Searching for patches and patch policies .....	92
Find servers that require a reboot .....	92
Change the SA patching mode .....	93
Disconnect SA managed servers from WSUS .....	93
Troubleshoot WSUS errors .....	94
Cannot install or unistall software in WSUS mode .....	94
Symptoms .....	94
Causes .....	95

Solution .....	95
Mesh conflicts after importing patches .....	95
Symptoms .....	95
Cause .....	95
Solution .....	95
Vendor patch key error when importing metadata .....	95
Symptom .....	95
Cause .....	95
Solution .....	95
Patch management for HP-UX .....	96
Features .....	96
Prerequisites .....	97
Patch installation .....	97
Scheduling a Patch Installation for Remediation .....	100
Setting up email notifications .....	100
Previewing a patch installation .....	100
Viewing job progress .....	102
Supported operating systems .....	102
HP-UX depots .....	102
HP-UX software catalog file .....	104
Software policy management .....	105
Create an HP-UX software policy .....	106
Library—By Type .....	106
Library—By Folder .....	107
View an HP-UX software policy .....	107
Search .....	108
Devices .....	108
Library—By Type .....	108
Library—By Folder .....	109
Edit an HP-UX software policy .....	109
Add an HP-UX patch to a software policy .....	110
Remove software from a software policy .....	110
View software policy history .....	111
View servers attached to a software policy .....	111
Find a software policy in folders .....	111
Custom attributes .....	112
Patch compliance .....	112
Patch uninstallation .....	114
Patch management for Solaris .....	114
Features .....	115
Quick start .....	119
Install a patch .....	120
Install a patch cluster .....	120
Install manual patches—patchadd .....	121
Detect benign error codes .....	121
Install patches using a patch policy .....	122

Remediate a server against a patch policy .....	123
Troubleshoot Solaris patch installation .....	125
Install patches using offline volumes .....	127
Patch management process .....	127
Patch compliance .....	130
Run a patch compliance scan .....	132
Patch Policy Management .....	132
Create a Solaris patch policy .....	133
Library—By folder .....	134
solpatch_import .....	134
View a Solaris patch policy .....	135
Edit a Solaris patch policy .....	136
Add a Solaris patch to a patch policy .....	136
Remove a patch from a Solaris patch policy .....	137
Resolve patch dependencies .....	138
Custom attributes .....	141
View patch policy history .....	142
View software policies associated with a patch policy .....	142
View OS sequences associated with a patch policy .....	142
View servers attached to a patch policy .....	142
Find a Solaris patch policy in folders .....	143
Patch Management Tasks .....	143
Patches and patch clusters .....	143
Viewing patch cluster contents .....	144
Viewing patch clusters associated with a patch .....	144
Viewing software policies associated with a patch or patch cluster .....	144
Viewing patch policies associated with a patch or patch cluster .....	145
Viewing patch policies associated with a patch or patch cluster .....	145
Deleting a patch or patch cluster .....	145
Run solpatch_import .....	145
Initialize the Solaris patch database .....	146
Maintain the Solaris patch database .....	147
Retrieve the latest patch data from Oracle .....	147
Retrieve the Solaris patch supplementary data file .....	147
Manually download the Solaris patch supplementary data file .....	148
Find Solaris patches .....	149
Import a patch or patch cluster .....	151
solpatch_import .....	152
Import a Solaris patch to SA Client .....	152
Export a patch or patch cluster .....	153
Open a Solaris patch .....	153
Manage properties .....	154
Install parameters .....	156
Import custom documentation .....	159
Solaris zones .....	159
Uninstall a Solaris patch .....	160



- Patch management for Solaris 11 ..... 160
  - Get started with Solaris 11 patching ..... 161
  - Set up Solaris 11 managed server for SA patching ..... 162
  - SA patching in Solaris 11 ..... 169
- Patch management for Ubuntu ..... 172
  - Features ..... 173
  - SA Client Library ..... 174
  - SA management of Debian metadata database ..... 176
  - Roles for Ubuntu patch management ..... 176
  - Patch management process ..... 177
  - Specify Ubuntu patch settings ..... 178
    - Ubuntu patch settings: Specify the general logging options ..... 182
  - Ubuntu patch management tasks ..... 183
    - View package information ..... 183
    - Package dependencies and supersedence ..... 183
    - View Ubuntu packages ..... 184
    - Edit Ubuntu package properties ..... 184
    - Find Ubuntu packages ..... 184
    - Find servers that have an Ubuntu package installed ..... 186
    - Find servers that do not have an Ubuntu package installed ..... 186
    - Import an Ubuntu patch from the SA Client Library ..... 187
    - Import Ubuntu patch contents from the managed servers view ..... 187
    - Export an Ubuntu package ..... 188
- Policy management ..... 188
- Remediate patch policies ..... 191
  - Set remediate options ..... 191
  - Set reboot options for remediation ..... 192
  - Specify pre-installation and post-installation scripts for remediation ..... 193
  - Schedule a patch installation for remediation ..... 193
  - Set up email notifications for remediation ..... 194
  - Preview and start a remediation ..... 194
  - Verify patch policy compliance ..... 196
  - Create a patch policy ..... 196
  - Delete a patch policy ..... 197
  - Add a patch to a patch policy ..... 197
  - Remove a patch from a patch policy ..... 197
  - Attach a patch policy to a server ..... 198
  - Detach a patch policy from a server ..... 198
- Patch compliance ..... 199
  - Patch compliance scans ..... 199
  - Start a patch compliance scan ..... 199
  - Start a patch compliance scan immediately ..... 199
  - Refresh the compliance status of selected servers ..... 200
  - View scan failure details ..... 200
  - Patch compliance icons ..... 200
  - Patch compliance levels ..... 201

- Patch compliance rules ..... 201
- Patch administration ..... 202
- Patch locale configuration tasks ..... 206
- Patch installation ..... 207
  - Install an Ubuntu patch ..... 208
  - Set Ubuntu install options ..... 209
  - Set reboot options for an Ubuntu patch installation ..... 209
  - Specify install scripts for an Ubuntu patch installation ..... 210
  - Schedule an Ubuntu patch installation ..... 211
  - Set up email notifications for an Ubuntu patch installation ..... 211
  - Preview an Ubuntu patch installation ..... 212
  - View job progress of an Ubuntu patch installation ..... 213
- Patch management for Unix ..... 214
  - Track patches on managed servers ..... 214
  - Support for Unix patch testing and installation standardization ..... 215
  - View patches in the SA Client ..... 215
  - Search for patches ..... 216
  - Patch management roles for Unix ..... 216
    - Patch Administrator ..... 217
    - System Administrator ..... 217
  - Patch management for specific Unix operating systems ..... 217
    - AIX patches ..... 219
    - Solaris patches ..... 222
    - HP-UX patches ..... 222
    - Upload Unix patches into the SA Library ..... 222
  - Unix patch information ..... 223
    - View and edit Unix patch properties ..... 226
    - Find servers that have a Unix patch installed ..... 226
    - Export a patch ..... 227
    - Delete a patch ..... 227
  - Use software policies to manage patches ..... 227
  - Patch administration for Unix ..... 228
  - Patch installation ..... 229
    - Installation flags ..... 230
    - Application patches ..... 230
    - Install a patch ..... 230
      - Set install options ..... 231
      - Set reboot options ..... 232
      - Specify install scripts ..... 232
      - Schedule a patch installation ..... 233
      - Set up email notifications ..... 234
      - Preview a patch installation ..... 234
      - View job progress for a patch installation ..... 235
  - Patch uninstallation ..... 235
  - Set uninstall options ..... 237
    - Set reboot options ..... 238

- Specifying pre-installation and post-installation scripts ..... 238
- Scheduling a patch uninstallation ..... 239
- Set up email notifications ..... 239
- Preview a patch uninstallation ..... 240
- View job progress for a patch uninstallation ..... 240
- Patch management for Red Hat Enterprise Linux ..... 241
  - Import patches for Red Hat platforms ..... 242
    - Importing Red Hat Errata and channels in SA using SA Red Hat Importer tool ..... 242
    - Red Hat Subscription Management overview ..... 243
    - RHN Classic, RHSM, and Satellite ..... 244
    - Content import using Red Hat Subscription Management ..... 245
    - Entitlement certificates ..... 245
    - Install Red Hat CA certificates ..... 246
    - Content labels ..... 248
    - Sample use cases ..... 249
    - Migration ..... 253
    - Supported RHEL versions ..... 259
    - Reuse a Red Hat import configuration file ..... 259
    - View errata based and channel based policies in the SA Client ..... 260
  - Manage Red Hat patches ..... 262
  - Scan managed servers for recommended patches ..... 263
  - Policy management ..... 265
  - Patch compliance ..... 266
  - Best practices for managing minor RHEL releases ..... 267
  - Frequently asked questions ..... 269
- Patch management for Oracle Enterprise Linux ..... 271
  - Before you begin ..... 271
  - Get started ..... 272
    - Editing the configuration file ..... 273
    - Register the system with the ULN ..... 277
      - Subscribing and unsubscribing channels from the ULN ..... 280
    - Use the SA patch importer for Oracle Enterprise Linux ..... 286
      - Disable channels at runtime ..... 288
      - Enable channels at runtime ..... 288
      - Import packages without creating the corresponding software policies ..... 288
      - View the enabled channel information ..... 289
      - View the supported channels for the Agent platforms ..... 290
      - Add a channel label to a platform ..... 294
      - Remove a channel label from a platform ..... 294
- Patch management for SUSE Linux Enterprise ..... 294
  - Import patches for SUSE platforms ..... 295
    - Importing SUSE Errata and channels in SA using SA SUSE Importer tools ..... 295
  - SA SUSE Manager Importer tool ..... 297
    - Installing the SUSE Manager CA certificate ..... 297
    - Configuring the SA SUSE Manager Importer ..... 298
    - Working of SUSE Manager Importer tool ..... 299

Usage of SUSE Manager Importer tool .....	299
SMT Importer tool .....	300
Installing the SMT server certificate .....	301
Configuring the SMT Importer .....	301
Working of SMT Importer .....	302
Content labels .....	302
Usage of SMT Importer .....	303
View errata-based and channel-based policies in the SA Client .....	303
Manage SUSE patches .....	305
Send Documentation Feedback .....	307

## Server patching overview

Server Automation (SA) lets you patch the operating systems on managed servers in your environment, such as Windows, HP-UX, Solaris, and Unix. Using the SA Client, you can create patch policies and software policies that ensure standardization and compliance across your enterprise.

This section describes how to create and modify patch policies and software policies, attach them to your managed servers, remediate the servers to install and uninstall patches, and perform routine audits that identify compliance status.

See the following topics:

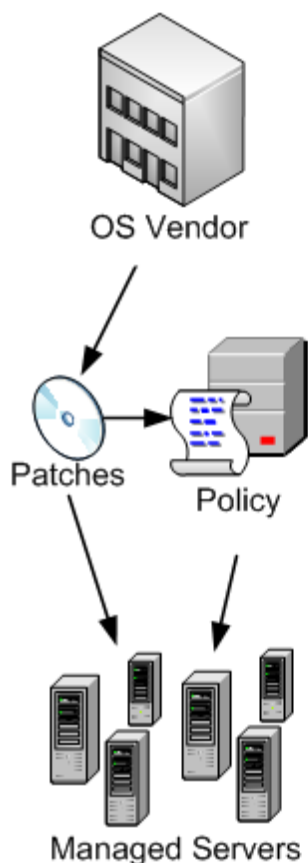
- ["Quick start to patch management" below](#)
- ["Patch management for Windows " on the next page](#)
- ["Patch management for HP-UX" on page 96](#)
- ["Patch management for Solaris " on page 114](#)
- ["Patch management for Solaris 11 " on page 160](#)
- ["Patch management for Ubuntu " on page 172](#)
- ["Patch management for Unix " on page 214](#)
- ["Patch management for Oracle Enterprise Linux " on page 271](#)
- ["Patch management for SUSE Linux Enterprise" on page 294](#)

## 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.

The following figure 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.

### **Patch management workflow**



**1. Download patches from vendor into SA Library.**

**2. Test patches.**

**3. Add patches to SA policies.**

**4. Attach policies to managed servers.**

**5. Attach managed servers to policies.**

**6. Remediate servers to install patches.**

**7. Run a compliance scan.**

**8. Remediate servers to ensure compliance.**

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

- ["Patch management for Windows " below](#)
- ["Patch management for HP-UX" on page 96](#)
- ["Patch management for Solaris " on page 114](#)
- ["Patch management for Solaris 11 " on page 160](#)
- ["Patch management for Ubuntu " on page 172](#)
- ["Patch management for Unix " on page 214](#)
- ["Patch management for Red Hat Enterprise Linux" on page 241](#)
- ["Patch management for Oracle Enterprise Linux " on page 271](#)
- ["Patch management for SUSE Linux Enterprise" on page 294](#)

## Patch management for Windows

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 SA-supported Managed Server platforms.

**Note:**

See the SA Support and Compatibility Matrix for the list of SA-supported Managed Server platforms for your version of SA.

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.

## 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.

**Note:**

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

## 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
- Multibinary patch support that enables you to install Windows multibinary patches
- All Windows product support for patching any Windows products or operating system

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.

You can also 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.

The preview process provides an up-to-date report of the patch state of servers. The preview process 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.

## 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.

## Windows patch database conflict report

After importing your Windows patch database, check whether there are any duplicate patches in your patch library. Depending on your selected patching mode, SA reports import results under:

- **Administration > Patch Settings > Patch Database > Last Import Summary** when working in **Offline Catalog** patching mode.
- **Administration > Patch Settings > Patch Database > Last Metadata Import and Import Summary** when working **WSUS** patching mode.

After performing a patch import, SA updates these fields to reflect the state of the imported database. If these fields are still blank after running an import, the import might be taking a long time to finish updating the patch library or there is a rendering delay. Clear the SA Client cache from **Tools > Options > Reload Cache**.

Field value	Description
<b>Successful</b>	The import operation completed.
<b>Warning: &lt;number&gt; duplicates found.</b>	There is a conflict in the patch database due to duplicate patches.  Remove the duplicates then run a new compliance scan/remediation job.

## 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.
- `unzip.exe` - Extracts info-zip compatible zip archives.
- Windows Update Agent (WUA) - Enables access to the Microsoft framework for patch installations and updates.
- WSUS Web service - Enables communication with the Windows Server Update Services in WSUS patching mode.

## 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.

**Note:**

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.

**Note:**

Server Automation also provides predefined patch user groups for patch deployers and patch policy setters. See ["Predefined patch user groups" below](#).

## 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.
- **Software policy setters**—Access to set software policy. (For Ubuntu patch policy management, you need both Patch Policy Setters and Software Policy Setters user groups.)

Next to the predefined action permissions, you must grant the necessary resource 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 for more information.

## Requirements for managed servers

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

- Microsoft Core XML Services (MSXML) or Internet Explorer (IE) must be installed on the managed servers. The versions of MSXML and IE that you install must support the Microsoft XML parser and related DLL files.
- Windows Installer must be installed on managed servers that are running Windows servers. This installer is available on the Microsoft support site, such as:  
<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 Servers, the **Add and Remove Programs** dialogue must be closed when you run Windows patch management tasks.
- To install and uninstall patches, and to perform remediation, a supported version of the SA Agent must be installed.
- Managed servers must be set to a supported language for the SA Agent that is installed on the server.

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.

**Note:** See the SA Support and Compatibility Matrix for more information about platform version support and compatibility.

## Supported Windows versions

See the SA Support and Compatibility Matrix for the list of SA-supported Managed Server platforms for your version of SA.

**Note:**

In order to apply patches to Managed Servers running Windows Server 2003 RTM, you must first ensure that the Microsoft update MS04-011 (or a subsequent update) has been applied to those servers.

## Supported products in the Microsoft patch database

SA Windows Patching supports all Microsoft products, which includes operating systems (OS) and other non-OS products.

Previously, SA Windows Patching only supported OS patches. Most product-specific patches, such as those for MS Office 2010 or MS Word, were not supported. Windows product patches were present in the Microsoft Offline Catalog file (wsusscn2.cab), but they were not uploaded to the SA database when you imported the .cab file.

Now, when you import the Microsoft Offline Catalog file or you connect to a WSUS server, SA retrieves all product-specific patches according to your [specified patch products and locales](#).

## Requirements

Product-specific patches can only be installed on servers that have the product installed.

The product installation and upgrade scripts make any necessary configuration adjustments. No additional configuration steps on the core are required.

## About unsupported products

Windows Patch Import will only import patches for operating systems (OS) that SA supports. Patches for any unsupported OS will be excluded at import time. This exclusion applies to any unsupported Windows OS as well as any OS-specific product for any unsupported Windows OS. For information on the SA-supported operating systems, see the SA Support and Compatibility Matrix for your version of SA.

### Note:

The Microsoft patch database may include patches for Windows OS or OS-specific products that SA does not support. These unsupported patches may still appear under **Administration > Patch Settings > Patch Products**. However, SA excludes unsupported Windows patches from the patch import, even if they are selected in the product selection list.

## Identifying product names for missing recommended patches

If the Vendor Recommended Patch Policy (VRPP) recommends any patches for a server that are not included in the imported patches, the compliance scan will show these missing patches in gray. To determine the MS product necessary to import these missing patches, a KB#-to-Product Mapping script is available. Contact SA Customer Support for details.

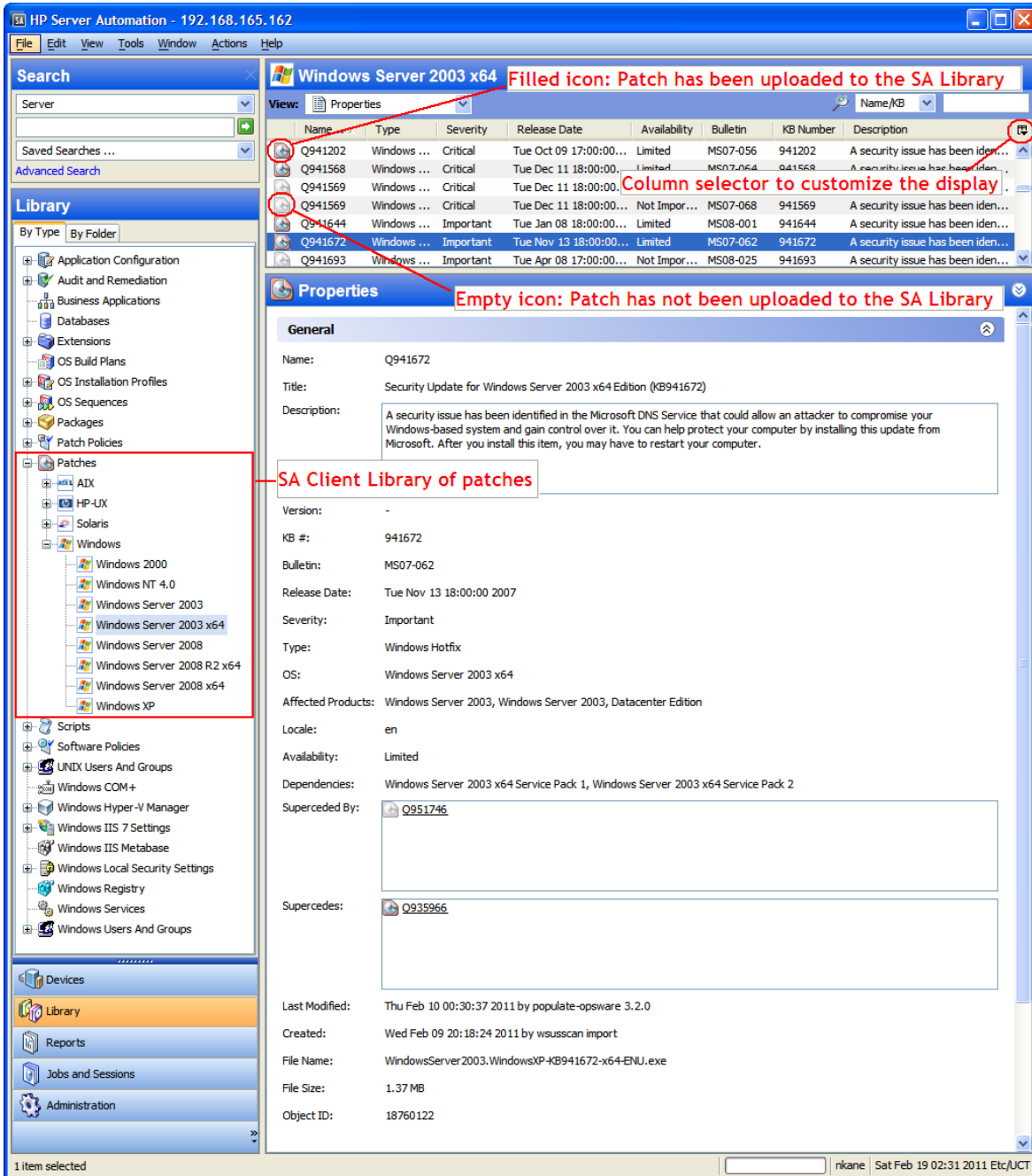
## About the SA Client patch library

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.

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.

The **Windows** folder of the SA Client Library shows patch information pulled from your Microsoft patch database. You can access the Microsoft patch database from the Microsoft Offline Catalog or from a WSUS server. This view shows the parsed patch data from Microsoft at the time of your most recent update.

### Windows patches in the SA Client Library



## Windows server patch management support

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

- Windows Server patches appear under **Library** after the patch database is imported.
- Select the specific Windows Server version under **Administration > Windows Patch Downloads > Patch Products** to specify whether to import Windows Server patch metadata.

- To manage Windows Server patches 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 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 patch policies to servers and server groups.
- You can define patch policy exceptions for Windows Server patches on servers and server groups.

## SA patching modes

To patch your Windows managed servers with applicable Microsoft updates, SA requires access to the Microsoft patching database. You can access this database either by importing Microsoft's offline catalog of patches or by connecting SA to a WSUS server in your network.

Depending on your available network infrastructure, enable one of the available SA patching modes:

- **Offline Catalog** - imports the `wsusscn2.cab` file from the SA Client or from the `populate-opsware-update-library` script. The `wsusscn2` file contains only security updates. HP can provide missing non-security updates via HPLN.
- **WSUS** - connects to a WSUS server to retrieve Microsoft patches from a custom Windows patching repository. Unlike the **Offline Catalog** mode, **WSUS** patching requires access only to the WSUS server on your network from where it can retrieve both security and non-security updates.

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

The `populate-opsware-update-library` script automates the download of the Microsoft's offline catalog of patches and the import of these patches into SA. The `populate-opsware-update-library` downloads the `wsusscn2.cab` file and imports its contents (hotfixes, service packs, and update rollups) into SA.

The `populate-opsware-update-library` script is specific to **Microsoft Offline Catalog** patching and does not run in **WSUS** patching mode.

For more information about running the script and the available options, see ["Downloading the Microsoft Offline patch catalog from the command line" on page 33](#)

## Policies and exceptions for Windows server patches

SA provides a recommended patch policy for Windows Servers. You can also define additional custom patch policies in the same way as described in Application Deployment in the SA Developer Guide.

## Remediate and ad-hoc install/uninstall

You can remediate Windows Server patch policies and perform ad-hoc Windows Server patch installations and uninstallations. Windows Server patches can be remediated in software policies and ad-hoc installations using install/uninstall software. However, software compliance does not account for applicability.

## Patch compliance

You can perform patch compliance scans on Windows Server servers to determine compliance relative to attached 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 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 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.

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
```

**Note:**

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

## Patch Settings window

This window enables you to configure the following settings for patching Windows and Ubuntu servers:

- Patch metadata and binaries import
- Supported Microsoft products and locales
- Ubuntu patching methods for your environment

## Windows Patch Settings

Setting	Description
Patch Availability	When Windows patches are imported into



	<p>Server Automation (SA), they are assigned a default value for Availability. To specify the default value, select either <b>Available</b> or <b>Limited</b>.</p> <p>The populate-opsware-update-library script that automatically imports patches in <b>Offline Catalog</b> mode can override the selection in this window.</p>
<b>Patching Mode</b>	<p>Depending on your available network infrastructure, enable one of the available SA patching modes:</p> <ul style="list-style-type: none"><li>• <b>Offline Catalog</b> - imports the wsusscn2.cab file from the SA Client or from the populate-opsware-update-library script. The wsusscn2.file contains only security updates. HP can provide missing non-security updates via HPLN.</li><li>• <b>WSUS</b> - connects to a WSUS server to retrieve Microsoft patches from a custom Windows patching repository. Unlike the <b>Offline Catalog</b> mode, WSUS patching requires access only to the WSUS server on your network from where it can retrieve both security and non-security updates.</li></ul>
<b>Windows Patch Downloads</b>	<p>This section contains information about the Windows patch database used in SA:</p> <ul style="list-style-type: none"><li>• <b>Patch Database:</b> Depending on your network infrastructure, you can get the Microsoft patching database into SA either by importing the Windows patching catalog (wsusscn2.cab file) or by connecting to a WSUS server on your network.</li><li>• <b>Patch Products:</b> This section lists the Microsoft Windows products affected by the patches tracked by SA.</li><li>• <b>Patch Locales:</b> This section lists the patch languages managed by SA.</li></ul> <p>In WSUS mode, filtering by patch product and locale is done on the WSUS server side. SA only displays the read-only list of products and locales selected by the WSUS administrator.</p>

<b>Windows Patch Utilities</b>	In <b>Offline Catalog</b> patching mode, SA requires the Windows Patch utilities to deploy the latest version of the Microsoft Update agent onto the managed servers. Windows Update Agent (WUA) scans computers for security updates without connecting to Windows Server Update Services (WSUS) server.
--------------------------------	---

## Ubuntu Patch Settings

Setting	Description
<b>Proxy</b>	Define the Ubuntu proxy configuration.
<b>Repositories</b>	Define the Ubuntu repositories to access.
<b>Policy Settings</b>	Configure the Ubuntu Patch Policy Settings.
<b>Scanner Options</b>	Specify the Ubuntu scanner behavior.
<b>General</b>	Specify the Ubuntu log settings.

## Patch management process

To deploy Windows patches, import the required patches, test them, update or create new policies and specify install options. The following steps detail the patch management workflow and main task involved:

- [Step 1 - Configure patch settings](#)
- [Step 2 - Configure patch policies](#)
- [Step 3 - Scan servers for compliance](#)
- [Step 4 - Import applicable binaries](#)
- [Step 5 - Install patches/Remediate servers](#)
- [Step 6 - Check for patch updates](#)

## Configure patch settings

To patch your Windows managed servers, SA requires the following resources:

- [Access to the Microsoft database](#). This tells SA where to look for patches and associated metadata.
- [The list of products and locales for which you want to track patches](#). This ensures SA imports only relevant patches for your applicable Microsoft products.
- [The metadata for the selected patch products and locales](#). This contains information that SA requires to install Microsoft patches on your managed servers.

- [The binary files for the patches required to remediate non-compliant servers](#). These contain the Microsoft update files themselves.

## Access the Microsoft patch database

The Microsoft patch database contains information about released patches and how they should be applied. SA requires access to this database in order to get the appropriate resources for patching your managed Windows servers.

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.

Depending on your network infrastructure, you can get the Microsoft patching database into SA:

- by importing the Windows patching catalog (wsusscn2.cab file) from the Microsoft website. The Microsoft offline catalog only contains security updates. SA provides missing and non-security updates as patch supplements via HPLN.
- by connecting to a WSUS server on your network. WSUS synchronizes with Microsoft Update to regularly download both security and non-security updates to a central WSUS repository on your network. Access the Microsoft patch database via WSUS if you are working in a tightly secured environment, where you cannot connect to Microsoft and HPLN.

Once every 24 hours, the SA Agent on a Windows server compares the server's current state against the Microsoft patch database 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 Model Repository as well.

The Vendor patch key is currently available for Ubuntu and Windows database views. The vendor patch key is a vendor-specific value that allows users to tie a unit (patch) in SA back to the specific patch supplied by the vendor.

## Importing Windows patch database from the MS offline catalog

SA can retrieve Windows updates from wsusscn2.cab, the offline version of the Windows patch database. This cabinet file is available on the Microsoft website and contains security-related patch metadata published by Microsoft.

Microsoft updates this file every second Tuesday of the month to include new or revised Windows security patches. To keep your managed servers up-to-date, make sure to reimport this file into SA monthly, and to connect to HPLN for downloading non-security Microsoft updates.

Alternatively, if you cannot connect to HPLN or to the Microsoft website, you can get all Windows updates from a WSUS server on your network. For more information, see ["Importing the Windows patch database from WSUS" on page 37](#).

To import the offline catalog of Windows patches into SA:

1. Go to the **Administration > Patch Settings**.
2. In the **Patch Downloads** section, enable the Microsoft **Offline Catalog** patching mode.

3. Select the **Patch Products** tab and click **Edit** to add the products for which you want SA to import patches and patch metadata.
4. Select the **Patch Locales** tab and click **Edit** to add the languages for which you want SA to import patches and patch metadata. During patch installation, SA matches the locale of the patch with the locale of each managed server.
5. Select the **Patch Database** tab to import patch metadata for your selected patch products and locales. You can choose to either:
  - **Import from File** - to import the patch metadata from the wsusscn2.cab file available on your local machine.  
Before you can import the Microsoft patch database from a local file, you must configure your browser to not use the web proxy when communicating with your SA core. See "[Configuring your browser for importing the MS offline catalog](#)" below
  - **Import from Vendor** - to import the patch metadata directly from the Microsoft website. By default, this points to the URL where the wsusscn2.cab is available on the Microsoft website.
6. Click **Import**. SA displays the **Importing Microsoft Patch Database** showing the import progress and an option to run the import in the background.
7. Click **Close** when the patch metadata import is complete.

### Prerequisites for importing the MS offline catalog

If you are working in the **Offline Catalog** patching mode, check the following prerequisites before importing the wsusscn2.cab file from Microsoft:

- "[Configuring your browser for importing the MS offline catalog](#)" below
- "[Importing Windows patch utilities for the offline patch catalog](#)" on the next page
- Make sure that Windows Installer 3.1, Windows Update Agent and MSXML 3+ are installed on your Windows managed servers. MSXML is a general requirement for all Windows managed servers.
- The Windows Update service on your managed servers is not be disabled but is set to never check for updates.

### Configuring your browser for importing the MS offline catalog

If you are working in **Offline Catalog** patching mode and you want to import the wsusscn2.cab file from your local network, configure your browser to not use the web proxy when communicating with your SA core.

If you are importing the offline catalog using the **Import from Vendor** option, make sure to use a proxy to be able to connect to Microsoft for accessing the Windows patch database.

To configure your browser for importing the Windows offline catalog file stored locally:

1. In the **Log in to 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.

## Importing Windows patch utilities for the offline patch catalog

Windows Patch utilities deploys the latest version of the Microsoft Update agent onto the managed servers. SA uses Windows Update Agent (WUA) to scan computers for security updates without connecting to Windows Server Update Services (WSUS) server.

Import the Windows Patch utilities only if you are working in **Offline Catalog** patching mode. Windows Update Agent (WUA) automatically updates itself when it is connected to the WSUS server.

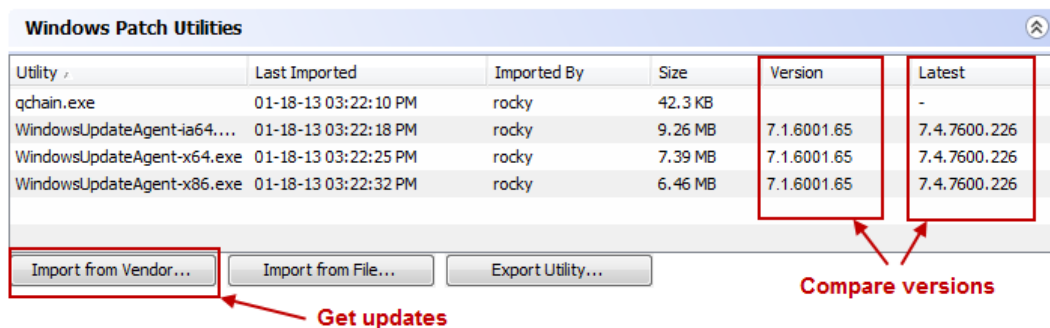
- If you do not plan to use SA to manage your Windows servers, you can optionally choose not to install these files and still successfully complete the installation process. However, if these files are not installed, no operations against Windows servers should be performed. These files are required for many Windows-based operations other than Windows patching.
- During an SA core installation, if you set the `windows_util_loc` 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 Install 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 ["Prerequisites for importing the MS offline catalog " on the previous page](#) for instructions.

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

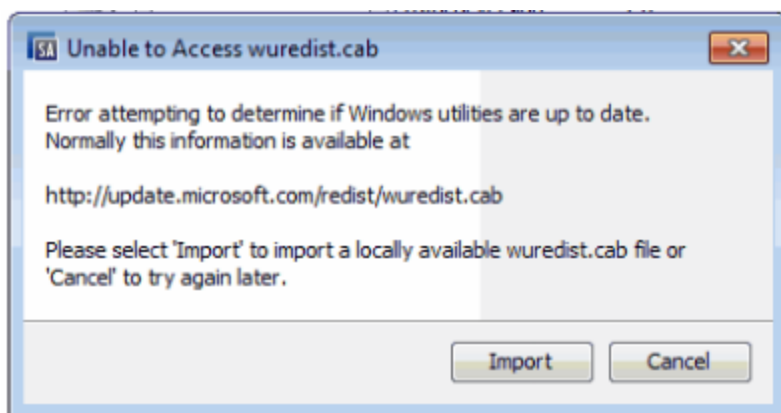
- WindowsUpdateAgent-ia64.exe
- WindowsUpdateAgent-x64.exe
- WindowsUpdateAgent-x86.exe

To update and import Windows patch utilities:

1. In the navigation pane, select **Administration > Patch Settings**.
2. The **Patch Settings** window appears and SA checks for Windows patch utility updates. The **Latest** column in the **Windows Patch Utilities** section of the window indicates that SA is checking for updates.
  - The **Latest** column displays the latest version that is available from the vendor.
  - The **Version** column displays the version of the utility that is already in the SA database.
3. If you are connected to the internet, the **Latest** column is updated to the latest version that is available from the vendor.
  - a. Compare the values in the **Latest** column to the **Version** column.
  - b. If the Version in the SA database is lower than the Latest version that is available from the vendor your utilities need to be updated.



- c. Click **Import from Vendor** to get the latest utilities.
  - d. 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.
    - o If the job complete, the Status column will display the success icon ✓.
    - o If the job fails, the Status column will display the error icon ✗. Double-click the error icon to display the error message.
  - e. After the process completes, click **Close**.
4. If you are not connected to the internet, the Unable to Access wuredist.cab window appears providing an option to import the Windows Update Agent (wuredist.cab) from a local file.



- a. Click **Import**.
  - b. In the **Import Patch Utility** dialog, find and select the wuredist.cab file locally.
  - c. Click **Import** to import the utility update.
  - d. After the import is complete, the **Latest** column shows which utilities have updates available.
1. Manually importing the Windows patching utilities

If you are working in **Microsoft Offline Catalog** patching mode and you did not install the Windows patch management files during core installation, get the following Microsoft files from a machine with internet access and add them to the core.

If you need to work in a tightly secured environment, consider switching to **WSUS** patching mode as this enables you to get Windows patches from a WSUS server on your network.

**Note:** The links to the following Microsoft files are provided as a convenience. However,

Microsoft Corporation may change the links after the release of this document. Therefore, we cannot guarantee that these links will be valid when you use them and you may need to search the Microsoft Support website to find the correct files.

a. **wsuscn2.cab**

The wsuscn2.cab file contains the Microsoft patch database.

Download wsuscn2.cab from:

<http://go.microsoft.com/fwlink/?LinkId=76054>

b. **WindowsUpdateAgent30-x86.exe**

The WindowsUpdateAgent30-x86.exe file is required when SA scans x86-based managed servers to determine which Windows patches/hotfixes are installed.

- i. Download the package containing WindowsUpdateAgent30-x86.exe from:

<http://go.microsoft.com/fwlink/?LinkID=100334>

- ii. After downloading, rename the file "WindowsUpdateAgent-x86.exe".

c. **WindowsUpdateAgent30-x64.exe**

The WindowsUpdateAgent30-x64.exe file is required when SA scans x64-based managed servers to determine which Windows patches/hotfixes are installed.

- i. Download the package containing WindowsUpdateAgent30-x64.exe from:

<http://go.microsoft.com/fwlink/?LinkID=100335>

- ii. After downloading, rename the file "WindowsUpdateAgent-x64.exe".

d. **WindowsUpdateAgent30-ia64.exe**

The WindowsUpdateAgent30-ia64.exe file is required when SA scans Itanium x64-based managed servers to determine which Windows patches/hotfixes are installed.

- i. Download the package containing WindowsUpdateAgent30-ia64.exe from:

<http://go.microsoft.com/fwlink/?LinkID=100336>

- ii. After downloading, rename the file "WindowsUpdateAgent-ia64.exe".

## Retrieving Microsoft patch supplements from HPLN

In **WSUS** patching mode, SA retrieves all required patches directly from a WSUS Server in your network. However, if you are working in **Microsoft Offline Catalog** patching mode, SA retrieves information about Microsoft patches from the wsuscn2.cab file. This file contains patches and associated metadata only for security Microsoft updates. SA provides non-security patches via the HP Live Network.

When HP updates this supplemental data, you can configure the HP Live Network to automatically upload it to the SA Microsoft patch database.

You cannot download patches from HPLN in **WSUS** patching mode.

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

- a. Obtain an HP Passport ID from:

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

- b. Log in to the HP Live Network portal using your HP Passport credentials:  
<https://hpln.hpe.com/group/hp-live-network-connector>
- c. The HP Live Network connector (LNC) is installed on the core server where the SA Software Repository component is installed.  
You can download the HP Live Network Connector User Guide from the Live Network Connector community on the HP Live Network at:  
<https://hpln.hpe.com/group/hp-live-network-connector>  
Click the **Resources** tab and open the **Documentation** folder.
- d. On the system where the LNC is installed, run the following commands to enable the Microsoft patching service:  

```
live-network-connector write-config --add --setting=content.ms_patch_supp=1  
and  
live-network-connector write-config --setting=sas.force_win_patch_import=1 -  
-add
```
- e. (Optional) To disable the Microsoft patching service, run the same command with the value set to 0:  

```
live-network-connector write-config --setting=content.ms_patch_supp=0  
and  
live-network-connector write-config --setting=sas.force_win_patch_import=0
```

Alternatively, you can manually download the supplemental patch data file from the HP Live Network and upload it to the SA database. See "[Manually downloading the Microsoft patch supplements from HPLN](#)" below.

## Manually downloading the Microsoft patch supplements from HPLN

This section describes how to manually download the supplementary Microsoft patch data file from the HP Live Network and upload it into the SA patch database.

This is only required if you are working in **Offline Catalog** patching mode as the `wsusscn2.cab` file contains updates for security issues. In **WSUS** patching mode, WSUS synchronizes with Microsoft Update to regularly download both security and non-security updates to a central WSUS repository on your network.

We recommend that you set up the LNC to automatically upload this file whenever it changes as described in "[Retrieving Microsoft patch supplements from HPLN](#)" on the previous page. 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 an HP Passport ID from:  
<http://h20229.www2.hp.com/passport-registration.html>
2. Log in to the HP Live Network portal using your HP Passport credentials:  
<https://hpln.hpe.com/group/hp-live-network-connector>
3. The HP Live Network connector (LNC) is installed on the core server where the SA Software Repository component is installed.



You can download the HP Live Network Connector User Guide from the Live Network Connector community on the HP Live Network at:

<https://hpln.hpe.com/group/hp-live-network-connector>

Click the Resources tab and open the Documentation folder.

4. Click Content Catalog from the HP Live Network menu and search for "MS Patch Supplement for Server Automation" under the Server Automation product.
5. Download the latest Microsoft Patch Supplement, named latest\_OPSSWinPatchDB.zip, and place it in the Core slice server directory:

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

6. Import the Microsoft Patch Supplement metadata via the following command:

```
./import_win_patch_bundle --bundle latest_OPSSWinPatchDB.zip
```

7. Since HP updates the Microsoft 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.

## Downloading the Microsoft Offline patch catalog from the command line

The `populate-opsware-update-library` shell script downloads the Offline Microsoft Catalog from the Microsoft site and imports the Windows database and patches into Server Automation.

- This script is specific to **Microsoft Offline Catalog** patching and does not run in **WSUS** patching mode.
- Do not run concurrent instances of the script.

### Prerequisites

Before running the command line script, ensure that:

- your patching mode in SA Client > **Administration** > **Patch Settings** > **Patch Downloads** is set to **Microsoft Offline Catalog**.
- your SA Core has access to the internet or to a web proxy.
- the patch metadata is available in the currently loaded Microsoft patch database. SA maps patch binaries to available patch metadata during patch import. For more information, see "[Import metadata for Windows patches](#)" on page 51.

Note: the metadata import method has the same capabilities as this shell script.

### Script vs. SA Client imports

You can import patches from the Microsoft Offline Catalog either from the SA Client using this script. The command line script is better when you want to download all the available patches to the system. If you updated your patches monthly, for example, you would most likely use the command line tool, and save the arguments.

For information about importing the offline Microsoft catalog via the SA Client, see "[Importing Windows patch utilities for the offline patch catalog](#)" on page 29

### Running the script

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

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

To run the script:

1. Log on to the Software Repository server as `root`.
2. Schedule the script to run periodically as a cron job on the Software Repository server. From the SA Client, the patches imported with the script show up as automatically imported.
3. Run the `populate-opsware-update-library` script with `--help` parameter for a complete list of available options.

### Script Options

- This shell script sets the initial status of newly imported patches to **Available** or **Limited**.
- The script can also filter the patches imported according to operating system, such as specific versions of Windows Servers. When you run this script, patches from all products that are selected in the **Patch Settings** product list will be imported, unless they are specifically omitted by one of the command-line options. See "[Parameters for the populate-opsware-update-library script](#)" below.
- This script provides options for omitting patches from certain Windows operating systems; but it does not provide options for omitting non-OS products, such as Microsoft Office or Exchange.

### Parameters for the `populate-opsware-update-library` script

Option	Description
<code>--spin</code> <hostname-or-IP>	Hostname or IP address of the Data Access Engine (spin) host. Default: spin
<code>--theword</code> <hostname-or-IP>	Hostname or IP address of the Software Repository (theword) host. Default: theword
<code>--cert_path</code> <file-path>	File specification of the cert file to be used for the spin connection. Default: /var/opt/opsware/crypto/wordbot/wordbot.srv
<code>--ca_path</code> <file-path>	File specification of CA file to be used for Spin connection. Default value: /var/opt/opsware/crypto/wordbot/opsware-ca.crt
<code>--verbose</code>	Display copious output.
<code>--no_nt4</code>	Do not process NT4 patches.
<code>--no_w2k</code>	Do not process W2K patches.
<code>--no_xp</code>	Do not process XP patches.
<code>--no_w2k3</code>	Do not process W2K3 patches.
<code>--no_w2k3x64</code>	Do not process W2K8 x64 patches.
<code>--no_w2k8</code>	Do not process W2K8 patches.
<code>--no_w2k8x64</code>	Do not process W2K8 x64 patches.
<code>--no_</code>	Do not process W2K8 R2 x64 patches.

Parameters for the populate-opsware-update-library script, continued

Option	Description
w2k8r2x64	
--no_w2k8r2ia64	Do not process W2K8 R2 IA64 patches.
--no_w2k12x64	Do not process W2K12 x64 patches.
--no_w2k12r2x64	Do not process W2K12 R2 x64 patches.
--no_w7x64	Do not process W7 x64 patches.
--no_w7	Do not process W7 patches.
--no_w81x64	Do not process W8.1 x64 patches.
--no_w10x64	Do not process W10 x64 patches.
--no_w2k16x64	Do not process W16 x64 patches.
--wget_path <file-path>	Use wget for the downloads vs built-in download support. File specification of the wget utility.
--wget_http_proxy <server:port>	wget HTTP proxy server in format proxyserver:httpport. This option is ignored if wget http proxy is configured in wget user startup file .wgetrc.
--wget_ftp_proxy <server:port>	wget FTP proxy server in format proxyserver:ftpport. This option is ignored if wget ftp proxy is configured in wget user startup file .wgetrc.
--use_proxy_url <url>	When downloading binaries, connect via this proxy URL. This option overrides the proxy settings specified via the http_proxy environment variable.
--proxy_userid <userid>	Basic-auth userid to provide to proxy server. Another way of providing the proxy userid is by setting the POP_OPSW_LIB_PROXY_USER environment variable. This option overrides the proxy userid specified via the POP_OPSW_LIB_PROXY_USER environment variable.
--proxy_passwd <passwd>	Basic-auth passwd to provide to proxy server. Another way of providing the proxy password is by setting the POP_OPSW_LIB_PROXY_PASSWD environment variable. This option overrides the proxy password specified via the POP_OPSW_LIB_PROXY_PASSWD environment variable. Please note that specifying the proxy password via this option makes the password visible to any user on the process command line. To avoid this do not use this option and specify the password via the POP_OPSW_LIB_PROXY_PASSWD environment variable.
--set_	Set availability status to Available when uploading patches.

Parameters for the populate-opsware-update-library script, continued

Option	Description
available	
--set_limited	Set availability status to Limited when uploading patches.
--no_hotfixes	Do not upload hotfixes.
--no_servicepacks	Do not upload service packs.
--no_updaterollups	Do not upload updatерollups.
--no_wsusscan_upload	Do not upload the MBSA 2.1x patch database.
--wsusscan_url_override <url>	Download the MBSA 2.1x patch database from this URL.
--force_msutil_upload	Force new Microsoft utilities to be fetched and uploaded This option is ignored if --download_only is also specified.
--no_msutil_upload	Skip Microsoft utilites check and upload
--wua_x86_url_override <url>	Download x86 Windows Update Agent from this URL.
--wua_x64_url_override <url>	Download x64 Windows Update Agent from this URL.
--wua_ia64_url_override <url>	Download ia64 Windows Update Agent from this URL.
--update_all	Refresh the patches already uploaded into Opsware SAS.
--download_only <path>	Download files from the vendor's web site to the specified path, but do not upload them into Opsware SAS.
--download_only_if_not_exists	If --download_only specified, only download patches that don't yet exist.
--upload_from_update_root <path>	Upload files from specified directory instead of from vendor's website. This option is ignored if --download_only is also specified.

### Parameters for the populate-opsware-update-library script, continued

Option	Description
<code>--use_temp_download_path &lt;path&gt;</code>	Download files to temporary download directory instead of a subdirectory under <code>/var/tmp</code> .
<code>--log_file &lt;path&gt;</code>	Log the output to the specific file.
<code>--parallel_uploads &lt;number&gt;</code>	Number of patch uploads to run in parallel. System specific default value will be used.
<code>--download_retry &lt;number&gt;</code>	Number of times to retry the download of patches
<code>--help</code>	Display this message.  Note that <code>--set_limited</code> and <code>--set_available</code> cannot both be set at the same time.  <code>./populate-opsware-update-library.pyc: version 3.2.0</code>  This script has been developed and test-run on a word server, but should run on any core server with word or spin crypto. No parsing of the cab is done in this script.

### Exporting Windows patch utilities

If you are working in **Offline Catalog** patching mode, you can export the following Windows utilities from Server Automation to your local file system:

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

To export a Windows patch utility:

1. In the navigation pane, select **Administration>PatchSettings**.
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**.

### Importing the Windows patch database from WSUS

If you are working in an environment where Microsoft patches are downloaded centrally to a Windows Server Update Services (WSUS) internal server, you can use your WSUS repository as your SA patch database. The WSUS patch repository synchronizes regularly with Microsoft Update which ensures that the WSUS patches you import into SA are always up-to-date.

Unlike the **Offline Catalog** patching mode, WSUS patching does not require access to the Microsoft website and to HPLN for importing patch updates. SA integrates with WSUS on your network to:

- pull security and non-security patches into your SA patch library.
- assess which Windows updates are required for your SA managed servers.
- deploy applicable updates to SA servers.

When you import the Windows patch database, SA only imports the patch metadata for the available patches. After importing the patch database, run a compliance scan and import binaries only for the patches required to remediate non-compliant servers.

To import the Windows patch database from a WSUS server:

**Prerequisite:** "[Connecting SA to a WSUS server](#)" on the next page before importing the Windows patch database.

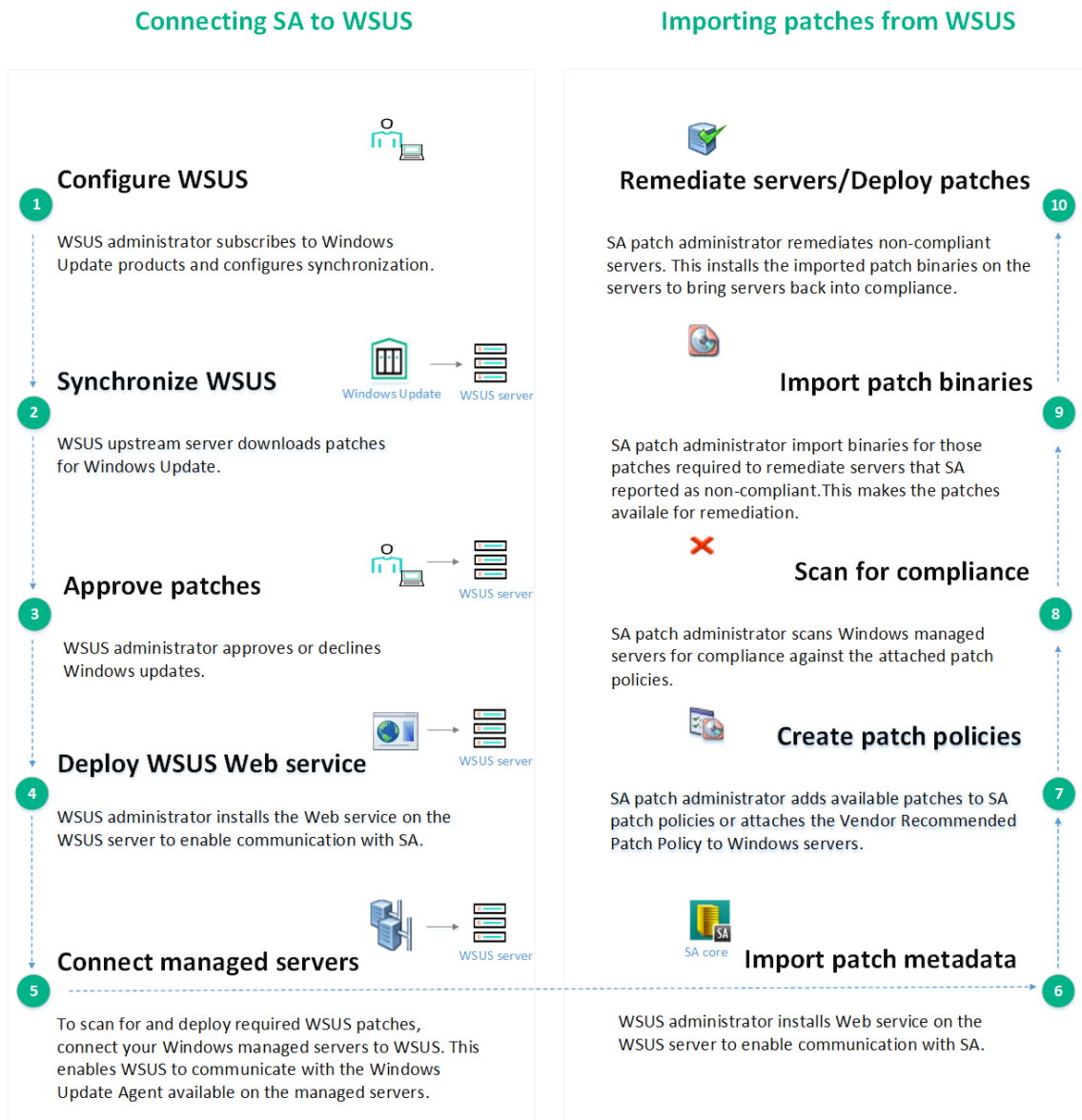
1. Go to the **Administration > Patch Settings**.
2. In the **Patch Downloads** section, select the Microsoft **WSUS** patching mode.
3. On the **General** page, specify the URL of the WSUS Web service: `http(s)://hostname/<your_folder_name>/WsusREST`. SA downloads patches to the SA core via the WSUS Web service and distributes them to connected managed servers, as required.
4. Select your preferred **Binaries Import Mode** to indicate which patch executables to import from WSUS:
  - **Recommended** - imports the list of Microsoft recommended patches.
  - **All** - imports required patch executables for all patch metadata retrieved from WSUS.
5. Select the **Patch Database** tab and click:
  - **Import Metadata** - to import patch metadata for all patches filtered from WSUS. By default, SA imports metadata only for patches that the WSUS Administrator marks as **Approved**. To import **Declined** and **Not Approved** patches as well, change the settings of the WSUS Web service. This option runs the **Import WSUS Metadata** script on the core slice.

**Note:** SA uses patch metadata during compliance scans to identify which servers require the patches approved by the WSUS administrator.

- **Import Binaries** - to import binaries for the patches required to remediate servers reported as non-compliant following a compliance scan. This runs the **Import WSUS Package Binaries** script on the core slice.
6. On the **Run Server Script** wizard, click **Next** and specify any custom import options for the script import steps.
  7. Click **Start Job** then click **Close** when the import is complete.

## Workflow diagram - Importing WSUS patches into SA

The diagram below illustrates the detailed workflow for importing and deploying Windows patches to SA managed servers.



## Connecting SA to a WSUS server

Before importing patch and patch metadata from WSUS, configure SA to communicate with your WSUS server.

To connect SA to an upstream WSUS server:

1. Configure WSUS to synchronize with Microsoft Update.
2. Approve/decline patches in WSUS to filter which patches are visible in SA.
3. [Deploy the WSUS Web Service](#) to set up the communication with the SA core. SA downloads all patches and associated metadata to the SA core and then distributes them, as required, to the managed servers that you connect to WSUS.

4. ["Connecting SA managed servers to WSUS" on page 44](#) to make them visible for compliance scans against WSUS patches.

## Deploying the WSUS Web service

SA communicates with Windows Server Update Services through a Web service installed on the WSUS server. The Web service sends the requested patches and patch metadata to the SA core which then distributes them to the appropriate SA managed servers.

WSUS Web service is deployed only in front of the WSUS upstream server visible to SA. All patches and associated metadata are retrieved from this upstream server. The WSUS administrator is responsible for keeping any downstream servers synchronized with the upstream server.

**Prerequisite:** Before deploying the WSUS Web service, install OpenSSL (on any other machine) if you want to allow HTTPS requests.

To install the WSUS Web service on the WSUS upstream server and enable SA client connections:

1. Deploy the Web Service into IIS
  - a. In the SA Client, go to **Library > By Folder > Opware > Tools > Patching**.
  - b. Right-click on archived Web service file, **hpsa\_wsus\_ws\_versionnumber.zip** file and select **Export Software**.
  - c. Unpack the Web service ZIP file on the machine that holds the WSUS server, in a new folder under `C:\inetpub\wwwroot`.
  - d. Click the Windows **Start** button, type **IIS** and open Internet Information Services.
  - e. Under the **Default Web Site**, right-click on the folder you have created in step **c** and select **Convert to Application**.
2. Add a Web Service Manager user to the WSUS Administrators group

Skip the first three steps if you are using Windows Small Business Server 2008.

  - a. Click the Windows **Start** button and type **Computer Management**.
  - b. Go to **Local Users and Groups > Users** and create a new user that will manage the Web service.
  - c. Add the new user to the WSUS Administrators group under the **Groups** folder.
  - d. In IIS, right-click **Application Pools** above the **Sites** section and select **Add Application Pool**.
  - e. If .NET 4.0 is not already installed on your system, install it and run the following command as Administrator: `c:\WINDOWS\Microsoft.NET\Framework\v4.0.30319\aspnet_regiis.exe -iru`
  - f. Enter a name for your application pool, select .NET 4 or above and click **OK**.
3. Configure IIS to use the new Web Service Manager user for running the Web service

Skip the first two steps if you are using Windows Small Business Server 2008.

  - a. Right-click the newly created application pool and select **Advanced Settings**.
  - b. Under **Process Model**, change the identity configuration to use a custom account and provide the credentials for your newly created Web Server Manager account.
  - c. In IIS, select the Web service under the **Default Web Site** and click **Basic Settings**.



- d. Select your newly created application pool as the default one and click **OK**. The Web service will now use your new application pool.
4. Configure IIS to accept HTTP and HTTPS requests for WCF

By default, IIS does not accept HTTP and HTTPS requests for a .NET WCF Web Service. To enable this option manually:

- a. Click the Windows **Start** button and type *Turn Windows features on or off*.
  - b. Expand **Features > .NET Framework 4.5 Features > WCF Services** and enable **HTTP Activation**.
  - c. Click **Install** then click **Next** until you reach the end of the wizard.
5. Setting up SSL certificates for IIS and the Web service clients (SA core and SA client)
    - a. Cmd to the OpenSSL installation directory. By default OpenSSL installs under Program Files (x86)\GnuWin32\bin
    - b. Type the following command to create a new system variable pointing to the openssl.cnf . Edit the command if you installed OpenSSL at a different location than the default one:  
Set OPENSSL\_CONF=C:\Program Files (x86)\GnuWin32\share\openssl.cnf
    - c. Create a private and a public key using the following command:  
openssl req -x509 -newkey rsa:2048 -keyout *your\_private\_key.pem* -out *your\_public\_key.pem* -days *XXX*. Change *XXX* to the number of days you want the certificate to be valid for and give a custom name to the two .pem files.
    - d. Type the following command in the OpenSSL installation directory to convert the two .pem files into a single .pfx file: openssl pkcs12 -inkey *your\_private\_key.pem* -in *your\_public\_key.pem* -export -out *your\_pkcs12\_cert.pfx*.
    - e. Copy the .pfx file on WSUS Web service machine to import the server certificate into IIS:
      - i. Go to IIS and select your server from the **Connections** pane.
      - ii. Double-click **Server Certificates** select your certificate and click **Import**.
      - iii. Browse to your .pfx file and type in the password you created for your public and private keys.
    - f. Create a new binding for the Web service, to use HTTPS with this certificate.
      - i. In the IIS, select **Default Web Site** from the **Connections** pane.
      - ii. Click **Bindings** from the **Actions** pane. This displays the **Site Bindings** dialog box.
      - iii. Click **Add** and select **https** from the **Type** drop-down menu.
      - iv. Pick your IP address and/or hostname from the **SSL certificate** drop-down menu.
      - v. Click **Apply** to save your changes.
    - g. **Configure the Web service to require SSL.**
      - i. Select your Web service from the IIS **Connections** menu, under **Default Web Site**.
      - ii. Click **SSL Settings**.
      - iii. Check **Require SSL** checkbox and click **Apply**.
    - h. Paste the content of *your\_public\_key.pem* at the bottom of the following file:  
/opt/opsware/openssl/certs/ca-bundle.crt. This copies the public certificate into the KnownCertification Authorities file on your SA core.

Do not delete any existing certificates from the `bundle.crt` file.

6. Setting up SSL certificates for securing the Web service-WSUS communication
  - a. Edit the `wsusConfig.config` file to set **secureConnection** to **True** and change the port to WSUS's HTTPS port. For Windows Server 2012, the default port is 8531.
  - b. Use a self-signed certificate generated and import it into IIS as described in step 5. When OpenSSL prompts you for the **Common Name**, type the FQDN or IP of your machine that holds WSUS and the Web service.
  - c. In the IIS **Connections** pane, expand your host server > **Sites** and select the **WSUS Administration** node. Depending on your operating system, this is displayed either under **Default Web Site** or on the same level.
  - d. Click **Bindings** from the **Actions** pane. This displays the **Site Bindings** dialog box.
  - e. Select the **https** binding and click **Edit**.
  - f. Pick your IP address and/or hostname from the **SSL certificate** drop-down menu.
  - g. Choose your imported certificate and click **OK** to close the **Edit Site Bindings** dialog box.
  - h. In the **WSUS Administration** node, enable the **Require SSL** option for the following subnodes: **APIRemoting30**, **ClientWebService**, **DssAuthWebService**, **ServerSyncWebService** and **SimpleAuthWebService**.
  - i. Open the **Content** node and make sure the **Require SSL** option is disabled. The Web service does not require SSL to secure content coming from the WSUS server. WSUS updates are signed by Microsoft by default, thus they are already secure.
  - j. Click **Apply** to save your changes.
  - k. Install your generated public key on the computer that holds WSUS and the Web service.
7. Configuring connection and import settings for the WSUS Web service

The Web service archive that you unpacked under `C:\inetpub\wwwroot\[your folder]` contains two configuration files: `wsusConfig.config` and `web.config`. Edit these XML files to configure the connection and metadata import settings for patches for the WSUS Web service.

a. **WsusConfig.config**

Attribute	Description
<b>serverName</b>	IP or hostname of the WSUS server. This is included in the URL of the WSUS Web service. The WSUS Web service supports both IPv6 and IPv4 hosts.
<b>port</b>	The port where WSUS is located on the server. Default HTTP port is 8530.
<b>secureConnection</b>	Set to <b>True</b> if you want the connection between Web Service and the WSUS server to be secure.
<b>ignoredProperties</b>	Specify which metadata properties to ignore when the Web service retrieves WSUS patches and associated metadata.
<b>includeApprovedUpdatesOnly</b>	Specify which type of patch metadata SA retrieves from the WSUS server: <b>True</b> - Web service imports only metadata for the patches marked as <b>Approved</b> in WSUS. <b>False</b> - Web service imports metadata for all patches available in WSUS: <ul style="list-style-type: none"><li>◦ <b>Approved</b></li><li>◦ <b>Declined</b></li><li>◦ <b>Not Approved</b></li></ul>

b. **Web.config**

The following lines in this XML file define the two endpoints available for connecting the Web service to WSUS:

- `<endpoint address="" binding="webHttpBinding" bindingConfiguration="secureHttpBinding" contract="WsusREST.IWsusREST" behaviorConfiguration="web"></endpoint>`
- `<endpoint address="" binding="webHttpBinding" contract="WsusREST.IWsusREST" behaviorConfiguration="web"></endpoint>`

Make sure these endpoints mirror the IIS binding settings that you have configured in step 5.

**HTTP connection:**

If your IIS configuration specifies an HTTP binding, remove the `bindingConfiguration="secureHttpBinding"` line from this file, otherwise the Web service call fails.

**HTTPS connections:**

If your IIS configuration specifies an HTTPS binding, keep the `bindingConfiguration="secureHttpBinding"` line

**HTTP and HTTPS connections:**

If your IIS configuration specifies both HTTP and HTTPS bindings, keep both lines.

#### 8. Hide IIS version information

For security reasons, We recommend limiting the information that the WSUS Web service provides to remote clients. To hide the IIS version that the WSUS Web service is using:

- a. [Install UrlScan](#) from the Microsoft website. This security extension enables you to filter IIS connection requests.
- b. Navigate to %WINDIR%/System32/inetsrv/urlscan and open the UrlScan.ini file.
- c. Search for the RemoveServerHeader attribute and change it from 0 to 1. This stops sending the HTTP server header to remote clients.
- d. Save the UrlScan.ini file and close it.

#### 9. Access the deployed Web service

- a. Enter the following URL in your browser to test the WSUS-Web service connection. This downloads a JSON file containing all the languages enabled on your WSUS Server.
  - secure binding: https://<hostNameOrIP>/<your\_folder\_name>/wsusREST/Locales
  - non-secure binding: http://<hostNameOrIP>/<your\_folder\_name>/wsusREST/Locales
- b. Check that each Windows managed server is able to access this WSUS Web service URL. SA cannot patch servers that do not have direct access to WSUS as these connections are not routed through the SA gateway mesh.

### Connecting SA managed servers to WSUS

To be able to scan for and deploy required WSUS patches, connect your Windows managed servers to WSUS. This enables WSUS to communicate with the Windows Update Agent available on the managed servers.

#### Prerequisites

- Make sure each SA managed server can access the WSUS URL set for it as a custom attribute at the Facility/Customer/Device group/Server level. SA cannot patch servers that do not have direct access to WSUS as these connections are not routed through the SA gateway mesh.
- Check that the managed servers you want to connect to WSUS are using the SA Agent version, which is packaged along with the SA 10.23.007 Patch.

You can connect managed servers to WSUS either:

#### When installing the SA Agent

1. Go to the **Administration > Patch Settings** and make sure that the Microsoft **WSUS** patching mode is enabled.
2. Add the following custom attribute at **Facility** or **Customer** level:

Name	Value
WSUS_URL	<protocol>://<WSUShostnameOrIP>:<portNumber>

- Go to **Devices > SA Agent installation** and select the servers on which you want to install the SA agent.

Optionally, you can specify extra installer options:

Flag	Arguments
	Enclose multiple arguments in double quotes.
--wsus_ cfg_args	--setupConnection. Mandatory argument.  --wsusURL - specifies a WSUS URL that overrides any custom attributes already set for the selected managed servers. Optional argument.  --ignoreWSUSModeCheck - ignores that <b>WSUS</b> patching mode is not enabled on the core. Optional argument.
--wsus_ cfg_skip	Does not run the WSUS configuration script.

#### When upgrading the SA Agent

- Go to **Administration > Patch Settings** and make sure that the Microsoft **WSUS** patching mode is enabled.
- Add the following custom attribute at **Facility, Customer, Device Groups** or **Servers** level:

Name	Value
WSUS_URL	<protocol>://<WSUShostnameOrIP>:<portNumber>

- Go to **Devices > All Managed servers**, right-click on the servers on which you want to upgrade the SA Agent and select **Run > Agent Upgrade**.

Optionally, you can specify extra installer options:

Flag	Arguments
	Enclose multiple arguments in double quotes.
--wsus_ cfg_args	--setupConnection. Mandatory argument.  --wsusURL - specifies a WSUS URL that overrides any custom attributes already set for the selected managed servers. Optional argument.  --ignoreWSUSModeCheck - ignores that <b>WSUS</b> patching mode is not enabled on the core. Optional argument.
--wsus_ cfg_skip	Does not run the WSUS configuration script.

#### When provisioning a server

- Go to the **Administration > Patch Settings** and make sure that the Microsoft **WSUS** patching mode is enabled.

2. Add the following custom attribute at **Facility** or **Customer** level:

Name	Value
WSUS_URL	<protocol>://<WSUShostnameOrIP>:<portNumber>

3. Start the provisioning process. See **Performing provisioning** in the SA Administration Guide.

### Before running compliance scans

If you have not connected your Windows servers to the WSUS server during Agent installation or upgrade, you can run an SA script to manually make your servers available for WSUS patching.

1. Go to the **Administration > Patch Settings** and make sure that the Microsoft **WSUS** patching mode is enabled.
2. Add the following custom attribute at **Facility, Customer, Device Groups** or **Servers** level:

Name	Value
WSUS_URL	<protocol>://<WSUShostnameOrIP>:<portNumber>

3. Go to **Devices > Servers > All Managed Servers** and right-click on a server that you want to connect to WSUS.
4. Select **Run Script > Configure Server With WSUS** from the context menu. This launches the **Configure Server With WSUS.bat** script file from **Library > By Folder > Opware > Tools > Patching**.
5. On the **Run Server Script** wizard, click **Next** and specify any custom options for the script.
6. Click **Start Job** then click **Close** when the import is complete.

### Parameters for the Configure Server With WSUS script

The following parameters enable you to change the default behavior for running the **Configure Server With WSUS** .bat file on the selected servers.

- --wsusURL - specifies a WSUS URL that overrides any custom attributes already set for the selected managed servers.
- --ignoreWSUSModeCheck - ignores that **WSUS** patching mode is not enabled on the core.

### Changing configuration settings for the WSUS Web service

As part of deploying the WSUS Web service on a WSUS server, you define how SA connects and imports patches from WSUS via the WSUS Web service.

You can change your settings at any time, from the two WSUS Web service configuration files: `WsusConfig.config` and `Web.config`. These XML files are available on the machine that holds the WSUS server, under `C:\inetpub\wwwroot\[your folder]`.

You cannot change the list of patch products and patch locales that SA reads from WSUS. This list is defined by the WSUS administrator on the WSUS side.

To change metadata import settings:

1. On the WSUS machine, go to `C:\inetpub\wwwroot\<folder_where_you_deployed_the_WSUS_Web_service>` and open `WsusConfig.config`.

2. Find the `includeApprovedUpdatesOnly` attribute and set it to **False**.
3. Save your changes and close the XML file.
4. Restart the IIS site that holds the WSUS Web service.

By default, SA imports metadata only for patches that the WSUS Administrator marked as **Approved**. You can edit this filter to import **Declined** and **Not Approved** patches as well.

To change connection settings:

The **WsusConfig.config** XML file defines the IP, port number and specifies whether the connection between the WSUS server and your WSUS Web service is secure or not. To change the connection or the URL of the WSUS Web service:

1. On the WSUS machine, go to `C:\inetpub\wwwroot\<folder_where_you_deployed_the_WSUS_Web_service>` and open `WsusConfig.config`.
2. Find the `serverName` attribute and change it to use the new hostname or IP of your WSUS Web service.
3. Change the `port` number if required.
4. Set the `secureConnection` to **True** if you want to create an SSL HTTPS connection between the Web service and the WSUS server.
5. Save your changes and close the **WsusConfig.config** XML file.
6. Open the XML file **Web.config** and remove the `bindingConfiguration="secureHttpBinding` line if you want to create an HTTP connection. To create an HTTPS or both an HTTP and HTTPS connection, make sure the following line is available in the XML file: `<endpoint address="" binding="webHttpBinding" bindingConfiguration="secureHttpBinding" contract="WsusREST.IWsusREST" behaviorConfiguration="web"></endpoint>`.
7. Go to IIS and ensure that the connection endpoints defined in the **Web.config** XML file mirror your current IIS binding settings. For secure HTTPS connections, make sure the **Require SSL** option is enabled for the following pages of the **WSUS Administration** node in the **Connections** pane: **APIRemoting30**, **ClientWebService**, **DssAuthWebService**, **ServerSyncWebService** and **SimpleAuthWebService**.
8. Restart the IIS site that holds the WSUS Web service.

## Select Windows patch products and locales for import

You can limit the patches tracked by Server Automation to specific Windows products and locales of these products. When you import the Microsoft Patch Database, SA retrieves only the products and locales that you selected. This minimizes data storage issues in the SA Core and Software Repository (Word).

A product is a specific edition of an operating system or application, for example Windows Server 2008 R2. The locale of a patch identifies the language of the Windows servers that should receive the patch.

To specify patch products and patch locales for your Microsoft patch database:

### In WSUS patching mode

In WSUS mode, filtering by patch product and locale is done on the WSUS server side. SA only displays the read-only list of products and locales selected by the WSUS administrator.

### In Offline Catalog patching mode

By default, when you import the Microsoft Offline Catalog, SA imports patch metadata for all patches listed in the database. The default product list is based on the Microsoft product list at the time this version of SA was released. Modify the list of products according to the products in your environment. If there are products in the default selected list that you do not want, deselect them before you import patch binaries.

From the SA client

1. In the navigation pane, select **Administration>PatchSettings**.
2. In the **Microsoft** 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. To populate the list of available products from Microsoft, click either:
  - **Update Products from Vendor:** to update the list of products directly from the vendor site. The vendor site URL is the default URL for the Microsoft Offline Catalog on the Microsoft website. If you modified the default URL, select **Revert to Vendor Default** go back to the URL defined in your system implementation settings.
  - **Update Products from File:** Use this option to update the list of products from the wsuscn2.cab file on your local machine. This method is useful for air-gapped environments, where the managed servers do not have internet access.
5. Click **OK** to save your settings. The next time you run import Windows patches, patches for the selected products will be included in the download.

From the populate-opsware-update-library shell script

To limit the patches tracked to specific Windows operating systems, run the command-line script that automatically imports patches.

The script can filter the patches imported according to operating system, such as specific versions of Windows Servers. When you run this script, patches from all products that are selected in the **Patch Settings** product list will be imported, unless they are specifically omitted by one of the command-line options. See [Script Options](#).

## 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

Depending on your selected patching mode, SA supports the following locales for Windows patching:



### For patches coming from the Offline Catalog of Microsoft patches

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

### For patches coming from a WSUS server

SA supports all patch locales specified on the WSUS side.

### Locale configuration tasks

By default, Windows patch management supports only the English locale.

### Configuring the SA Core for non-English locales

**Note:**

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

To configure the core for non-English locales, complete the following steps on each core server that is running the SA 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 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"](#) below.

### Selecting the locales of patches to import

**Note:**

Complete the instructions in ["Configuring the SA Core for non-English locales"](#) on the [previous page](#) before performing the steps in this section.

You can only edit the list of patch locales when SA is set to **Offline Catalog** patching mode. In **WSUS** patching mode, this list is configured on the WSUS side and is displayed in SA as read-only information only.

When you select the locales of the Windows patches to import in **Offline Catalog** patching mode, the changes 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:

- In the navigation pane, select **Administration**.
- Select **Patch Settings**.
- In the Microsoft tab, select **Patch Locales**.
- Click **Edit**.
- 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 48, contact Support.
- Click **OK** to save your settings.
- Complete the steps in ["End user requirements for non-English locales"](#) below.

### End user requirements for non-English locales

To view non-English fonts in the SA Client:

Verify that the Windows desktop running the SA Client uses the Arial Unicode MS font.

After the system administrator performs the steps in ["Configuring the SA Core for non-English locales"](#) on the [previous page](#), the end user logs on to the SA Client and selects their "Logged in as" link in the upper right corner of the SA Client window. This displays the User window. Select the Properties view.

On the **User Properties** view, the end user updates the Locale field in the User Preferences section. For example, if the system administrator configured the core for Japanese, then the end user sets the Locale field to Japanese.

## Import metadata for Windows patches

When you import the Windows patch database from Microsoft's Offline Catalog or from a WSUS server, SA only imports the patch metadata for your filtered patches. The imported patch metadata is stored in the Software Repository (Word) and displayed under **Library > Patches > Windows**.

Patch metadata contains the information that SA requires to install Microsoft patches on your managed servers. Metadata supplies information for the properties of an update, thus enabling you to find out whether the patch is relevant for your Windows managed servers. The metadata package downloaded for an update is typically much smaller than the update file itself.

To import patch metadata:

- in **Offline Catalog** mode, see [Importing Windows patches from the offline MS catalog](#).
- in **WSUS** mode, see ["Importing the Windows patch database from WSUS" on page 37](#).

### Filtering metadata for import

Depending on your patching mode, SA applies different levels of filtering to ensure that you only import patches for the relevant Microsoft products on your Windows managed servers.

- In **Offline Catalog** patching mode, you can [filter imported metadata by patch product and patch locale](#).
- in **WSUS** patching mode, you can also filter metadata by approval status. SA imports metadata only for patches that the WSUS Administrator marked as **Approved**. You can cancel this filter to import **Declined** and **Not Approved** patches as well by ["Changing configuration settings for the WSUS Web service" on page 46](#).  
In WSUS mode, filtering by patch product and locale is done on the WSUS server side. SA only displays the read-only list of products and locales selected by the WSUS administrator.

SA retrieves patch metadata from the upstream server where you deployed the WSUS Web service. The WSUS administrator is responsible for keeping any downstream servers synchronized with the upstream server. This ensure you always get the complete and up-to-date list of patch metadata into SA.

After configuring and importing the metadata, you can import the Microsoft patch binaries by using the SA Client. If you are working in **Offline Catalog** mode, you can also import patch binaries from the `populate-opsware-update library` command-line script.

### Check the list of imported MS patch metadata

After importing Windows patch database from the Microsoft Offline Catalog or from a WSUS server, go to **Library > Patches > Windows** to verify that SA has imported the metadata for your filtered patches. Patches for which you imported only metadata show up in dimmed, indicating that their binaries are not available in SA yet.

Import patch binaries only for the patches required to remediate non-compliant servers. Before importing binaries, run a compliance scan to find out which patches require your managed servers.

To search for a product patch, select **Description** as the search value and enter the name of the product, such as Office 2003, in the text box.

For more information see, ["Import applicable Windows patch binaries" on page 70](#).

## Set patch availability

### From the SA Client

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** (Default) - for patches imported into Server Automation that can be installed only by patch administrators with required permissions. To obtain these permissions, contact your system administrator. See the SA Administration Guide for an explanation of these permissions.
  - **Available** - patches can be installed on managed servers.

### From the command-line script

If you are working in **Offline Catalog** patching mode, you can also change patch availability from the `populate-opsware-update-library` command-line script.

The default used by the script overrides the default set by the SA Client. For information about the script, see "[Downloading the Microsoft Offline patch catalog from the command line](#)" on page 33.

## Configure patch policies

Patch policies and patch policy exceptions enable you to customize which patches are distributed for installation in your environment.

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.

**Note:**

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. If you are working in WSUS patching mode,

enable the **Recommended** binaries import option. In **Offline Catalog** mode, SA retrieves the recommended set of patches from the wsuscn2.cab file.

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:** Depending on your selected patching mode, the list of recommended patches is retrieved on a server-by-server basis either by WSUS or from the wsuscn2.cab file. Vendor-recommended patch policies are system defined and cannot be edited or deleted by a user.

**Note:**

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.
- A patch policy is associated with an operating system version.
- 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.
- 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.

**Note:**

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 device group.
- 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.

## Add items to a Windows patch policy using the Object ID

The method for adding items to Windows Patch Policies has changed in order to prevent duplicate KB errors. SA identifies Windows hotfixes by the Object ID, now, instead of the KB number. This enables you to be more selective about the patches you add to the policy. However, it also means that when you select a patch of a certain KB number, SA will not automatically select all the other patches with that KB number—you must select them individually or use shift-click to multi-select items.

## Set 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 "[Set reboot options for remediation](#)" on page 57.
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.

## Windows patch policy remediation job option—Windows Patch Installation Order

When working in **Offline Catalog** patching mode, the **Windows Patch Installation Order** option enables you to control patch installation sequence during remediation. Because the Microsoft Offline Catalog of patches (wsusscn2.cab) only contains security updates, HP provides patch supplements via HPLN. Selecting this option prevents the collision of Windows patch data derived from different sources.

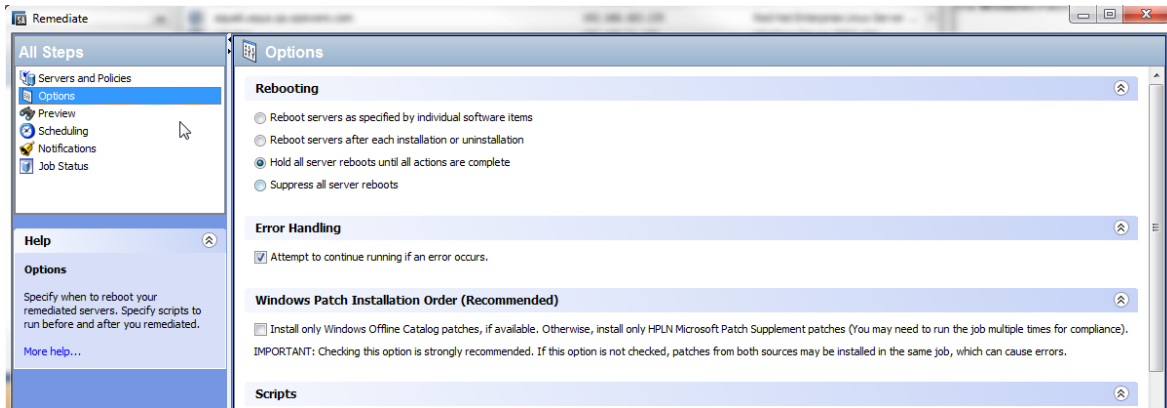
Some newer patches from the offline catalog have incorporated or enhanced the fixes that were previously defined in the patch supplement, which rendered the supplement patches obsolete. Consequently, patch data can be corrupted if you install the patch supplement patches before the wsusscn2.cab patches.

- HP strongly recommends using this option when remediating Windows patch policies in **Offline Catalog** patching mode.
- This setting is not available in **WSUS** patching mode. This is because SA can retrieve all required Microsoft updates from your WSUS server. For more information see [Accessing the Microsoft patch database](#)

### How it works:

1. When running a Windows Patch Policy remediation job, select the **Windows Patch Installation Order** setting in the **Options** view.

### Windows Patch Installation Order setting in the Remediate window



2. When you run the remediation job, all the Microsoft Offline Catalog patches (wsusscn2.cab) will be deployed first, and the HPLN Patch Supplement patches will be excluded until the job no longer contains any Microsoft Offline Catalog patches.

**Note:** When this option is not selected, the default order is by KB #, which can cause problems if you are installing patches from both sources: Windows Offline Catalog (wsusscn2.cab) and HPLN Microsoft Patch Supplement.

3. You will need to run the remediation job multiple times in order to deploy all the patches and achieve full compliance.

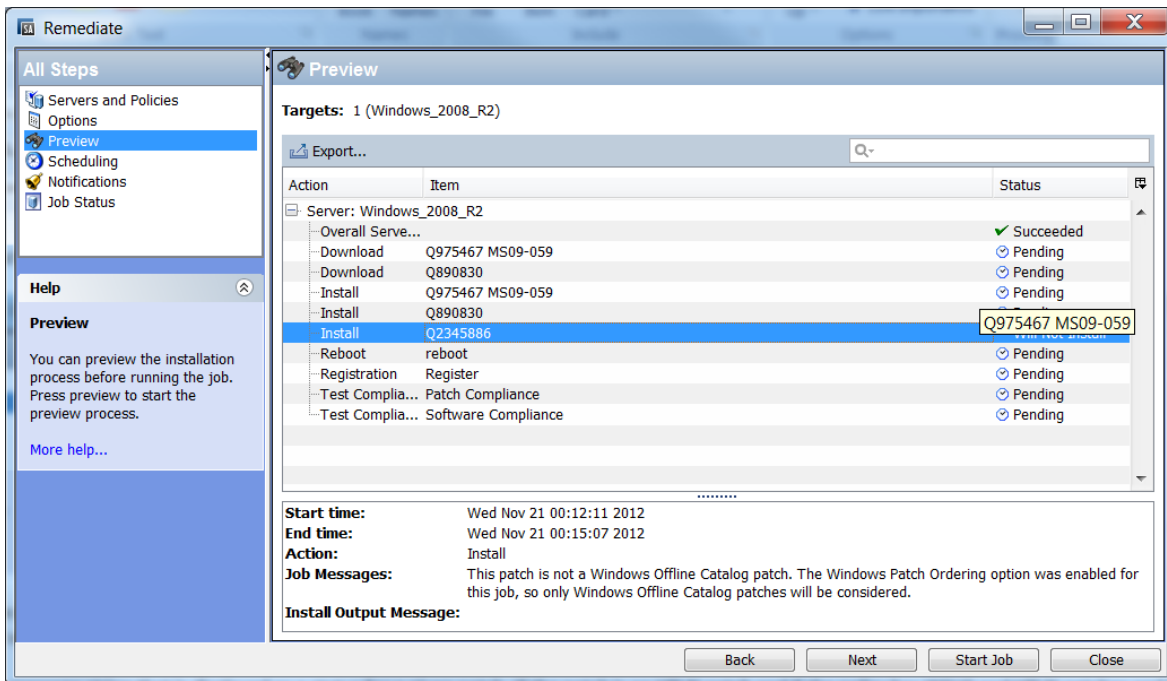
**Note:** If you use this option, you must run multiple remediation jobs to make a server fully compliant.

4. The status of each patch installation is provided in the **Preview** or **Job Status** view of the **Remediate** window.

To view additional details about a specific item, select the row in the table to display details in the bottom pane, as shown in the "[Preview Patch Install Status](#)" below figure.

#### Preview Patch Install Status





**Note:** If the policy has patches from both sources, wsusscn2.cab and the HPLN supplement, then the job will not install the HPLN patches. The following message should be displayed:

This patch is not a Windows Offline Catalog patch. The **Windows Patch Ordering** option was enabled for this job, so only Windows Offline Catalog patches will be considered.

## Set 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 and 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.

### Specify pre-installation and post-installation 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 SA 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\preinstall1.log`. If you do not enter a drive letter, the default is %SYSTEMDRIVE%, which is where the system folder of Ubuntu 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.

## Schedule 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.

## Set 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.

**Note:**

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

## Preview and start 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. This verification is based on the imported Microsoft patch database. 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.

**Note:**

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
- In the navigation pane, select Jobs and Sessions to review detailed information about the job. See "Browsing Job Logs" in the SA User Guide.
8. In the navigation pane, select Jobs and Sessions to review detailed information about the job. See "Browsing Job Logs" in the SA User Guide.
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 the "Cancelling or Terminating Installation, Uninstallation or Remediation Jobs" section in the SA Administration Guide.

## Verify 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.

## Create 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.

(Optional) In the Name field of the Properties, enter a name that describes the purpose or contents of the policy.

## Delete 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**.

## Add 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**.

## Remove 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**.

## Attach 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**.

## Detach 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**.

### Set 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**.

### Find 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.



## Copy 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**.

## Remove 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**.

## Run compliance scans

After importing all the patches for all the desired Windows products, run a compliance scan and remediate any necessary servers according to the scan results.

### Note:

The remaining steps assume that Vendor Recommended Patch Policies (VRPPs) are already attached to your Windows servers. If the VRPP is not attached to a server, attach it as you normally would before running the compliance scan. See ["Attach a patch policy to a server" on page 63](#).

1. Scan a Windows server with the VPRR attached for patch compliance.
2. From Devices, select the Windows server you wish to scan.
3. Select **Actions > Scan > Patch Compliance**.

The scan results will indicate if you need to remediate the server to apply any product-specific patches.

4. Remediate the recommended patches as you normally would. See ["Deploy patches/Remediate servers" on page 71](#).

**Note:**

When you run this script, patches from all products that are selected in the Patch Settings product list will be imported. This script does not provide an option to omit patches for specific products other than Operating System from the import. This script does provide options for omitting patches from certain Windows operating systems; but it does not provide options for omitting non-OS products, such as Microsoft Office or Exchange.

## Patch compliance

You can perform patch compliance scans on Windows Server servers to determine compliance relative to attached 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 servers.

### 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 ["Start a patch compliance scan immediately" on the next page](#).
- Periodically, by setting up a schedule.  
See ["Schedule a patch compliance scan" on page 69](#). 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:
  - ["Patch installation for Windows" on page 72](#)
  - ["Uninstall a Windows patch" on page 87](#)
  - ["Deploy patches/Remediate servers" on page 71](#)

## Start 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.


## Refresh 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.

## View 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:

1. In the navigation pane, select **Devices**.
2. Drill down to the server you want to check.
3. In the contents pane, select a server.
4. Right-click and then select **Scan > Show Patch Compliance Scan Failure Details**.
5. 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 the ["Patch Compliance Status Icons"](#) below table

### Patch Compliance Status Icons

Status/Icon	Description
 Compliant	The server is compliant for all patches. Patches in policies attached to the server are all installed on the target server.
 Partial	The server is partially compliant for patches. An exception has been set for these patches.

### Patch Compliance Status Icons, continued

Status/Icon	Description
 Non-Compliant	The installed patches on the server do not match the conditions defined in the patch policy.
 Scan Failed	The scan operation failed. Patch Management is unable to check the compliance of the server.

### 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 exceptions, 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.

## Schedule 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.

## Set 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**
  - **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.

## Import applicable Windows patch binaries

When you import the Windows patch database from the offline Microsoft Catalog or from a WSUS server in your network, SA only imports the patch metadata for the available patches.

This enables SA to save disk space, as your managed servers might not require all the patches imported from Microsoft. After importing the patch database from WSUS or from the `wsusscn2.cab` file, run a compliance scan on your Windows managed servers. Import patch binaries only for the patches reported as required to remediate non-compliant servers.

Patch binaries contain the Microsoft update files themselves and are stored together with associated metadata in the Software Repository (Word). When you import binaries for patches, SA maps the executables for the selected patch metadata available under **Library > Patches**.

Depending on your network infrastructure, you can import Microsoft patches into the SA Patch Library from Microsoft's Offline Patching Catalog or from a WSUS server.

## Importing binaries in Offline Catalog patching mode

In **Offline Catalog** mode, you can download binaries from the SA Client or with the `populate-opsware-update-library` script. For information about using the script, see "[Downloading the Microsoft Offline patch catalog from the command line](#)" on page 33.

1. In the navigation pane, select **Library>By Type>Patches**.
2. Expand the Windows tree and select an OS version.
3. In the content pane, right-click on a patch, select **Import Contents** and choose:
  - **From Vendor** - to import the patch directly from the Microsoft website. By default, this points to the URL where the patch executable is available on the Microsoft website.
  - **Import from File** - to import the patch executable stored locally your local machine.
4. Click **Import**.

## Importing binaries in WSUS patching mode

SA uses a script to import WSUS patch binaries from the SA Client. This script is available on the SA Core under `/opt/opsware/patch_importer/wsus_importer`. To import WSUS patch binaries:

1. In the SA Client, select **Administration > Patch Settings**.
2. In the **Patch Downloads** section, make sure the **WSUS** patching mode is enabled.
3. On the **General** page, make sure you are WSUS Web server URL points to the correct WSUS server in your network.
4. Check your selected **Binaries Import Mode**:
  - **Recommended** - imports required patch executables only for those patches that the WSUS Administrator has specified for your SA servers.
  - **All** - imports required patch executables for all patch metadata imported from WSUS. By default, SA imports metadata only for patches that your WSUS Administrator marked as **Approved**. You can cancel this filter to import **Declined** and **Not Approved** patches as well by ["Changing configuration settings for the WSUS Web service" on page 46](#).
5. On the **Patch Database** page, click **Import Binaries**. This launches the **Run Server Script** wizard with the **Import WSUS Package Binaries** script selected by default.
6. Edit the script options as required and click **Start Job**.
7. Click **Close** when SA finishes importing the available binaries on your selected managed servers.

SA retrieves patch metadata from the upstream server where you deployed the WSUS Web service. The WSUS administrator is responsible for keeping any downstream servers synchronized with the upstream server. This ensure you always get the complete and up-to-date list of patch into SA.

## Deploy patches/Remediate servers

After running a compliance scan, remediate any necessary servers according to the scan results. If the Vendor Recommended Patch Policy (VRPP) recommends any patches for a server that are not included in the imported patches, the compliance scan will show these missing patches in a subdued gray font.

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:

- ["Set reboot options for remediation" on page 57](#)
- ["Set reboot options for remediation" on page 57](#)
- ["Specify pre-installation and post-installation scripts for remediation" on page 193](#)
- ["Schedule a patch installation for remediation" on page 193](#)
- ["Set up email notifications for remediation" on page 194](#)
- ["Preview and start a remediation" on page 194](#)

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.

## Patch installation for Windows

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.

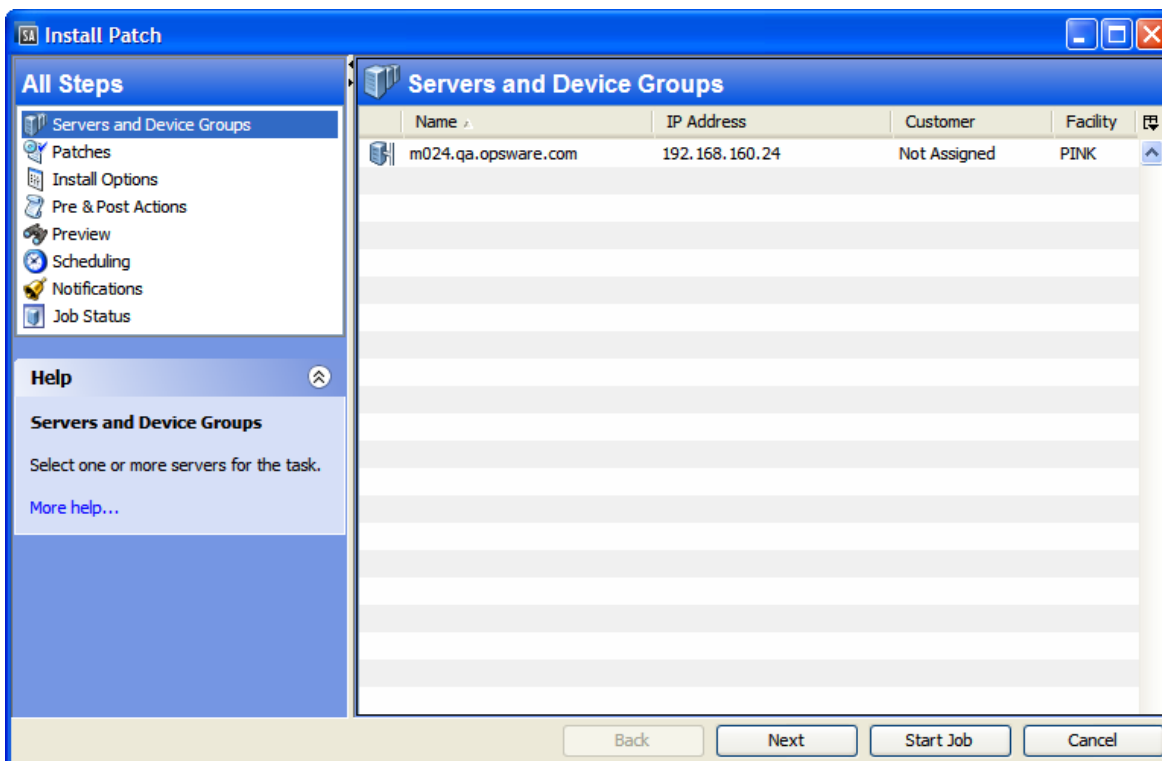
You can specify whether you want the installation to occur immediately after the patch is downloaded (staged) or you can schedule it to occur at a later date and time. Patch management also supports the need for best-effort installations of multiple patches by allowing you to specify that the patch installation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

### **Install Patch wizard**





## Installation flags Windows

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 ["Set install options" on page 75](#) for information about how to specify commands and flags.

**Note:**

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.

### Default installation flags

Windows patch type	Flags
Windows Hotfix	-q -z
Windows Security Rollup Package (treated identically like a Hotfix by WIndows patch management)	-q -z
Windows OS Service Pack	-u -n -o -q -z

## 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.

## Install a 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.

**Note:** 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:

- ["Set reboot options" on page 232](#)
- ["Specify install scripts" on page 232](#)
- ["Scheduling a patch uninstallation" on page 239](#)
- ["Set up email notifications" on page 234](#)

- ["Preview a patch installation" on page 234](#)
- ["View job progress for a patch uninstallation" on page 240](#)

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.

## Set 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.

## Set 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.

**Note:** 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.

**Note:** 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 ["Find servers that require a reboot" on page 92](#).

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 and 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.

## Specify 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 Server Automation with the SA 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 Runtime Options. If you choose a user account other than root, enter the User Name and Password. 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.

## Schedule 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.

### Note:

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



- ["Set install options" on page 75](#)
- ["Set reboot options for a Windows patch installation" on page 88](#)
- ["Schedule a Windows patch installation" above](#)

- ["Set up email notifications for a Windows patch installation" below](#)
- ["Preview a Windows patch installation" below](#)
- ["View job progress of a Windows patch installation" on the next page](#)

## Set 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.

**Note:**

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

- ["Set install options" on page 75](#)
- ["Set reboot options for a Windows patch installation" on page 88](#)
- ["Schedule a Windows patch installation" on the previous page](#)
- ["Set up email notifications for a Windows patch installation" above](#)
- ["Preview a Windows patch installation" below](#)
- ["View job progress of a Windows patch installation" on the next page](#)

## Preview 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.

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.

**Note:** 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.

## View 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** for more information about browsing job logs.  
  
When a **Vendor Recommended Patch Policy** is remediated on a Windows managed server, depending on what patches were applied, the server may require an additional remediation. This can occur when the remediation installs a patch that requires subsequent vendor updates.
  3. Click **Close** to close the **Install Patch** window or click **End Job** to prevent the job from running.

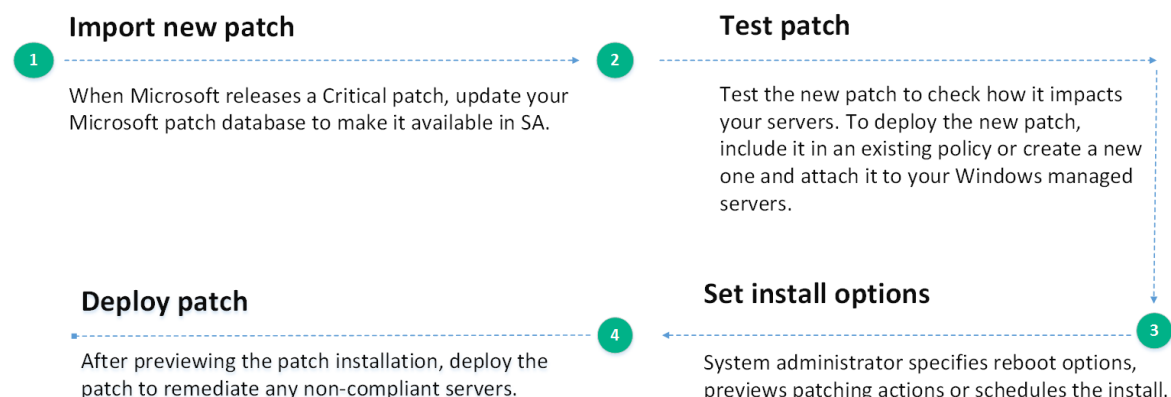
## Check for patch updates

Microsoft releases updates for Windows products regularly. New patches are immediately available in WSUS and also included in the Windows Update offline scan file every Patch Tuesday. To make new Windows patches available in SA:

- in **Offline Catalog** patching mode - reimport the wsusscn2.cab file
- in **WSUS** patching mode - reimport patch metadata and patch binaries

The following figure illustrate the patch update phases and their required steps:

### Install Windows patches on demand



## Patch management administration

### View 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.

**Note:**

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.

## Supersedence relationships in WSUS patching mode

SA may not always mirror exactly the WSUS hierarchy of patch supersedence. This is because, by default, SA only imports approved patches. If your WSUS administrator declines a patch involved in a supersedence relationship, this patch does not show up in SA. Consequently, supersedence details related to non-imported patches are ignored.

## Skipping superseded patches

The following patchman parameters allow SA to be configured to skip the import of superseded patches.

- `patchman.ms_mbsa20_skip_import_superseded`: Skip import of superseded patches
- `patchman.ms_mbsa20_skip_import_superseded_overrides`: To be used if you need specific patches imported even if they are superseded by other patches

## View 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.

## Edit Windows patch properties

You can edit the Description, Availability, Install Parameters, and Uninstall parameters of a patch.

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.

## Import 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**.

## Delete 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**.

## Find 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. In the content pane, select **Patches** from the **View** drop-down list.
3. Select a server that is running a supported Windows server.
4. In the details pane, select **Patches Recommended By Vendor** from the drop-down list to display the types of patches for the selected server.

## Find servers that have 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.

## Find servers that do not have 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.

## Export 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**.

## Enable/disable Windows Server 2008 Itanium (IA64) patches

Starting in 9.14, SA Windows Patching does not import Itanium (IA64) patches by default. However, a script is available to enable importing Windows Server IA64 patches.

Previously, Itanium patches were imported by default when the Windows Server 2008 R2 patch product was selected. In SA 9.14 and later, Itanium patches are not imported by default. The default setting was changed to reduce the patch import footprint, saving storage space and download time, for the customers who do not need Itanium patches.

About the enable-itanium-patches script:

- Location: `/opt/opsware/mm_wordbot/util/enable-itanium-patches`
- Usage: `enable-itanium-patches enable|disable`

To enable importing of Windows Server IA64 patches:

1. Log in to the SA Core as root.
2. Run the enable-itanium-patches script:

```
/opt/opsware/mm_wordbot/util/enable_itanium_patches enable
```

To disable importing of Windows Server IA64 patches:

1. Log in to the SA Core as root.
2. Run the enable-itanium-patches script:

```
/opt/opsware/mm_wordbot/util/enable_itanium_patches disable
```

To view the current setting:

1. Log in to the SA Client as an administrator with Opsware System Administrators privileges.

**Note:** SA configuration parameters are accessible only through the SA Client. Only system administrators with the Opsware System Administrators user group permission can change these settings.

2. Navigate to the SA Software Repository system settings: **Administration > System configuration > Software Repository.**

The `patchman.ms_mbsa20_import_architectures` setting will indicate enabled or disabled.

- ['x86', 'x64'] is the default
- ['x86', 'x64', 'ia64'] indicates that Itanium patches are enabled

**Note:** Do not change this setting from this view; use the script instead. Only use this view to verify the current setting. Changes to certain SA Core configuration parameter values, as listed in this document, are verified by HP and you can safely apply them as directed. However, exercise caution when modifying any default SA Core configuration parameter values as modifications can have a negative effect on core functionality and performance.

## Export 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:

- **ServerName:** 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.

## Patch uninstallation

Patch Management provides granular control over how and under what conditions 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.

## 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.

The following table lists the default uninstallation flags used in SA.

### Default uninstallation flags

Windows patch types	Flags
Windows Hotfix	-q -z
Security Rollup Package	-q -z

### Default uninstallation flags, continued

Windows patch types	Flags
Windows OS Service Pack	Not uninstallable

## Uninstall a Windows patch

You can uninstall a Service Pack if it was originally installed by SA and can be uninstalled 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:

- ["Set uninstall options" on page 237](#)
- ["Set reboot options for a Windows patch installation" on the next page](#)
- ["Specify install scripts for a Windows patch uninstallation" on page 89](#)
- ["Schedule a Windows patch uninstallation" on page 90](#)
- ["Set up email notifications for a Windows patch uninstallation" on page 90](#)
- ["View job progress of a patch uninstallation" on page 91](#)

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.

## Set 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.

## Set 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.

**Note:** 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.

**Note:** 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 ["Find servers that require a reboot" on page 92](#).

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 and 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.

## Specify 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 SA 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 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**.

## Schedule 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.  
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.

Click **Next** to go to the next step or click **Cancel** to close the Uninstall Patch window.

## Set 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.

## Preview 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 the imported patch database.

**Note:** 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.

## View 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 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" in the SA Administration Guide.

**Note:** Some secondary binaries may fail to uninstall because prior binaries already uninstalled the same components; some may fail because they were non-installing components originally, such as a script that edits the registry. In these cases, a File Not Found error may appear. To verify the uninstall, run a compliance scan.

## Searching for patches and patch policies

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.

## Find 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.

### Note:

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” in the SA User Guide.

## 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" in the SA User Guide.

## Reboot required for multiple servers and 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" in the SA User Guide.

## Change the SA patching mode

Depending on your network infrastructure, you can choose to import the Windows patching database into SA either from a WSUS server or from the offline catalog of Microsoft patches.

Unlike the **Offline Catalog** mode, **WSUS** patching requires access only to the WSUS server on your network from where it can retrieve both security and non-security updates.

To change your current patching mode:

1. Go to **Administration > Patch settings** and enable either the **Offline Catalog** or the **WSUS** option.
2. Run a new metadata import to tag all patches in the database with the new patch source. This enables SA to update the patch library and use the right source when importing the binaries for existing patches.

## Disconnect SA managed servers from WSUS

If you are no longer using a WSUS infrastructure for patching your SA Windows servers, disconnect these servers from WSUS before switching SA to **Offline Catalog** patching mode.

This ensures that your SA managed servers are no longer visible on the WSUS side and removes any WSUS information from their Windows registries.

To disconnect SA managed servers from WSUS:

1. Go to **Devices > Servers > All Managed Servers** and right-click on the server that you want to disconnect from WSUS.
2. Select **Run Script > Select Script** and browse for **Configure Server With Offline Catalog** from the list of saved scripts. This launches the **Configure Server With Offline Catalog.bat** script file from **Library > By Folder > Opware > Tools > Patching**.
3. Click **Next** on the **Run Script** wizard and specify any custom script options before starting the job.

## Troubleshoot WSUS errors

These troubleshooting topics detail the possible errors you might encounter when working in **WSUS** patching mode.

To fix these issues, review the **Solution** section of each troubleshooting topic and check the list of known issues in the SA Release Notes.

["Cannot install or uninstall software in WSUS mode" below](#)

["Mesh conflicts after importing patches" on the next page](#)

["Vendor patch key error when importing metadata" on the next page](#)

## Cannot install or uninstall software in WSUS mode

### Symptoms

Running any patch or software management job on SA managed servers fails with the following error message:

The operation to install or uninstall software failed.Execution error:

[...]

OpwareError:

been\_cascaded: 0

error\_id: None

error\_name: cogbot.WUAerror

faultCode: 101

faultString: cogbot.WUAerror

hostname: dimsum33

line: 1696

method: searchCatalog

module: nt\_patch\_lib.py

params: {'message': 'WUA searchCatalog error, db path :None'}

request: UNKNOWN

[...]

## Causes

Your managed servers are not connected to the WSUS server although the SA core is set to **WSUS** patching mode.

## Solution

See "[Connecting SA managed servers to WSUS](#)" on page 44.

## Mesh conflicts after importing patches

### Symptoms

After importing patch metadata in **WSUS** patching mode, SA shows a list of mesh conflicts in the **Conflict** view.

### Cause

You have enabled **WSUS** patching mode on a core while another core in the SA mesh is trying to import patches from the **Offline Catalog**.

SA cannot synchronize incompatible patching actions across the cores of a mesh.

### Solution

1. Make sure that all your mesh cores are set to the same patching mode.
2. Check any scheduled cron jobs to make sure you are not running the **populate-opsware-update-library** script while the **WSUS** patching mode is enabled on a core.
3. Resolve all the reported mesh conflicts.

## Vendor patch key error when importing metadata

### Symptom

SA shows the following error message when importing patch metadata from WSUS:

*"Vendor patch key x is not unique. Remove patches [x, x] associated with this VPK and reimport the patch metadata"*

### Cause

The WSUS patch metadata importer is trying to import a patch which has more than one duplicate in the SA Patch Library. These duplicates have been previously imported from the Microsoft Offline Catalog and/or from HPLN.

### Solution

Remove duplicate patches from the SA library and reimport patch metadata from WSUS:

1. Go to **Library > Patches > Windows > [your Windows version]**.
2. In the **Object ID** search field, enter the patch IDs listed in the error message.
3. Right-click on each duplicate patch and select **Delete**.
4. Go to **Administration > Patch Settings > WSUS Patching Mode** and click **Import Metadata** on the **Patch Database** page.
5. Click **Start Job** on the **Run Server Script** wizard.

## Patch management for HP-UX

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 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 103.
- 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`.

## 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.

- ["Installing an HP-UX patch" below](#)
- ["Setting HP-UX install options" on the next page](#)
- ["Setting reboot options" on the next page](#)
- ["Specifying Install Scripts for a HP-UX patch installation" on page 99](#)
- ["Scheduling a Patch Installation for Remediation" on page 100](#)
- ["Setting up email notifications" on page 100](#)
- ["Previewing a patch installation" on page 100](#)
- ["Viewing job progress" on page 102](#)

## 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 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, We recommend 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 a HP-UX 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 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 or post-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**. To specify the script, click **Select**. An Ad-Hoc script runs only for this operation and is not saved in Server Automation.
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 and Password. 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 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

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 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. 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.
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.

The screenshot shows the 'Remediate' application window with the 'Preview' tab selected. The left sidebar contains navigation options: 'All Steps' (Servers and Policies, Options, Preview, Scheduling, Notifications, Job Status) and 'Help' (Preview, More help...). The main area displays a table of actions for target 'm195.qa.opsware.com'. The table has columns for 'Action' and 'Status'. The actions listed include various patch installations (e.g., PHCO\_36744-1.0, PHCO\_36744.LUX-TCH-U-MSG-1.0, PHCO\_36744.LVM-MIRROR-RUN-1.0) and a registration step. The status for most actions is 'Pending'. Below the table, there are tabs for 'Output' and 'Errors', and a 'Job Messages' section with a message: 'The unit is added to the list as it is a dependent unit. The unit was pulled in by patch dependency resolver. This unit is superseded by unit PHCO\_38717. Please replace the unit with the newer unit.'

Action	Status
Install and Reboot   PHCO_36744-1.0	Pending
Install   PHCO_36744-1.0	Pending
Install   PHCO_36744.LUX-TCH-U-MSG-1.0	Pending
Install   PHCO_36744.LVM-MIRROR-RUN-1.0	Pending
Install   PHCO_36744.LVM-RUN-1.0	Pending
Install   PHCO_36744.LUX-FRE-I-MSG-1.0	Pending
Install   PHCO_36744.LUX-FRE-U-MSG-1.0	Pending
Install   PHCO_36744.LUX-GER-I-MSG-1.0	Pending
Install   PHCO_36744.LUX-GER-U-MSG-1.0	Pending
Install   PHCO_36744.LUX-ITA-I-MSG-1.0	Pending
Install   PHCO_36744.LUX-ITA-U-MSG-1.0	Pending
Install   PHCO_36744.LUX-JPN-E-MSG-1.0	Pending
Install   PHCO_36744.LUX-JPN-S-MSG-1.0	Pending
Install   PHCO_36744.LUX-JPN-U-MSG-1.0	Pending
Install   PHCO_36744.LUX-KOR-E-MSG-1.0	Pending
Install   PHCO_36744.LUX-KOR-U-MSG-1.0	Pending
Install   PHCO_36744.LUX-SCH-H-MSG-1.0	Pending
Install   PHCO_36744.LUX-SCH-U-MSG-1.0	Pending
Install   PHCO_36744.LUX-SPA-I-MSG-1.0	Pending
Install   PHCO_36744.LUX-SPA-U-MSG-1.0	Pending
Install   PHCO_36744.LUX-TCH-B-MSG-1.0	Pending
Install   PHCO_36744.LUX-TCH-E-MSG-1.0	Pending
Install   PHCO_36744.LVM-ENG-A-MAN-1.0	Pending
Registration   Register	Pending
Test Compliance   Software Compliance	Pending

## 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.
  - FinalReboot: 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.

## Supported operating systems

See the SA Support and 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".

"Options of `import_hpux_depot`" below describes the script's options.

#### 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</code> How to split each depot (default: product): 'product', 'instance', 'none'	Products that are already in the SA Library are not re-imported unless <code>--force</code> is specified.  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

Options of import\_hpux\_depot, continued

Option	Description
	<p>depot. The split behavior is controlled by the --split option:</p> <p>none—Source depots are not split but are imported as is.</p> <p>product—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.</p> <p>instance—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. Source depots are split by product. No HPUXPatchBundleUnits will be created and individual depot files will be generated for each product. If a depot contains multiple instances of the same product (by name), the instances are kept together. This is the default.</p>
--timeout=USER_TIMEOUT	Override default timeout values (2 hours if split is 'none', else 5 minutes)
-u USERNAME, --username=USERNAME	Upload packages as specified user (default: opsware).
-v, --verbose	Display verbose output
--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

"Options of the HP-UX Metadata Script" below describes the script's options.

### 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 all.



### Options of the HP-UX Metadata Script, continued

Option	Description
-c HPUX_SW_CATALOG_FILE, --catalog_file=HPUX_SW_CATALOG_FILE	Specifies the source location of the HP-UX software catalog file. The swa_catalog.xml catalog file can be downloaded from ftp://ftp.itrc.hp.com/export/patches. 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 all.
-f, --force	Forces catalog upload. If catalog upload is specified, either through the -u and -p options or the -c option, this option ensures that a new catalog will be uploaded even if checksum matches current catalog.
-h, --help	Displays the help message.
-n, --no_supersedence	Flag is used with the -a 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.
-p PASSWORD, --password=PASSWORD	The password that is required to access the itrc.hp.com website to automatically download the swa_catalog.xml file. Both user ID and password must be specified.
-t TEST_OPTION, --test=TEST_OPTION	Test mode option. Options are 'bundle', 'product' and 'all'.
-u USERID, --user=USERID	The user ID that is required to access the itrc.hp.com website to automatically download the swa_catalog.xml file. Both user ID and password must be specified.
-w UPLOAD_WAIT, --wait=UPLOAD_WAIT	Specifies the number of seconds to wait between file uploads and subsequent updates when the catalog upload is specified. If 'optimistic concurrency' failures occur, this value may need to be increased.

## 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.

## Create an HP-UX software policy

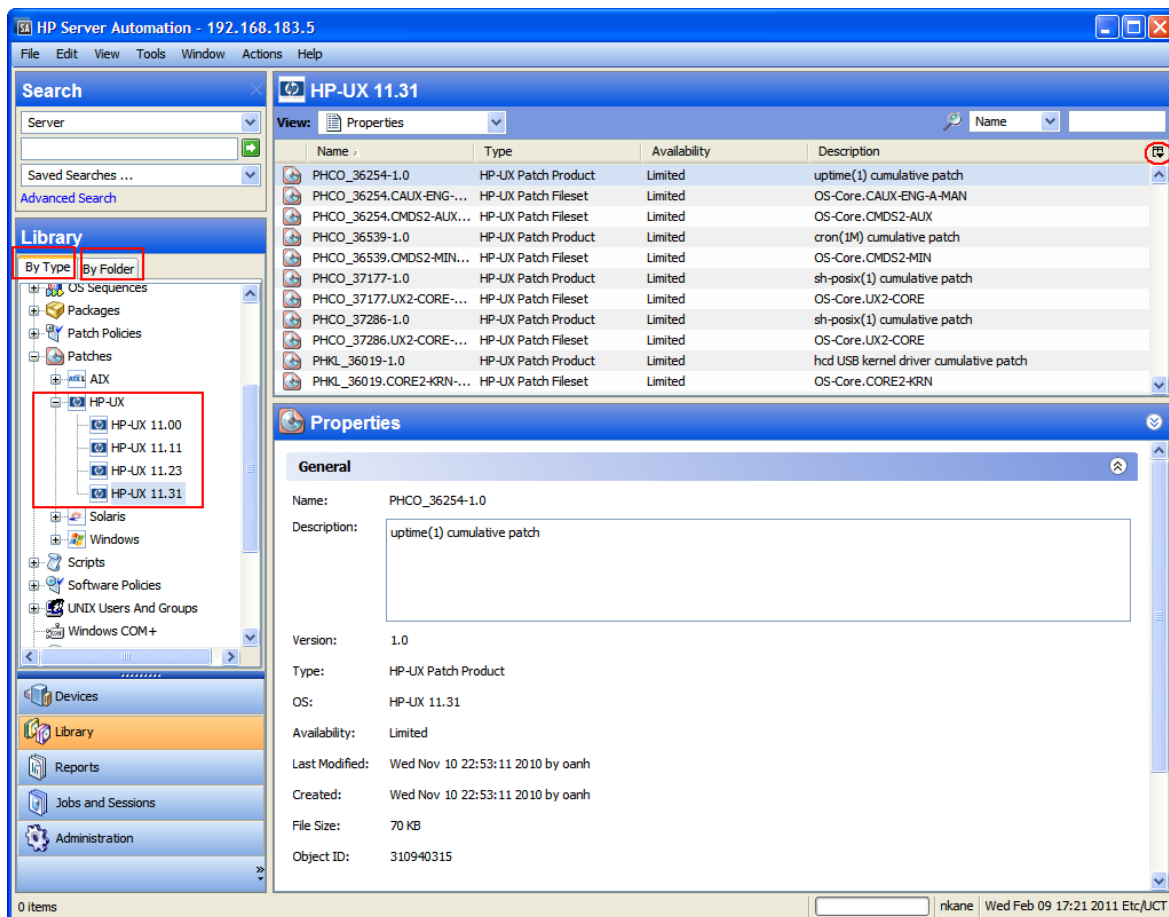
In the SA Client, you create a software policy by using either one of the following Library features:

- "Library—By Type" below
- "Library—By Folder" on the next page

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.

### 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 > ByType > SoftwarePolicies > 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 > ByFolder**. 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 > SoftwarePolicy** 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**.

## View an HP-UX software policy


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

- ["Search" on the next page](#)
- ["Devices" on the next page](#)

- ["Library—By Type" below](#)
- ["Library—By Folder" on the next page](#)

## 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.
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 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**.

## Edit 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 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 "[Create an HP-UX software policy](#)" on page 106 for guidelines about information in these fields.
5. After you have made your changes, from the File menu, select **Save**.

## Add 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 "[Remove software from a software policy](#)" below for more information about this action.
10. From the File menu, select **Save** to save the changes you made to the policy.

## Remove 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.

## View 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.

## View 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.

## Find a software policy in folders

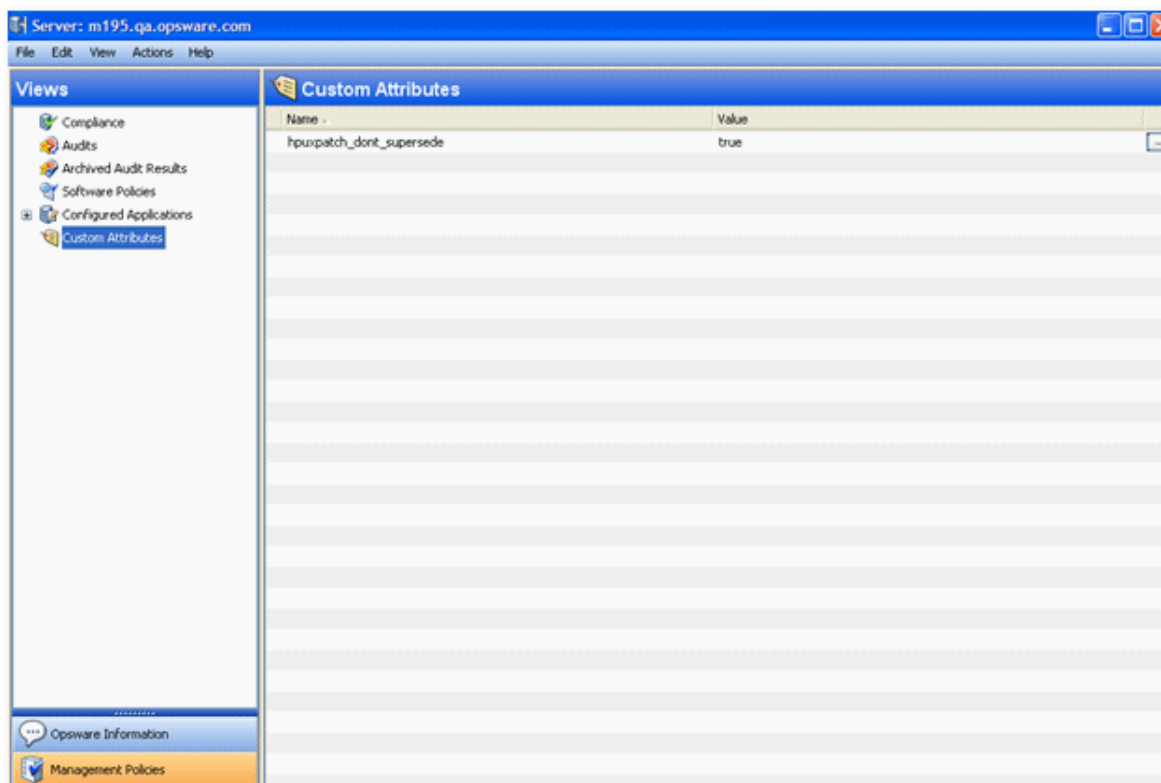
To find an HP-UX software policy in the folder hierarchy:

1. In the navigation pane, select **Library > ByType > 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.

### 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.

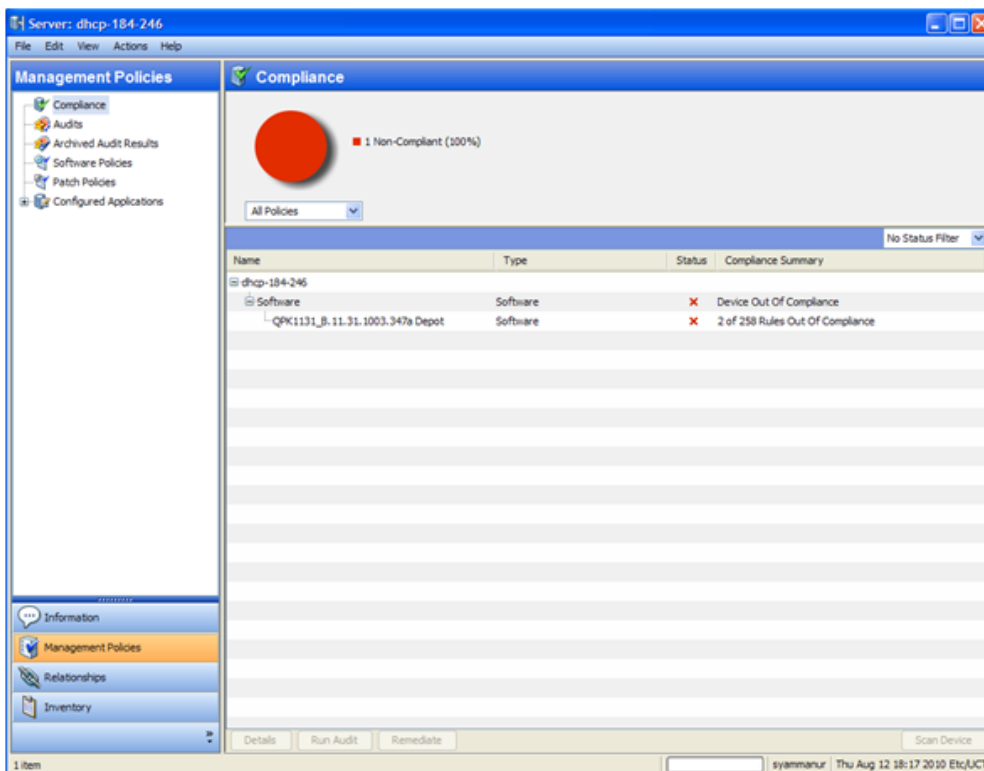
The SA Client displays the following compliance information for a patch policy:

#### Compliance status for a managed server

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

See the following figure for an example of patch compliance status for the Standard HP-UX bundle.

#### 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 uninstallation

Uninstalling HP-UX patches and bundles are 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.

## Patch management for Solaris

In Server Automation (SA), patch management for Solaris enables you to identify, install, and remove Solaris patches and IPS packages, 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:

## Supported operating system version

OS version	Architecture
Solaris 10 (Update 1 through Update 9)	Sun SPARC, 64bit x86, 32 bit x86, and Niagara
Solaris 11	Sun SPARC, 64bit x86, 32 bit x86, and Niagara

In Oracle Solaris 11, a patch unit is referred to as an Image Packaging System (IPS). IPS is a network-based package management system that provides a framework for software lifecycle management such as installation, upgrade and removal of software packages. For information and instructions specific to Solaris 11, see ["Patch management for Solaris 11 " on page 160](#).

See the SA Support and Compatibility Matrix for complete Managed Server platform support information.

## Features

SA automates Solaris patching by enabling you to:

- **Determine which patches and IPS packages your managed servers need.**

SA can determine the patches and IPS packages 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, IPS packages 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 and IPS packages in the correct install order.
- **Install Solaris patches, patch clusters and IPS packages on managed servers.**

SA allows you to directly install Solaris patches, patch clusters and IPS packages 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, patch bundles and IPS packages 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. (See ["Troubleshoot Solaris patch installation" on page 125](#) for additional tips about install modes.)

- **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.

## 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 policies, 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. See "[Troubleshoot Solaris patch installation](#)" on page 125 for additional tips about install modes.
  - **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.

- i. Log in as root to the SA core where the SA patch has been installed.
- ii. Locate the log file from the patch install, which is typically located at:  
`/var/log/opsware/install_opsware/patch_opsware.<time stamp>.log`
- iii. Search this log file for a message with “update\_supplements.” For example, you could use the following grep command:  
`grep update_supp patch_opsware*`
- iv. 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.
- v. Log in as root to an SA core system where the `solpatch_import` command is installed.
- vi. Change to the directory where the `solpatch_import` command is:  
`/opt/opsware/solpatch_import/bin.`
- vii. Run the following command:  
`./solpatch_import -a update_supplements`
- viii. 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.

## 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 `-a policy` or `--action=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.

## 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/bin/solpatch_import --manual
```

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

## 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 at `/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 ["Maintain the Solaris patch database" on page 147](#).

## Install 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 130](#).

## Install 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.

## Install 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.

## Detect 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. Select the **Administration** tab in the SA Client.
3. In the navigation pane select **System Configuration > Configuration Parameters**. This displays the SA components, facilities and realms that have system configuration parameters.

4. In the list of SA components, select **Command Engine**. This displays the system configuration parameters for this component.
5. Locate the parameter `way.remediate.sol_parse_patchadd_output` and set it to 1.
6. Click **Revert** to discard your changes or **Save** to save your changes.

## Install 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" below](#)
- ["Attaching a server to a patch policy" below](#)

### 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.

**Note:** 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.

## Remediate 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 Software Management.

- ["Analyzing patch applicability" below](#)
- ["Install parameters " on the next page](#)
- ["Rebooting options" on the next page](#)

### 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

The following figure 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" below](#).

### Install Parameters in the Patch Properties window

The screenshot shows a window titled "Install Parameters" with the following settings:

- Install Flags:** An empty text input field.
- Reboot Required:** Radio buttons for "Yes" (selected) and "No (Oracle default)".
- Install Mode:** Radio buttons for "Single User Mode" and "Multi User Mode (Oracle default)" (selected).
- Reboot Type:** Radio buttons for "Standard (Oracle default)" (selected) and "Reconfiguration".
- Reboot Time:** Radio buttons for "Normal (Oracle default)" (selected) and "Immediate".

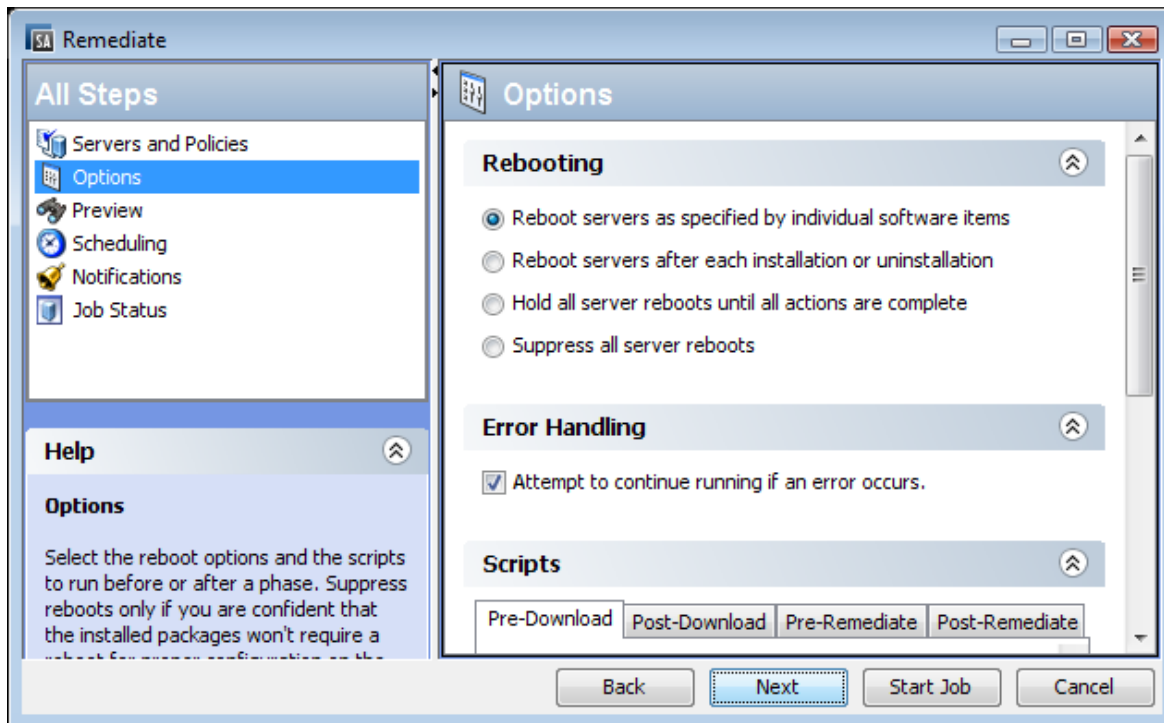
- **Install Flags:** (Optional) Arguments that are used when the patch or patch cluster is installed on a managed server.
- **Reboot Required:** Specifies whether the managed server will be rebooted when the patch or patch cluster is successfully installed. Oracle’s recommendation is labeled “Oracle 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.

## 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. The following figure shows the Options settings for the Remediate patch policy job.

## Rebooting Options window



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 all actions are complete: 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.)

## Troubleshoot Solaris patch installation

### Changing the Solaris patch install mode

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.
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:
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 path installation fails.

## Mounting the staging directory in single-user mode

When one item in a remediation process requires a server to restart in single-user mode it can prohibit the rest of the items from being processed if the item is stored in an atypical directory that is not available in single-user mode.

Single-user mode will need to mount the staging directory upon startup. The default staging directory is `/var/opt/opsware/agent`. If the next item is not in the default directory, then the remediation process will not be able to find it and the job will fail.

To resolve this, the managed server just needs to mount the staging directory where the items are stored prior to running the remediation. The simplest way to do this is to write a server script with mount instructions and add it to an existing Solaris start-up script.

For example:

```
echo "mount<stage_dir>">>/etc/rcS.d/S99mount_stage
```

where '`<stage_dir>`' is the directory where the item is stored and '`/etc/rcS.d/S99mount_stage`' is the start-up script on a Solaris managed server.

## Install 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 ["Create a Solaris patch policy" on page 133](#).
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.

## Patch management process

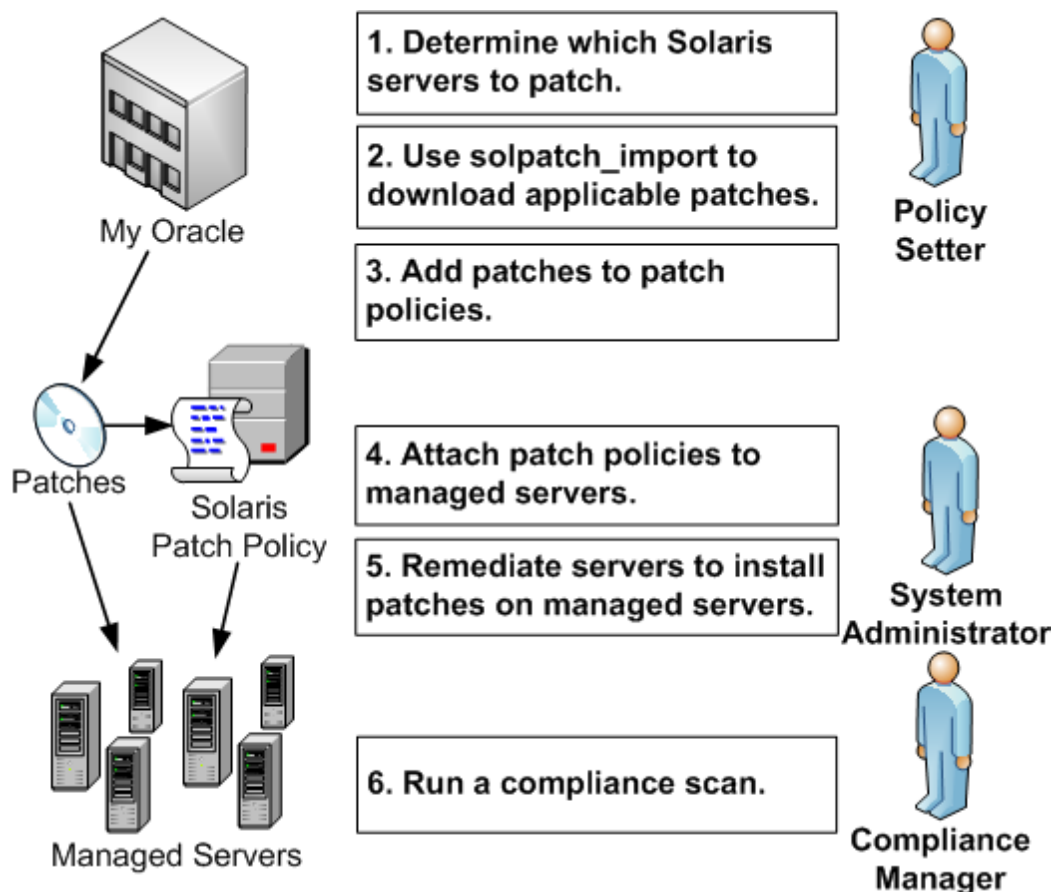
There are two main use cases in Solaris patching:

- ["Patching selected servers" on the next page](#)
- ["Installing selected patches" on page 129](#)

## Patching selected servers

The following figure 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.

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.

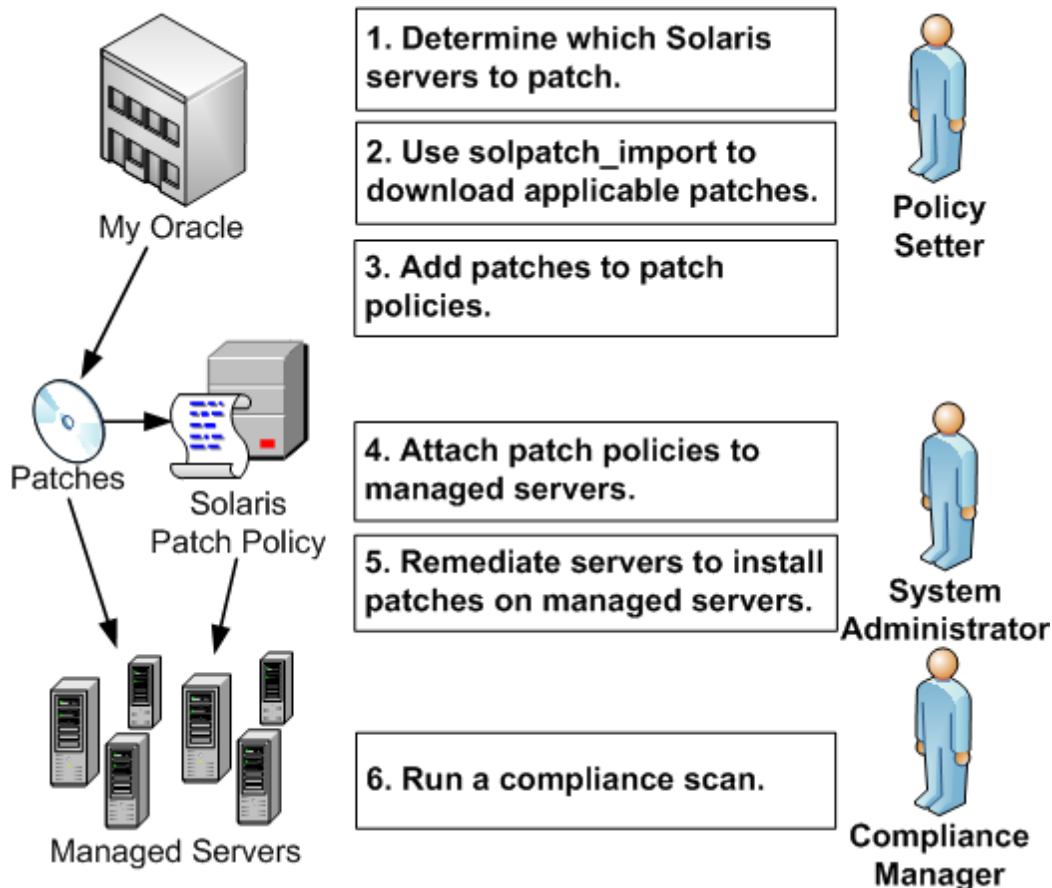


4. A system administrator attaches the patch policies to managed servers.  
Your system administrator can test the patches by attaching the patch policy to one or more test servers, to make sure they behave as expected. If problems occur, you can add or remove patches from the patch policy and then test 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 selected patches

The following figure 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.

### 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:

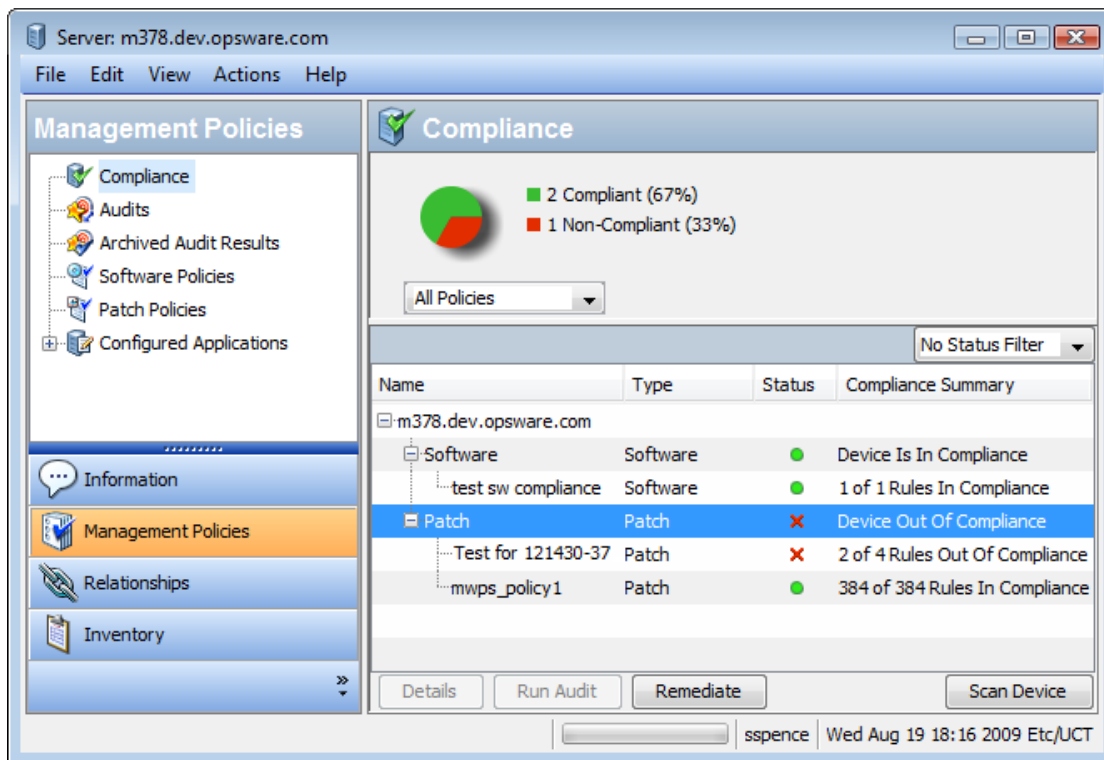
- If a policy contains a patch for the package “SUNWpkgA”, but “SUNWpkgA” is not installed on a particular server, the patch is not applicable to that server and that patch will not impact the results of the compliance scan for that server. The Compliance Summary does not include non-applicable patches. 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 ["Resolve patch dependencies" on page 138.](#))
- 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 ["Install manual patches—patchadd" on page 121.](#)

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.

The following figure 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.

**Compliance results for a Solaris server**



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

**Compliance status for a managed server**

Compliance Icon	Compliance Status	Description
	Compliant	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.
	Non-compliant	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.
	Scan Started	The patch compliance information is currently being gathered.
	Scan Failed	The patch compliance scan was unable to run.

### Compliance status for a managed server, continued

Compliance Icon	Compliance Status	Description
☐	Scan Needed	The patch compliance information needs to be gathered or the compliance information may be inaccurate.
—	Not Applicable	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.

## Run 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.
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 User 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:

- ["Create a Solaris patch policy" below](#)
- ["View a Solaris patch policy" on page 135](#)
- ["Edit a Solaris patch policy" on page 136](#)
- ["Add a Solaris patch to a patch policy" on page 136](#)
- ["Remove a patch from a Solaris patch policy" on page 137](#)
- ["Resolve patch dependencies" on page 138](#)
- ["Custom attributes" on page 141](#)
- ["View patch policy history" on page 142](#)
- ["View software policies associated with a patch policy" on page 142](#)
- ["View OS sequences associated with a patch policy" on page 142](#)
- ["View servers attached to a patch policy" on page 142](#)
- ["Find a Solaris patch policy in folders" on page 143](#)

## Create a Solaris patch policy

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

You must have permissions to create and manage a Solaris patch policy. To obtain these permissions, contact your system administrator. See the 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"
```


## View a Solaris patch policy

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

- ["Search" below](#)
- ["Devices" below](#)
- ["Library—By Type" on the next page](#)
- ["Library—By Folder" on the next page](#)

## 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.
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 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.

## Edit 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 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 ["Create a Solaris patch policy" on page 133](#) for guidelines about information in these fields.
6. After you have made your changes, from the File menu, select **Save**.

## Add 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.




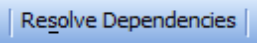
You must have permissions to add Solaris patches, Solaris patch clusters, and server scripts to a Solaris patch policy. To obtain these permissions, contact your system administrator. See the SA Administration Guide for more information about these permissions.

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.


## Remove 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.

## Resolve 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.

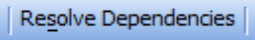
When you add patches manually to a patch policy, SA can determine the dependencies for all patches in the patch policy.

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.

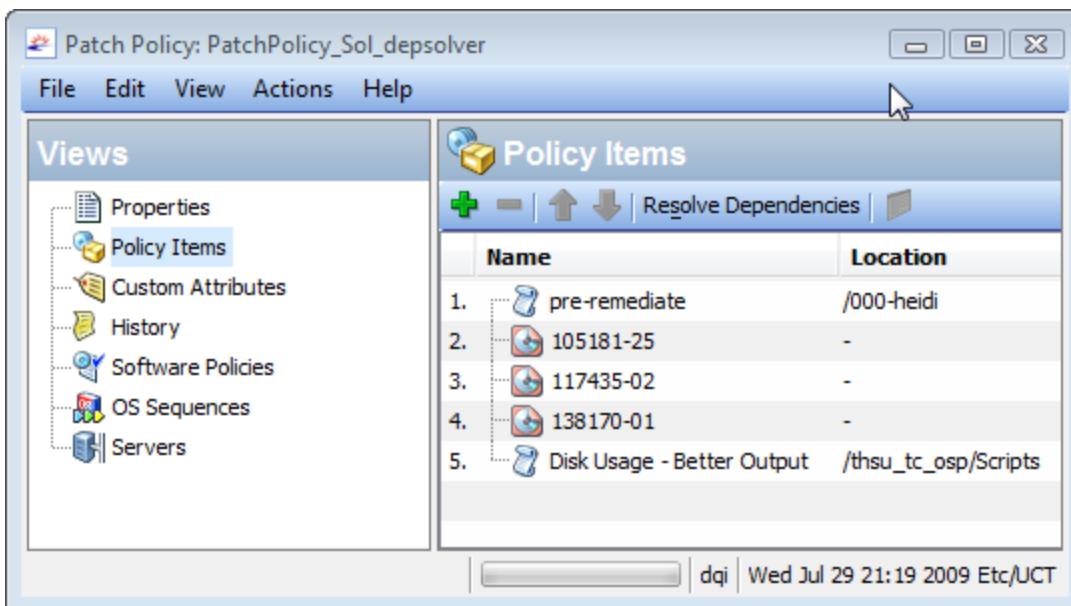
To resolve dependent patches in a patch policy:

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

The following figure 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

### **Solaris patch policy: Resolve dependencies**



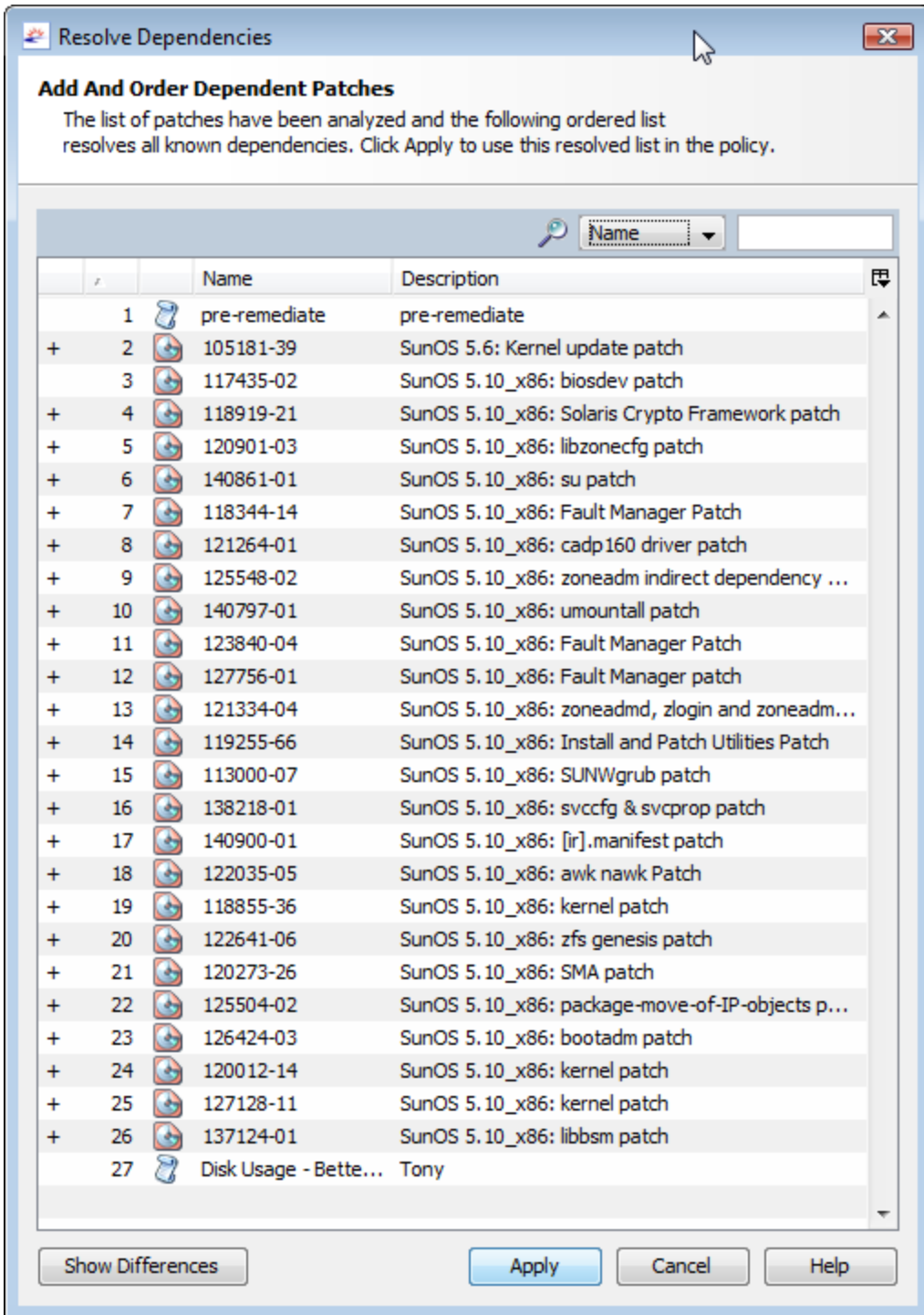
The following figure shows the results of selecting Resolve Dependencies for this patch policy. The following changes have been made to this patch policy:

- 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.

**Note:**

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.

**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.

### 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.

## View 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.

## View 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.

## View 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.

## View 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.

## Find 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:

- ["Patches and patch clusters" below](#)
- ["Run solpatch\\_import" on page 145](#)
- ["Initialize the Solaris patch database" on page 146](#)
- ["Maintain the Solaris patch database" on page 147](#)
- ["Retrieve the latest patch data from Oracle" on page 147](#)
- ["Retrieve the Solaris patch supplementary data file" on page 147](#)
- ["Manually download the Solaris patch supplementary data file" on page 148](#)
- ["Find Solaris patches" on page 149](#)
- ["Import a patch or patch cluster" on page 151](#)
- ["solpatch\\_import" on page 152](#)
- ["Import a Solaris patch to SA Client" on page 152](#)
- ["Export a patch or patch cluster" on page 153](#)
- ["Open a Solaris patch" on page 153](#)
- ["Manage properties" on page 154](#)
- ["Import custom documentation" on page 159](#)
- ["Solaris zones" on page 159](#)

## Patches and patch clusters

The SA Client provides the following capabilities that help you manage Solaris patches and patch clusters:

- ["Viewing patch cluster contents" below](#)
- ["Viewing patch clusters associated with a patch" below](#)
- ["Viewing software policies associated with a patch or patch cluster" below](#)
- ["Viewing patch policies associated with a patch or patch cluster" on the next page](#)
- ["Viewing patch policies associated with a patch or patch cluster" on the next page](#)
- ["Deleting a patch or patch cluster" on the next page](#)

## 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 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.

## 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**.

## Run solpatch\_import

**Note:** 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:

#### 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.
“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
```

## Initialize 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
```

3. 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.

**Note:**

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

4. Make sure your Solaris patch database contains the latest patch information. See "[Maintain the Solaris patch database](#)" below.

## Maintain the Solaris patch database

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

- "[Retrieve the latest patch data from Oracle](#)" below
- "[Retrieve the Solaris patch supplementary data file](#)" below
- "[Retrieve the Solaris patch supplementary data file](#)" below

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

### Retrieve 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
```

### Retrieve 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 Live Network. When HP updates this supplementary data, you can configure the HP Live 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 an HP Passport ID from:  
<http://h20229.www2.hp.com/passport-registration.html>

2. Log in to the HP Live Network portal using your HP Passport credentials:  
<https://hpln.hpe.com/group/hp-live-network-connector>
3. The HP Live Network connector (LNC) is installed on the core server where the SA Software Repository component is installed.  
You can download the HP Live Network Connector User Guide from the Live Network Connector community on the HP Live Network at:  
<https://hpln.hpe.com/group/hp-live-network-connector>  
Click the Resources tab and open the Documentation folder.
4. 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
```
5. (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 Live Network and upload it to the SA database. See "[Manually download the Solaris patch supplementary data file](#)" below.

## Manually download the Solaris patch supplementary data file

This section describes how to manually download the supplementary Solaris patch data file from the HP Live 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 "[Retrieve the Solaris patch supplementary data file](#)" on the previous page. 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 an HP Passport ID from:  
<http://h20229.www2.hp.com/passport-registration.html>
2. Log in to the HP Live Network portal using your HP Passport credentials:  
<https://hpln.hpe.com/group/hp-live-network-connector>
3. The HP Live Network connector (LNC) is installed on the core server where the SA Software Repository component is installed.  
You can download the HP Live Network Connector User Guide from the Live Network Connector community on the HP Live Network at:  
<https://hpln.hpe.com/group/hp-live-network-connector>  
Click the Resources tab and open the Documentation folder.
4. Click Content Catalog from the HP Live Network menu and search for "Solaris Patching for Server Automation" under the Server Automation product.
5. Download the latest Solaris patching package, named `solpatchdb_supplement.zip`, and place it in the 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.

## Find 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.

### Specifying actions for the `solpatch_import` Command

Option to <code>solpatch_import</code> command	Description
-a show or --action show	Displays information about the specified patches.
-a import or --action import	Downloads the specified patches and imports them into the SA Library.
-a policy or --action policy	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.

"[Specifying desired patches with the Filter option to `solpatch\_import`](#)" below lists the `solpatch_import` command filters that specify which Solaris patches you want:

### 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	rec server	-f "rec,server=sys01.hpe.com"	Specifies all patches recommended by Oracle for the

### Specifying desired patches with the Filter option to solpatch\_import, continued

Desired set of patches	Filter options to use	Example filter option	Description of example Filter option
for a particular server			sys01.hp.com managed server.
All patches recommended by Oracle for a set of servers	rec platform	-f "rec,OS=5.10"	Specifies all patches recommended by Oracle for all managed servers running Solaris 5.10.
All Oracle security patches for a particular server	sec server	-f "sec, server=sys01.hpe.com"	Specifies all Oracle security patches for the sys01.hp.com managed server.
All Oracle security patches for a set of servers	sec OS	-f "sec, OS=5.9"	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.	rec sec server	-f "rec, sec, OS=5.8"	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" below](#)
- ["Finding Oracle recommended patches for your servers" on the next page](#)
- ["Finding Oracle security patches for your servers" on the next page](#)
- ["Finding a specific set of patches" on the next page](#)

For complete information, run `solpatch_import --manual` as described in ["Run solpatch\\_import" on page 145](#).

### 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.hpe.com"
solpatch_import --action=import --filter="server=sys01.hpe.com"
solpatch_import --action=policy --policy_path="SolPatches/MyPolicy"\
  --filter="server=sys01.hpe.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 ["Run solpatch\\_import" on page 145](#).

## Import 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.

## Import a Solaris patch to SA Client

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 the following table.

### Patch availability property settings

Patch availability setting	Description
Available	The patch has been imported into SA, has been tested, and can be installed on managed servers.
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.
Deprecated	The patch cannot be added to patch policies but can still be installed.
Not Imported	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
```

## Export 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**.

## Open a Solaris patch

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

- ["Search" below](#)
- ["Library—By Type" on the next page](#)
- ["Library—By Folder" on the next page](#)

## 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

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.

## Manage 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.

### **Patch Properties window**

**Views**

- Properties
- Custom Documentation
- Patch Cluster(s)
- Software Policies
- Patch Policies
- Servers

**Properties**

**General**

Name: 139997-03

Description: SunOS 5.10\_x86: i.rbac and patch postinstall patch

Version: 139997-03

Status: Released

Readme URL: <http://sunsolve.sun.com/search/printfriendly.do?asset...>

Type: Solaris Patch

OS: SunOS 5.10 X86

Availability: Limited

Last Modified: Tue Jul 20 00:29:15 2010 by heidi

Created: Tue Jul 20 00:29:12 2010 by heidi

File Name: 139997-03.zip

File Size: 81.72 KB

Object ID: 939090489

**Dependencies**

**Install Parameters**

**Install Scripts**

**Uninstall Parameters**

**Uninstall Scripts**

0 items | sspence | Fri Jul 23 21:15 2010 Etc/UCT

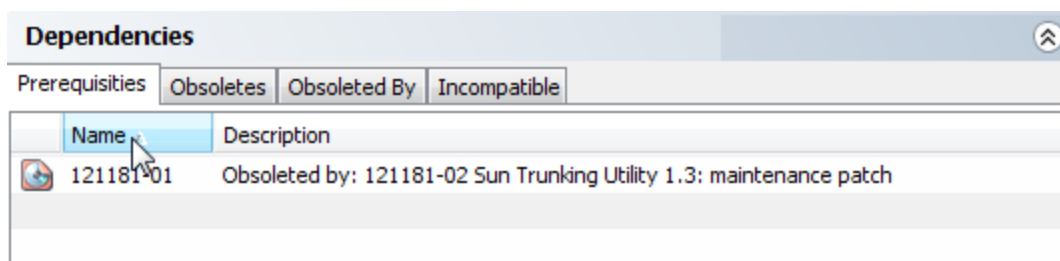
## General properties

- 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

The following figure shows the dependencies for a patch in the Patch Properties window.

### 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

The following figure 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 124](#).

### Install Parameters in the Patch Properties window

The screenshot shows a window titled "Install Parameters" with the following settings:

- Install Flags:** An empty text input field.
- Reboot Required:** Radio buttons for  Yes and  No (Oracle default).
- Install Mode:** Radio buttons for  Single User Mode and  Multi User Mode (Oracle default).
- Reboot Type:** Radio buttons for  Standard (Oracle default) and  Reconfiguration.
- Reboot Time:** Radio buttons for  Normal (Oracle default) and  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. (See "[Troubleshoot Solaris patch installation](#)" on [page 125](#) for additional tips about install modes.)
- **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.

**Note:**

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:

- a. In the Patch window, select a patch.
- b. Right-click to open the Patch Properties.
- c. 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:

- a. In the navigation pane, select **Library>By Type>Patches**. The patches are organized by operating system. Navigate to an OS version.
- b. In the content pane, select a Solaris patch, patch cluster, or patch bundle to view.
- c. From the Actions menu, select **Open**. This displays the patch information window.
- d. In the Views pane, select **Properties**. This displays information about the patch, including a URL link to the patch information.
- e. Select the Readme URL and enter your My Oracle credentials to view the vendor information.

## Import 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**.

## Solaris zones

The SA Client provides the following capabilities that help you manage Solaris zones:

- ["Patching Solaris zones" below](#)
- ["Viewing Solaris zones " on the next page](#)

## 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.

## Uninstall a Solaris 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.

## Patch management for Solaris 11



Oracle Solaris 11 uses IPS packages to deliver software and software updates. IPS (Image Packaging System) is a network-based package management system that is used for the entire software lifecycle, including package installation, upgrade and removal.

Server Automation's Solaris 11 platform support for server patching allows you to update your managed servers to the latest versions of existing software without installing new software. This is a powerful way to keep your system up to date in an environment that no longer supports explicit patch units.

Solaris 11 patching support leverages the existing Solaris patching functionality, with a few differences to adapt to the new Solaris IPS package delivery structure. Additionally, there are setup requirements for setting up the initial IPS Package database. This section describes the Solaris 11 Patching setup steps and the differences in SA patching with Solaris 11.



## Get started with Solaris 11 patching

The advantage of the IPS package structure is that it contains the metadata and the binaries, combined. IPS packages are used for everything from the initial software installation to the updates. Because IPS packages are so complete, they have internal integrity, which means they require the complete package and are not divided into patch units.

Because of these structural differences, there are some typical patching functions that are not relevant for Solaris 11.

The process for creating a vendor recommended patch policy is different. For example, Solaris 10 looks at installed packages and computes what needs to be updated based on the existing installations. With Solaris 11, Server Automation uses the IPS tools to find the recommended patches and their dependencies.

SA comes with a predefined software policy, Solaris 11 IPS Package Acquisition Tool, which enables you to set up the initial IPS Package database.

## Summary

Complete the following steps to set up your initial IPS Package database and enable Solaris 11 patching with SA. The initial IPS Package acquisition only needs to be done using one Solaris 11 managed server. After the initial acquisition, additional updates will need to be done periodically to maintain compliance. These instructions are just for the initial acquisition.

**RECOMMENDATION:** The entire IPS Package repository could be as large as 40 GB. To make sure there is ample room on your server, choose a Solaris 11 managed server with 100GB or more.

This summary has two parts:

- Set up your Solaris 11 IPS Package Database
- Create a recommended patch policy and remediate your Solaris 11 managed servers

Detailed instructions for each of these steps are provided under "[Set up Solaris 11 managed server for SA patching](#)" on the next page.

To set up your Solaris 11 IPS package database:

1. Remediate the chosen Solaris 11 managed server with the SA-provided software policy, Solaris 11 IPS Package Acquisition Tools.

This installs SA UAPI access and IPS import tools on the server, which will be used to acquire IPS packages from the vendor.

2. Complete the import prerequisite steps before importing IPS packages:
  - a. Setup Managed Server Customers to have visibility to all relevant IPS packages in the SA Library.
  - b. If your environment requires HTTP proxies to access the desired repository, set up the proxies on your managed server before attempting to import the IPS packages.
  - c. Configure `sol_ips_import.conf`
3. Import all IPS packages onto the core by running the IPS import script (`sol_ips_import`) from the

chosen Solaris 11 managed server.

4. If software registration has not yet occurred, run the Software Registration script (`bs_software`).

This completes the IPS Package Database set-up steps. Next, create the patch policy and remediate your Solaris 11 servers.

To create a recommended patch policy and remediate your Solaris 11 managed servers:

1. Create the recommended patch policy for the managed server by running the patch policy script (`solpatch_import`) on the core.
2. From the SA Client, attach the recommended patch policy to the server and remediate.

## Set up Solaris 11 managed server for SA patching

Use the following steps to set up Solaris 11 Managed Servers for SA Patching:

["STEP 1: Remediate the managed server with the Solaris 11 IPS Package Acquisition software policy" below](#)

["STEP 2: Complete the Import prerequisites" below](#)

["STEP 3: Import all IPS packages onto the core by running the IPS import script \(`sol\_ips\_import`\)" on page 165](#)

["STEP 4: Register the software" on page 168](#)

["STEP 5: Create the recommended patch policy \(run `solpatch\_import`\)" on page 168](#)

["STEP 6: Attach the recommended patch policy to a server and remediate " on page 169](#)

### STEP 1: Remediate the managed server with the Solaris 11 IPS Package Acquisition software policy

1. From the SA Client, navigate to SA Library > By Type and select **Solaris 11 IPS Package Acquisition Tools**.
2. From the Actions menu, select **Attach Server....**
3. Select Remediate Servers Immediately. (This option enables the remediation process to run immediately after attaching the servers.)
4. Select the desired servers to remediate and click Attach.
5. In the Remediate window, accept all remaining defaults and click Start Job to remediate the selected servers.

### STEP 2: Complete the Import prerequisites

- Grant a managed server's customer visibility to all relevant IPS Packages in the SA Library
- Granting customer visibility is a prerequisite to running the `sol_ips_import` script to import the IPS packages.

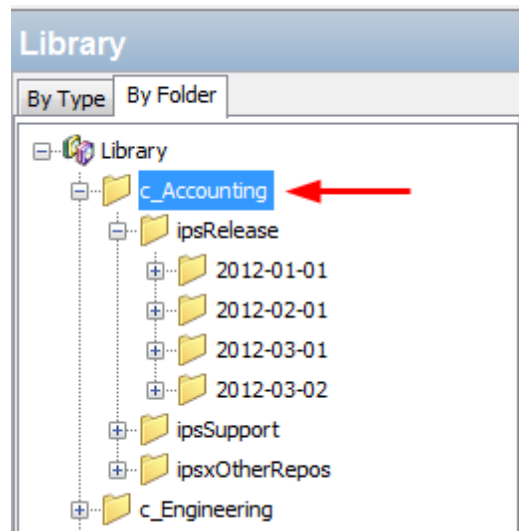
The IPS packages are delivered to a directory in the SA Library on the core, but the import script is run from the managed server. There is one customer per managed server and the customer governs the

managed server's visibility into the SA Library. When the `sol_ips_import` script runs, it bases the analysis of what to import on the set of IPS packages the managed server's customer can see. For this reason, the customer associated with the managed server where the import is being run must have visibility to all IPS packages.

To achieve that, grant the customer folder permission for the parent folder of the destination directory for the IPS packages.

1. Identify the managed server's customer from the managed server properties view.
  - a. From the SA Client, navigate to Devices and select the managed server you wish to update.
  - b. Select **View > Properties** to display the server properties in the details pane.
  - c. The customer is displayed under the Management Information section.
2. Grant IPS package folder permission to the customer:
  - a. From the SA Client, navigate to **SA Library > By Folder** and select the parent folder for the customer's Solaris 11 IPS packages.

For example, this is sample file structure for an "Accounting" customer:



In this example, the library has folders organized by customers; Accounting and Engineering. All the IPS packages associated with each customer are under the customer folders. In this case, you would select the "c\_Accounting" parent directory because you want to give the customer permission to the upper-most directory for that customer to make sure it has visibility to ALL the IPS packages.

- b. Select **Actions > Folder Properties > Customer** tab.
- c. Click Add and select the customer for the managed server with the IPS import tools.
- d. Click **Add** and then **OK**.

Running the `sol_ips_import` script without giving the managed server's customer visibility to this folder could have adverse effects. The customer's folder permissions affect what patches are recommended for the server. Without correct customer folder permissions, the script might unnecessarily re-upload thousands of patches to the core.

### Setting the HTTP proxies

If your environment requires HTTP proxies (e.g., `http_proxy`, `https_proxy`) to access your desired repository, make sure they are set correctly on your managed server before importing the IPS packages.

Configure the IPS package import configuration file (`sol_ips_import.conf`)

1. Setting up the `sol_ips_import.conf` configuration file before running the `sol_ips_import import` script is recommended to save time and improve reliability.
2. From a remote server window, log in to the Solaris 11 managed server.
3. Navigate to `/opt/opsware/solimport`
4. Open the configuration file: `sol_ips_import.conf`
5. Edit the configuration file to define your preferences for the IPS package download process:

IPS configuration file options defined

Configuration File option	Explanation and example
User name and password	Specify your SA login credentials
Local download directory	Specify the staging directory on your managed server where the packages are initially downloaded from the vendor.  For example: <code>download_dir=/var/&lt;UserFolderName&gt;/IPSPkg_Stage</code>  RECOMMENDATION: The entire IPS Package repository could be as large as 40 GB. To make sure there is ample room on your server, choose a Solaris 11 managed server with 100GB or more.
SA Folder Upload directory	Specify the final destination directory on the SA Core where the IPS packages will be stored.  For example: <code>core_destination_folder=/Home/&lt;AllSolaris11CustomersFolderName&gt;/</code>
URL of the IPS repository	Specify the URL of the vendor's IPS repository from which the packages will be acquired.  For example: <code>repo_url=https://pkg.oracle.com/solaris/support</code> or: <code>repo_url=https://pkg.oracle.com/solaris/release</code>  <b>Note:</b> This is an example of Oracle's repositories for demonstration purposes only. In this example, the <code>.../release</code> URL contains updates for each new release of Oracle Solaris, and <code>.../support</code> contains bug fixes and updates, but is restricted to those with support contract. Many vendors supply IPS packages and may deliver packages to different directories for various purposes. Specify the one for your purpose.
Get only the	Set to True to acquire all packages; False to only get the latest versions.

### IPS configuration file options defined, continued

Configuration File option	Explanation and example
latest packages	For example:all_versions=False
Certificate and Key files	If the vendor's repository requires a certificate and key authentication, you can set them up here.  For example:  cert=/var/pkg/ssl/Oracle_Solaris_11_Support.certificate.pem key=/var/pkg/ssl/Oracle_Solaris_11_Support.key.pem  Note: all examples are for demonstration purposes only.

## STEP 3: Import all IPS packages onto the core by running the IPS import script (sol\_ips\_import)

Unless otherwise specified in the command line, the sol\_ips\_import command will run according to the details specified in the sol\_ips\_import.conf configuration file in the previous step.

1. Log in to the Solaris 11 server where you installed the IPS Acquisition tools.
2. Test the connection to the remote repository before running the import, run the sol\_ips\_import command with a string filter first. For example, to display all packages containing 'telnet', run:

```
./sol_ips_import -f 'telnet' -n
```

where -n indicates preview instead of download, and -f specifies a filter.

3. Run the IPS Package import, run the command:

```
./sol_ips_import
```

The IPS packages will download from the vendor's repository to the local staging directory on the managed server and then upload to the final destination directory on the core as specified in the .conf file.

In order to construct an upgrade path, SA's repository needs to have all versions of a package, not just the latest. In order to import all versions of a package, you can use the following option to import all versions of a package: --all\_versions

For details about this and other command options, see the ["Command options for sol\\_ips\\_import" on the next page](#) table.

Options for handling upload failures:

When the IPS Package import process is complete, the fmrifail\_<DATE> file tracks any files that failed to upload to the core. This file can be manually run with the --fmri\_file option:

```
./sol_ips_import --fmri_file fmrifail_<DATE>
```

where <DATE> is the date and time that the upload started, as included in the filename.

If any files have failed to upload, the import script will automatically attempt to re-download and upload them. If the automatic upload does not work, you can also use the `--force_process` flag to manually force a re-download and upload.

```
./sol_ips_import -f '<package name>' --force_process
```

Options for setting the number of download retry attempts:

A failed package will attempt to download three times, by default. You can change the number of retries at the command line or by modifying the configuration file, `sol_ips_import.conf`.

The command-line option:

```
-a <MAX_RETRY_ATTEMPTS>
```

or

```
--max_download_attempts=<MAX_RETRY_ATTEMPTS>
```

where `<MAX_RETRY_ATTEMPTS>` is replaced by a whole number representing the maximum number of attempts

The configuration-file setting:

```
max_retry_attempts=3
```

where "3" is the default value, but can be any whole number representing the maximum number of attempts

As a rule, the command line option will supersede the configuration file setting. If the command line option is not used and there is no configuration file value defined for this setting, then the default is three retry attempts.

**Note:** Run `./sol_ips_import -h` for information about additional command options.

In the following Command Options table, variables are represented in ALL CAPS

Command options for `sol_ips_import`

Command option	Description
<code>-a MAX_RETRY_ATTEMPTS</code> <code>--max_download_attempts=MAX_RETRY_ATTEMPTS</code>	Specify the maximum number of times a failed package download will be retried. If no value is specified, the default behavior is three attempts.
<code>--all_versions</code>	Get ALL available package versions from the remote repository. Defaults to latest. Results in ~300% more packages.  By enabling this option, you will import the entire Oracle repository into SA.  This option is available to import all packages if you are unable to generate recommended packages using the default package import option.
<code>-c REPO_CERT, or --cert=REPO_CERT</code>	Certificate file for IPS repository such as <code>Oracle_Solaris_11_Support.certificate.pem</code>

Command options for sol\_ips\_import, continued

Command option	Description
--config=CONFIG_PATH	Read command line options from this file. Defaults to sol_ips_import.conf
-d DOWNLOAD_DIR, or --download_dir=DOWNLOAD_DIR	Directory on local system to store packages
--download_only	Download packages only
-f PKG_FILTER, or --filter=PKG_FILTER	Uses a Python regular expression string to filter available packages. In upload-only mode, this filters the file name
--fmri_file=FMRI_FILE	File containing one FMRI per line that will be used to filter the repository's available packages. In upload-only mode, this will filter against the FMRI associated with a file
--force_process	Force acquisition and upload of packages that have been previously uploaded to the core.
-h, or --help	Show this help message and exit
-k REPO_KEY, or --key=REPO_KEY	Key file for IPS repository such as Oracle_Solaris_11_Support.key.pem
-m, or --manual	Show manual page and exit
-n, or --preview	Show what would be downloaded from the remote repository (dry-run)
-p HPSA_PASS, or --hpsa_pass=HPSA_PASS	SA password that will be used to upload packages
-s REPO_URL, or --sourcerepourl=REPO_URL	URL of a IPS repository
-u HPSA_USER, or --hpsa_user=HPSA_USER	SA user that will be used to upload packages
--upload_only	Uploaded packages from local directory specified by --download_dir
--version	Show program's version number and exit

### Command options for sol\_ips\_import, continued

Command option	Description
<code>-w OPSWARE_ FOLDER, or --core_destination_ folder=OPSWARE_ FOLDER</code>	Destination folder in the SA folder system

## STEP 4: Register the software

Software Registration occurs automatically during SA Agent deployment or within 24 hours of deployment, depending on the options set during deployment.

If software registration has not yet occurred, you can run the Software Registration script manually:

1. Log in to the managed server.
2. Run the Software Registration script:  
`/opt/opsware/agent/pylibs/cog/bs_software -full`

## STEP 5: Create the recommended patch policy (run solpatch\_import)

1. Log in to the SA core server as root.
2. Create recommended patch policy for the managed server by running the solpatch\_import script.

For example:

```
/opt/opsware/solpatch_import/bin/solpatch_import -a policy --policy_path='svrname-policy-all-new' --filter="rec,server=svrname"
```

where `policy_path` = the name of the policy, `filter` = the name of the server, and `rec` = recommended patches.

**Note:** Both of the path and filter options are required to create a recommended patch policy for a particular server.

**Note:** To perform a preview before creating the policy use the `-a show` option.

For example, to preview the policy with recommended patches for the 'kakai' server, run:

```
/opt/opsware/solpatch_import/bin/solpatch_import -a show --filter="rec,server=kakai"
```

Then, to create a patch policy named 'kakai-policy-all-new' on the 'kakai' server, run:

```
/opt/opsware/solpatch_import/bin/solpatch_import -a policy --policy_path='kakai-policy-all-new' --filter="server=kakai"
```



**Note:** Run `/opt/opsware/solpatch_import/bin/solpatch_import-h` for information about additional command options. Additional details about the `solpatch_import` command options are provided in the ["Patch management for Solaris 11 "](#) on page 160.

## STEP 6: Attach the recommended patch policy to a server and remediate

To attach a Solaris patch policy to a server:

1. In the navigation pane, select **Devices > Servers > All Managed Servers** or **Devices > Device Groups**.
2. In the content pane, select the desired Solaris 11 servers or device group.
3. From the Actions menu, select **Attach > Patch Policy** to open the Attach Solaris Patch Policy window.
4. From either the Browse Solaris Patch Policies or Browse Folders tab, find and select the recommended patch policy that you just created.
5. **Select Remediate Servers Immediately.** (This option enables the remediation process to run immediately after attaching the servers.)
6. Click **Attach**.
7. In the Remediate window, accept all remaining defaults and click Start Job to remediate the selected server.

**Best practice:** You may remediate multiple servers at once, but since the IPS Packages in the policy are based on a specific server, the servers that you remediate must be at the same level of maintenance in order for the policy to be a perfect fit. The recommended best practice is to use one policy per server, or to manage servers via a device group to keep their maintenance levels in sync.

## SA patching in Solaris 11

Solaris 11 patching support leverages the existing Solaris patching functionality, with a few differences to adapt to the new Solaris IPS package delivery structure.

- ["IPS packages and server types in Solaris 11 recommended patch policies "](#) below
- ["Differences in Solaris 11 patch policies"](#) on the next page
- ["Differences in Solaris 11 remediation"](#) on the next page
- ["Solaris 11 patch policy rules"](#) on page 171
- ["Reasons an IPS package might not install"](#) on page 171
- ["Other differences"](#) on page 171

## IPS packages and server types in Solaris 11 recommended patch policies

The recommended Solaris 11 patch policy that is created via the `solpatch_import` command applies to both types of Solaris 11 servers: SunOS 5.11 (SPARC) or SunOS 5.11 x86 (x86). Individual IPS

Packages can apply to Solaris 11 servers with SPARC architecture, x86 architecture, or both. The SA remediation process prevents irrelevant or wrong packages from installing.

## Differences in Solaris 11 patch policies

- All patch units are IPS Packages, so when adding items to Solaris 11 patch policies, there are only two item types: IPS packages and scripts.
- The Resolve Dependency action is not needed because the dependency check is done during remediation for Solaris 11. For previous versions of Solaris, the Resolve Dependency action was a separate step that needed to be done within the policy before remediation.
- A Solaris 11 patch policy only performs applicable updates on IPS packages that are already installed on a managed server.

For instance:

If a managed server has the following files:

- X version 1 and
- Y version 2

and you try to install these files:

- X version 2,
- Y version 2, and
- Z version 2

only X version 2 will be installed because it is an update to X version 1, which is already installed on the server.

Package Y will be omitted from the install because it is already up to date; Z will be omitted because it was not updating a package that already existed on the server.

## Differences in Solaris 11 remediation

- Applicability analysis: SA verifies that the IPS package is relevant to the server by determining if a previous version of the package has already been installed on the server. If a previous version does not exist or if a superseding package does, then the IPS package is considered not applicable.
- Remediation process: Remediating IPS packages essentially installs the new IPS package version on top of the previous version.

After running the remediation job, a new boot environment (BE) may be created. In this case, the server will not be compliant until after the server reboots and the new packages are available. If a new BE is required, then the system will need to reboot. The reboot options defined for the remediation job will be obeyed.

We recommend not to change the Default Reboot Setting, **“Hold all server reboots until all actions have completed”** when remediating a Solaris 11 Patch Policy. Changing this default reboot setting may result in patches not being installed during a patch policy remediation.

See Solaris documentation for information on Solaris 11 boot environments and zones.

## Solaris 11 patch policy rules

### **Solaris 11 patch policy supersedence rules**

If IPS package Z version 1 and version 2 are included in a policy, Z version 1 will be marked as superseded by Z version 2 and will not be installed.

### **Solaris 11 patch policy applicability rules**

1. If IPS package Z version 2 is in the policy, and no previous version of Z is installed on the managed server, Z version 2 will not be installed.
2. If IPS package Z version 1 is in the policy, and Z version 2 is installed on the managed server, Z version 1 will be marked as superseded by an installed package and will not install.
3. If IPS package Z version 1 is in the policy, and Z version 1 is installed on the managed server, Z version 1 will be marked as already installed and will not install.

## Reasons an IPS package might not install

### **Patch policy rules are applied first:**

1. Base package does not exist: IPS Package A version 1 cannot install because there is no previous version of package A installed on the managed server
2. Newer version is already installed:
  - Package A version 1 cannot install because a newer version, package A version 2, was also included in the policy and was installed instead.
  - Package A version 1 cannot install because package A version 2 (newer package) is already installed on the managed server

### **Generic rules for all policies (software or patch) are applied second:**

- Dependency: Package B version 1 cannot install because it requires package A version 3, which is not in the SA repository.
- Blocker: Package A version 1 cannot be installed because package X, which is installed on the managed server, prevents it.
- Duplicate: Package A version 1 cannot install because it is already installed
- Other: Additional reasons may apply per Solaris IPS analysis. SA passes the Solaris error messages through to the SA remediation job.

## Other differences

The patchadd utility is not applicable to Solaris 11 because there is no concept of a patch unit like there is in previous versions (version) of Solaris. All units are IPS packages, which use the 'pkg' command instead.

# Patch management for Ubuntu



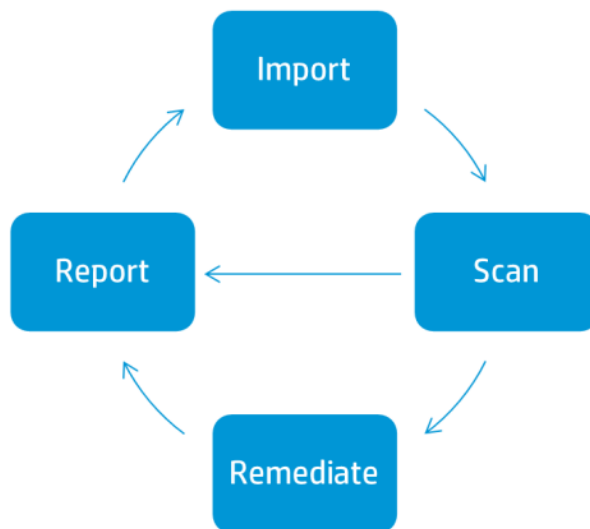
Server Automation (SA) patch management for Ubuntu enables you to identify, install, and remove Ubuntu Debian package updates, and maintain a high level of security across managed servers in your organization. You can identify and install Ubuntu packages that protect against security vulnerabilities for the SA-supported Managed Server platforms.

In Ubuntu, “patches” are Debian “packages.” SA uses Ubuntu patch management to apply Ubuntu packages.

SA automates the key aspects of patch management while offering a fine degree of control over how and under what conditions Ubuntu packages 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 Ubuntu package updates are often released to address serious security threats, an organization must be able to roll out packages quickly, before systems are compromised. However, the packages 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.

## SA Ubuntu Unified Patching Process



**Best Practice:** With Ubuntu patching in SA, you can import the metadata before importing the binary packages. You can run the Ubuntu scanner with only the metadata downloaded to determine the server vulnerabilities. Then you can run the Ubuntu package importer to import only those packages that are required by managed servers. This practice saves you storage space as well as scan and remediation processing time.

This documentation contains information about how to import Ubuntu metadata and packages, scan for vulnerabilities, and install Ubuntu package updates using patch policies.

## Features

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

- A central repository where packages are stored and organized in their native formats.
- A database that stores information about every package that has been applied.
- Dynamic Patch Policies that analyze platform vulnerabilities based on the latest metadata from the vendor.
- Advanced search abilities that identify servers that require package updates.
- Auditing abilities for tracking the deployment of important package updates.

### Types of Patch Browsing

The SA Client interface organizes Ubuntu packages and metadata by operating systems and displays detailed information about each package. You can also browse for usage information, such as software policy usage or server and device group usage. You can sort packages by the Date Created or Modified, by Object ID, OS, and so on. You can also browse all packages that are installed on a server, and view and edit package 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.

Ubuntu 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

To provide flexibility in how you identify and distribute packages on managed servers or groups of servers, Ubuntu patching allows you to create patch policies that define groups of packages you need to install. By creating a patch policy and attaching it to a server or a group of servers, you can manage which packages get installed, and where, in your organization.

The Patch Policy model that Ubuntu uses is based on software and packages that are imported as patches.

- Dynamic Policies can automatically import the latest Ubuntu packages from the vendor. When new Debian binary packages are imported, the icon shows that the policy now contains the latest package content and is active.

- Dynamic Policies are designed to remediate servers.
- Static Patch Policies contain metadata that defines the Debian binary package updates.

Best Practice: For reliable automated updates, use the Dynamic Policies.

For more information, see "[Create a patch policy](#) " on page 196.

## 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 scanned servers and have identified packages to install, Patch Management allows you to simulate (preview) the installation before you actually install a package. Use the preview process to identify whether the servers that you selected for the patch installation already have that package installed. In some cases, a server could already have a package installed if a system administrator had manually installed it.

After this type of package installation, if a compliance scan has not been run or the installed package has not been registered, SA does not know about it. Use the preview process for an up-to-date report of the package state of servers.

The preview process also reports on package dependency and supersedence information, such as packages that require certain Ubuntu products, and packages that supersede other packages or are superseded by other packages.

## 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.

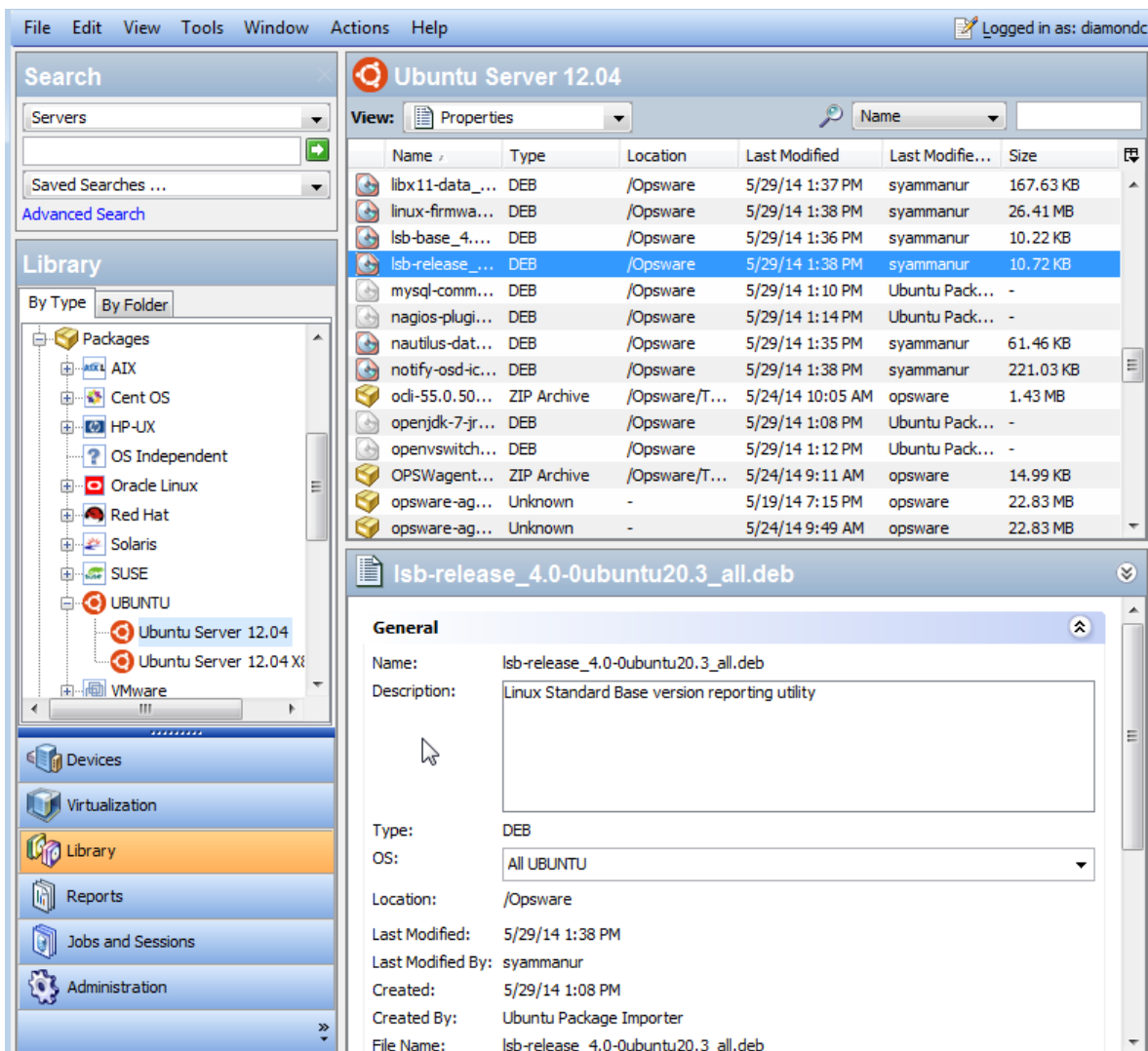
## SA Client Library

The SA Client Library provides flexibility in searching for and displaying Ubuntu packages and metadata by Object ID, Created or Modified Date, operating system, and so on.

In the content pane, a dimmed package icon indicates that the package's binary file has not been uploaded to the Library. After you upload the binary, the icon shows as Active. Use the column selector to control the columns of package metadata data that you want to display.

Because the Library is integrated with Ubuntu package metadata, you can review vendor information in real-time in the preview pane.

### **Ubuntu packages and metadata in the SA Client Library**



## Prerequisites - Patching a managed server

To patch an managed server, the following prerequisites must be met:

- Ubuntu metadata must be imported into SA.
- A compliance scan must be performed on the managed server after metadata import.

See the SA Support and Compatibility Matrix for platform version support information.

## Patch and 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 packages, patch policies, servers, and so on. See “SA Client Search” in the SA User Guide.

## SA management of Debian metadata database

The Debian metadata database contains information about released packages and how they should be applied. Patch Management compares all Ubuntu servers to the Debian metadata to identify which packages must be applied.

When a server is managed by Server Automation, the SA Agent installed on the server registers the server's configuration, including its installed packages, 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 packages. When you first provision a server with SA, the same data is immediately recorded.

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

In Ubuntu, Debian package metadata is imported automatically, but the package units are not. You have the option of importing all packages found in the Ubuntu database or importing only those packages you need for your managed servers. This feature allows you to limit the number of packages you import, which saves storage space and user time.

The Vendor patch key is currently available for Ubuntu and Windows database views. The vendor patch key is a vendor-specific value that allows users to tie a unit (patch) in SA back to the specific patch supplied by the vendor.

**Best Practice:** After an Ubuntu server is brought under SA management, you should install all Ubuntu packages by using SA Ubuntu patch management. If you install a package manually, SA does not have data about that package until the next software registration. However, when you install packages using SA Ubuntu patch management, the Agent immediately updates the information about the server in the Model Repository.

## Roles for Ubuntu 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.

**Note:** 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 package releases and identifies the vendor packages that will be included in the organization's patch policies. A Policy Setter is responsible for reviewing the latest security threats and the packages that vendors have released to address these problems. Policy Setters generally are experts in the operating systems and applications that they manage, and is able to assess the necessity of applying packages issued by vendors. A Policy Setter is also able to diagnose common problems that arise after packages are installed, allowing for a thorough test of the patch application process.

**Best Practice:** For reliable automated updates, use the dynamic patch policies instead of static manual patch policies.



- **Patch administrator:** The Patch Administrator has the authority to import, test, and edit package options. The Patch Administrator is often referred to as the security administrator in an organization. A Patch Administrator is granted specific permissions to import packages into Server Automation to test them and then mark them as available for use. Patch Administrators are also able to edit package options (such as installation scripts) through patch management. Other types of users are not allowed to import or edit packages. Typically, a Patch Administrator imports the Ubuntu Debian metadata database and tests package on non-production reference hardware. After testing the packages and determining that the packages are safe to apply to production systems, a Patch Administrator marks the packages available in the Library and then advises System Administrators to apply the approved packages.
- **System administrator:** The System Administrator installs packages 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 package, and install packages on a large number of managed servers. They are responsible for searching for servers that require the approved package, installing the packages, and verifying that the packages were successfully installed. The System Administrator can import packages but cannot install a package until the Patch Administrator has marked it as available. The System Administrator can also uninstall packages.
- Server Automation also provides predefined patch user groups for patch deployers and patch policy setters. See ["Roles for Ubuntu patch management" on the previous page.](#)

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.
- **Software policy setters**—Access to set software policy. (For Ubuntu patch policy management, you need both Patch Policy Setters and Software Policy Setters user groups.)

Next to the predefined action permissions, you must grant the necessary resource 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 for more information.

## Patch management process

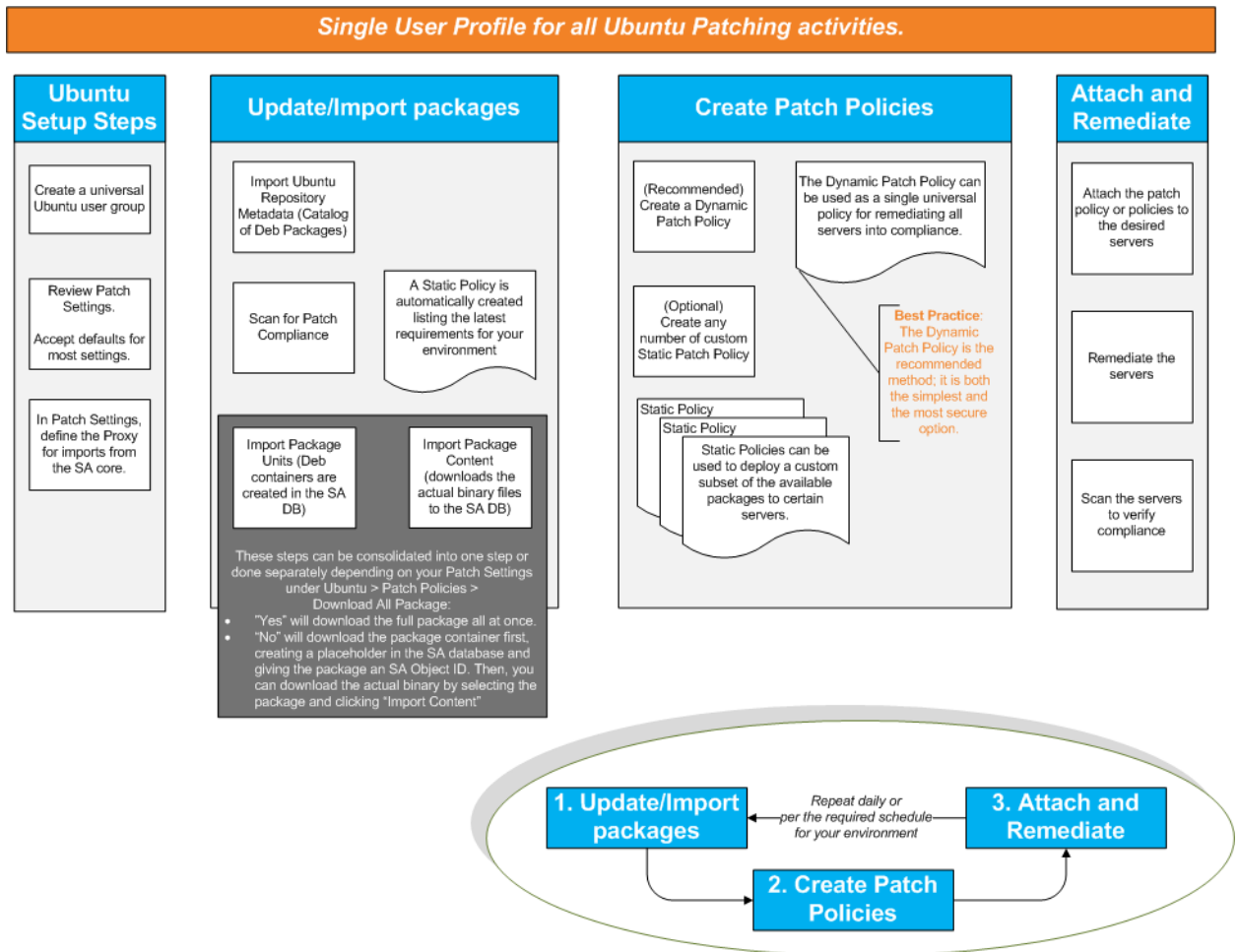
The Ubuntu patching process consists of the following phases:

- **Define Setup:** This phase includes configuring Ubuntu patching settings for the Ubuntu proxy, repositories, policy settings, and scanner behavior.
- **Import Metadata:** This phase includes getting the initial Ubuntu metadata into Server Automation.
- **Run Patch Compliance Scan:** This phase includes running compliance scans to determine whether a server is out of compliance. This is usually an automatic process that occurs every 24 hours based on the SA Agent settings of the server. You can also run a Patch Compliance Scan

manually using an empty policy. See ["Start a patch compliance scan" on page 199](#) and ["Start a patch compliance scan immediately" on page 199](#).

- **Import Package Binaries:** User must import package binaries before the Remediation phase.
- **Remediate:** This phase includes using a patch policy to download packages and install updates on recommended servers.

### Ubuntu Patching Process



## Specify Ubuntu patch settings

Ubuntu patch settings provide extensive options for configuring the patching options and functionality to fit your environment.

- ["Ubuntu patch settings: Set the proxy" on the next page](#)
- ["Ubuntu patch settings: Set the repositories" on the next page](#)
- ["Ubuntu patch settings: Configure the policy settings" on page 180](#)
- ["Ubuntu patch settings: Specify the scanner behavior" on page 181](#)
- ["Ubuntu patch settings: Specify the general logging options" on page 182](#)

## Ubuntu patch settings

Setting	Description
Proxy	Define the Ubuntu proxy configuration.
Repositories	Define the Ubuntu repositories to access.
Policy Settings	Configure the Ubuntu Patch Policy Settings.
Scanner Options	Specify the Ubuntu scanner behavior.
General	Specify the Ubuntu log settings.

## Ubuntu patch settings: Set the proxy

Specify the proxy information for your environment. Proxies provide network security and are used in most environments.

### Ubuntu proxy settings

Setting	Description
User ID	Enter the User ID to access the Web proxy.
Password	Enter the Password to access the Web proxy.
Proxy URL	Enter the full URL to access the Web proxy. For example: <code>http://web-proxy.company.com:8080</code>
User Agent	Specify the User Agent to pass to the proxy server, if required.

## Ubuntu patch settings: Set the repositories

Define the repository settings for your environment. The repository settings include the desired Ubuntu repository as well as how it will be stored in SA.

### Ubuntu repository settings

Setting	Description
Ubuntu URL	Enter the full URL to access the Ubuntu repositories. For example: <code>http://archive.ubuntu.com/ubuntu/dists/</code>
Repositories	Select one or more repositories to use: Security: Import security packages. Updates: Import updates to official packages.
Suite Code Name	Specify the Ubuntu Suite Code Names: Precise Pangolin

### Ubuntu repository settings, continued

Setting	Description
Component Name	<p>Specify the Ubuntu Component name(s):</p> <p>Main: Officially supported software. This is the major part of the distribution, and is supported by Ubuntu.</p> <p>Restricted: Supported software that is not available under a free license. This software is supported by Ubuntu.</p> <p>Universe: Community-maintained software; i.e., not officially supported software. (Note: Software from this repository is entirely unsupported by the Ubuntu team. Software in a Universe repository will not receive any review or updates from the Ubuntu Security Team.)</p> <p>Multiverse: Software that is not free. (Note: Software from this repository is entirely unsupported by the Ubuntu team. Software in a Multiverse repository will not receive any review or updates from the Ubuntu Security Team.)</p>
Architecture	<p>Select the SA-supported Ubuntu architectures in your environment:</p> <p>32 bit or 64 bit</p>
Repository Policy Name Format	<p>Choose whether to include date and time along with the Ubuntu Repository path name when creating the repository policy. Your format options are:</p> <p>Use Ubuntu Path: Uses only the Ubuntu path when creating the repository policy.</p> <p>Add Date to Ubuntu Path: Appends Year-Month-Day to the Ubuntu path when creating the repository policy.</p> <p>Add Date and Time to Ubuntu Path: Appends Year-Month-Day-HOUR:MINUTE to the Ubuntu path when creating the repository policy name.</p>

## Ubuntu patch settings: Configure the policy settings

Use the Policy Settings section to configure the default settings for handling Ubuntu patch policies:

### Ubuntu policy settings

Setting	Description
Automatically include dependent packages	<p>Specify whether to make Ubuntu patch remediation jobs automatically include dependent packages:</p> <p>Yes: Dependent packages will be included in Ubuntu patch remediation jobs by default.</p> <p>No: Dependent packages must be manually added to Ubuntu patch remediation jobs.</p>
Import based on Scan results	<p>Specify whether to filter import contents and only import what your environment needs. Note: Best policy practice is to leave the default value of Yes:</p> <p>Yes: (Default) A scan will be run, and import contents will be filtered based on the</p>

### Ubuntu policy settings, continued

Setting	Description
	<p>results.</p> <p>No: All content will be imported without first running a scan.</p>
Download Package Binaries	<p>Controls the import of all Ubuntu packages from the repository:</p> <p>Yes: Import Ubuntu packages at policy creation.</p> <p>No: Delay download of Ubuntu packages until a scan is run to determine the packages needed in your environment.</p>
Production Requirements	<p>Enter the full path to the file on the SA Slice server or single core server that specifies the packages needed for your production environment. You must be logged in to this server when you perform Ubuntu patch or package updates.</p> <p>When the package importer is run, it imports packages from this list if they match information in the Ubuntu metadata catalog.</p>
Create Static Policies	<p>Determine if static policies can be created based on the Debian packages defined in the repository:</p> <p>Yes: Enables creation of static policies.</p> <p>No: Prevents creation of static policies.</p>
Package Policy Name Format	<p>Choose whether to include date and time along with the Ubuntu Repository path name when creating the package policy:</p> <p>Use Ubuntu Path: Uses only the Ubuntu path when creating the package policy name.</p> <p>Add Date to Ubuntu Path: Appends Year-Month-Day to the Ubuntu path when creating the package policy name.</p> <p>Add Date and Time to Ubuntu Path: Appends Year-Month-Day-HOUR:MINUTE to the Ubuntu path when creating the package policy name.</p>

### Ubuntu patch settings: Specify the scanner behavior

Use the Scanner Settings section to configure the behavior of the Ubuntu scanner.

#### Ubuntu scanner settings

Setting	Description
Enable Ubuntu Scanner	<p>Determine whether to enable the Ubuntu Scanner:</p> <p>Yes: Enables the Ubuntu scanner</p> <p>No: Disables the Ubuntu scanner</p> <p>Note: The Ubuntu Scanner is critical to the Ubuntu Patching functionality. If this option is disabled, the Ubuntu Patching feature is essentially disabled.</p>

### Ubuntu scanner settings, continued

Setting	Description
Use Implicit Scan Policy	Enables the implicit scan policy which picks up the latest imported Ubuntu repository policy by default; bypasses the need to manually attach modified policies to servers.  Yes: Enable implicit policies.  No: Disable implicit policies: Ubuntu repository policies must be manually attached to each server
Logging Options	Defines the Managed Server logging options during scan and remediation.  Errors only: Logs only errors.  Errors and warning messages: Logs errors and warning messages.  Errors and debug messages: Logs errors and debug messages.  Errors and informational only: Logs only errors and informational messages.
Repository Scope	Define the repository scope on the Managed Server.  Public: Keeps the repository public on the Managed Server.  Private: Keeps the repository private on the Managed Server: the repo control file will be deleted after SA has used it and re-created the next time.
Repository Filename	Enter the name of the repository file to create on the Managed Server.
Repository Directory	Enter the name of the repository directory to create on the Managed Server.
Scanner Handler Directory	Enter the name of the handler directory to create on the Managed Server.
List information for all packages	Determine ability to get installed information for all packages even if they do not exist in the current repository.  Yes: Gets information about all packages that are installed on the Managed Server.  No: Collects information only about installed packages from the current repository.
Debug Servers	List of debug servers.

## Ubuntu patch settings: Specify the general logging options

The General section allows you to specify how you want to handle error logging.

### Ubuntu general logging settings

Setting	Description
Logging Options	Choose the Ubuntu Importer logging options: Errors only: Logs only errors. Errors and warning messages: Logs errors and warning messages. Errors and debug messages: Logs errors and debug messages. Errors and informational only: Log errors and informational messages.

## Ubuntu patch management tasks

This section describes how to find and manage information about an Ubuntu package.

- ["View package information" below](#)
- ["Package dependencies and supersedence" below](#)
- ["View Ubuntu packages " on the next page](#)
- ["Edit Ubuntu package properties" on the next page](#)
- ["Find Ubuntu packages" on the next page](#)
- ["Find servers that have an Ubuntu package installed " on page 186](#)
- ["Find servers that do not have an Ubuntu package installed" on page 186](#)
- ["Import Ubuntu patch contents from the managed servers view" on page 187](#)
- ["Export an Ubuntu package" on page 188](#)

## View package information

To view detailed information (properties) about a package:

1. In the navigation pane, select **Library**. In the **By Type** tab, select **Packages > Ubuntu**.
2. Expand **Ubuntu**, and select a specific Ubuntu operating system.  
The content pane displays all packages associated with that operating system.
3. In the content pane, open a package to view its properties in the Packages: Properties window.  
Press **F1** to display descriptions of the fields displayed in the Packages: Properties window.

## Package dependencies and supersedence

Package metadata identifies all known dependency and supersedence relationships between packages and Ubuntu products, and between packages and other packages.

In Server Automation:

- Dependency relationships identify Ubuntu products that must already exist on a server before you can install a certain package.

- Supersedence relationships identify packages that supersede or are superseded by other packages. In Ubuntu Patch Management, *supersedes* means that one package replaces another and *superseded by* means that the package you are installing is replaced by another package.

**Note:**

In Server Automation, Ubuntu patch management does not detect whether two packages are mutually exclusive—which is when either one can be installed but not both. Subsequently, Patch Management does not prevent you from installing both packages on a server. This means that you may be able to install both a superseded package and a superseding package on a server if both packages are recommended by an Ubuntu server.

## View Ubuntu packages

The SA Client displays information about Ubuntu packages that have been imported into Server Automation.

To view information about a package:

1. In the navigation pane, select **Library**. In the **By Type** tab, select **Packages > Ubuntu**.
2. Expand **Ubuntu**, and select a specific Ubuntu operating system.  
The content pane displays all packages listed in the Ubuntu Package Database for the Ubuntu operating system that you selected.
3. (Optional) Use the column selector to sort the packages according to Name, Type, Location, Last Modified, Last Modified By, and Size.
4. In the content pane, open a package to view its properties in the Package window.

## Edit Ubuntu package properties

You can edit a package's Name and Description.

To edit the package properties:

1. In the navigation pane, select **Library**. In the **By Type** tab, select **Packages > Ubuntu**.
2. Expand **Ubuntu**, and select a specific Ubuntu operating system.  
The content pane displays all packages listed in the Ubuntu Package Database for the Ubuntu operating system that you selected.
3. In the content pane, open a package to view its properties in the Package window.
4. Edit the following fields: **Name** and **Description**.
5. From the File menu, select **Save** to save your changes.

## Find Ubuntu packages

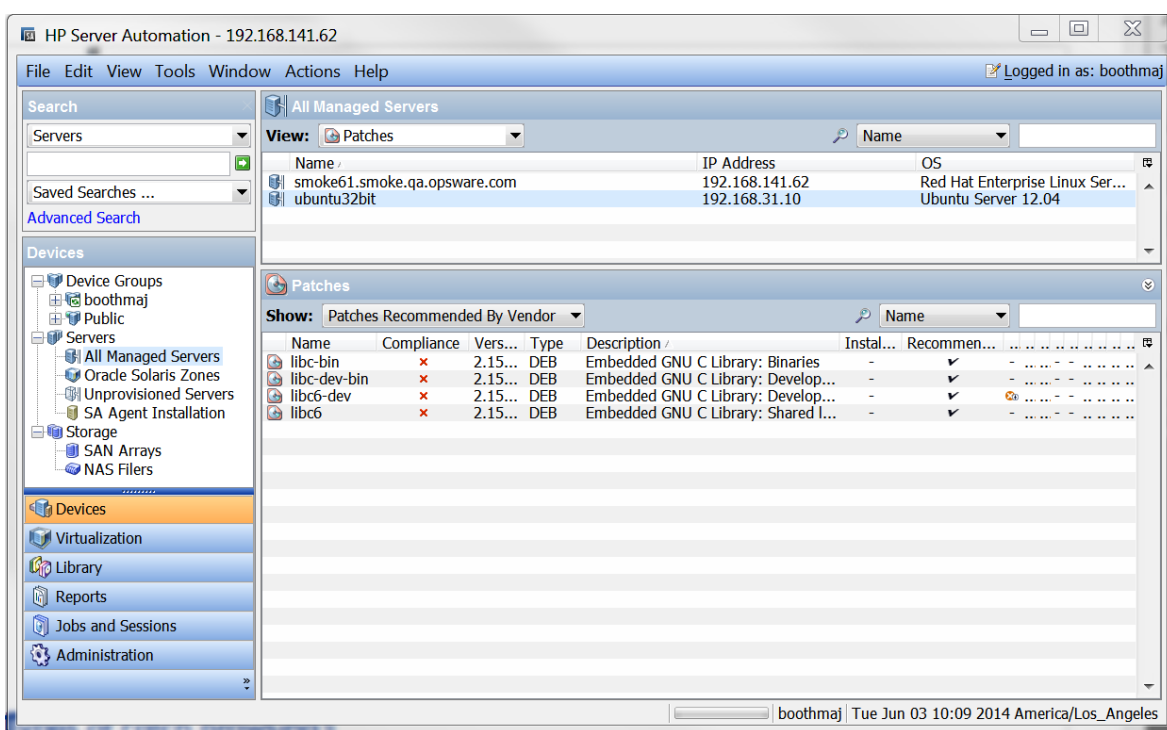
To find packages for a particular Ubuntu server:

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 Ubuntu.



4. In the preview pane, use the Show drop-down list to select any of the following for patch details:
  - Patches Needed
  - Patches Recommended by Vendor
  - Patches With Policies or Exceptions
  - Patches Installed
  - Patches With Exceptions
  - All Patches

### Patches recommended by vendor



The Patches window shows these values:

- Name - The name of the patch.
- Compliance - Shows whether or not the patch is compliant with the version of Ubuntu server used.
- Version - Version of the patch.
- Type of Patch - Debian package
- Description - Patch description
- Installed - Whether or not the patch is installed on the particular server.
- Recommended - Whether or not the patch is vendor-recommended.
- Exception - Whether or not the patch includes an exception.
- Bulletin - The Ubuntu Security Notice Bulletin number.

- Vendor Patch key - The Vendor Patch key.
- Release Date - The date on which the patch was provided.
- Exposure Time - Amount of time between when the patch was installed minus when the patch was released.
- Action - Information taken from the scanner
- Category - The patch category.
- Rating - Whether installation of this patch is Required or Optional.
- Object ID - The object ID of the patch.

## Find servers that have an Ubuntu package installed

To find servers that have a particular package installed:

1. In the navigation pane, select **Library**. In the **By Type** tab, select **Packages > Ubuntu**.
2. Expand **Ubuntu**, and select a specific Ubuntu operating system.  
The content pane displays all packages associated with that operating system.
3. In the content pane, select a package.
4. From the **Search** drop-down list in the content pane, select **Server Usage**.  
You can browse a server in this list to view a list of all installed packages. Notice that this list might display a more complete list of installed patches than the list you will find in the Ubuntu Add or Remove Programs utility.

### Note:

For each listed binary, the Exposure Time column shows the gap between the Release Date and the Install Date, so you can analyze vulnerability.

An alternative way to find servers that have a particular patch installed:

1. In the navigation pane, click on the **Advanced Search** link.
2. In the Advanced Search pane, set **Search: For Servers**.
3. Set Where: to Installed Software.
  - a. Set appropriate values (e.g., equals, contains, etc.).
  - b. Specify the name of the patch.
4. Press the **Search** button.

## Find servers that do not have an Ubuntu package installed

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

1. In the navigation pane, select Library. In the **By Type** tab, select **Packages > Ubuntu**.
2. Expand **Ubuntu** and select a specific Ubuntu operating system.  
The content pane displays all packages associated with that operating system.
3. In the content pane, select a package.
4. In the View drop-down list, select **Server Usage**.

## Import an Ubuntu patch from the SA Client Library

Ubuntu packages are downloaded from the Ubuntu web site and then imported (uploaded) into Server Automation. To verify whether a package has been imported, view the package's Availability property. The Availability of an imported package is either Limited, Available, or Deprecated.

To import a patch with the SA Client:

1. In the navigation pane, select Library. In the **By Type** tab, select **Packages > Ubuntu**.
2. Expand **Ubuntu** and select a specific Ubuntu operating system.  
The content pane displays all packages associated with that operating system.
3. In the content pane, select a package.
4. To import a package directly from the Ubuntu web site, from the Actions menu, select Import **Contents > Import** from Vendor.

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

Or

To import a package 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 package.

5. Click **Import**.

## Import Ubuntu patch contents from the managed servers view

An Import Contents menu option is available from the Managed Servers view that enables you to import package contents from a file. Ubuntu package contents (binaries) can be imported directly from the vendor as well.

To import patch contents from the All Managed Servers view:

1. Log in to the SA Client with Manage Patch (Read and Write) permissions.
2. Navigate to **Devices > All Managed Servers**.
3. Under View, select **Patches**.
4. In the Patches content pane, select one or multiple packages.
5. Right-click and select Import Contents and select **From Vendor...** or **From File....**

Singular package content can be downloaded from a local file or directly from a vendor. However, if multiple packages are selected, only the "**From Vendor...**" option is available.

- **From Vendor...**: This option enables you to import package contents directly from the vendor. (Note: This option is only available for Ubuntu packages.)
- **From File...**: This option enables you to import package contents from a local file that is accessible from the system where the SA Client is running.

## Export an Ubuntu package

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

1. In the navigation pane, select Library. In the **By Type** tab, select **Packages > Ubuntu**.
2. Expand **Ubuntu** and select a specific Ubuntu operating system.  
The content pane displays all packages associated with that operating system.
3. In the content pane, select a package.
4. From the Actions menu, select **Export**.
5. In the Export Patch window, enter the folder name that will contain the package file in the **File Name** field.
6. Click **Export**.

## Policy management

In Ubuntu patch management, patch policies and patch policy exceptions enable you to customize patch distribution in your environment. Policies and exceptions define the Ubuntu packages 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 packages get installed on servers.

### Patch policy

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

A patch policy provides broad flexibility for distributing packages. For example, you can create a patch policy that contains security packages that you want to distribute only to servers used by your sales force. You can also create a patch policy that contains security packages 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 packages ranked as critical by Ubuntu 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 packages (by operating system) as a default patch policy.

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 packages 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.

Ubuntu Patch Management supports the following types of patch policies:

- **User-defined patch policy:** This type of patch policy allows you to specify the packages 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 packages. The policy setter can create a user-defined patch policy that is a subset of all available packages that are in a vendor-recommended patch policy. This enables the policy setter to apply only those patches that their environment needs.

- **Dynamic patch policy:** Membership of packages is defined by Individual Ubuntu Managed Server Scan Results, based on Ubuntu package metadata. Dynamic 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:

- 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.
- 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.

## 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" in the SA *User Guide: Software Management* for information about the fundamentals of SA remediation.

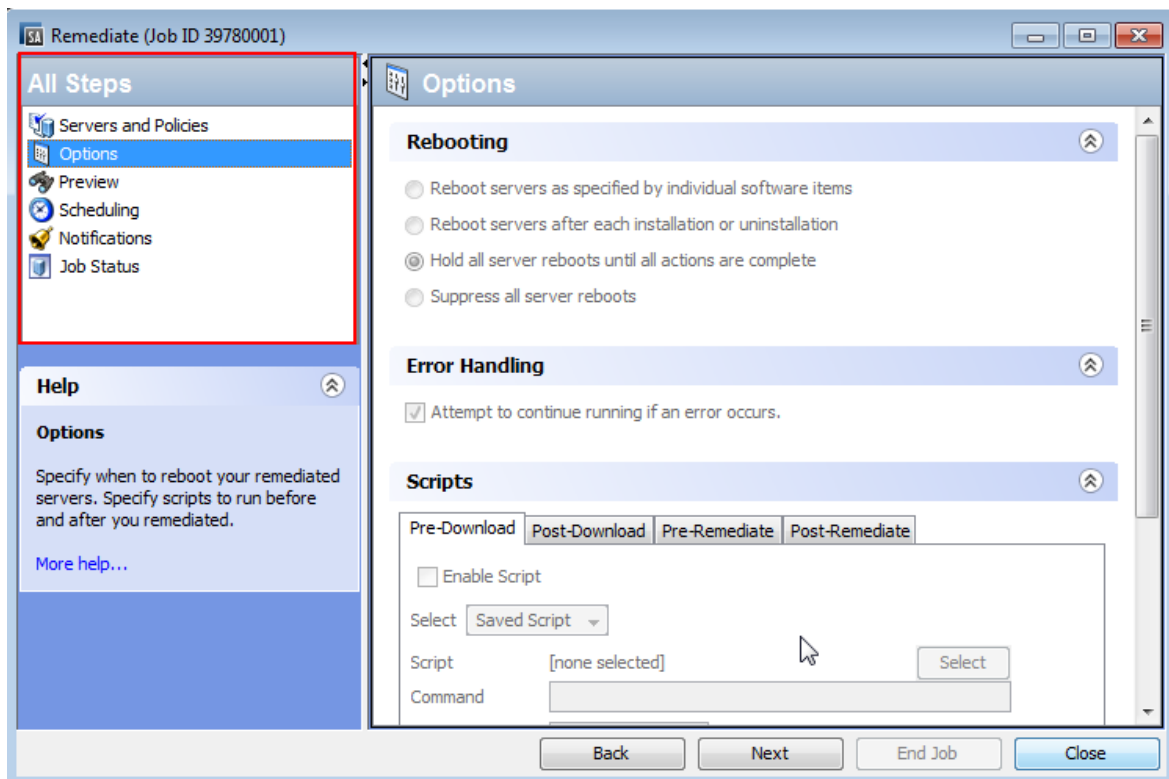
To ensure patch compliance, Ubuntu Patch Management identifies vulnerable managed servers and simultaneously deploys packages to many servers when a remediation process is performed. The remediation process examines and applies an entire patch policy, including multiple policies, to the managed servers to which it is attached. 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 Ubuntu package releases and subsequently update a patch policy by adding new packages 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 to which this policy is attached.

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

To help you manage 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.

### Remediate Wizard



## Remediate patch policies

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

To remediate a patch policy:

1. In the navigation pane, select **Library**. In the **By Type** tab, select **Packages > Ubuntu**.
2. Expand Ubuntu and select a specific Ubuntu 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:

- ["Set remediate options" below](#)
- ["Set reboot options for remediation" on the next page](#)
- ["Specify pre-installation and post-installation scripts for remediation" on page 193](#)
- ["Schedule a patch installation for remediation" on page 193](#)
- ["Set up email notifications for remediation" on page 194](#)
- ["Preview and start a remediation" on page 194](#)

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.

## Set 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 ["Set reboot options for remediation" on page 57](#).

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.

## Set 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 Ubuntu locations:

- 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 Ubuntu's reboot recommendations, which is the Reboot servers as specified by individual software items option. If it is not possible to use the Ubuntu 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 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.



## Specify pre-installation and post-installation 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 SA 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\preinstall1.log`. If you do not enter a drive letter, the default is %SYSTEMDRIVE%, which is where the system folder of Ubuntu 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.

## Schedule 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.

## Set 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.

### Note:

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

## Preview and start 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. This verification is based on the imported Microsoft path database. 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.

**Note:**

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
- In the navigation pane, select Jobs and Sessions to review detailed information about the job. See "Browsing Job Logs" in the SA User Guide.
8. In the navigation pane, select Jobs and Sessions to review detailed information about the job. See "Browsing Job Logs" in the SA User Guide.
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 the "Cancelling or Terminating Installation, Uninstallation or Remediation Jobs" section in the SA Administration Guide.

## Verify 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.

## Create 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.

As mentioned before the Ubuntu patches are just software/packages under the hood, and that is why, when imported from the "Patch Settings" they get populated in the Library/Packages/Ubuntu. However the icon in the tab distinguishes a patch from a package. Once a patch metadata is imported, it shows up qualified by a greyed out patch icon, if its binary has not been imported. User can right click on the greyed out patches in the Library/Packages/Ubuntu view and select "import from vendor" or "import from file" (just like Windows patches) and import the binaries to turn the icon green.

User can create a Generic Patch Policy by right clicking on the Library/Patch Policy/Ubuntu tab and select "Static Patch Policy" or "Dynamic Patch Policy" to create either a static or dynamic policy. Once

the new policy creation screen opens up, user can select the Policy Options there in. Though note that the “Policy Items” is enabled only for the Static Policies and not for Dynamic Policies as Dynamic policies cannot hold any item.

To create a patch policy:

1. In the navigation pane, select **Library > By Type > Patch Policies**.
2. Select a specific Ubuntu operating system.
3. From the Actions menu, select **New Dynamic Policy** or **New Static Policy**.
4. In the Properties window, give the policy a unique name. **Save** and **Close**.
5. In the content pane, open the New Patch Policy.
6. (Optional) In the **Name** field of the Properties, enter a name that describes the purpose or contents of the policy.

## Delete 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 Ubuntu operating system.
3. In the content pane of the main window, select a policy.
4. From the Actions menu, select **Delete Patch Policy**.

## Add 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 Ubuntu operating system and view the list of Ubuntu 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**.

## Remove 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 Ubuntu operating system and view the list of Ubuntu 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**.

## Attach 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 Ubuntu operating system and view the list of Ubuntu 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**.

## Detach 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 Ubuntu operating system and view the list of Ubuntu 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**.

## 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.

## 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 ["Start a patch compliance scan immediately" below](#).
- Periodically, by setting up a schedule.  
See ["Schedule a patch compliance scan" on page 69](#). 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:
  - ["Install an Ubuntu patch" on page 208](#)
  - ["Remediate patch policies" on page 191](#)

## Start a patch compliance scan immediately

To run a Patch Compliance Scan manually, you need to create an empty policy and attach it to the server(s) or device group(s).

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.


## Refresh the compliance status of selected servers

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

## View 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:

1. In the navigation pane, select **Devices**.
2. Drill down to the server you want to check.
3. In the contents pane, select a server.
4. Right-click and then select **Scan > Show Patch Compliance Scan Failure Details**.
5. 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 the "[Patch Compliance Status Icons](#)" below table

Patch Compliance Status Icons

Status/Icon	Description
 Compliant	The server is compliant for all patches. Patches in policies attached to the server are all installed on the target server.
 Partial	The server is partially compliant for patches. An exception has been set for these patches.
 Non-Compliant	The installed patches on the server do not match the conditions defined in the patch policy.



### Patch Compliance Status Icons, continued

Status/Icon	Description
 Scan Failed	The scan operation failed. Patch Management is unable to check the compliance of the server.

## 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.

Ubuntu 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.

Ubuntu 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

The section provides information on following topics:

- ["Prerequisites for importing the patch database \(metadata\)" below](#)
- ["Setting patch availability" below](#)
- ["Importing the Ubuntu patch database metadata and packages" on the next page](#)
- ["Scheduling a patch compliance scan" on page 204](#)
- ["Setting a patch compliance level" on page 206](#)
- ["Supported Ubuntu versions" on page 206](#)

### Prerequisites for importing the patch database (metadata)

Before you can import the Ubuntu patch database, you must configure your SA Client to use a Web proxy when communicating with your SA core.

To configure your SA Client:

1. In the Log in to 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 you want to use the same proxy as the browser, select **Use Browser**Or
  - If you want to set a different proxy, select **Manual** and enter the SA 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.

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 Ubuntu patch database metadata and packages

To import the Ubuntu metadata using the SA Client:

Before performing these steps, see ["Prerequisites for importing the patch database \(metadata\)" on the previous page.](#)

1. In the navigation pane, select **Administration>PatchSettings**.
2. Click the **Ubuntu** tab.
3. If a proxy is needed, set the Proxy value. If the proxy requires a user name, password or user agent, set those values as needed.
4. To import the metadata of the Ubuntu repository from the Ubuntu web site, click **Import Metadata**.

The Import Repository Metadata for Ubuntu window displays the overall progress of the unites as well as the units being processed.

To import the Ubuntu packages using the SA Client:

Before performing these steps, import the metadata and scan your servers for patch compliance. After scanning servers for compliance, you can import the Ubuntu patches using the SA Client.

1. In the navigation pane, select **Administration>Patch Settings**.
2. Click the **Ubuntu** tab.
3. To import the database from the Ubuntu web site, click **Import Packages**.

The Run Server Script window appears displaying the script to run (Import Ubuntu Packages is selected by default. You can switch to Import Ubuntu Metadata to just import the package metadata.

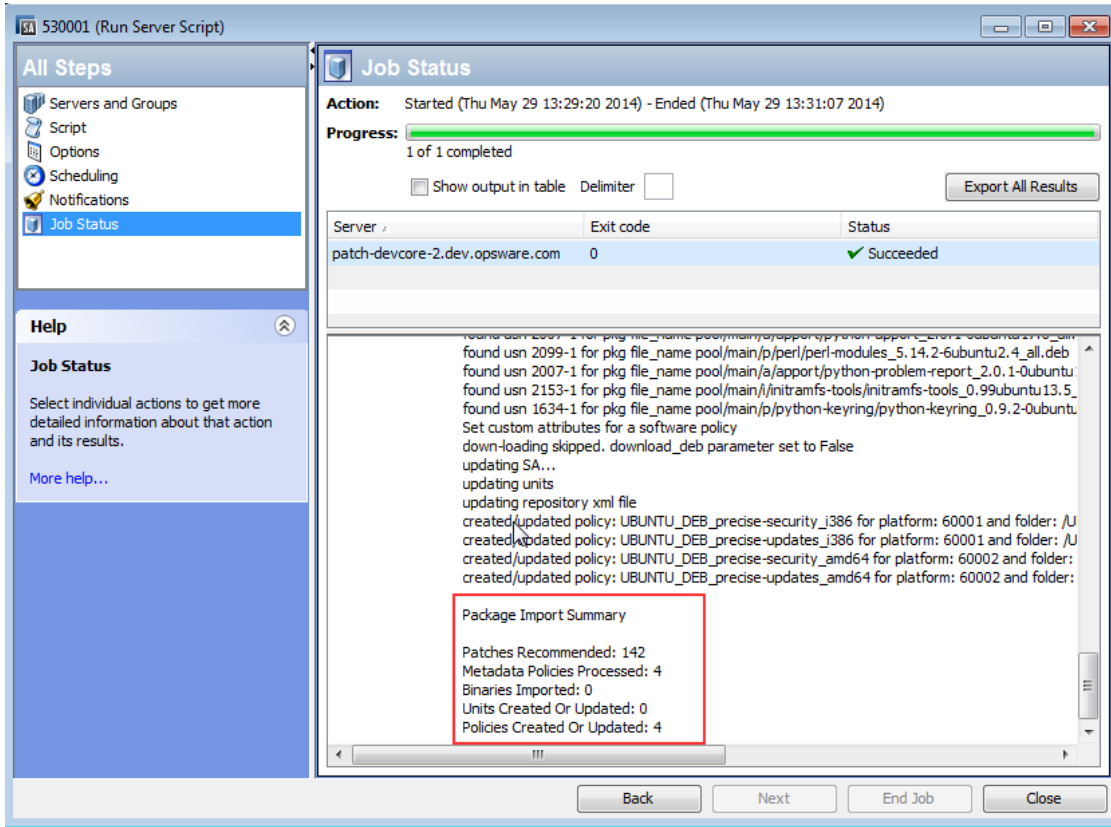
The script page also provides script metadata, such as the version, type, location (import destination) and description.

4. Click **Next** or select the next step to proceed through the Run Server Script steps:
  - Servers and Groups
  - Options
  - Scheduling
  - Notifications
  - Job Status

**Note:** For information on Run Server Script steps and options, see the SA User Guide for information on running server scripts.

5. When you are done defining the options, click **Start Job**.
6. The Job Status will display the results as the import is processing. The import may take a long time depending on the size of the import.

When the import job is complete, the Job Status will display the details of the job activity. Select any server to see a log of the job details on that server in the detail pane, including an Ubuntu Package Import Summary at the bottom of the job results log.

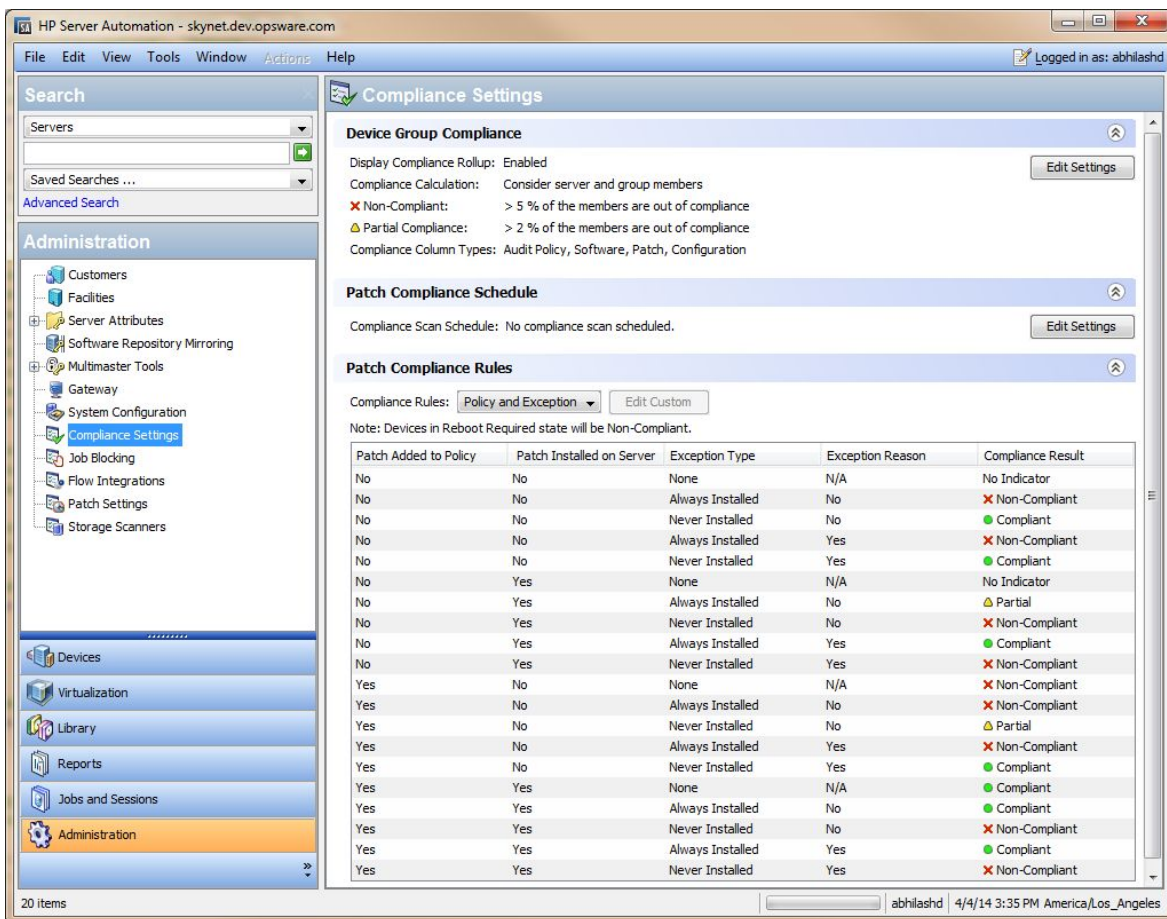


## Scheduling a patch compliance scan

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

1. In the navigation pane, select **Administration > Compliance Settings**.

### Compliance Scan window



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.

## Supported Ubuntu versions

See the SA Support and Compatibility Matrix for the list of SA-supported Managed Server platforms for your version of SA.

## Patch locale configuration tasks

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

- ["Configuring the SA Core for non-English locales" below](#)
- ["End user requirements for non-English locales" on the next page](#)

## Configuring the SA Core for non-English locales

To configure the core for non-English locales, complete the following steps on each core server that is running the SA 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 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.tmp1`
5. For the Japanese language, in the `<resources>` section of the `jnlp.tmp1` 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.tmp1` file, add the following XML element:  
`<property name="com.opsware.ngui.font.korean" value="Arial Unicode MS"/>`
7. In the `/opt/opsware/occclientdirectory`, if the following files exist, delete them:  
`$HOST_ja.jnlp`  
`$IP_ja.jnlp`  
`$HOST_ko.jnlp`  
`$IP_ko.jnlp`

## End user requirements for non-English locales

To view non-English fonts in the SA Client:

- a. Verify that the Ubuntu desktop running the SA Client uses the Arial Unicode MS font.
- b. After the system administrator performs the steps in ["Configuring the SA Core for non-English locales" on the previous page](#), the end user logs on to the SA Client and selects their "Logged in as" link in the upper right corner of the SA Client window. This displays the User window. Select the Properties view.
- c. On the User Properties view, the end user updates the Locale field in the User Preferences section. 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. Ubuntu 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.

Ubuntu Patch Management displays the name of the command, such as a `.deb` 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 Ubuntu 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.

## Install an Ubuntu 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 or device group:

1. In the navigation pane, select **Devices > All Manages Servers** (or **Device Groups**).
2. In the content pane, select a server or device group.
3. From the Show drop-down list, select **Patches Recommended by Vendors**.
4. Right-click on a patch which has the content imported and select Install.

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

For instructions on each step, see the following sections:

- ["Set Ubuntu install options" on the next page](#)
- ["Set reboot options for an Ubuntu patch installation" on the next page](#)
- ["Specify install scripts for an Ubuntu patch installation" on page 210](#)
- ["Schedule an Ubuntu patch installation" on page 211](#)
- ["Set up email notifications for an Ubuntu patch installation" on page 211](#)
- ["Preview an Ubuntu patch installation" on page 212](#)
- ["View job progress of an Ubuntu patch installation" on page 213](#)

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.

5. 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, Ubuntu 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 ["Remediate patch policies" on page 191](#) for another method of installing a patch.



## Set Ubuntu 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 (**.deb** file) that is displayed.
5. Click **Next** to go to the next step or click **Cancel** to close the Install Patch window.

## Set reboot options for an Ubuntu 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 Ubuntu's reboot recommendations, which is the Reboot servers as specified by individual software items option. If it is not possible to use the Ubuntu 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 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.

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.

When you suppress reboot during an Ubuntu 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.

## Specify install scripts for an Ubuntu 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 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 Ubuntu 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.

## Schedule an Ubuntu patch installation

Since the two phases of Ubuntu 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.



### Note:

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

## Set up email notifications for an Ubuntu 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.

**Note:**

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

## Preview an Ubuntu 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. In some cases, a server could already have the patch installed if a system administrator had manually installed it, which means that Ubuntu Patch Management does not know about it.

The preview process also reports on dependency and supersedence information, such as patches that require certain Ubuntu 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. If a patch is not needed, it will appear as 'will not install'.

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, 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.

**Note:** 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.

## View job progress of an Ubuntu 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 for more information about browsing job logs.

**Note:** When a Vendor Recommended Patch Policy is remediated on an Ubuntu managed server, depending on what patches were applied, the server may require an additional remediation. This can occur when the remediation installs a patch that requires subsequent vendor updates.

3. Click **Close** to close the Install Patch window or click **End Job** to prevent the job from running.

## Patch management for Unix

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.

## Track 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 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, 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 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.

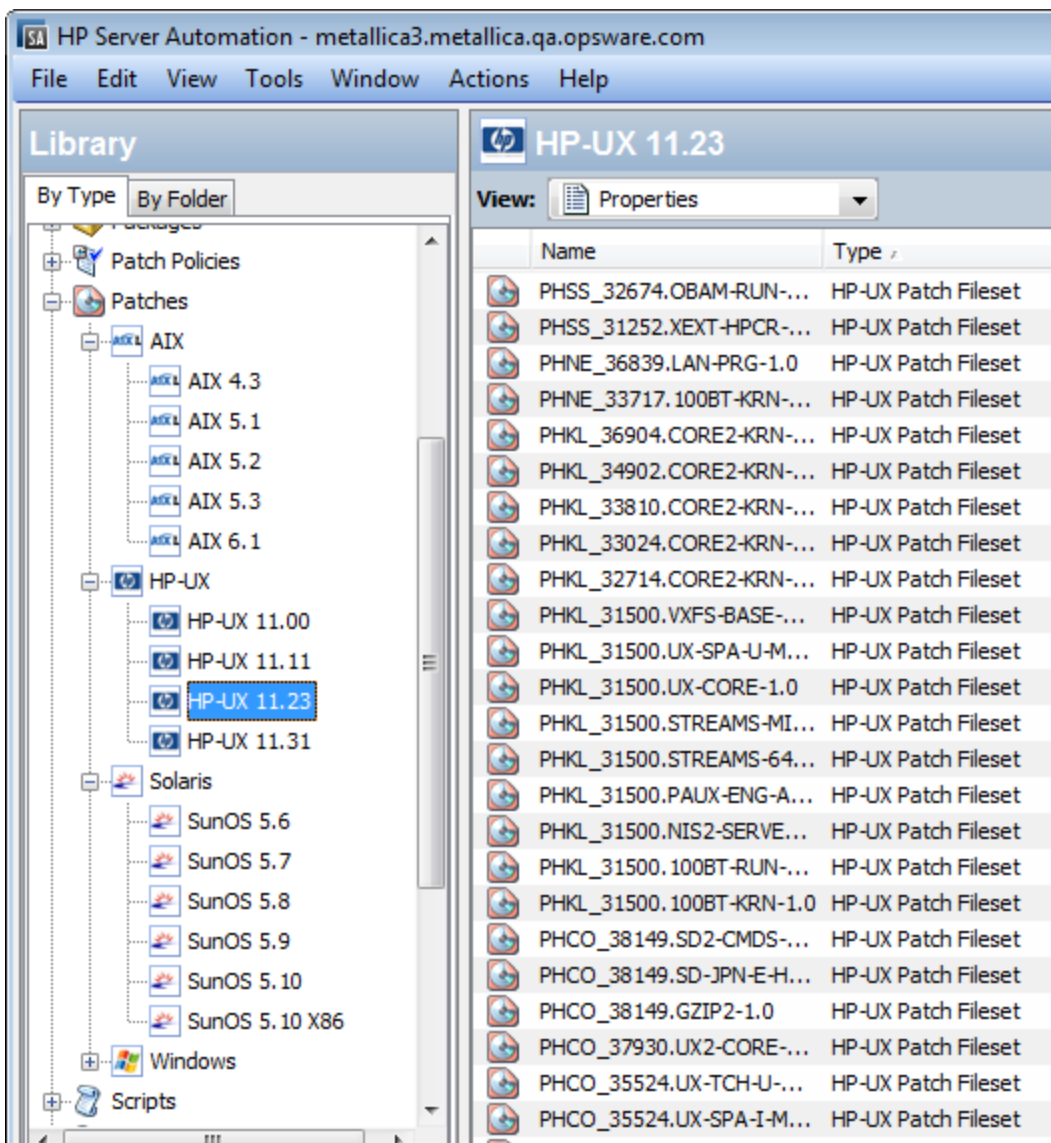
The patch administrator then defines patch installation and uninstallation options and tests the patch. Only after the patch is tested and the patch administrator marks it as available for use can other administrators install the patch.

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.

## View 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. The following ["HP-UX patches in the SA Library "](#) [below](#) figure 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 223](#) and ["View and edit Unix patch properties" on page 226](#).

### **HP-UX patches in the SA Library**



## Search for patches

In the SA Client, you can search for any information about your operational environment that is available in 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.

## Patch management roles for Unix

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.

**Note:** 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 section 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 Server Automation, patch administrators are granted specific permissions that allow them to upload patches into 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 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 Server Automation.

## Supported Unix versions and patch types

SA supports all of the operating system versions that 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 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 User 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.

## Underlying technologies for patch management on Unix

Although the utilities vary, Server Automation enables you to perform patching tasks by using a single interface. 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. 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.

### Supporting Technologies for Patch Management on Unix

<b>Solaris</b>	<b>AIX</b>	<b>HP-UX</b>
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
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, 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, Server Automation still associates the earlier version of the fileset with the APAR.

When uploading an LPP, 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 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.

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.

**Note:**

Patch files, such as AIX update filesets and APARS, cannot be added to a particular folder and cannot be owned by a particular user. See the the SA User Guide for information about how to use folders.

## Importing and remediating AIX patches

SA supports importing and remediating a set of AIX packages from a Maintenance Level (ML) or Technology Level (TL) to perform AIX package installations.

Packages and patches are imported into SA independently. In order to update a server to a particular ML or TL, you can import all the packages and patches that belong to the ML or TL into SA with a single

import. During this import, specify a new policy be created for the packages and patches. This will create a policy representing the ML/TL that you can then install on managed servers.

To import AIX patches:

1. Login to an SA Core as root.
2. Download all of the packages from an AIX Maintenance Level or Technology Level from IBM's website and place them in a temporary directory on the SA Core.
3. Import the patches into the SA Library using the `import_aix_packages` tool. This tool can also generate a software policy containing all of the packages that have been imported.

```
/opt/opsware/mm_wordbot/util/import_aix_packages <directory containing AIX packages>
```

where the import command always ends with the path for the directory containing the AIX packages. See ["AIX import options" below](#) for additional AIX import options.

### Sample import and remediate process for AIX

The following example imports AIX packages from a temporary directory on the SA Core, `/var/tmp/aix_package_files_directory`.

1. Run the AIX import tool:

- a. Sample A: Simple Import of AIX Packages and Patches

```
/opt/opsware/mm_wordbot/util/import_aix_packages /var/tmp/aix_package_files_directory
```

- By default, the `import_aix_packages` tool will attempt to identify the OS version of the package being imported. You can also use the `'-o'` or `'--os'` option to explicitly define the OS for the imported packages. See ["AIX import options" below](#) for options.
- The imported AIX files can be viewed in the SA Client under **Library > By Type > Packages > AIX** or **Library > By Type > Patches > AIX**.

- b. Sample B: Import AIX Packages /Patches and Create a Policy

Use the `'-p'` option to import patches and specify a policy:

```
/opt/opsware/mm_wordbot/util/import_aix_packages -p /AIX/AIX6.1/AIXPOLICY /var/tmp/aix_package_file_directory
```

- The newly created policy can be viewed in the SA Client under **Library > By Type > Software Policies** or **Library > By Folder** under the directory:

```
/AIX/AIX6.1/AIXPOLICY
```

2. Attach the newly created policy, `AIXPOLICY`, to an AIX managed server.
3. Remediate the server with the policy attached as you normally would to install the AIX package or patch.

## AIX import options

### Options for `import_aix_packages`

Option	Description
<code>-h,</code> <code>--help</code>	Show this help message and exit

### Options for import\_aix\_packages, continued

Option	Description
-f, --force	Force packages to be imported even if already in library.
-o OS, --os=OS	<p>OS version of packages: '4.3', '5.1', '5.2', '5.3', '6.1', '7.1'</p> <p>The -o parameter value works with or without quotes, but only one value can be specified at a time.</p> <p>For example, to specify Technology Level 6 Service Pack 1, you might say:</p> <pre>/opt/opsware/mm_wordbot/util/import_aix_packages -o '6.1' /var/tmp/aix_package_file_directory</pre> <p>OR</p> <pre>/opt/opsware/mm_wordbot/util/import_aix_packages -o 6.1 /var/tmp/aix_package_file_directory</pre>
-p POLICY_PATH, -- policy_path=POLICY_PATH	<p>Use this option to import AIX patches and generate a specified software policy containing the uploaded units in one step.</p> <p>Syntax:</p> <pre>/opt/opsware/mm_wordbot/util/import_aix_packages -p &lt;full name and path where SA Software Policy will be created&gt; &lt;directory containing AIX packages&gt;</pre> <p>Example:</p> <pre>/opt/opsware/mm_wordbot/util/import_aix_packages -p /AIX/AIX6.1/AIXPOLICY /var/tmp/aix_package_file_directory</pre>
--policy_ mode=POLICY_MODE	policy installation semantics: 'update_all', 'install_latest'
-s, --silent	Display errors only
-u USERNAME, -- username=USERNAME	Upload packages as specified user (default: opsware)
-v, --verbose	Display verbose output
--manual	Show manual page and exit

#### Using multiple options

If you are using multiple options, there is no rule about the sequence of the options as long as the command ends with the <directory containing AIX packages> parameter.

For example, these commands would work equally well to import AIX 6.1 patches and create a policy with the uploaded fileset:

```
/opt/opsware/mm_wordbot/util/import_aix_packages -p /AIX/AIX6.1/aix_policy -o '6.1'  
/var/tmp/aix_package_file_directory
```

OR

```
/opt/opsware/mm_wordbot/util/import_aix_packages -o '6.1' -p /AIX/AIX6.1/aix_  
policy/var/ tmp/aix_package_file_directory
```

## 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, 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.

## 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 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.

## Upload 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**.

The selected item should appear in the File(s) field in the Import Software window.

6. Select the appropriate type from the Type drop-down list.

The type is often populated based on the extension of the selected file. Review the listed types to make sure the best one is selected for your import.

7. In the **Folder** field, select the desired directory of the SA Library.

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.

When the import is complete, the Status column will indicate the results:

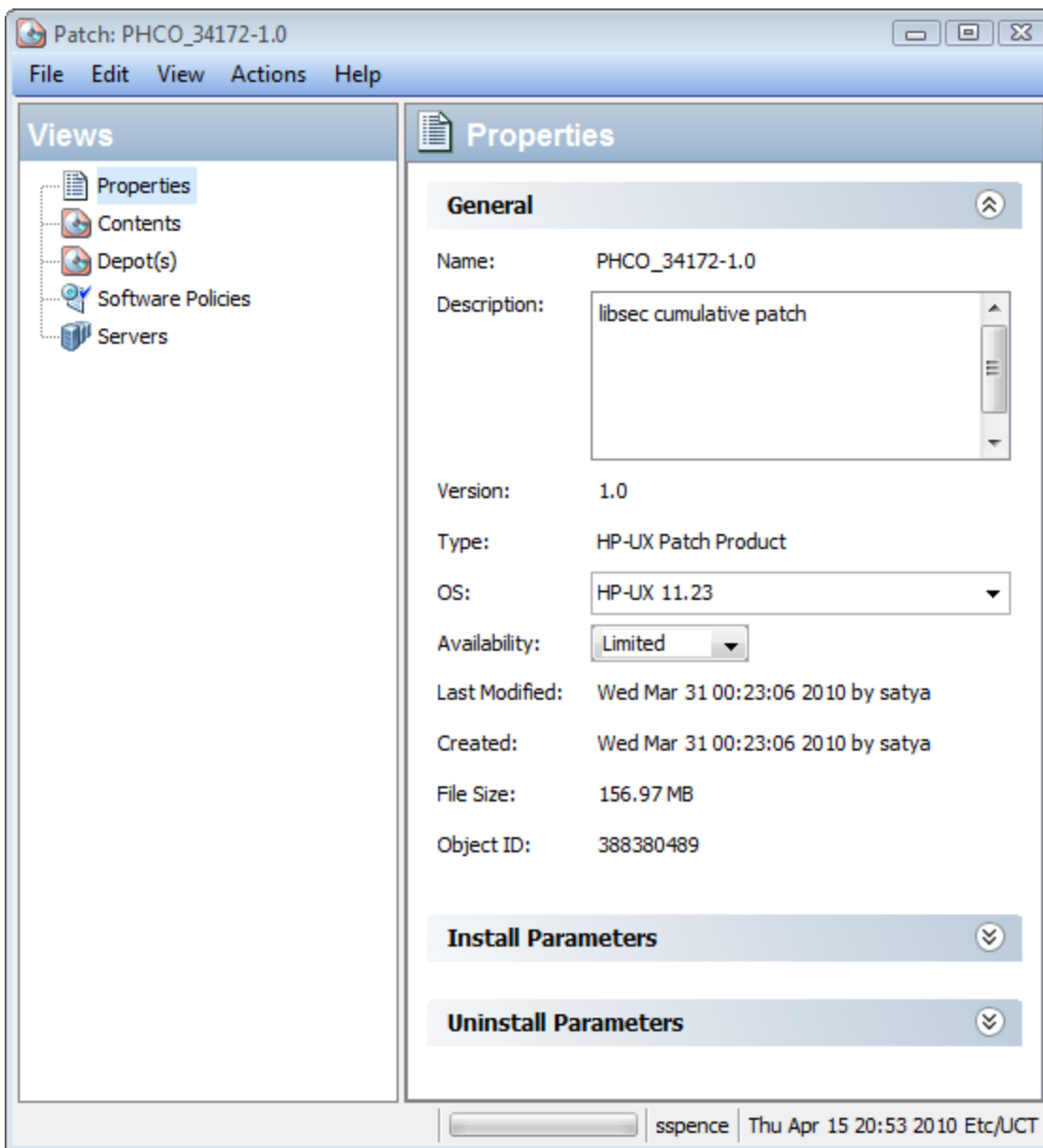
- A check mark in the Status column indicates success.
- An X in the Status column indicates an error. Click the **X** to view the error details.

10. To find the imported patch, use the Search tool from the **By Type** tab in the SA Library.

## Unix patch information

The SA Client displays detailed information about a patch in several different views. For example, the following figure 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 "[View and edit Unix patch properties](#)" on page 226.

### 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 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 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 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 ["Manage properties" on page 154](#).
- 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.

## 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.

## 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 114](#).

## 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.

## View and edit Unix patch properties

The SA Client displays information about Unix patches that have been imported into Server Automation as described in "[Unix patch information](#)" on page 223. 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.

## Find 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.

## Export 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**.

## Delete 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**.

## Use 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 14 and "[Patch](#)

[management for Solaris "](#) on page 114.

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 Administration 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 Administration 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 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 two phases:

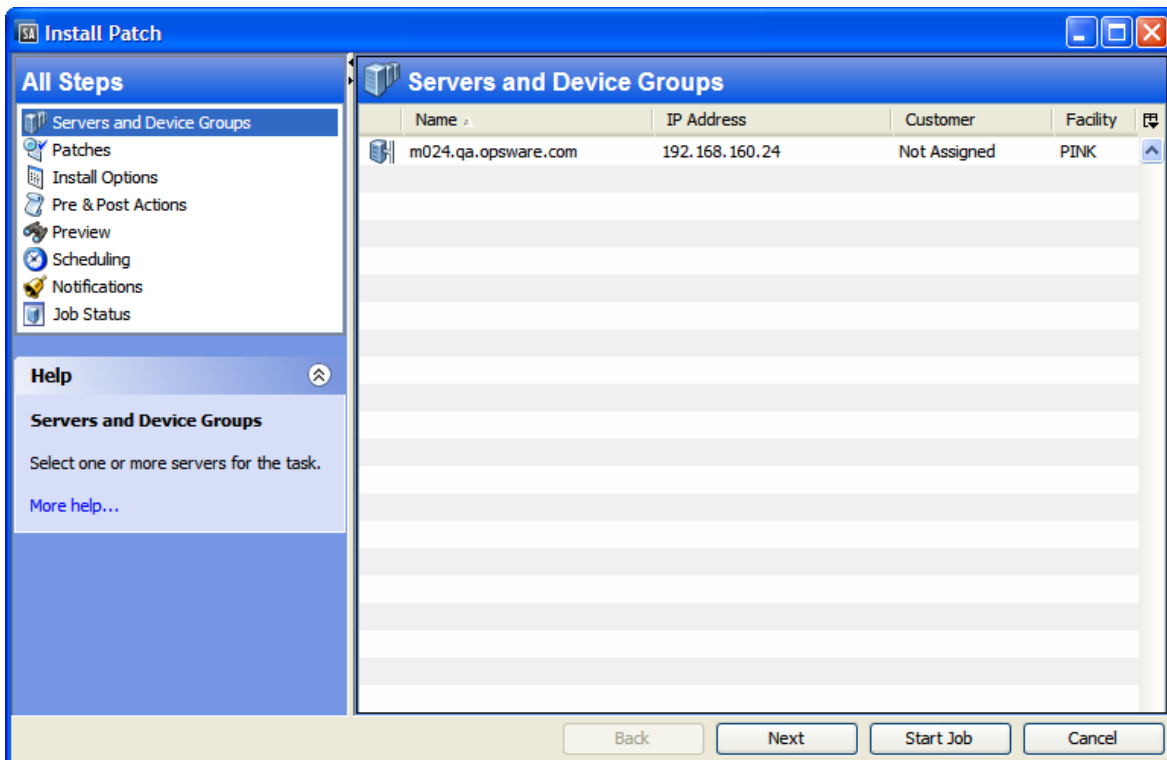
- **Download phase** - This is when the patch is downloaded from Server Automation to the managed server. This phase is commonly referred to as staging.
- **Installation phase** - This is when the patch is installed on the managed server. This phase is commonly referred to as deployment.

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 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.

### Install Patch wizard



## Installation flags

You can specify installation flags that are applied whenever a Unix patch is installed. However, 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 Server Automation. See ["Set install options" on the next page](#) for information about how to specify commands.

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

### 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.

## Install a 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.

**Note:** 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:

- ["Set reboot options" on the next page](#)
- ["Specify install scripts" on the next page](#)
- ["Scheduling a patch uninstallation" on page 239](#)
- ["Set up email notifications" on page 234](#)
- ["Preview a patch installation" on page 234](#)
- ["View job progress for a patch uninstallation" on page 240](#)

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.

## Set 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.

## Set 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.

## Specify 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 Server Automation with the SA 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 Runtime Options. If you choose a user account other than root, enter the User Name and Password. 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.

## Schedule 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.



**Note:**

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

## Set 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.

**Note:**

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

## Preview 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. 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.
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.

## View 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: 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 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

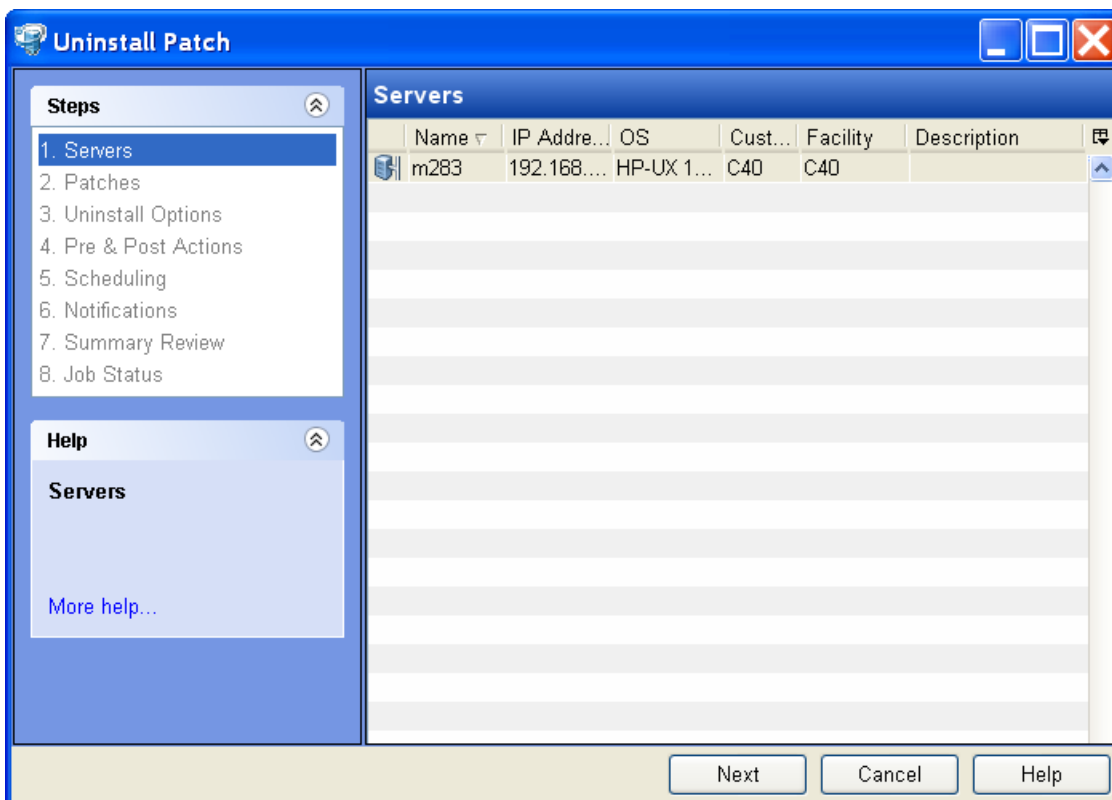
SA provides granular control over how and under what conditions Unix patches are uninstalled (removed) from managed servers. To minimize problems, you can only uninstall one patch at a time. You cannot use SA to uninstall a patch that was not installed using SA.

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.

### Uninstall Patch window



## Uninstallation flags

You can specify uninstallation flags that are applied whenever a Unix patch is uninstalled. However, 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 Server Automation.

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

### 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 **UninstallPatch**.

The first step of the Uninstall Patch window appears: Servers. For instructions on each step, see the following sections:

- ["Set reboot options" on the next page](#)
- ["Specifying pre-installation and post-installation scripts" on the next page](#)
- ["Scheduling a patch uninstallation" on page 239](#)
- ["Set up email notifications" on page 239](#)
- ["View job progress for a patch uninstallation" on page 240](#)

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.

## Set 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.

## Set 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-installation and post-installation 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 Server Automation with the SA 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 **Runtime** Options. If you choose a user account other than root, enter the User Name and Password. 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.

## Set 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.

## Preview 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.

## View 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**: 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. .

3. Click **End Job** to prevent the job from running or click **Close** to close the Uninstall Patch window.

## Patch management for Red Hat Enterprise Linux

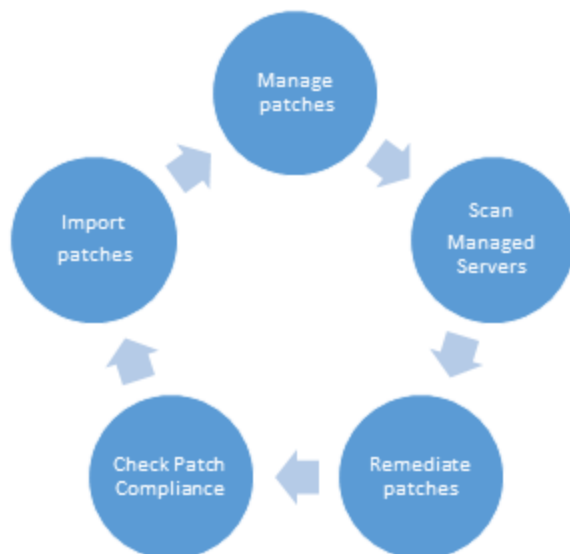
Server Automation patch management for Red Hat Enterprise Linux enables you to manage security and non-security patches for your Red Hat supported Managed Servers. It allows you to identify, install, and audit Red Hat package updates, keeping a high level of security across managed servers in your organization.

In Server Automation, patches are the equivalent of Red Hat errata. The latter are package updates, bug fixes, and security patches for Red Hat Linux. They have been tested and approved by Red Hat, Inc. and can be found at <https://rhn.redhat.com/errata/>.

### High-level architecture

Server Automation Red Hat patching mechanism allows you to import patches from Red Hat or from other sources, scan managed servers to determine their current patching level and perform the deployment of patches. Finally, the server can be checked for compliance against the recommended set of patches.

The following figure displays the high level architecture for the Server Automation Red Hat patching mechanism.



A typical Red Hat patching use case follows a well-defined process. Patches are first imported into Server Automation. This is followed by an optional step where you can manage the patches. In the third step we need to determine what patches are recommended for the Red Hat managed patches. The result of this step is dependent on the patching levels of each of your managed servers. In other words,

two machines with the same Red Hat platform can have different patches recommended. Once the recommended patches are found, the managed servers can be remediated. After the remediation occurs, the patched servers can be checked for compliance.

## Import patches for Red Hat platforms

A Red Hat patch in the Server Automation terminology is equivalent to an RPM package. This means that you can have your own custom packages imported in Server Automation that can be found applicable to a set of managed servers. The import process uploads the RPM patches into the SA Library and, since they are treated as normal RPM packages, you can use them in operations like Software Installation, Software Policy creation and remediation, Software Compliance, and so on.

Currently, there are three ways to import Red Hat patches into Server Automation. The first one will be to upload the RPM packages into SA Library using the Server Automation Command Line Interface. For details on OCLI, see the SA User Guide.

The second way of importing Red Hat packages into Server Automation is through SA Client built in importer. This tool allows importing of multiple RPM packages simultaneously. If a RPM package that is being uploaded already exists in the SA Library, you can replace (overwrite) the contents of the existing package, skip the package import (useful when importing multiple packages), or cancel the import in progress. When overwriting an existing software package, SA preserves any reboot options or flags previously set for the package. For a detailed guide on how to import Red Hat patches using the SA Client see the SA User Guide, specifically the Import Software Packages section.

The first two approaches work best for scenarios where custom patches must be imported into SA. To import the official patches issued by Red Hat you have to use the Server Automation Red Hat Importer tool which comes preinstalled with the slice component. You can find the binaries for this tool in `/opt/opsware/rhn_import/bin`.

## Importing Red Hat Errata and channels in SA using SA Red Hat Importer tool

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

The `rhn_import` and `redhat_import` CLI programs provided by Server Automation enable you to create policies which correspond to Red Hat errata and channels. Using the CLI programs, you can create the following types of policies:

- **Channel-based software policy:** A Red Hat Network channel contains a list of packages. A channel allows you group packages as per your organizational requirements. For example, a channel may contain packages for a particular Red Hat operating system version or architecture. A channel may contain other child channels. When you run the importer, Server Automation downloads the latest packages from the Red Hat Network channel, imports the packages to the Server Automation Library and creates a channel based software policy.

Thus, a channel based policy reflects a particular channel. In the SA Client, you can view the name, description, location, availability, and the operating system version of the channel based policy in the Library.

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

To create and maintain policies from the Red Hat Linux errata, erratum, and channels, log into the core server running the Software Repository component (part of the Slice Component bundle) and run the `redhat_import` program located in the `/opt/opsware/rhnc_import/bin/redhat_import` directory.

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

Importing RPM packages from the Red Hat Network to Server Automation requires a large amount of disk space. Over a period of time, the amount of disk space required increases as new versions of packages are released by Red Hat. HP recommend having at least 5 GB of disk space available in Software Repository for every Red Hat channel you enable using the importer.

To view the complete documentation run the program with the following option:

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

When you run the importer you can specify the options listed in the documentation provided by the tool or use the Configuration File provided by Server Automation. This is located in the `/etc/opt/opsware/rhnc_import/redhat_import.conf` file.

Users of `redhat_import` should notice improved performance when importing from Red Hat Subscription Management (RHSM) compared to importing the same content from Red Hat Network Classic (RHN).

## Red Hat Subscription Management overview

RHSM is the primary subscription management service provided by Red Hat and is the replacement for Red Hat Network Classic (RHN). RHSM is an end-to-end solution with status, inventory, organization, and reporting for Red Hat subscriptions via a hosted web-interface accessed from the Red Hat Customer Portal.

Although subscription management was primarily established on Red Hat Enterprise Linux, all Red Hat products are expected to be integrated with Red Hat Subscription Management. Red Hat Subscription

Services are available for systems running Red Hat Enterprise Linux 5 (5.7 or later), 6 (6.1 or later) and 7.

Systems running RHEL 5 (5.7+) and 6 (6.1+) can subscribe to both RHN and RHSM. However, RHEL 7 systems can only subscribe to RHSM, unless using Red Hat Satellite 5.6 or above. A direct consequence of this is that the RHEL 7 channels are not available in RHN which means that the old `rhncp` cannot be used to import RHEL 7 content into the SA Library. The RHEL 7 channels are only available when using Satellite 5.6 or above. The old `rhncp` tool can only be used to import RHEL 7 content when used behind a Satellite 5.6 or Satellite 5.7.

**Note:** More details about the specific supported versions can be found in the SA Support and Compatibility Matrix associated with your SA version.

The following table provides a mapping between the subscription tools provided by Red Hat and the content they provide.

Subscription Type	Content Provided	SA Import Tool
Red Hat Network Classic (RHN)	Everything except channels for Red Hat Enterprise Linux 7	<code>rhncp</code> <code>redhatcp</code>
Red Hat Subscription Management (RHSM)	Everything including channels for Red Hat Enterprise Linux 7 and above	<code>redhatcp</code>
Red Hat Satellite 4.x and 5.x (up to and including version 5.5)	Everything except channels for Red Hat Enterprise Linux 7	<code>rhncp</code> <code>redhatcp</code>
Red Hat Satellite 5.6 and 5.7	Everything including channels for Red Hat Enterprise Linux 7	<code>rhncp</code> <code>redhatcp</code>
Red Hat Satellite 6.x	Everything including channels for Red Hat Enterprise Linux 7 and above	<code>redhatcp</code>

The new `redhatcp` tool is the preferred way to import Red Hat content and will be detailed in the sections that will follow.

## RHN Classic, RHSM, and Satellite

There are some conceptual differences between Red Hat Subscription Management and RHN Classic, and this translates into differences in the way that subscriptions are defined. In older subscription models — the model used by RHN Classic and Satellite 5 — a system required channel entitlements which granted access to sets of content and software — commonly known as channels.

Red Hat Subscription Management and Satellite 6 uses public-key infrastructure (PKI) certificates to uniquely identify the system, the products on the system, and their attached subscriptions.

The old and new subscription models are fundamentally different. The old `rhncp` tool is associated with the old subscription model and thus is only capable of importing content from RHN Classic, and Satellite 5. To support Red Hat Customer Portal and Satellite 6 with the new subscription model — that is RHSM — a new tool has been added.

## Content import using Red Hat Subscription Management

The Server Automation RHN import has been enhanced to support content import from both RHN and RHSM. This allows for content import for RHEL 7 and other Red Hat products using RHSM.

### redhat\_import binary

To support content import from RHSM, a new binary has been added: `redhat_import`. This binary is capable of importing from both RHN and RHSM and uses an updated configuration file format (see ["redhat\\_import configuration file" below](#)). The behavior of the old `rhn_import` binary has not been changed and it uses the old configuration file format. Users that do not need to import content from RHSM can still use the `rhn_import` binary without any changes to the configuration file. However users are encouraged to migrate to the new `redhat_import` binary.

### redhat\_import configuration file

Users using the new binary file will have to migrate the existing configuration files to the new format. The new `redhat_import` binary does not work with old configuration files.

The `redhat_import` configuration file adds two new sections [RHN] and [RHSM] to control the import from RHN and RHSM respectively. For more details on the format of the `redhat_import` configuration file, see the manual page of `redhat_import`:

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

A sample configuration file is available at:

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

## Entitlement certificates

Red Hat subscriptions provide software entitlements. The actual content is delivered through the Red Hat Content Delivery Network (CDN) or through Red Hat Satellite 6.

**Note:** In the following sections, CDN is used to denote content imported from either Red Hat CDN or Satellite 6. When there are specifics to the online portal, Red Hat CDN will be used to denote the difference.

RHSM uses the following X.509 certificates for managing subscriptions:

- **Identity certificate** - Issued to a system upon registration with the subscription management service. This certificate is used to authenticate and identify the system to the subscription management service.
- **Product certificate** - Generated and installed on a system once a product is installed. This certificate contains information about the specific system that the product is installed on (such as its hardware and architecture) and the product name, version, and namespace.
- **Entitlement certificate** - Contains a list of subscriptions for a system, including information about the products and quantities, content repositories, roles, and different namespaces.

To be able to connect to Red Hat CDN or Satellite 6 and download content, `redhat_import` requires an entitlement certificate from RHSM. This must be available on the SA Core where `redhat_import` is run. `redhat_import` does not use the identity and product certificates.

The entitlement certificate must be generated on the Red Hat Customer Portal or on the Satellite 6 if you want to import content from the Satellite. The next step is to download the certificate and place it on the SA Core.

To generate an entitlement certificate, perform the following steps:

1. Register a system (unit):
  - For Red Hat Customer Portal, the easiest way to achieve this is to register an offline system by providing the system details on the Red Hat Customer Portal. However, if you already have a suitable system that is registered on the Red Hat Customer Portal, you can reuse it.
  - For Red Hat Satellite 6, there is no official way of registering offline systems. To proceed to the next step, you need to have a suitable system that can be registered to the Satellite server using the `subscription_management` tool provided by Red Hat.
2. Attach a subscription to the registered system.
  - The attached subscription is required to cover the Red Hat product(s) that you need to download using `redhat_import`. For example, if you need to download content for RHEL 7, `x86_64`, the subscription needs to cover Red Hat Enterprise Linux product.
  - For the Red Hat Customer Portal, the entitlement certificate is available on the portal.
  - For Satellite 6, the default path for entitlement certificate is `/etc/pki/entitlement`. This is available on the system registered with the Satellite server. Usually you will find two `.pem` files (a public and a private key). You should concatenate these two files into a single `.pem` file. This will be the entitlement certificate that must be downloaded to the SA Core.

## Multiple entitlement certificates

`redhat_import` supports multiple entitlement certificates. If you need to import content that is not covered by any of the existing entitlement certificates, you can generate a new entitlement certificate, covering the required CDN content and add it to the `redhat_import` configuration file.

No entitlement certificate is required for `rhn_import` binary or when `redhat_import` binary is only used to download content from RHN.

**Note:** As a best practice, do not mix entitlements for Red Hat Customer Portal with entitlements for Red Hat Satellite 6.

## Install Red Hat CA certificates

SA Red Hat importer validates the server certificates for Red Hat Network Classic (RHN), Red Hat Subscription Management (RHSM) and Red Hat Satellite. By default SA comes bundled with CA certificates only for RHN. Out of the three content providers only Red Hat Network Classic is signed by a certificate authority trusted by both SA and Red Hat.

RHSM and Red Hat Satellite servers have self signed certificates so by default there is no CA certificate bundled for these two content providers with SA `rhn_import` component. To enable access

to Red Hat Subscription Management and/or Red Hat Satellite you need to install the self signed server certificate in the openssl trust store.

Depending on your use cases you only need to install the RHSM server certificate if you are using the new Red Hat Subscription Management content provider, or the satellite server certificate in case you have a Red Hat Satellite and want to import from it. Otherwise, if you only use RHN as a provider you can safely skip this section.

The process of installing a certificate in the trust store is split in three steps:

1. Download the self signed certificate from RHSM/Red Hat Satellite
2. Install the self signed certificate in SA trust store
3. Verify that openssl is validating the server certificate

The first step is different on RHSM and Red Hat Satellite server while the last two steps are the same for both content providers.

## Downloading the self-signed certificate

### Download RHSM self-signed certificate

The RSHM server certificate is not signed by a public certificate authority. You have to use the openssl tool to download the certificate chain for `cdn.redhat.com`. After download, extract the last certificate issued by `Entitlement Master CA` and copy it into a `.pem` file:

A command example to download the certificate chain for RHSM:

```
/opt/opsware/bin/openssl s_client -connect cdn.redhat.com:443 -prexit -showcerts
```

**Note:** The latest released version of openssl (i.e openssl-1.0.2h) does not work with HTTP proxies. The easiest option is to use a web browser to download the certificate.

### Download Red Hat Satellite self-signed certificate

The self signed certificate is made public by Red Hat Satellite server at `/pub/RHN-ORG-TRUSTED-SSL-CERT`. Run the following command to download the certificate file:

```
wget -O /tmp/RHN-ORG-TRUSTED-SSL-CERT http://redhat.satellite.hostname/pub/RHN-ORG-TRUSTED-SSL-CERT
```

If you need proxy access to the Red Hat Satellite server, you can export the `http_proxy` environment variable and `wget` will use the value exported.

## Installing the self-signed certificate in SA trust store

At the end of the downloaded certificate, a block similar to the following appears:

```
-----BEGIN CERTIFICATE-----  
MIIE4TCCA8mgAwIBAgIJANwa50FPkBHMA0GCSqGSIb3DQEBCwUAMIGGMQswCQYD  
haXhmbq+5pEkpxGAactW+tORsJmpgTdAXeq2rreYtgZ2/vCwdM0iwSVakGNFAvni  
T9lnSVrADc0/S8V/Dzch30RzSpIS44beE23zag82019fCrsZg9VkYJER4Fn0tRq4  
6U9I40gBSPSU34MXc1Gld0BAN+mANWHQYacZ7hHQJtMRP+mc8ZgHIVsKNnKR0H0d  
Rh1a7cP7GYrXn/piQAxRW66fOYJOeVIsAWJvgUb+A8ecwb+s6k56cQdLkkm0wKD0 2zUFMAg= -----END  
CERTIFICATE-----
```

Append the block to the end of `/opt/opsware/openssl/cert.pem`. At this point, the certificate is installed in the SA trust store. Ensure that `openssl` tool can verify the RHSM and/or Red Hat Satellite server certificate.

## Verifying that openssl is validating the server certificate

After the CA certificate is installed in SA trust store, you must verify if the SA-bundled `openssl` validates the installed certificates before running the importer. To do so, run the following command:

```
/opt/opsware/bin/openssl s_client -connect rhsm.or.satellite.hostname:443 -verify 3
```

If the verification succeeds at the end of the output, the following message appears:

```
Verify return code: 0 (ok)
```

In case of an error, a return code different than 0 appears, for example:

```
Verify return code: 21 (unable to verify the first certificate)
```

**Note:** Since `openssl` cannot work behind a proxy, the above command might not work if there is an HTTP proxy in your local network.

## Content labels

When importing from RHSM, `redhat_import` uses content labels to identify the CDN content to import. The format of the content label is the following:

```
<entitlement_content_label>{<releasever>-<basearch>}
```

where:

- `<entitlement_content_label>` is the content label as specified in the entitlement certificate
- `<releasever>` is the release version of Red Hat Enterprise Linux. This has the same value as the `$releasever yum` variable
- `<basearch>` is the base architecture of the system. This has the same value as the `$basearch yum` variable

`<releasever>` is not required for all contents; when it is not used, the format of the content label becomes `<entitlement_content_label>{<basearch>}`

To determine the label of the CDN content to import, the following steps can be performed:

- If the content to import belongs to one of the SA-supported platforms then the content label to use can be found by running:  

```
redhat_import --show_labels
```
- If the content to import belongs to any other Red Hat product that is not listed by `--show_labels`, the content label to use can be determined as follows:
  - Locate the content section for the product in the entitlement certificate. The content of the entitlement certificate can be visualized using the `rct` tool. For more details on the `rct` tool, see [https://access.redhat.com/documentation/en-US/Red\\_Hat\\_Subscription\\_Management/1/html/RHSM/rct-tool.html](https://access.redhat.com/documentation/en-US/Red_Hat_Subscription_Management/1/html/RHSM/rct-tool.html)
  - Extract the content label from the entitlement certificate and construct the `redhat_import` content label by appending the `<releasever>` and `<basearch>` between curly braces.



For example, to import content for RHEL Server 6.4 from Red Hat Extended Update Support, the content in the example below needs to be located in the entitlement certificate.

### Content for RHEL Server 6.4 from Red Hat extended update support

Content:

```
Type: yum
Name: Red Hat Enterprise Linux 6 Server - Extended Update Support (RPMs)
Label: rhel-6-server-eus-rpms
Vendor: Red Hat
URL: /content/eus/rhel/server/6/$releasever/$basearch/os
GPG: file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Enabled: True
Expires: 86400
Required Tags: rhel-6-server
Archives: x86_64, x86
```

The entitlement content label is “rhel-6-server-eus-rpms”. To import version 6.4 for x86\_64, the content label needs to be specified as:

```
rhel-6-server-eus-rpms{6.4-x86_64}
```

As another example, to import content from RHEL 7 Server Extras repository, the content in the example below needs to be located in the entitlement certificate.

### Content for RHEL 7 Server Extras Repository

Content:

```
Type: yum
Name: Red Hat Enterprise Linux 7 Server - Extras (RPMs)
Label: rhel-7-server-extras-rpms
Vendor: Red Hat
URL: /content/dist/rhel/server/7/7Server/$basearch/extras/os
GPG: file:///etc/pki/rpm-gpg/RPM-GPG-KEY-redhat-release
Enabled: False
Expires: 86400
Required Tags: rhel-7-server
Archives: x86_64
```

The entitlement content label is “rhel-7-server-extras-rpms”. In this case, the content URL does not contain the <releasever> variable so this should not be included in the redhat\_import content label. To import the packages for x86\_64 architecture, the content label needs to be specified as:

```
rhel-7-server-extras-rpms{x86_64}
```

## Sample use cases

### Import only from RHN

To import content only from RHN, the [RHSM] section should not be present in the configuration file.

#### Sample RHN configuration file

```
# main section
```

```
[main]

package_search_path=
    /Package Repository/OS Media/$opsware_platform
    /Package Repository/All Red Hat Linux/$opsware_platform
    /Migrated/Package Repository/Customer Independent/$opsware_platform

# RHN section. Contains options specific to import from RHN that apply to all
channel labels
[RHN]

# Required options to login to Red Hat Network
rhn_user=USERNAME
rhn_pass=PASSWORD

channels: rhel-x86_64-server-5 rhel-x86_64-server-6

# SA recommendations:
package_path=/RHN/Packages/$channel_name
channel_path=/RHN/Channels/$parent_channel_name/$channel_name Policy
erratum_path=/RHN/Errata/$erratum_type Policies/$erratum_name
errata_path =/RHN/Errata/$parent_channel_name/$channel_name Advisory Roll-Up Policy

Provided that this configuration file is available at the default location (/etc/opt/opsware/rhn_
import/redhat_import.conf), redhat_import can be run without any command line options to
import content for the channels with the following labels as specified by the “channels” option in the
above sample configuration file.

• rhel-x86_64-server-5
• rhel-x86_64-server-6
```

## Import only from RHSM

To import content only from RHSM, the [RHN] section should not be present in the configuration file.

### Sample RHSM configuration file

```
# main section
[main]

package_search_path=
    /Package Repository/OS Media/$opsware_platform
    /Package Repository/All Red Hat Linux/$opsware_platform
    /Migrated/Package Repository/Customer Independent/$opsware_platform

# RHSM section. Contains options specific to import from CDN that apply to all
content labels
[RHSM]
# To sync from Red Hat Network Satellite 6.1 or later:
; satellite_host=HOSTNAME
```

```
# Specify one or more paths to entitlement certificates. To specify multiple paths,  
# place each path on its own line, indenting any additional lines.  
certificate_paths=/etc/opt/opsware/rhn_import/8a85f981478d1fa601478e12507f36e8.pem  
  
content_labels=rhel-7-server-rpms{7Server-x86_64} rhel-6-server-rpms{6Server-x86_64}  
  
# SA recommendations:  
package_path=/RHSM/Packages/$content_name  
content_policy_path=/RHSM/Content/$content_name Policy  
erratum_policy_path=/RHSM/Errata/$erratum_type Policies/$erratum_name  
errata_policy_path =/RHSM/Errata/$content_name Advisory Roll-Up Policy
```

Provided that this configuration file is available at the default location, (/etc/opt/opsware/rhn\_import/redhat\_import.conf), redhat\_import can be run without any command line options to import the CDN contents with the following labels:

- rhel-7-server-rpms{7Server-x86\_64}
- rhel-6-server-rpms{6Server-x86\_64}

### RHSM options

The following table describes the options presented in the sample RHSM configuration file:

Option	Description
satellite_host	This option defines whether or not to import from Satellite 6. When this option is enabled and a valid hostname is provided, the importer will connect to the Satellite 6 and import from there. If this option is not enabled, then the importer will connect to Red Hat CDN for content import.
certificate_paths	This option defines the path to the entitlement certificate. The certificate must provide entitlement to content you wish to download. You can download the certificate from the Red Hat Customer Portal after a subscription is attached to a system that is registered with Red Hat Customer Portal. For more information about the subscription and entitlement certification process, see Entitlement Certificates.
content_labels	This option defines the labels of the CDN contents that need to be imported into the SA Library. See " <a href="#">Content labels</a> " on page 248 for more details on the format of the content labels.

## Importing from both RHN and RHSM

```
[main]
```

```
package_search_path=  
  /Package Repository/OS Media/$opsware_platform  
  /Package Repository/All Red Hat Linux/$opsware_platform  
  /Migrated/Package Repository/Customer Independent/$opsware_platform
```

```
# RHN section. Contains options specific to import from RHN that apply to all
channel labels
[RHN]
rhn_user=USERNAME
rhn_pass=PASSWORD

channels: rhel-x86_64-server-6

# SA recommendations:
package_path=/RHN/Packages/$channel_name
channel_path=/RHN/Channels/$parent_channel_name/$channel_name Policy
erratum_path=/RHN/Errata/$erratum_type Policies/$erratum_name
errata_path =/RHN/Errata/$parent_channel_name/$channel_name Advisory Roll-Up Policy

[rhel-x86_64-server-extras-6]
enabled=1
; platform = Red Hat Enterprise Linux Server 6 X86_64
# RHSM section. Contains options specific to import from CDN that apply to all
content labels
[RHSM]
# To sync from Red Hat Network Satellite 6.1 or later:
; satellite_host=HOSTNAME

# Specify one or more paths to entitlement certificates. To specify multiple paths,
# place each path on its own line, indenting any additional lines.
certificate_paths=/etc/opt/opsware/rhn_import/8a85f981478d1fa601478e12507f36e8.pem

content_labels=rhel-7-server-rpms{x86_64}

# SA recommendations:
package_path=/RHSM/Packages/$content_name
content_policy_path=/RHSM/Content/$content_name Policy
erratum_policy_path=/RHSM/Errata/$erratum_type Policies/$erratum_name
errata_policy_path =/RHSM/Errata/$content_name Advisory Roll-Up Policy

[rhel-7-server-extras-rpms{x86_64}]
enabled=1
platform=Red Hat Enterprise Linux Server 7 X86_64

Provided that this configuration file is available at the default location (/etc/opt/opsware/rhn_
import/redhat_import.conf), redhat_import can be run without any command line options to
import content for the following RHN channels and RHSM contents:

RHN:

• rhel-x86_64-server-6
• rhel-x86_64-server-extras-6

RHSM:
```

- `rhel-7-server-rpms{x86_64}`
  - `rhel-7-server-extras-rpms{x86_64}`
- RHN channels have a parent-child relationship. In this example “`rhel-x86_64-server-extras-6`” is a child of “`rhel-x86_64-server-6`”. By default, child channels are imported under the platform of the parent channel in the SA Library. This is why the “`platform`” option is commented out under “`rhel-x86_64-server-extras-6`” section and the import still works fine.
  - CDN contents do not have any parent-child relationship. As a result of this any content that is not mapped by default to one of the SA-supported platforms needs to have its own content section and define the “`platform`” option. This is the case for “`rhel-7-server-extras-rpms{x86_64}`” above. Failure to define the “`platform`” option for such contents will result in the content label being ignored during import with a warning message being displayed, similar to the following:

```
Unable to process content label rhel-7-server-extras-rpms{x86_64}. No
platform could be associated with this label. This content label will be
dropped. If you need to import this content, add the 'platform' option to the
configuration file.
Ignoring unknown content label rhel-7-server-extras-rpms{x86_64}
```

## Migration

Users of the old `rhn_import` binary are encouraged to migrate to the new `redhat_import` binary. Multiple migration paths are available as described in the following sections.

### Continue usage of RHN

Users can migrate from `rhn_import` to `redhat_import` and continue to use RHN to import content. In this case the only requirement is to migrate the configuration file from the old format to the new format. For more details on the `redhat_import` configuration file format see `redhat_import` configuration file.

Once the configuration is migrated to the new format, while preserving the existing SA Library paths, `redhat_import` will update the existing packages and software policies, making the migration transparent. Moreover, new products that have not been imported in the SA Library can be imported from RHSM while the old products continue to be imported from RHN. For example, a user who is already importing RHEL 5 and 6 content from RHN can start importing RHEL 7 content from RHSM while still using RHN for the older RHEL 5 and 6. For a sample configuration that allows import from both RHN and RHSM see [Import from both RHN and RHSM](#).

### Partial migration to RHSM

This section only applies to users who are using the SA-recommended library paths. Users using custom SA Library paths should derive their own migration procedure based on the instructions in this section. The SA-recommended library paths are as follows:

- RHN
  - `package_path=/RHN/Packages/$channel_name`
  - `channel_path=/RHN/Channels/$parent_channel_name/$channel_name Policy`
  - `erratum_path=/RHN/Errata/$erratum_type Policies/$erratum_name`
  - `errata_path =/RHN/Errata/$parent_channel_name/$channel_name Advisory Roll-Up Policy`
- RHSM
  - `package_path=/RHSM/Packages/$content_name`
  - `content_policy_path=/RHSM/Content/$content_name Policy`
  - `erratum_policy_path=/RHSM/Errata/$erratum_type Policies/$erratum_name`
  - `errata_policy_path =/RHSM/Errata/$content_name Advisory Roll-Up Policy`

This section describes the scenario where a user is currently using RHN to import some channels and would like to start using RHSM to import a subset of these channels while still using RHN for the other channels.

To achieve partial migration to RHSM, perform the following steps:

1. Migrate from `rhn_import` to `redhat_import` and convert the configuration file to the new format
2. In the SA Library, move the channel policies of the channels that need to be migrated to the RHSM **content\_policy\_path** folder (`/RHSM/Content`). Rename these channel policies to content policies "`$content_name Policy`". The value of the "`$content_name`" variable can be found in the entitlement certificate or by using `--show_labels` for CDN contents mapped to SA-supported platforms. This ensures that `redhat_import` will update these content policies instead of creating new ones.
3. Move the errata policies of the channels that need to be migrated to the RHSM **errata\_policy\_path** folder (`/RHSM/Errata`). Rename these errata policies to be compliant with RHSM format "`$content_name Advisory Roll-Up Policy.`" The value of the "`$content_name`" variable can be found in the entitlement certificate or by using `--show_labels` for CDN contents mapped to SA-supported platforms. This ensures that `redhat_import` will update these errata policies instead of creating new ones.
4. Move the package folders of the channels that need to be migrated to the RHSM **package\_path** folder (`/RHSM/Packages`). Rename these package folders to be compliant with RHSM format "`$content_name`". The value of the "`$content_name`" variable can be found in the entitlement certificate or by using `--show_labels` for CDN contents mapped to SA-supported platforms. This ensures that `redhat_import` will import packages into these folders instead of creating new folders.
5. Ensure that `redhat_import` will use the same erratum library path for both RHN and RHSM. An erratum can be available in multiple RHN channels. When using the SA-recommended library paths a single erratum policy is created even for an erratum available in multiple channels and this policy is updated with content from all channels. As not all channels are migrated to RHSM the erratum policies cannot be moved to the RHSM folders. Instead, the RHSM "`erratum_policy_path`" is updated to point to the path used by RHN (`/RHN/Errata/$erratum_type`

Policies/\$erratum\_name). The “erratum\_policy\_path” should be updated as described above only for the contents migrated from RHN, so for each such content a new content section needs to be defined in the configuration file and define the “erratum\_policy\_path” option as “/RHN/Errata/\$erratum\_type Policies/\$erratum\_name”.

6. Finally, the configuration file should be updated to ensure that the migrated channels are no longer imported from RHN and that the new CDN contents are imported from RHSM (e.g. by updating the “content\_labels” option).

**Tip:** Review your `repo.restrict.custom` attributes. If any of them refer to package folders that were moved and renamed, you need to edit the attributes to make them refer to the new package folder locations.

### Sample scenario: partial migration to RHSM

As an example, consider the case where the following channels are imported from RHN:

Red Hat Enterprise Linux (v. 5 for 64-bit x86\_64)

Red Hat Enterprise Linux Server (v. 6 for 64-bit x86\_64)

The SA Library structure concerning RHN and RHSM import would initially look as shown below

#### Example: SA Library structure for RHN and RHSM import—before partial migration

```
- RHN
| - Channels
| |   Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) Policy
| |   Red Hat Enterprise Linux Server (v. 6 for 64-bit x86_64) Policy
| - Errata
| | + Bug Fix Advisory Policies
| | + Product Enhancement Advisory Policies
| | + Security Advisory Policies
| |   Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) Advisory Roll-Up Policy
| |   Red Hat Enterprise Linux Server (v. 6 for 64-bit x86_64) Advisory Roll-Up
Policy
| - Packages
| | + Red Hat Enterprise Linux (v. 5 for 64-bit x86_64)
| | + Red Hat Enterprise Linux Server (v. 6 for 64-bit x86_64)
- RHSM
| - Content
| - Errata
| - Packages
```

If Red Hat Enterprise Linux Server (v. 6 for 64-bit x86\_64) needs to be migrated to RHSM while Red Hat Enterprise Linux (v. 5 for 64-bit x86\_64) continues to be imported from RHN, the partial migration steps would be as follows.

#### Steps for sample scenario—Partial migration to RHSM:

1. Migrate the existing configuration file to the new format required by `redhat_import`. For details on the `redhat_import` configuration file format see `redhat_import` configuration file. The precise details on how to migrate the configuration file depend on the actual content of the existing

configuration file. However the resulted migrated configuration is expected to allow `redhat_import` to import the same RHN channels into the SA Library. In other words, running `redhat_import` with the migrated configuration file should yield the same result as running `rhn_import` with the old configuration file.

2. Move Red Hat Enterprise Linux Server (v. 6 for 64-bit x86\_64) Policy policy to **/RHSM/Content** folder. Rename the policy to Red Hat Enterprise Linux 6 Server (RPMs) (6Server-x86\_64) Policy.
3. Move Red Hat Enterprise Linux Server (v. 6 for 64-bit x86\_64) Advisory Roll-Up Policy policy to **/RHSM/Errata** folder. Rename the policy to Red Hat Enterprise Linux 6 Server (RPMs) (6Server-x86\_64) Advisory Roll-Up Policy.
4. Move the package folder “Red Hat Enterprise Linux Server (v. 6 for 64-bit x86\_64)” to **/RHSM/Packages** folder. Rename the package folder to “Red Hat Enterprise Linux 6 Server (RPMs) (6Server-x86\_64)”.
5. Create a new content section in the configuration file: **[rhel-6-server-rpms{6Server-x86\_64}]**. Define the `erratum_policy_path` as follows under the above section: `erratum_policy_path=/RHN/Errata/$erratum_type Policies/$erratum_name`
6. Update the configuration file to ensure that RHN channel “rhel-x86\_64-server-6” is no longer imported from RHN and the equivalent CDN content “rhel-6-server-rpms{6Server-x86\_64}” is imported from RHSM.

Following this, the SA Library folders concerning RHN and RHSM import should look as shown below.

#### Example: SA Library folders for RHN and RHSM import—after partial migration

```
- RHN
| - Channels
| | Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) Policy
| - Errata
| | + Bug Fix Advisory Policies
| | + Product Enhancement Advisory Policies
| | + Security Advisory Policies
| | Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) Advisory Roll-Up Policy
| - Packages
| | + Red Hat Enterprise Linux (v. 5 for 64-bit x86_64)
- RHSM
| - Content
| | Red Hat Enterprise Linux 6 Server (RPMs) (6Server-x86_64) Policy
| - Errata
| | Red Hat Enterprise Linux 6 Server (RPMs) (6Server-x86_64) Advisory Roll-Up
Policy
| - Packages
| | + Red Hat Enterprise Linux 6 Server (RPMs) (6Server-x86_64)
```

## Full migration to RHSM

This section only applies to users who are using the SA-recommended library paths. Users using custom SA Library paths should derive their own migration procedure based on the instructions in this section. Also this section only applies if there are no errata imported from RHSM for any CDN content. If errata are already imported from RHSM under the SA-recommended library path (`/RHSM/Errata`) and you would like to migrate some or all RHN channels to RHSM please use the instructions in Partial



migration to RHSM. This is because moving erratum policies from RHN folder structure to RHSM might conflict with existing erratum policies under the RHSM folder structure.

For a list of SA-recommended library paths, see ["Partial migration to RHSM" on page 253](#).

This section describes the scenario where a user is currently using RHN to import some channels and would like to start using RHSM to import all of these channels. Basically, after migration, no channels will be imported from RHN. To migrate only some RHN channels to RHSM, see ["Partial migration to RHSM" on page 253](#).

To achieve full migration to RHSM, perform the following steps:

1. In the SA Library, move the channel policies of the channels that need to be migrated to the RHSM **content\_policy\_path** folder (/RHSM/Content). Rename these channel policies to content policies "\$content\_name Policy". The value of the "\$content\_name" variable can be found in the entitlement certificate or by using `--show_labels` for CDN contents mapped to SA-supported platforms. This ensures that `redhat_import` will update these content policies instead of creating new ones.
2. Move the errata policies of the channels that need to be migrated to the RHSM **errata\_policy\_path** folder (/RHSM/Errata). Rename these errata policies to be compliant with RHSM format "\$content\_name Advisory Roll-Up Policy". The value of the "\$content\_name" variable can be found in the entitlement certificate or by using `--show_labels` for CDN contents mapped to SA-supported platforms. This ensures that `redhat_import` will update these errata policies instead of creating new ones.
3. Move the package folders of the channels that need to be migrated to the RHSM **package\_path** folder (/RHSM/Packages). Rename these package folders to be compliant with RHSM format "\$content\_name". The value of the "\$content\_name" variable can be found in the entitlement certificate or by using `--show_labels` for CDN contents mapped to SA-supported platforms. This ensures that `redhat_import` will import packages into these folders instead of creating new folders.
4. Move the erratum policies folders ("**Bug Fix Advisory Policies**", "**Product Enhancement Advisory Policies**", "**Security Advisory Policies**") to the RHSM "**erratum\_policy\_path**" (/RHSM/Errata).
5. Migrate from `rhn_import` to `redhat_import` and convert the configuration file to the new format. During the migration process ensure that no channels are imported from RHN and that the new CDN contents are imported from RHSM (e.g. by updating the "`content_labels`" option). The [RHN] section should not be present in the `redhat_import` configuration file.

**Tip:** Review your `repo.restrict.custom` attributes. If any of them refer to package folders that were moved and renamed, you need to edit the attributes to make them refer to the new package folder locations.

### Sample scenario: full migration to RHSM

As an example, consider the case where the following channels are imported from RHN:

- Red Hat Enterprise Linux (v. 5 for 64-bit x86\_64)
- Red Hat Enterprise Linux Server (v. 6 for 64-bit x86\_64)

The SA Library structure concerning RHN and RHSM import would initially look as shown below

### Example: SA Library folders for RHN and RHSM import—before full migration

- RHN

```
| - Channels
| |   Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) Policy
| |   Red Hat Enterprise Linux Server (v. 6 for 64-bit x86_64) Policy
| - Errata
| | + Bug Fix Advisory Policies
| | + Product Enhancement Advisory Policies
| | + Security Advisory Policies
| |   Red Hat Enterprise Linux (v. 5 for 64-bit x86_64) Advisory Roll-Up Policy
| |   Red Hat Enterprise Linux Server (v. 6 for 64-bit x86_64) Advisory Roll-Up
Policy
| - Packages
| | + Red Hat Enterprise Linux (v. 5 for 64-bit x86_64)
| | + Red Hat Enterprise Linux Server (v. 6 for 64-bit x86_64)
- RHSM
| - Content
| - Errata
| - Packages
```

If both “Red Hat Enterprise Linux Server (v. 6 for 64-bit x86\_64)” and “Red Hat Enterprise Linux (v. 5 for 64-bit x86\_64)” channels need to be migrated to RHSM, the full migration steps would be as follows:

#### Steps for Sample Scenario—pull migration to RHSM:

1. Move the following software policies to **/RHSM/Content** folder:
  - Red Hat Enterprise Linux (v. 5 for 64-bit x86\_64) Policy
  - Red Hat Enterprise Linux Server (v. 6 for 64-bit x86\_64) PolicyRename the policies to:
  - Red Hat Enterprise Linux 5 Server (RPMs) (5Server-x86\_64) Policy
  - Red Hat Enterprise Linux 6 Server (RPMs) (6Server-x86\_64) Policy
2. Move the following software policies to **/RHSM/Errata** folder:
  - Red Hat Enterprise Linux (v. 5 for 64-bit x86\_64) Advisory Roll-Up Policy
  - Red Hat Enterprise Linux Server (v. 6 for 64-bit x86\_64) Advisory Roll-Up PolicyRename the policies to:
  - Red Hat Enterprise Linux 5 Server (RPMs) (5Server-x86\_64) Advisory Roll-Up Policy
  - Red Hat Enterprise Linux 6 Server (RPMs) (6Server-x86\_64) Advisory Roll-Up Policy
3. Move the following package folders to **/RHSM/Packages** folder:
  - Red Hat Enterprise Linux (v. 5 for 64-bit x86\_64)
  - Red Hat Enterprise Linux Server (v. 6 for 64-bit x86\_64)Rename the folders to:

- Red Hat Enterprise Linux 5 Server (RPMs) (5Server-x86\_64)
  - Red Hat Enterprise Linux 6 Server (RPMs) (6Server-x86\_64)
4. Move the erratum policies folders (**Bug Fix Advisory Policies, Product Enhancement Advisory Policies, Security Advisory Policies**) to **/RHSM/Errata**.
  5. Migrate the configuration file and ensure that the CDN contents “`rhel-5-server-rpms{5Server-x86_64}`” and “`rhel-6-server-rpms{6Server-x86_64}`” are imported from RHSM. There should be no [RHN] section in the `redhat_import` configuration file as no channels are imported from RHN.

After the above steps are completed, the SA Library folders concerning RHN and RHSM import should look as shown in below.

#### Example: SA Library folders for RHN and RHSM import—after full migration

```
- RHN
| - Channels
| - Errata
| - Packages
- RHSM
| - Content
| | Red Hat Enterprise Linux 5 Server (RPMs) (5Server-x86_64) Policy
| | Red Hat Enterprise Linux 6 Server (RPMs) (6Server-x86_64) Policy
| - Errata
| | + Bug Fix Advisory Policies
| | + Product Enhancement Advisory Policies
| | + Security Advisory Policies
| | Red Hat Enterprise Linux 5 Server (RPMs) (5Server-x86_64) Advisory Roll-Up
Policy
| | Red Hat Enterprise Linux 6 Server (RPMs) (6Server-x86_64) Advisory Roll-Up
Policy
| - Packages
| | + Red Hat Enterprise Linux 5 Server (RPMs) (5Server-x86_64)
| | + Red Hat Enterprise Linux 6 Server (RPMs) (6Server-x86_64)
```

## Supported RHEL versions

When importing from RHSM, `redhat_import` supports the RHEL versions that can be managed by Red Hat Subscription Management: 5.7+, 6.1+, and 7+.

When importing from RHN, `redhat_import` supports the same channels as the old `rhncore_import` binary.

## Reuse a Red Hat import configuration file

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

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

To reuse an **rhn\_import.conf** file containing encrypted passwords on another core:

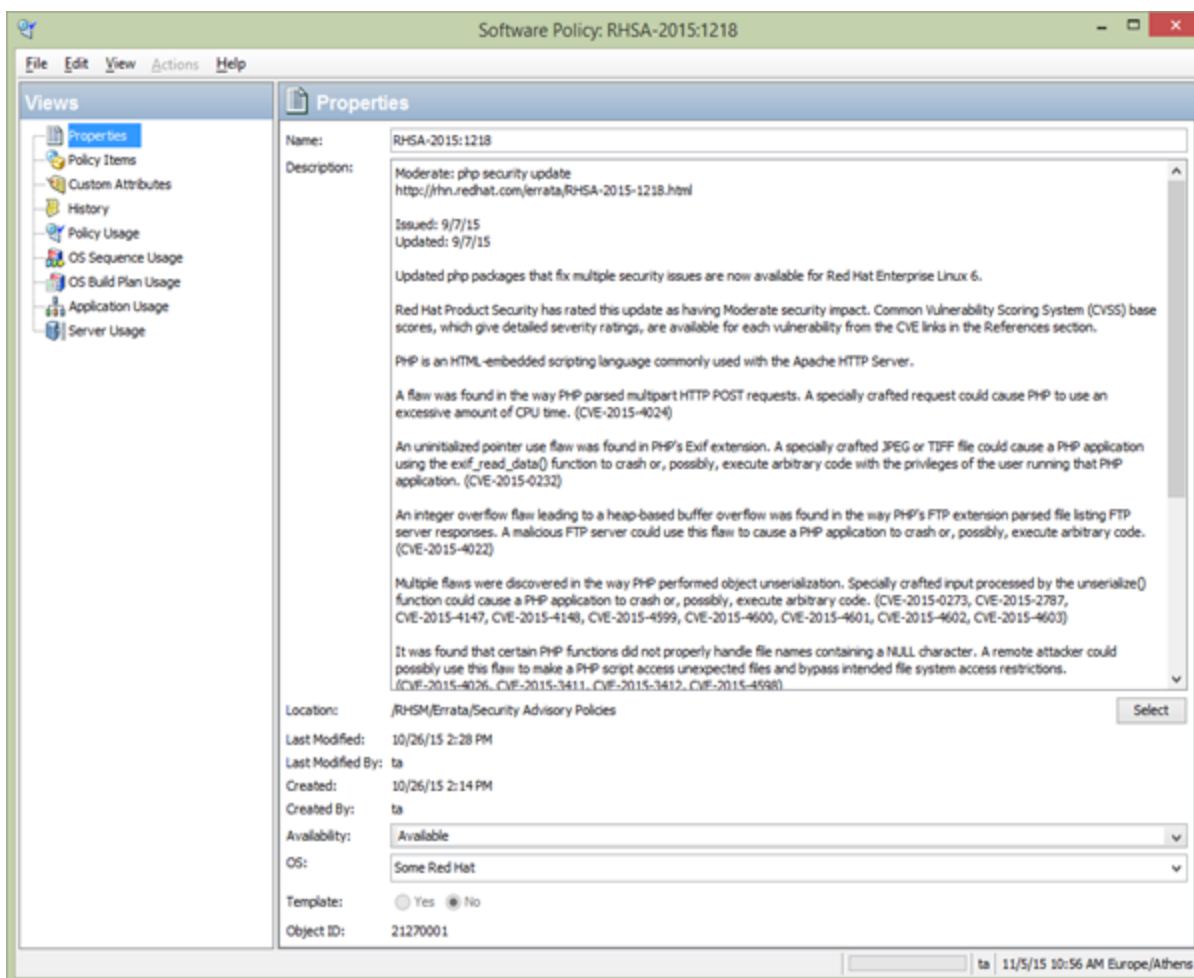
1. Change all encrypted passwords in the file into clear text.
2. Copy the **rhn\_import.conf** file to the other core.
3. Reuse the `-hide_passwords` option when running the RHN import on the new core.

## View errata based and channel based policies in the SA Client

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

To view the properties of a software policy:

1. From the navigation pane, select **Library > By Folder**.
2. Select the Red Hat Network Folder (RHN).
3. From the content pane, select the errata-based or channel-based policy and open it. The policy window appears.
4. From the Views pane, select **Properties**. You can view the properties for the policy in the content pane.



- **Name:** Contains the errata reference for the errata based software policy.
- **Description:** Includes all the errata documentation for the errata.
- **Location:** Specifies the location of the policy in the folder hierarchy. To change the location click select to specify the location for the policy in the folder hierarchy. The Select Location window appears. Select a folder in the Library to specify the location of the policy and then click **Select**.
- **Created:** Corresponds to the time when the errata was downloaded by SA to create the software policy.
- **Last Modified:** Corresponds to the time when the errata based policy was modified.
- **Availability:** Contains the SA server life cycle values for the errata based software policy. The default value for an errata based policy is set to Available.
- **Platform:** Specifies the operating systems applicable to the errata. You can expand the list to see the selected platforms.

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

## Errata caching

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

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

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

```
/var/opt/opsware/rhn_import
```

The file name uses the following pattern:

```
prev_import_ch_<label>.dat
```

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

- **prev\_import\_ch\_rhel-x86\_64-server-6.dat**
- **prev\_import\_ch\_rhel-7-server-rpms{7Server-x86\_64}.dat**

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

- An erratum is imported into SA Library and then it is removed / renamed / moved to another folder. When `rhn_import` or `redhat_import` are run next time, the erratum will not be reimported into the SA Library. This is because the erratum details are present in the cache file so it is skipped during the import.
- The errata roll-up policy is created and then it is removed, renamed, or moved to another folder (for example, by using the SA Client). When `rhn_import` or `redhat_import` are run next time the errata roll-up policy will be recreated but it will contain only the errata that has been previously published by Red Hat.

## Manage Red Hat patches

The second phase of the Red Hat Patching mechanism – although optional, sometimes can be very important in the patching process. Since Red Hat patches are just normal RPM packages you can do all the operations that SA Client allows you to do on Red Hat packages:

- Open the package
- Viewing and editing package properties
- Viewing package contents
- Viewing all software policies associated with a package
- Deleting a package
- Renaming a package
- Locating packages in Folders

## Restricting access to RPM folders

SA builds a custom RPM repository for use by both Red Hat Patching mechanism and the software management jobs. This is built on a server-by-server basis, taking into account several packages and server properties and user-defined settings.

The repository that SA downloads to a managed server before actually scanning the server for recommended patches is built as follows:

- Packages whose platform set does not include the server platform are excluded from the RPM repository.
- Packages in folders whose customer constraints do not include the customer of the server are excluded from the RPM repository.
- If one or more `repo.restrict` custom attributes are defined for a particular server, only packages in the folders specified by these custom attributes are included in the RPM repository.

In SA, you can specify in a custom attribute the folders in the SA Library that the server has access to. All other folders will be inaccessible to the server. This gives you folder-level control over which versions of RPMs can be applied to a given server, allowing you to precisely manage platform update versions, for example Red Hat Linux Server 6 Update 4 versus Update 5.

**Note:** This is not intended as a user-level access control mechanism, but rather to restrict the library and folder view of a managed server from access to the full set of RPMs in the SA Library.

## Scan managed servers for recommended patches

Before actually remediating the patches to a Red Hat managed server, SA needs to know what patches are applicable to a Red Hat server. Not all errata issued by Red Hat is applicable to a managed server. This depends on what packages are installed and at what level of patching is the server. The job of Red Hat patch scanning is to report RPM units that are recommended for a managed server. After the scanning runs and recommended RPM units are found, the remediation can occur. The scanner responsible for determining the recommended patches uses the RPM repositories generated after importing the patches. If there is a `repo.restrict` custom attribute (please read the previous section – Managing Red Hat patches) then the RPM repository metadata downloaded to the managed server will reflect the value of the custom attribute.

The Red Hat patch scanner is implemented using dynamic handlers, meaning that the actual software implementing the scan resides on the core and is passed to the managed server during scan. The scanner downloads the RPM repository from core locally on the managed server and then it uses the native tools to run a scan on the machine. The scan results are sent up to the core and then can be used for remediation. The native tool used for Red Hat is yum.

**Note:** For the scanner to work, you will require Yum version 2.4.3 or later.

## Running patch scanning on managed servers periodically

Red Hat patch scanning runs on a periodic basis on the managed server, that is each time software registration is performed. But in order to get some recommended patches you must first perform patch import.

Besides depending on the patch scanning that runs periodically with the software registration you can force the scanner to run either from HSA Client or directly from the managed server.

## Running patch scanning manually from SA Client

From the SA Client you can perform a patch scan on a managed server in two ways:

- Run a Software Compliance Check
- Run a Patch Compliance check

The first method is simpler, in the sense that you don't have any prerequisite to run the scanning (apart from the patches that need to be imported in SA Library in order to get some recommended patches). The second methods implies that the Red Hat managed servers on which the patch compliance is run must have a Dynamic Patch Policy attached, otherwise the scanner will not be executed on the managed servers. More about Dynamic Patch Policies can be found in the next section: Remediate Red Hat Patches.

To run a Software Compliance check that starts the scanning process on a list of managed servers:

1. From the navigation pane, select **Devices > Servers >All Managed Servers**.
2. Select one or more Red Hat Servers.
3. From the context menu, right click and select **Scan**.
4. From the new menu list, select **Software Compliance**.

To run a Patch Compliance check, first make sure that each managed server that you want to scan has a Dynamic Patch Policy attached, followed by these steps:

1. From the navigation pane, select **Devices > Servers >All Managed Servers**.
2. Select one or more Red Hat Servers.
3. Right click. From the context menu select **Scan**.
4. From the new menu list, select **Patch Compliance**.

## Run patch scanning manually on the managed server

The user can explicitly invoke a scan on the managed server by running the following command:

```
/opt/opsware/agent/pylibs/cog/bs_software [--full]
```

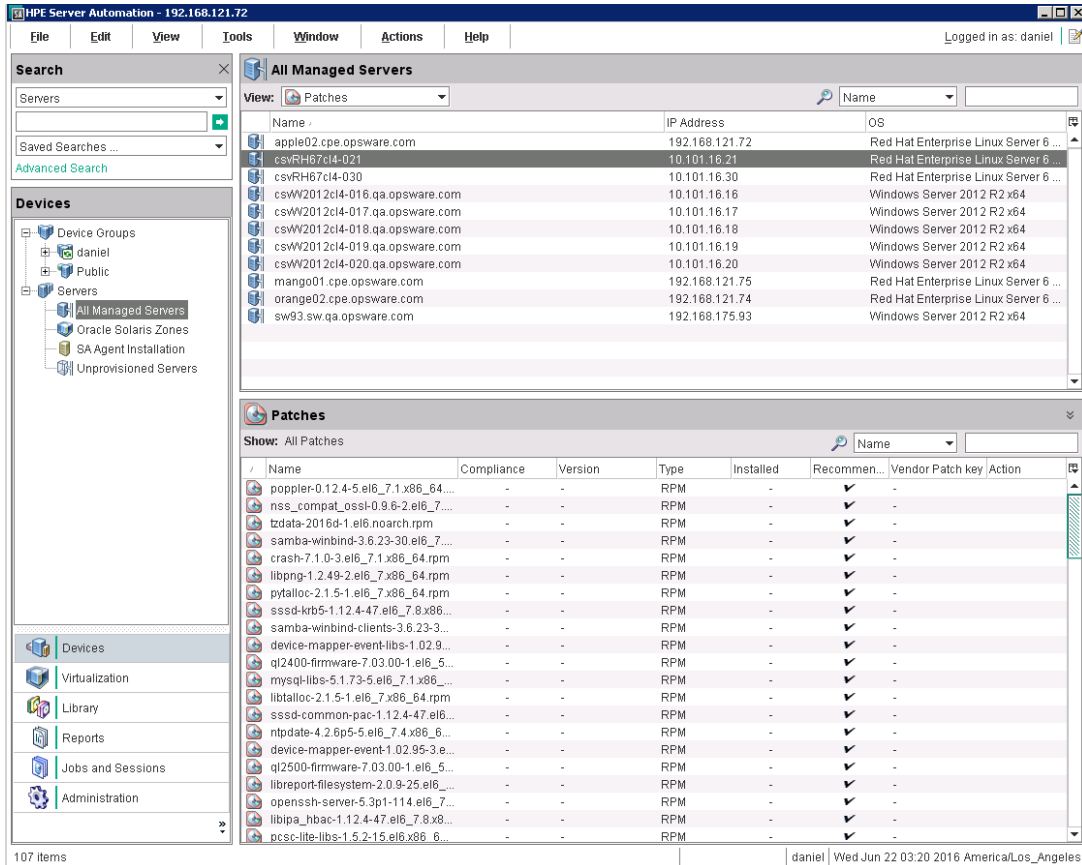
## Viewing the recommended patches

The result of scanning produces a list of patches that are applicable to a managed server. In Red Hat Patching terminology we call these recommended patches.



You can view the recommended patches applicable to a managed server from the SA Client. There are two ways to do this. You can either:

1. From the navigation pane, select **Devices > Servers > All Managed Servers**.
2. Select a Red Hat managed server
3. From the **View** combo box, select **Patches**.



The second option involves opening the Server Browser:

1. From the navigation pane, select **Devices > Servers > All Managed Servers**.
2. Open a Red Hat managed server.
3. In the new window, select **Inventory** tab.
4. In the navigation pane, select **Patches**. A window much like the one depicted above should be rendered.

## Policy management

Patches recommended in the scanning phase can be remediated on the managed server. A typical software remediation job involves a software policy with some policy items to be remediated. In the case of Red Hat Patch remediation, a Dynamic Patch Policy is involved.

A Red Hat Dynamic Patch Policy is very similar with a normal (static) policy. It contains the same properties like name, description, platforms associated, can be attached to multiple managed servers

and it allows the same management operations that software policies and static patch policies allow. The difference comes from the fact that Red Hat Dynamic Patch Policies do not allow editing policy items. Upon remediation of a dynamic patch policy, the process will populate the policy items at runtime with patches.

## Creating a Red Hat dynamic patch policy

To create a dynamic patch policy for a Red Hat managed servers:

1. In the navigation pane, select **Library > By Type > Patch Policies**.
2. Select a specific Red Hat operating system
3. Select **Actions** or right click in the patch policies pane.
4. Select **New Dynamic Policy**.
5. Provide a name and description to the policy. Save and close.

## Attaching a dynamic patch policy to a Red Hat managed server

After a dynamic patch policy is created, the policy must be attached and then the remediation can occur. To attach a dynamic patch policy:

1. In the navigation pane, select **Library > By Type > Patch Policies**.
2. Select a specific Red Hat operating system, and view the list of Red Hat patch policies.
3. Select a patch policy from the content pane and open it.
4. In the server browser from the **Views** drop-down list, select **Servers**.
5. From the Actions menu, select **Attach**.
6. From the new dialog select a Red Hat server click **Attach**. If you want the server to be remediated immediately, select the **Remediate Servers Immediately**.

## Remediating Red Hat dynamic patch policies

After this step, the recommended patches from the scan phase are installed to the system. To remediate a patch policy:

1. In the navigation pane, select **Library > By Type > Patch Policies**.
2. Select a specific Red Hat operating system, and view the list of Red Hat patch policies.
3. Select a patch policy from the content pane and open it.
4. In the server browser from the **Views** drop-down list, select **Servers** and then select a server to remediate on.
5. From the Actions menu, select **Remediate**.

## Patch compliance

SA performs conformance checks against managed servers and device groups to determine whether all patches in a policy were installed successfully. In case of Red Hat Patching, although the dynamic patch policy is empty, this will be populated with items at runtime. The items that fill the patch policy

are none other than the recommended patches from the Scan phase. In other words, the patch compliance scan for Red Hat will check if all patches recommended by the scan phase are installed on the managed server.

There are multiple ways of starting a compliance scan. The most important are:

- Manually start of patch compliance scan
- Scheduled
- As a result of a Patch Policy Remediation

## Manually starting a patch compliance scan

To manually start a patch compliance scan on one or more managed servers:

1. In the navigation pane, select **Devices**.
2. Select the **device(s)** and right click. From the context menu select **Scan**.
3. From the new menu list, select **Patch Compliance**.

## Scheduling patch compliance scans

To schedule a patch compliance scan on all Red Hat 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 and then click **OK** to save the settings.

## Patch compliance scans as part of other tasks

SA performs a patch compliance scan on a managed server at the end of remediating a patch policy or at the end of installing a recommended patch.

## Best practices for managing minor RHEL releases

The current SA model differentiates between Red Hat platforms based on the major version number. A major version is denoted by a whole number version change. For example, Red Hat Enterprise Linux 5.0 and Red Hat Enterprise Linux 6.0 are both major versions of Red Hat Enterprise Linux while RHEL 6.6 and 7.1 are considered minor releases.

SA follows Red Hat practices and allows managing of packages and upgrades between minor versions. A customer with a Red Hat Enterprise Linux 7.0 can use SA to patch the system and upgrade to Red Hat Enterprise Linux 7.2 minor release.

The most common use cases that involves the SA Red Hat patching mechanism are upgrade scenario and keeping a point-release up to date. This chapter is only addressed to customers that want to keep a minor release up to date or want to upgrade to another minor release.

## Guidelines for upgrading a RHEL minor release

This involves importing the content into SA, setting a proper value for `repo.restrict` custom attribute, scanning the managed servers and then remediating a policy. The guidelines in this section apply to both software policies and dynamic patch policies, unless otherwise specified.

Let's take the following scenario: a Red Hat Enterprise Linux Server 7 needs to be upgraded to the Update 2 minor version.

### Importing minor release packages

Red Hat Enterprise Linux minor releases are an aggregation of enhancement, security, and bug fix errata since the last major release.

To be able to upgrade the managed servers at Update 2 you will have to import the 7.2 content repository. The upgrade operation does not need to go through all subsequent releases. In our case we don't need to upgrade the system at 7.1 release and then at 7.2 release. You can upgrade directly to 7.2.

For the import process, besides configuring `redhat_import.conf` you need to add at the end of the file the following three lines:

```
[rhel-7-server-rpms{7.2-x86_64}]  
platform=Red Hat Enterprise Linux Server 7 X86_64  
enabled=1
```

This assigns a platform for the Update 2 content repository and enables it for import.

### Setting up `repo.restrict` custom attributes

By default, the Red Hat Importer tool imports packages in specific folders. Each minor release version will be imported in its own path. For example, the packages for Red Hat Enterprise Linux 7 Update 2 will be stored in `/RHSM/Packages/Red Hat Enterprise Linux 7 Server (RPMs) (7.2-x86_64)` folder. Similarly, content for 7.1 and 7.0 will be imported in their own custom folder.

**Note:** This step is mandatory for dynamic policies. For software policies, although not mandatory, having a `repo.restrict` in place is recommended when remediating the content software policy.

Typically, a content repository can have thousands of packages but not all of them are eligible for upgrade. The scan procedure queries the managed server for the RPMs already installed. Then it will mark only RPMs with newer version than the ones installed for upgrade.

The scan mechanism by default – builds an RPM repository with all available RPM packages in SA Software Repository. If you have content imported for 7.1 and 7.2, the repo will contain packages for both releases. The `repo.restrict` custom attribute comes in handy when you want to upgrade some machines at Update 1 and some others at Update 2. It will help you restrict the folders in the SA Library that the server has access to. All other folders will be inaccessible to the server. This gives you folder-level control over which versions of RPMs can be applied to a given server, allowing you to precisely upgrade to a specific version per each managed server.

In other words, please set the `repo.restrict` custom attribute value to the path where Update 2 packages are located. This can be set per device, or per device group. You can even set it on the dynamic patch policy/software policy if you are sure that the policy will be attached only on devices that need to be upgraded to the 7.2 release.

For more information about `repo.restrict`, see ["Manage Red Hat patches" on page 262](#).

## Scanning managed servers

This step only applies to dynamic patch policies. Once the custom attribute is set you need to create a dynamic patch policy, attach it on the devices that need to be upgraded and then run a patch compliance scan. This will trigger the actual scanning for building the recommended RPMs to install.

## Remediating the patch policy

In case the patching happens with dynamic patch policies you can remediate the recommended patches – discovered in the previous step - by starting a remediation job against the dynamic patch policy previously attached to the managed servers. For more information, see ["Policy management" on page 265](#).

For patching with static software policy things are a little bit different. You can't benefit from the scanning procedure that occurred in the previous step. You will have to remediate all packages imported from the minor content repository. Fortunately – `redhat_importer` tool already groups all imported packages into a software policy. Using the default configurations for the importer the policy you can find the policy in SA Client under `/RHSM/Content/ Red Hat Enterprise Linux 7 Server (RPMs) (7.2-x86_64) Policy`.

The remediation job for this policy will determine the eligible packages for upgrade in the analyze phase and install them.

**Note:** HP recommends upgrading minor releases through dynamic patch policies because it offers better performance.

## Keeping a minor release up to date

Patching a Red Hat minor release with fixes, updates and security errata involves exactly the same steps used for upgrading. Just make sure that `repo.restrict` custom attribute restricts the SA repo to the packages corresponding to your particular minor version.

## Frequently asked questions

### The importer fails with SSL: CERTIFICATE\_VERIFY\_FAILED

One of the most common issues when importing Red Hat packages through Red Hat Importer tool is the:

```
Unexpected error: URLError: <urlopen error [SSL: CERTIFICATE_VERIFY_FAILED]
certificate verify failed (_ssl.c:590)
```

This error means that the importer could not validate the server certificate during SSL handshake. Most probably because the CA certificate of the Red Hat server from where packages are imported is not imported in the SA trusted store. If you are importing from RHSM or from a Red Hat Satellite make sure you import the certificate from <https://cdn.redhat.com> or from your satellite using the steps provided in "Install Red Hat CA certificates" on page 246.

## Configuration file error: Invalid option [main] 'package\_path'

The most likely cause for this error is an invalid structure in the configuration file. In this particular case the [RHN] section was removed from the config, and all of its properties are now children of [main] section. But [main] section can only have a predefined set of attributes. In this case the fix is to add back the [RHN] section in the config. A second solution is to make sure that when you removed the [RHN] label, all of its children are either commented or removed from the configuration file.

As a general rule, don't remove and don't comment the [main], [RHN] and [RHSM] sections tag. If you don't want to import content from [RHN] you can set the channels property to an empty value. If you still insist to remove/comment a particular section please make sure the member properties are also commented out. Also please note that the [main] section can't be removed otherwise the importer will fail if the section is not found in the configuration file

## Import fails with: HTTP Error 403: Forbidden

If the import fails with a trace like the one below most probably your entitlement certificate is expired.

```
Requesting https://cdn.redhat.com/content/dist/rhel/server/7/7.2/x86_64/os/repodata/repomd.xml
```

```
Unexpected error: HTTPError: HTTP Error 403: Forbidden
```

Please read the Entitlement certificates chapter to find out more details on how you can get an up to date entitlement certificate.

## Unable to process content label. No platform could be associated with this label.

As the error suggests it means that redhat\_import tool could not associate the CDN content for the label to a specific SA supported platform.

Internally we have some default labels like rhel-7-server-rpms{7Server-x86\_64} that have an SA platform associated. But most of them don't have.

In this case all you need to do is edit the redhat\_import.conf file, go to the bottom and configure the platform. For example if the original error is:

```
Unable to process content label rhel-7-server-rpms{7.2-x86_64}. No platform could be associated with this label. This content label will be dropped. If you need to import this content, add the 'platform' option to the configuration file.
```

The fix in the config file should be:

```
[rhel-7-server-rpms{7.2-x86_64}]
```

```
platform=Red Hat Enterprise Linux Server 7 X86_64
```

## The `--show_labels` option does not list all content labels from entitlement

The `--show_labels` lists an intersection of labels configured in `redhat_import.conf` and the labels found in entitlement. The option will render only labels that have an SA Red Hat platform associated in the `redhat_import.conf` (or `/etc/opt/opsware/rhn_import/content_labels.json`) and only if they exist in the entitlement file.

For example, if you have the following three labels in the entitlement:

1. `rhel-5-server-rpms`
2. `rhel-7-server-debug-rpms`
3. `rhel-7-server-optional-rpms`

And in the `redhat_import.conf` file you only have the `rhel-7-server-optional-rpms{7Server-x86_64}` content label associated with Red Hat Enterprise Linux Server 7 X86\_64 platform, then `--show_labels` will only list two labels: `rhel-5-server-rpms` and `rhel-7-server-optional-rpms`. Why? Because the first is configured by default in `/etc/opt/opsware/rhn_import/content_labels.json` while the second one is configured in the `redhat_import.conf` file.

Please note that `/etc/opt/opsware/rhn_import/content_labels.json` contains the default configured labels by SA and it should not be modified.

## Patch management for Oracle Enterprise Linux



The SA Patch Importer for Oracle Enterprise Linux (OEL) allows users to import packages for the subscribed channels from the Oracle Unbreakable Linux Network (ULN) and automatically create the corresponding software policies for each imported channel in SA. It can be run from the command line manually, or can be part of a `cron` job which performs the import on a recurring basis.

## Before you begin

### Prerequisites

The following prerequisites must be met before using SA Patch Importer for Oracle Enterprise Linux.

- Purchase a support license from the Oracle Unbreakable Linux Store to obtain a valid CSI (Customer Support Identifier). See <https://linux.oracle.com> for more details.
- Register with the Oracle Unbreakable Linux Network (ULN) to obtain the username/password for single sign-on.
- At least 100GB of free disk space is required on the system in which this tool will be used.

Depending on the type of support license purchased from Oracle, you may be able to subscribe to any channels that Oracle is currently supporting. However, the SA Patch Importer will only import packages for the platforms that SA supports.

## Limitations

The SA Patch Importer for Oracle Enterprise Linux is intended to run on SA Core platforms only.

## Patch importer file locations

### Importer file locations

Binaries	/opt/opsware/patch_importer/bin/
Configuration File	/etc/opt/opsware/patch_importer/uln_import.conf
Log File	/var/log/opsware/patch_importer/patch_importer.log
Package Download Directory (where the downloaded packages will be temporarily stored). Make sure you have at least 100 GB of free disk space on the file system.	/var/opt/opsware/patch_importer/
Libraries	/opt/opsware/patch_importer/patch_importer/

## Get started

Using SA Patch Importer for Oracle Enterprise Linux encompasses the following tasks:

1. Edit the configuration file, `/etc/opt/opsware/patch_importer/uln_import.conf`, to provide the requirement information.
2. Register the system with the ULN.
3. Log on to the ULN to subscribe the channels.
4. Import the packages.

The first three tasks should be done once, or infrequently. The fourth task, importing the packages, can be scheduled on a recurring basis.

**Note:**

This tool must be run as root user on a core host.



## Editing the configuration file

The configuration file for SA Patch Importer for Oracle Enterprise Linux is located in `/etc/opt/opsware/patch_importer/uln_import.conf`. It is divided into various sections. It has two mandatory sections, `[main]` and `[system_id]`, and zero or more optional sections. The optional sections are used to control channel-specific behaviors.

The following tables describe the various configuration sections.

### [main] Section

The `[main]` section has the general configuration options.

#### [main] Section options

Property name	Expected values	Description
username	String (in the form of email)	ULN username
password	String	ULN password
CSI	String (a sequence of numbers)	Oracle Customer Support Identifier
hide_passwords	1, 0 (Default: 1)	<p>Indicates whether to obfuscate the passwords.</p> <p>If set to 1, all the passwords in this file will be obfuscated the very first time the tool is used. Once a password is obfuscated, it will remain obfuscated, there's no way to de-obfuscate it.</p> <p>If the password has changed, you can simply re-enter the clear text password and it will be obfuscated on the next run, assuming <code>hide_passwords</code> is still set to 1.</p> <p>You may also use the <code>--hide_passwords</code> command line option to obfuscate the passwords. If <code>--hide_passwords</code> option is specified at the command line, it will be used instead of the one from the configuration file.</p>
server_uri	A valid URI (Default: <code>https://linux-update.oracle.com/XMLRPC</code> )	URI to the ULN RPC server. It points to the default ULN instance. We do not support a server list for live failover at this point. If the primary server is down, you have to manually change it to point to one of the mirrors.
system_id	A valid file path. ( Default: <code>/var/opt/opsware/uln_import/system_id</code> )	<p>The location to store the <code>system_id</code>. Once the system is registered with the ULN.</p> <p>Warning: Please do not remove or change the location of this file. Otherwise, you will have to re-register with</p>

[main] Section options, continued

Property name	Expected values	Description
		the ULN.
proxy_ host	<FQHN>:[<port>]	If HTTP proxy is used, specify it here.
proxy_ user	String	If HTTP proxy authentication is required, specify the proxy username. It will be ignored if proxy_host is not specified.
proxy_ pass	String	If HTTP proxy authentication is required, specify the proxy user password. It will be ignored if proxy_host is not specified.
proxy_ agent	String	If HTTP proxy authentication is required, you may optionally specify the proxy_agent HTTP header for identification purposes.
opsware_ user	String	You may elect to import the packages in the context of an SA user. If so, specify the username here. If opsware_user is omitted, package import will be run in the context of a system (internal) user.
opsware_ pass	String	Password for the SA user. It will be ignored if opsware_user is not specified.
continue_ on_error	1, 0 (Default: 1)	This option is for not supported.
import_ threads	Number (Default: 10)	Maximum number of import threads. Setting this to an unreasonable value may cause service outage since some source networks may not be capable of supporting heavy load.
limit_ policy_ description	1, 0 (Default: 1)	This option is not supported
channels	An explicit list of channels may be given separated by spaces and/or newlines:  channels:  LABEL1  LABEL2  LABELn	If the channels option is not specified, then all SA supported top-level (parent) channels are enabled, plus any channels that have their own [channel] sections in this configuration file.

[main] Section options, continued

Property name	Expected values	Description
package_path	A valid directory path. (Default: /ULN/Packages/\$channel_name)	The folder in which the package will be uploaded for a given channel. "\$channel_name" is a special placeholder. It will be replaced by the channel at runtime. Packages can be quarantined to prevent their use until they are approved. Note that you must ensure that the permissions on the Unapproved folder limit the servers that can access it. You can configure package_path to a special folder for this purpose. For example: package_path=/ULN/Packages/Unapproved/\$channel_name
channel_path	A valid directory path. (Default: /ULN/Channels/\$channel_name Policy)	The folder in which the channel software policies will be created for a given channel. "\$channel_name" is a special placeholder. It will be replaced by the channel at runtime.
erratum_path	A valid directory path. (Default: /ULN/Errata/\$erratum_type Policies/\$erratum_name)	The folder in which the erratum software policies will be created for the given channel. "\$erratum_type" and "\$erratum_name" are special placeholders. They will be replaced by erratum type and erratum name respectively at runtime. Instead of creating a roll-up policy by channel, you might choose to create it by month For example, errata_path=/ULN/Errata/\$Y-\$m Advisory Roll-Up Policy Notice that "\$Y" and "\$m" are special placeholders for year and month respectively. This configuration is currently not being used.
errata_path	A valid directory path. (Default: /ULN/Errata/\$channel_name Advisory Roll-Up Policy)	The folder in which the errata software policies will be created for the given channel. "\$channel_name" is a special placeholder. It will be replaced by the channel at runtime. This configuration is currently not being used.
package_search_path	An explicit list of directory paths may be given separated by spaces and/or newlines: channels:	The paths to search for previously uploaded packages. "\$opsware_platform" is a special placeholder. It will be replaced by the platform name at runtime.

[main] Section options, continued

Property name	Expected values	Description
	PATH1 PATH2 PATHn  Default: /Package Repository/OS Media/\$opsware_platform /Package Repository/All Red Hat Linux/\$opsware_platform /Migrated/Package Repository/Customer Independent/\$opsware_ platform	

[system\_profile] section

This section is used to specify the properties for the system profile. The information is used to register with the ULN. Typically, before downloading packages, the system must first register with the ULN. A system profile is created, which contains OS and hardware information, upon registration. Once the system is registered, the ULN will automatically assign the default channels associated with the platform in which the system is running. However, since SA can be run on a non-OEL system, this essentially generates a pseudo system profile.

The system profile is created using the information from the [system\_profile] section:

[system\_profile] Section Options

Property name	Expected values	Description
profile_name	String (Default: FQDN of the system where the tool is run)	Name of the profile. Typically it is the Fully Qualified Domain Name of the host where the tool is run.
os_release	Number (Default: 5)	Oracle Enterprise Linux OS release number.
release-name	String (Default: enterprise-release)	Oracle Enterprise Linux OS release name.
architecture	X86 or x86_64 (Default: x86_64)	OS architecture. We only support x86 and x86_64 right now.
uuid	String	UUID. Will be generated in runtime.

### [system\_profile] Section Options, continued

		Warning: Do not modify this property unless you are not certain of how it will affect your system. Misuse of this property can break the import tool and require you need to re-register.
rhnuuid	String	RHN UUID. Will be generated in runtime.  Warning: Do not modify this property unless you are not certain of how it will affect your system. Misuse of this property can break the import tool and require you to re-register.

## Channel-specific sections

Here is an example of a channel specific section. In this case, it enables the Oracle Enterprise Linux 5 Update 6 Patch channel, creating a policy composed of all the packages in that channel. Note that this section is enabled by default as long as the 'channels' option is not specified in the [main] section. If the 'channels' option is specified in the [main] section, then it must be explicitly enabled via the "enabled" option. Also, channel\_path is defined here only as we don't wish to create channel policies for top-level channels

```
[o15_u6_x86_64_patch]
; enabled=1

# You may wish to import all versions of each packages in the channel. By
# default, only the latest version of each package is imported. Note that
# when importing all versions, it is recommended that packages_only=1 also be
# used since it is not useful to have a policy with more than one version of
# each package.
; which_packages=all

# You may wish to download the packages for this channel only and then
# create the policies manually. Also useful in combination with
# which_packages=all:
; packages_only=1

# To locate a child channel's packages next to the corresponding policy in
# the library, use a path such as the following:
; package_path=/ULN/Channels/$channel_name Packages
```

## Register the system with the ULN

After editing the configuration file, you are now ready to register the system with the ULN.

To register the system with the ULN:

1. Run the `/opt/opsware/patch_importer/bin/uln_import` with the `--show_conf` option.

This option has two main purposes. It shows your current configuration as well as registering the system if the system has not been previously registered with the ULN.

```
[root@vc002 patch_importer]# /opt/opsware/patch_importer/bin/uln_import --show_conf
```

```
***** Configuration For ULN *****
```

```
Retrieving platform information from SA
```

```
Retrieving channel information from Oracle ULN
```

```
|
```

```
[system_profile]
```

```
rand_key_path      : /var/opt/opsware/crypto/wordbot/.randkey-rhn_import
```

```
package_path      : /var/opt/opsware/patch_importer/packages
```

```
which_packages    : latest
```

```
server_uri        : https://linux-update.oracle.com/XMLRPC
```

```
cache_path        : /var/opt/opsware/uln_import/cache
```

```
dbg_random_fail   : 0
```

```
erratum_path      : /$network_name/Errata/$erratum_type Policies/$erratum_name
```

```
download_server_uri : http://linux-update.oracle.com/XMLRPC
```

```
package_search_path :
```

```
    /Package Repository/OS Media/$opsware_platform
```

```
    /Package Repository/All Red Hat Linux/$opsware_platform
```

```
    /Migrated/Package Repository/Customer Independent/$opsware_platform
```

```
packages_only     : False
```

```
errata_path       : /$network_name/Errata/$parent_channel_name/$channel_name  
Advisory Roll-Up Policy
```

```
hide_passwords   : 1
```

```
import_threads    : 5
```

```
show_config_only  : 0
```

```
tmp_path         : /var/opt/opsware/patch_importer
```

```
system_id        : /etc/opt/opsware/patch_importer/system_id
```

```
mode             : all
```

```
continue_on_error : 1
```

```
channel_path      : /$network_name/Channels/$parent_channel_name/$channel_
name Policy
```

```
[main]
```

```
rand_key_path    : /var/opt/opsware/crypto/wordbot/.randkey-rhn_import
```

```
erratum_path     : /ULN/Errata/$erratum_type Policies/$erratum_name
```

```
which_packages  : latest
```

```
package_path     : /ULN/Packages/$channel_name
```

```
download_server_uri : http://linux-update.oracle.com/XMLRPC
```

```
package_search_path :
```

```
/Package Repository/OS Media/$opsware_platform
```

```
/Package Repository/All Red Hat Linux/$opsware_platform
```

```
/Migrated/Package Repository/Customer Independent/$opsware_platform
```

```
packages_only   : False
```

```
csi             : 1234567
```

```
proxy_host      : abc.acme.com:8080
```

```
errata_path     : /ULN/Errata/$channel_name Advisory Roll-Up Policy
```

```
import_threads  : 10
```

```
tmp_path        : /var/opt/opsware/patch_importer
```

```
system_id       : /etc/opt/opsware/patch_importer/system_id
```

```
channel_path    : /ULN/Channels/$channel_name Policy
```

```
continue_on_error : 1
```

```
username        : test@hpe.com
```

```
server_uri      : https://linux-update.oracle.com/XMLRPC
```

```
cache_path      : /var/opt/opsware/uln_import/cache
```

```
dbg_random_fail : 0
```

```
password        : (Hidden)
```

```
hide_passwords  : 1
```

```
show_config_only : 1
```

```
mode            : all
```

```
<Configuration For Channel: ol5_x86_64_latest>
```

```
Enabled          : True
Packages Only    : False
Which Packages   : latest
Package Path     : /ULN/Packages/$channel_name
```

\*\*\*\*\*

2. Once the system is registered, you should be able to view it under the Systems tab at the ULN: <https://linux.oracle.com>. By default, the ULN automatically assigns the latest platform channel to the newly registered system.

A `system_id` file is created in `/etc/opt/opsware/patch_importer/uln/`. If you are unable to register with the ULN, you can check the log file at `/var/log/opsware/patch_importer/patch_importer.log` for possible errors. You can also run `uln_import` in debug mode if necessary.

```
/opt/opsware/patch_importer/bin/uln_import --show_conf -v
```

If you need to register with the ULN, make sure to remove the old `system_id` and delete the registered system from the ULN before doing so.

```
rm -rf /etc/opt/opsware/patch_importer/uln/system_id
```

```
/opt/opsware/patch_importer/bin/uln_import -show_conf
```

## Subscribing and unsubscribing channels from the ULN

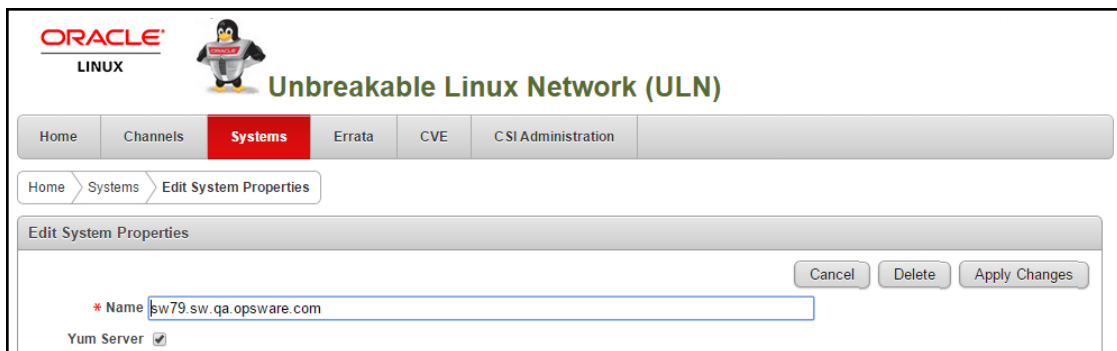
Subscribing and unsubscribing channels must be done with the ULN. Before you can perform the subscription/unsubscription step, you need designate the system as a YUM server.

To designate the registered system as a YUM server:

1. If you have different flavors of Enterprise Linux deployed in your environment, check the Yum Server box in the Edit System Properties tab of your registered system in order to subscribe to all the available channels.

**IMPORTANT:** It is important to select the Yum Server box. If it is not selected, the ULN will restrict the channels to only those that are relevant to the registered system's platform. By designating the registered system as a Yum Server, the ULN will allow it to subscribe to any currently available channels.

2. Click Apply Changes to submit the changes.

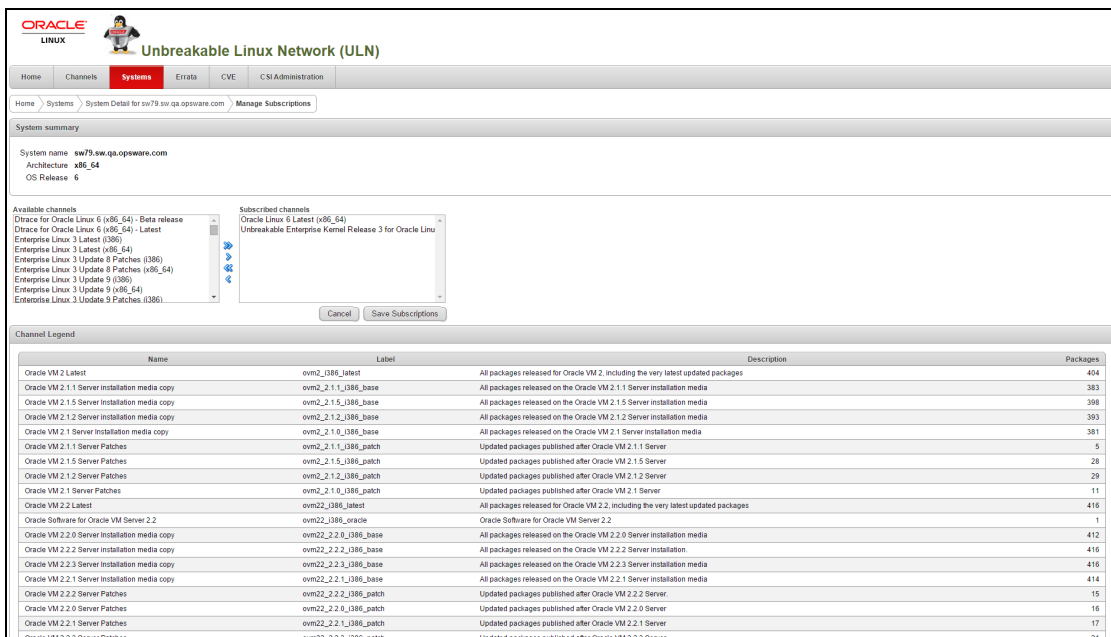


Once the registered system is designated as a Yum Server, it is capable of subscribing any channels currently available.



To subscribe/unsubscribe channels:

1. Navigate to the Manage Subscriptions tab of the registered system.  
Keep in mind that some channels do not contain any updates. They are just base RPMs from the ISO or the release media. Some channels are superset of others. Also, unlike the RedHat network, the ULN has no concept of "parent channels."
2. Select the desired channels.
3. To subscribe to a channel, move it from the Available channels column to the Subscribed channels column.
4. To unsubscribe, move it from the Subscribed channels column to the Available channels column.
5. Click Save Subscriptions.



6. Once you subscribe to the desired channels from the ULN, you may want to verify it by running `/opt/opsware/patch_importer/bin/uln_import` with the `-show_conf` option to make sure the channels are enabled.

```
[root@vc002 bin]# /opt/opsware/patch_importer/bin/uln_import --show_conf
***** Configuration For ULN *****

Retrieving platform information from SA
Retrieving channel information from Oracle ULN
|
[system_profile]
rand_key_path      : /var/opt/opsware/crypto/wordbot/.randkey-rhn_import
package_path      : /var/opt/opsware/patch_importer/packages
which_packages    : latest
server_uri        : https://linux-update.oracle.com/XMLRPC
```

```
cache_path          : /var/opt/opsware/uln_import/cache
dbg_random_fail     : 0
erratum_path        : /$network_name/Errata/$erratum_type Policies/$erratum_
name
download_server_uri : http://linux-update.oracle.com/XMLRPC
package_search_path :
    /Package Repository/OS Media/$opsware_platform
    /Package Repository/All Red Hat Linux/$opsware_platform
    /Migrated/Package Repository/Customer Independent/$opsware_platform

packages_only       : False
errata_path         : /$network_name/Errata/$parent_channel_name/$channel_name
Advisory Roll-Up Policy
hide_passwords      : 1
import_threads      : 5
show_config_only    : 0
tmp_path            : /var/opt/opsware/patch_importer
system_id           : /etc/opt/opsware/patch_importer/system_id
mode                : all
continue_on_error   : 1
channel_path        : /$network_name/Channels/$parent_channel_name/$channel_
name Policy

[main]
rand_key_path       : /var/opt/opsware/crypto/wordbot/.randkey-rhn_import
erratum_path        : /ULN/Errata/$erratum_type Policies/$erratum_name
which_packages      : latest
package_path        : /ULN/Packages/$channel_name
download_server_uri : http://linux-update.oracle.com/XMLRPC
package_search_path :
    /Package Repository/OS Media/$opsware_platform
    /Package Repository/All Red Hat Linux/$opsware_platform
    /Migrated/Package Repository/Customer Independent/$opsware_platform
```

```
packages_only      : False
csi                : 12345678
proxy_host        : test.acme.com:8080
errata_path       : /ULN/Errata/$channel_name Advisory Roll-Up Policy
import_threads    : 10
tmp_path          : /var/opt/opsware/patch_importer
system_id         : /etc/opt/opsware/patch_importer/system_id
channel_path      : /ULN/Channels/$channel_name Policy
continue_on_error : 1
username          : abc@hpe.com
server_uri        : https://linux-update.oracle.com/XMLRPC
cache_path        : /var/opt/opsware/uln_import/cache
dbg_random_fail   : 0
password          : (Hidden)
hide_passwords    : 1
show_config_only  : 1
mode              : all
```

<Configuration For Channel: e15\_u5\_i386\_patch>

```
Enabled           : True
Packages Only     : False
Which Packages    : latest
Package Path      : /ULN/Packages/$channel_name
```

<Configuration For Channel: e15\_u5\_x86\_64\_patch>

```
Enabled           : True
Packages Only     : False
Which Packages    : latest
Package Path      : /ULN/Packages/$channel_name
```

\*\*\*\*\*

Keep in mind that SA will filter out the channels for the platforms that it does not currently support. For example, you may subscribe to Enterprise Linux 3 channels, but they will be ignored by SA.

## Importing packages

By default, the SA Patch Importer will create a software policy for each channel, unless users elect not to do so by specifying the `-package_only` option.

To import the packages:

1. Run `/opt/opsware/patch_importer/bin/uln_import`

```
[root@vc002 bin]# /opt/opsware/patch_importer/bin/uln_import
```

```
***** Importing Packages From ULN *****
```

```
Retrieving platform information from SA
```

```
Retrieving channel information from Oracle ULN
```

```
Processing package information
```

```
|
```

```
**** Import Phase ****
```

```
Importing 649 packages for channel Enterprise Linux 5 Update 5 Patch (x86_64)
```

```
|=====| 100% 00:00:00
```

```
Elapsed Time: 912 seconds
```

```
Importing 530 packages for channel Enterprise Linux 5 Update 5 Patch (i386)
```

```
|=====| 100% 00:00:00
```

```
Elapsed Time: 978 seconds
```

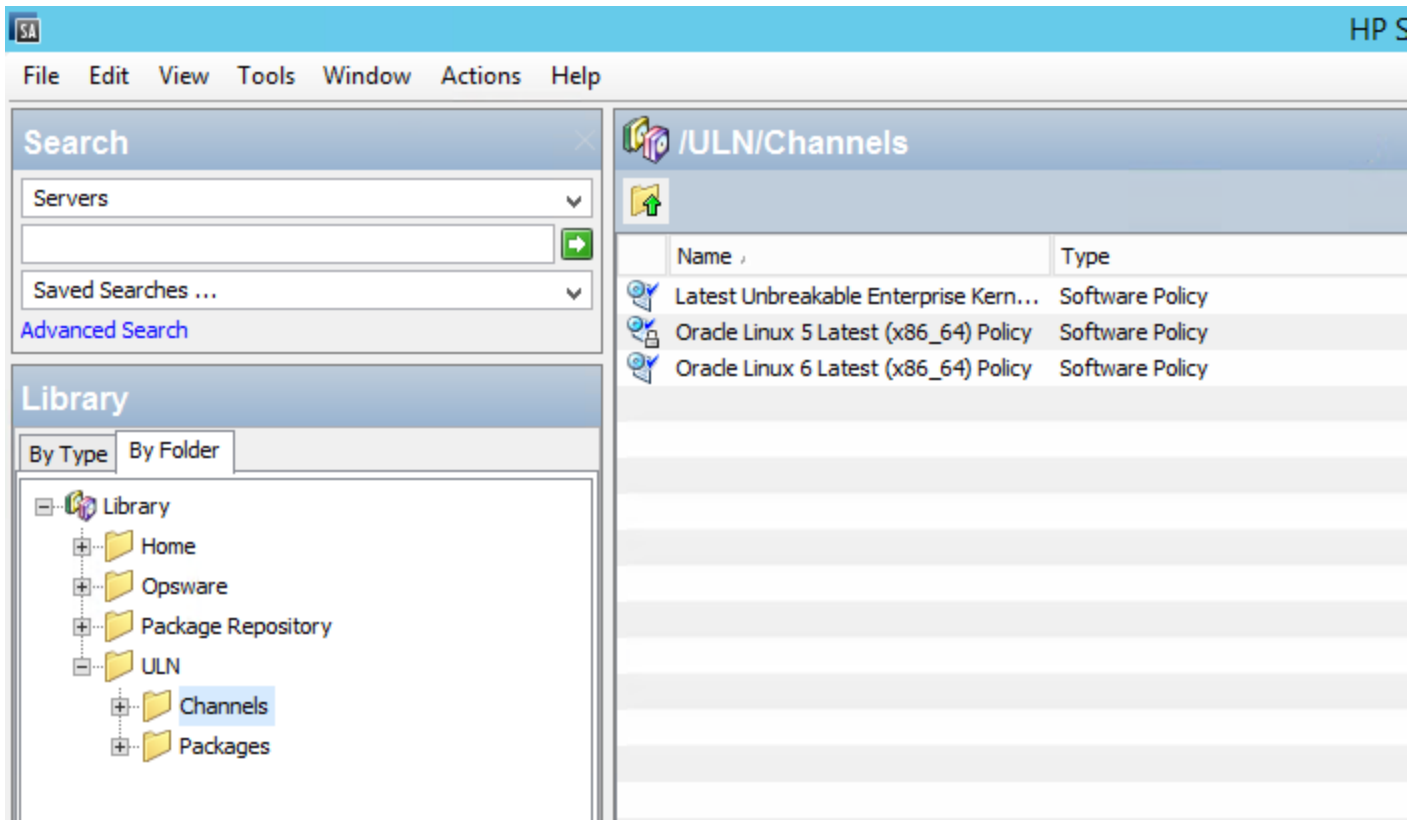
```
ULN Import Completed
```

```
*****
```

2. When the import process is complete, you can logon to the SA Java Client to view the newly created policies.
3. By default, the policies are created in the `/ULN/Channels/` folder and will be named, `<Channel`

Name> Policy, where <Channel Name> is the name of the channel. For example:  
/ULN/Channels/Enterprise Linux 5 Update 5 Patch (i386) Policy.

'Read' (or greater) permission to the /ULN/Channels/ folder is required to view the newly created policies.



4. By default the packages are imported into the /ULN/Packages/<Channel Name>/ folder, where <Channel Name> is the name of the channel. For example: /ULN/Packages/Enterprise Linux 5 Update 5 Patch (i386)/

'Read' (or greater) permission to the channel folder is required to view the newly imported

packages.

Name	Type	Last Modified	Last Modified By	Created	Created By	Object ID
389-ds-base-1.2.11.15-60.el6.x86_64	RPM	Fri Aug 28 04:09:36 2015	opsware	Fri Aug 28 04:09:36 2015	opsware	478570001
389-ds-base-devel-1.2.11.15-60.el6.x86_64	RPM	Mon Aug 31 04:25:52 2015	opsware	Mon Aug 31 04:25:52 2015	opsware	507630001
389-ds-base-devel-1.2.11.15-60.el6.x86_64	RPM	Mon Aug 31 04:25:52 2015	opsware	Mon Aug 31 04:25:52 2015	opsware	504870001
389-ds-base-libs-1.2.11.15-60.el6.x86_64	RPM	Fri Aug 28 04:11:30 2015	opsware	Fri Aug 28 04:11:30 2015	opsware	482780001
389-ds-base-libs-1.2.11.15-60.el6.x86_64	RPM	Fri Aug 28 04:06:46 2015	opsware	Fri Aug 28 04:06:46 2015	opsware	471530001
abrt-1.14-13.el6.x86_64	RPM	Fri Aug 28 04:09:31 2015	opsware	Fri Aug 28 04:09:31 2015	opsware	493550001
abrt-1.14-13.el6.x86_64	RPM	Fri Aug 28 04:05:11 2015	opsware	Fri Aug 28 04:05:11 2015	opsware	467610001
abrt-2.0.8-34.0.2.el6.x86_64	RPM	Fri Aug 28 04:04:07 2015	opsware	Fri Aug 28 04:04:06 2015	opsware	464770001
abrt-addon-ccpp-2.0.8-34.0.2.el6.x86_64	RPM	Mon Aug 31 04:28:37 2015	opsware	Mon Aug 31 04:28:37 2015	opsware	513040001
abrt-addon-ferret-2.0.8-34.0.2.el6.x86_64	RPM	-	-	-	-	537460001
abrt-addon-python-2.0.8-34.0.2.el6.x86_64	RPM	Mon Aug 31 04:28:14 2015	opsware	Mon Aug 31 04:28:13 2015	opsware	511050001
abrt-addon-vmtoolsd-2.0.8-34.0.2.el6.x86_64	RPM	Fri Aug 28 04:11:45 2015	opsware	Fri Aug 28 04:11:45 2015	opsware	483500001
abrt-d-2.0.8-34.0.2.el6.x86_64	RPM	Fri Aug 28 04:04:59 2015	opsware	Fri Aug 28 04:04:59 2015	opsware	467110001
abrt-console-notification-2.0.8-34.0.2.el6.x86_64	RPM	Mon Aug 31 04:21:52 2015	opsware	Mon Aug 31 04:21:51 2015	opsware	494230001
abrt-devel-2.0.8-34.0.2.el6.x86_64	RPM	Mon Aug 31 04:31:42 2015	opsware	Mon Aug 31 04:31:41 2015	opsware	517630001
abrt-devel-2.0.8-34.0.2.el6.x86_64	RPM	Fri Aug 28 04:13:52 2015	opsware	Fri Aug 28 04:13:52 2015	opsware	486990001
abrt-devel-2.0.8-34.0.2.el6.x86_64	RPM	Fri Aug 28 04:11:22 2015	opsware	Fri Aug 28 04:11:21 2015	opsware	482280001
abrt-gui-2.0.8-34.0.2.el6.x86_64	RPM	Mon Aug 31 04:26:04 2015	opsware	Mon Aug 31 04:26:03 2015	opsware	505460001
abrt-gui-2.0.8-34.0.2.el6.x86_64	RPM	Mon Aug 31 04:31:58 2015	opsware	Mon Aug 31 04:31:58 2015	opsware	518550001
abrt-libs-2.0.8-34.0.2.el6.x86_64	RPM	Mon Aug 31 04:22:04 2015	opsware	Mon Aug 31 04:22:04 2015	opsware	494880001
abrt-plugin-bugzilla-1.1.16-3.0.1.el6.x86_64	RPM	Mon Aug 31 04:20:07 2015	opsware	Mon Aug 31 04:20:03 2015	opsware	490120001
abrt-plugin-firefox-1.1.16-3.0.1.el6.x86_64	RPM	Mon Aug 31 04:32:16 2015	opsware	Mon Aug 31 04:32:16 2015	opsware	519250001
abrt-plugin-gdb-1.1.16-3.0.1.el6.x86_64	RPM	Mon Aug 31 04:26:16 2015	opsware	Mon Aug 31 04:26:15 2015	opsware	505690001
abrt-plugin-matix-1.1.16-3.0.1.el6.x86_64	RPM	Mon Aug 31 04:31:38 2015	opsware	Mon Aug 31 04:31:37 2015	opsware	517660001
abrt-plugin-reportloader-1.1.16-3.0.1.el6.x86_64	RPM	Mon Aug 31 04:34:15 2015	opsware	Mon Aug 31 04:34:14 2015	opsware	524650001
abrt-plugin-rundeck-1.1.16-3.0.1.el6.x86_64	RPM	Fri Aug 28 03:57:56 2015	opsware	Fri Aug 28 03:57:56 2015	opsware	469690001
abrt-plugin-vmtoolsd-1.1.16-3.0.1.el6.x86_64	RPM	Fri Aug 28 04:11:01 2015	opsware	Fri Aug 28 04:11:00 2015	opsware	481260001
abrt-python-2.0.8-34.0.2.el6.x86_64	RPM	Fri Aug 28 04:09:38 2015	opsware	Fri Aug 28 04:09:37 2015	opsware	478660001
abrt-tui-2.0.8-34.0.2.el6.x86_64	RPM	Fri Aug 28 04:07:03 2015	opsware	Fri Aug 28 04:07:02 2015	opsware	472130001
abrt-tui-2.0.8-34.0.2.el6.x86_64	RPM	Fri Aug 28 03:57:49 2015	opsware	Fri Aug 28 03:57:47 2015	opsware	468680001
abrt-vmtoolsd-1.1.16-3.0.1.el6.x86_64	RPM	Mon Aug 31 04:32:33 2015	opsware	Mon Aug 31 04:32:31 2015	opsware	520120001
acpid-1.0.10-2.1.el6.x86_64	RPM	Mon Aug 31 04:26:26 2015	opsware	Mon Aug 31 04:26:25 2015	opsware	506500001
adapto-0.9.13-8.1.el6.x86_64	RPM	Mon Aug 31 04:33:03 2015	opsware	Mon Aug 31 04:33:03 2015	opsware	521410001
adapto-doc-0.9.13-8.1.el6.x86_64	RPM	Mon Aug 31 04:32:24 2015	opsware	Mon Aug 31 04:32:23 2015	opsware	522800001
adapto-libs-0.9.13-8.1.el6.x86_64	RPM	Fri Aug 28 04:07:45 2015	opsware	Fri Aug 28 04:07:44 2015	opsware	474200001
acfnoc-firmware-30-2.el6.noarch	RPM	Fri Aug 28 04:07:01 2015	opsware	Fri Aug 28 04:07:00 2015	opsware	472060001
aide-0.14-7.el6.x86_64	RPM	Fri Aug 28 04:13:20 2015	opsware	Fri Aug 28 04:13:19 2015	opsware	485980001
alorand-1.2.1-3.el6.x86_64	RPM	Mon Aug 31 04:25:02 2015	opsware	Mon Aug 31 04:25:01 2015	opsware	502790001
alorand-1.2.1-3.el6.x86_64	RPM	Fri Aug 28 04:05:06 2015	opsware	Fri Aug 28 04:05:05 2015	opsware	467400001
alorand-devel-1.2.1-3.el6.x86_64	RPM	Fri Aug 28 04:09:21 2015	opsware	Fri Aug 28 04:09:21 2015	opsware	477800001
alorand-devel-1.2.1-3.el6.x86_64	RPM	Mon Aug 31 04:22:41 2015	opsware	Mon Aug 31 04:22:41 2015	opsware	496580001
aliscare-0.12-4-1.el6.noarch	RPM	Fri Aug 28 04:05:13 2015	opsware	Fri Aug 28 04:05:13 2015	opsware	467890001
alsa-libs-1.0.22-3.el6.x86_64	RPM	Mon Aug 31 04:26:22 2015	opsware	Mon Aug 31 04:26:22 2015	opsware	506230001
alsa-libs-1.0.22-3.el6.x86_64	RPM	Fri Aug 28 04:05:26 2015	opsware	Fri Aug 28 04:05:26 2015	opsware	468400001
alsa-libs-devel-1.0.22-3.el6.x86_64	RPM	Mon Aug 31 04:21:36 2015	opsware	Mon Aug 31 04:21:36 2015	opsware	493520001
alsa-libs-devel-1.0.22-3.el6.x86_64	RPM	Mon Aug 31 04:20:14 2015	opsware	Mon Aug 31 04:20:13 2015	opsware	514960001
alsa-plugins-ecm3com-1.0.21-3.el6.x86_64	RPM	Fri Aug 28 04:14:05 2015	opsware	Fri Aug 28 04:14:05 2015	opsware	487690001
alsa-plugins-ecm3com-1.0.21-3.el6.x86_64	RPM	Mon Aug 31 04:20:20 2015	opsware	Mon Aug 31 04:20:19 2015	opsware	505510001
alsa-plugins-maemo-1.0.21-3.el6.x86_64	RPM	Mon Aug 31 04:05:05 2015	opsware	Mon Aug 31 04:05:04 2015	opsware	467700001
alsa-plugins-maemo-1.0.21-3.el6.x86_64	RPM	Fri Aug 28 04:11:01 2015	opsware	Fri Aug 28 04:11:00 2015	opsware	482100001
alsa-plugins-usb-1.0.21-3.el6.x86_64	RPM	Fri Aug 28 04:05:32 2015	opsware	Fri Aug 28 04:05:32 2015	opsware	468740001

- After you verify the newly created software policies, you may start remediating the OEL servers. You must have the proper permissions to perform remediation tasks. See the the SA User Guide for more information on software remediation.

## Use the SA patch importer for Oracle Enterprise Linux

The SA Patch Importer for Oracle Enterprise Linux can be run from the command line, or can be part of a cron job, which runs the import on the recurring basis. By default, the importer will import the packages for the subscribed channels from the ULN and create the corresponding software policies for each of the imported channels.

A full set of command line options gives you full control over the import action. For example, you can:

- Selectively enable or disable one or more channels at runtime
- Decide whether to import the packages without creating the corresponding software policies
- Add new channels to a supported platform
- Remove channels from a supported platform
- View supported channels for the supported platforms
- Do a dry run on the import to see what actions will be performing

The following table describes the command line options for `uln_import`:

### Command Line Options for uln\_import

Option	Description
--version	Show the version number of this program and exit.
-h, --help	Show this help message and exit.
-E LABEL [LABEL...], --enable=LABEL [LABEL...]	<p>Enable a previously disabled channel; multiple labels may be provided; use 'all' to enable all configured channels.</p> <p>A channel can be disabled by setting the 'enabled=0' in the channel section in the configuration file, /etc/opt/opsware/patch_importer/uln_import.conf.</p> <p>Use this option to dynamically enable it at run time.</p>
-D LABEL [LABEL...], --disable=LABEL [LABEL...]	<p>Disable a previously enabled channel at run time; multiple labels may be provided; use 'all' to disable all configured channels.</p> <p>Using 'all' will effectively disabled all channels, which means no channels will be imported. It's as good as running a no-op.</p> <p>This option does not permanently disabled channels; it only disables the given channels for this particular run.</p>
-m MODE, --mode=MODE	Import mode: 'channel', 'erratum', 'errata', 'all' [default: all]
--source=SUPPORTED_SOURCES	Source: 'uln', 'all' [default: all]
-c FILE, --conf=FILE	<p>Configuration file [default: none]</p> <p>Use this option to specify an alternative configuration file.</p>
--packages_only	Don't create policies, download packages only.
-n, --preview	Show what would be done (dry-run).
-s, --silent	Display errors only.
-v, --verbose	<p>Debug mode.</p> <p>Debug messages are available in the log file.</p>
--show_conf	Show configuration settings and exit.
--show_labels	Show default RHN channel labels and exit.
--hide_passwords	Rewrite the configuration file hiding any plain-text passwords and exit.
--show_platform_labels	List the platforms and their supported channel labels; may use the --platform_name option to filter the platforms to be displayed.
--add_platform_label	Add channel labels to a given platform; must use the --platform_name

### Command Line Options for uln\_import, continued

Option	Description
	option to specify a platform, along with the labels to be added.
<code>--remove_platform_label</code>	Remove channel labels from a given platform; must use the <code>--platform_name</code> option to specify a platform, along with the labels to be removed.
<code>--platform_name=PLATFORM_NAME</code>	Specify the platform name; when used with <code>--show_platform_labels</code> option, it will be used as a name filter; when used with <code>--add_platform_label</code> option, it must be an exact match; when used with <code>--remove_platform_label</code> option, it must be an exact match.

### Disable channels at runtime

By default, a subscribed channel is enabled if it meets the following conditions:

1. It is one of the supported channels of a supported SA agent platform.
2. It has no [`<Channel Label>`] section the configuration file `/etc/opt/opsware/patch_importer/uln_import.conf`.
3. It has a [`<Channel Label>`] section the configuration file `/etc/opt/opsware/patch_importer/uln_import.conf` and it has “`enabled=1`” specified.

You may disable one or more channels at runtime by using the `-D` or `--disable` option. For example,

```
/opt/opsware/patch_importer/bin/uln_import -D e15_u5_x86_64_patch e15_u5_i386_patch
```

This option does not permanently disable channels. It merely disables the given channels for this particular run.

### Enable channels at runtime

By default, a subscribed channel is disabled if it meets the following condition:

It has a [`<Channel Label>`] section the configuration file `/etc/opt/opsware/patch_importer/uln_import.conf` and it has “`enabled=0`” specified.

You may enable one or more disabled channels at runtime by using the `-E` or `--enable` option. For example,

```
/opt/opsware/patch_importer/bin/uln_import -E e15_u5_x86_64_patch e15_u5_i386_patch
```

**Limitations:** You can only use this option to enable channels for platforms that SA supports. You cannot use it to enable channels for platforms that SA does not support.

### Import packages without creating the corresponding software policies

By default, SA will create the corresponding software policy for a given channel unless one of the following conditions is true:

1. “`packages_only=1`” exist in the [main] section of the configuration file `/etc/opt/opsware/patch_importer/uln_import.conf`.



2. It has a [`<Channel Label>`] section the configuration file `/etc/opt/opsware/patch_importer/uln_import.conf` and it has “`packages_only=1`” specified.

However, you may choose to override the default behavior by specifying the `-packages_only` option at runtime. For example:

```
/opt/opsware/patch_importer/bin/uln_import -packages_only
```

Like other runtime options, this option does not cause permanent changes in the configuration file.

## View the enabled channel information

You can view the enabled channels information by specifying the `-show_labels` option. For example:

```
[root@vc002 bin]# /opt/opsware/patch_importer/bin/uln_import --show_labels
***** Supported Channels For ULN *****

Retrieving platform information from SA
Retrieving channel information from Oracle ULN
Processing package information

Supported Labels: ['e15_u5_x86_64_patch', 'e15_u5_i386_patch']

----- Channels Details -----

Channel Label      : e15_u5_x86_64_patch
Channel Name       : Enterprise Linux 5 Update 5 Patch (x86_64)
Channel Description : Updated packages published after release of Enterprise Linux
5 Update 5 (x86_64)
Channel Version    : 20110111133047
Number of Packages : 649

Channel Label      : e15_u5_i386_patch
Channel Name       : Enterprise Linux 5 Update 5 Patch (i386)
Channel Description : Updated packages published after release of Enterprise Linux
5 Update 5 (i386)
Channel Version    : 20110111125211
Number of Packages : 530

*****
```

## View the supported channels for the Agent platforms

You can view the list of channels SA currently support, along with its corresponding platform, by specifying the `--show_platform_labels` option. For example:

```
[root@vc002 bin]# /opt/opsware/patch_importer/bin/uln_import --show_platform_labels
```

```
Retrieving platform information from SA
```

```
|
----- Channel Label -----      ----- Platform Name -----
e15_exadata_i386_latest            Oracle Enterprise Linux 5
e15_exadata_x86_64_latest          Oracle Enterprise Linux 5 X86_64
e15_ga_i386_base                   Oracle Enterprise Linux 5
e15_ga_i386_patch                  Oracle Enterprise Linux 5
e15_ga_x86_64_base                 Oracle Enterprise Linux 5 X86_64
e15_ga_x86_64_patch                Oracle Enterprise Linux 5 X86_64
e15_i386_addons                    Oracle Enterprise Linux 5
e15_i386_lsb4                      Oracle Enterprise Linux 5
e15_i386_ocfs2                     Oracle Enterprise Linux 5
e15_i386_oracle                    Oracle Enterprise Linux 5
e15_i386_oracle_addons             Oracle Enterprise Linux 5
e15_rds_i386_latest                Oracle Enterprise Linux 5
e15_rds_x86_64_latest              Oracle Enterprise Linux 5 X86_64
e15_u1_i386_base                   Oracle Enterprise Linux 5
e15_u1_i386_patch                  Oracle Enterprise Linux 5
e15_u1_x86_64_base                 Oracle Enterprise Linux 5 X86_64
e15_u1_x86_64_patch                Oracle Enterprise Linux 5 X86_64
e15_u2_i386_base                   Oracle Enterprise Linux 5
e15_u2_i386_patch                  Oracle Enterprise Linux 5
e15_u2_x86_64_base                 Oracle Enterprise Linux 5 X86_64
e15_u2_x86_64_patch                Oracle Enterprise Linux 5 X86_64
e15_u3_i386_base                   Oracle Enterprise Linux 5
e15_u3_i386_patch                  Oracle Enterprise Linux 5
e15_u3_x86_64_base                 Oracle Enterprise Linux 5 X86_64
e15_u3_x86_64_patch                Oracle Enterprise Linux 5 X86_64
```

e15_u4_i386_base	Oracle Enterprise Linux 5
e15_u4_i386_patch	Oracle Enterprise Linux 5
e15_u4_x86_64_base	Oracle Enterprise Linux 5 X86_64
e15_u4_x86_64_patch	Oracle Enterprise Linux 5 X86_64
e15_u5_i386_base	Oracle Enterprise Linux 5
e15_u5_i386_patch	Oracle Enterprise Linux 5
e15_u5_x86_64_base	Oracle Enterprise Linux 5 X86_64
e15_u5_x86_64_patch	Oracle Enterprise Linux 5 X86_64
e15_unsupported_i386_latest	Oracle Enterprise Linux 5
e15_unsupported_x86_64_latest	Oracle Enterprise Linux 5 X86_64
e15_x86_64_addons	Oracle Enterprise Linux 5 X86_64
e15_x86_64_lsb4	Oracle Enterprise Linux 5 X86_64
e15_x86_64_ocfs2	Oracle Enterprise Linux 5 X86_64
e15_x86_64_oracle	Oracle Enterprise Linux 5 X86_64
e15_x86_64_oracle_addons	Oracle Enterprise Linux 5 X86_64
ol5_i386_latest	Oracle Enterprise Linux 5
ol5_u5_x86_64_patch	Oracle Enterprise Linux 5 X86_64
ol5_u6_i386_base	Oracle Enterprise Linux 5
ol5_u6_i386_patch	Oracle Enterprise Linux 5
ol5_u6_x86_64_base	Oracle Enterprise Linux 5 X86_64
ol5_u6_x86_64_patch	Oracle Enterprise Linux 5 X86_64
ol5_x86_64_latest	Oracle Enterprise Linux 5 X86_64
redhat-advanced-server-i386	Red Hat Enterprise Linux AS 2.1
redhat-ent-linux-i386-es-2.1	Red Hat Enterprise Linux ES 2.1
redhat-ent-linux-i386-ws-2.1	Red Hat Enterprise Linux WS 2.1
rhel-i386-as-3	Red Hat Enterprise Linux AS 3
rhel-i386-as-4	Red Hat Enterprise Linux AS 4
rhel-i386-client-5	Red Hat Enterprise Linux Desktop 5
rhel-i386-es-3	Red Hat Enterprise Linux ES 3
rhel-i386-es-4	Red Hat Enterprise Linux ES 4
rhel-i386-server-5	Red Hat Enterprise Linux Server 5
rhel-i386-ws-3	Red Hat Enterprise Linux WS 3
rhel-i386-ws-4	Red Hat Enterprise Linux WS 4

rhel-ia64-as-3	Red Hat Enterprise Linux AS 3 IA64
rhel-ia64-as-4	Red Hat Enterprise Linux AS 4 IA64
rhel-ia64-es-3	Red Hat Enterprise Linux ES 3 IA64
rhel-ia64-es-4	Red Hat Enterprise Linux ES 4 IA64
rhel-ia64-server-5	Red Hat Enterprise Linux Server 5 IA64
rhel-ia64-ws-3	Red Hat Enterprise Linux WS 3 IA64
rhel-ia64-ws-4	Red Hat Enterprise Linux WS 4 IA64
rhel-x86_64-as-3	Red Hat Enterprise Linux AS 3 X86_64
rhel-x86_64-as-4	Red Hat Enterprise Linux AS 4 X86_64
rhel-x86_64-client-5	Red Hat Enterprise Linux Desktop 5 X86_64
rhel-x86_64-es-3	Red Hat Enterprise Linux ES 3 X86_64
rhel-x86_64-es-4	Red Hat Enterprise Linux ES 4 X86_64
rhel-x86_64-server-5	Red Hat Enterprise Linux Server 5 X86_64
rhel-x86_64-ws-3	Red Hat Enterprise Linux WS 3 X86_64
rhel-x86_64-ws-4	Red Hat Enterprise Linux WS 4 X86_64

You can also filter the platforms by using the `-platform_name` option. This is a case-sensitive partial match. For example, to display only platforms with the string "Oracle" in their name:

```
[root@vc002 bin]# /opt/opsware/patch_importer/bin/uln_import --show_platform_labels  
--platform_name Oracle
```

Retrieving platform information from SA

```
|  
----- Channel Label -----      ----- Platform Name -----  
e15_exadata_i386_latest             Oracle Enterprise Linux 5  
e15_exadata_x86_64_latest           Oracle Enterprise Linux 5 X86_64  
e15_ga_i386_base                     Oracle Enterprise Linux 5  
e15_ga_i386_patch                    Oracle Enterprise Linux 5  
e15_ga_x86_64_base                   Oracle Enterprise Linux 5 X86_64  
e15_ga_x86_64_patch                  Oracle Enterprise Linux 5 X86_64  
e15_i386_addons                       Oracle Enterprise Linux 5  
e15_i386_lsb4                         Oracle Enterprise Linux 5  
e15_i386_ocfs2                       Oracle Enterprise Linux 5  
e15_i386_oracle                       Oracle Enterprise Linux 5
```

e15_i386_oracle_addons	Oracle Enterprise Linux 5
e15_rds_i386_latest	Oracle Enterprise Linux 5
e15_rds_x86_64_latest	Oracle Enterprise Linux 5 X86_64
e15_u1_i386_base	Oracle Enterprise Linux 5
e15_u1_i386_patch	Oracle Enterprise Linux 5
e15_u1_x86_64_base	Oracle Enterprise Linux 5 X86_64
e15_u1_x86_64_patch	Oracle Enterprise Linux 5 X86_64
e15_u2_i386_base	Oracle Enterprise Linux 5
e15_u2_i386_patch	Oracle Enterprise Linux 5
e15_u2_x86_64_base	Oracle Enterprise Linux 5 X86_64
e15_u2_x86_64_patch	Oracle Enterprise Linux 5 X86_64
e15_u3_i386_base	Oracle Enterprise Linux 5
e15_u3_i386_patch	Oracle Enterprise Linux 5
e15_u3_x86_64_base	Oracle Enterprise Linux 5 X86_64
e15_u3_x86_64_patch	Oracle Enterprise Linux 5 X86_64
e15_u4_i386_base	Oracle Enterprise Linux 5
e15_u4_i386_patch	Oracle Enterprise Linux 5
e15_u4_x86_64_base	Oracle Enterprise Linux 5 X86_64
e15_u4_x86_64_patch	Oracle Enterprise Linux 5 X86_64
e15_u5_i386_base	Oracle Enterprise Linux 5
e15_u5_i386_patch	Oracle Enterprise Linux 5
e15_u5_x86_64_base	Oracle Enterprise Linux 5 X86_64
e15_u5_x86_64_patch	Oracle Enterprise Linux 5 X86_64
e15_unsupported_i386_latest	Oracle Enterprise Linux 5
e15_unsupported_x86_64_latest	Oracle Enterprise Linux 5 X86_64
e15_x86_64_addons	Oracle Enterprise Linux 5 X86_64
e15_x86_64_lsb4	Oracle Enterprise Linux 5 X86_64
e15_x86_64_ocfs2	Oracle Enterprise Linux 5 X86_64
e15_x86_64_oracle	Oracle Enterprise Linux 5 X86_64
e15_x86_64_oracle_addons	Oracle Enterprise Linux 5 X86_64
o15_i386_latest	Oracle Enterprise Linux 5
o15_u5_x86_64_patch	Oracle Enterprise Linux 5 X86_64
o15_u6_i386_base	Oracle Enterprise Linux 5

o15_u6_i386_patch	Oracle Enterprise Linux 5
o15_u6_x86_64_base	Oracle Enterprise Linux 5 X86_64
o15_u6_x86_64_patch	Oracle Enterprise Linux 5 X86_64
o15_x86_64_latest	Oracle Enterprise Linux 5 X86_64

## Add a channel label to a platform

Sometime vendors may add channel labels to a given platform. SA must be aware of the new labels before the new channels can be supported.

To add the new labels to the SA's supported list:

```
[root@vc002 bin]# /opt/opsware/patch_importer/bin/uln_import --add_platform_label -  
-platform_name "Oracle Enterprise Linux 5" e15_new_label
```

```
Adding channel label e15_new_label for platform Oracle Enterprise Linux 5
```

```
Done
```

## Remove a channel label from a platform

Sometime a channel is obsolete and can be removed from SA's supported list.

To remove an obsolete channel from the supported list:

```
[root@vc002 bin]# /opt/opsware/patch_importer/bin/uln_import --remove_platform_  
label --platform_name "Oracle Enterprise Linux 5" e15_new_label
```

```
Removing channel label e15_new_label for platform Oracle Enterprise Linux 5
```

```
Done
```

# Patch management for SUSE Linux Enterprise

Server Automation patch management for SUSE Linux Enterprise enables you to manage security and non-security patches for your SUSE-supported managed servers. It allows you to identify, install, and audit SUSE package updates, keeping a high level of security across managed servers in your organization.

In SA, patches are the equivalent of SUSE errata. The latter are package updates, bug fixes, and security patches for Linux Enterprise.

## High-level architecture

The SA SUSE patching mechanism allows you to import patches from SUSE or from other sources, scan managed servers to determine their current patching level, and perform the deployment of patches. Finally, the server can be checked for compliance against the recommended set of patches.

A typical SUSE patching use case follows a well-defined process. Patches are first imported into SA. This is followed by an optional step where you can manage the patches. Once the recommended patches are included in one or multiple software policies, the servers can be remediated. After the remediation occurs, the patched servers can be checked for compliance.

## Import patches for SUSE platforms

In SA, SUSE platforms can be customized and kept up-to-date by using RPM packages. These packages can be imported and applied to a set of SUSE-supported managed servers in SA. The import process uploads RPM patches into the SA Library and can be used in operations like software installation, software policy creation and remediation, software compliance, and so on.

Currently, there are three ways to import SUSE patches into SA:

- Upload the RPM packages into the SA Library using the SA Command Line Interface.
- Import the SUSE packages into SA through the SA Client built-in importer. This tool allows you to import multiple RPM packages simultaneously. If an RPM package that is being uploaded exists in the SA Library already, then you can:
  - Replace (overwrite) the content of the existing package
  - Skip the package import (useful when importing multiple packages)
  - Cancel the import in progress

When you overwrite an existing software package, SA preserves any reboot options or flags previously set for the package.

**Note:** The approaches listed above work best for scenarios where custom patches must be imported into SA.

- Import the official patches issued by SUSE using one of the following SA SUSE tools, which comes preinstalled with the slice component:
  - SUSE Manager Importer tool
  - Subscription Management Tool (SMT) Importer

You can find the binaries for these tools in `/opt/opsware/sles_import/bin`.

## Importing SUSE Errata and channels in SA using SA SUSE Importer tools

SUSE publishes Errata that contains information describing security patches, bug fixes, and package updates for SUSE Linux Enterprise. To install the packages in the Errata, you must download the Errata from the SUSE web-site and then import into SA. Using SA, you can automatically download the Errata released by SUSE, convert them to policies, and store the policy in a folder in the SA Library.

In addition, SUSE publishes repositories that contain packages from a particular repository. Using SA, you can automatically download the packages in a channel (SuSE Manager Importer) or content label (SMT), convert them to policies, and store the policies in a folder in the SA Library. The `suse_manager_import` and `smt_import` tools provided by SA enable you to create policies that correspond to the

SUSE errata and channels/content labels. Using these tools, you can create the following types of policies:

- **Channel-based software policy:** A SUSE Network channel contains a list of packages. A channel allows you to group packages as per your organizational requirements. For example, a channel may contain packages for a particular SUSE operating system version or architecture. A channel may contain other child channels. When you run the importer, SA downloads the latest packages from the SUSE Network channel (SUSE Manager Importer), imports the packages to the SA Library and creates a channel-based or content-based software policy. Channels are equivalent to SMT content, the only difference being the source of the packages.  
Thus, a channel-based policy reflects a particular channel. In the SA Client, you can view the name, description, location, availability, and the version of the operating system of the channel-based policy in the SA Library.
- **Errata-based software policy:** SUSE Network Errata contains information on a particular problem and the associated packages to resolve the problem. An errata-based policy contains all the individual erratum-based policies for a given channel. SA downloads the latest packages from the SUSE Network Errata and then imports the packages to the SA Library and creates an errata-based software policy.

There are three types of SUSE Network Errata, specific to SUSE Manager:

- Bug Fix Advisories
- Product Enhancement Advisories
- Security Advisories

The SMT Importer uses the following types of errata:

- Security Advisories
- Recommended Advisories
- Optional Advisories

In the SA Client, you can view the name, description, location, availability, and the operating system version of the errata-based policy in the SA Library.

- **Erratum-based software policy:** Erratum-based policies contain packages associated with a particular erratum. When you run the `suse_manager_import` or `smt_import` tool, SA downloads the latest packages from the SUSE Network erratum and then imports the packages to the SA Library and creates an Erratum-based software policy.

To create and maintain policies from the SUSE Linux errata, erratum, and channels, log into the core server running the Software Repository component (part of the Slice Component bundle) and run the `suse_manager_import` or `smt_import` tool located in the `/opt/opsware/sles_import/bin` directory.

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

Importing RPM packages from the SUSE Network to SA requires a large amount of disk space. Over a period of time, the amount of disk space required increases as new versions of packages are released by SUSE. HP recommends having at least 5 GB of disk space available in Software Repository for every SUSE channel you enable using the importer.



To view the complete documentation, run one of the following commands:

- `/opt/opsware/sles_import/bin/suse_manager_import --manual`
- `/opt/opsware/sles_import/bin/smt_import --manual`

When you run the importer, you can specify the options listed in the documentation provided by the tools or use the sample configuration files provided by SA, located at `/etc/opt/opsware/sles_import/suse_manager.conf-sample` or `/etc/opt/opsware/sles_import/smt_import.conf-sample`.

## SA SUSE Manager Importer tool

The SA SUSE Manager Importer is a tool based on the SA RedHat Importer. The tool imports packages and errata from a SUSE Manager server, creates SA software policies for errata and packages hosted by SUSE Manager.

The following topics are discussed in this section:

- ["Installing the SUSE Manager CA certificate" below](#)
- ["Configuring the SA SUSE Manager Importer" on the next page](#)
- ["Working of SUSE Manager Importer tool" on page 299](#)
- ["Usage of SUSE Manager Importer tool" on page 299](#)

## Installing the SUSE Manager CA certificate

By default, the importer binary `suse_manager_import` validates the SUSE Manager server certificate. The remote server certificate is self-signed, therefore there is no CA bundled with the SA OSPWopenssl component. To enable access for `suse_manager_import` to SUSE Manager server, you must install the self-signed server certificate in the OSPWopenssl trust store.

To install SUSE Manager CA certificate:

1. Download the self-signed certificate from SUSE Manager.
  - a. Install the self-signed certificate in the SA trust store.
2. Verify if OPSWopenssl is validating the server certificate.

### Downloading the self-signed certificate from SUSE Manger

The self-signed certificate is made public by SUSE Manager at `/pub/RHN-ORG-TRUSTED-SSL-CERT`. Run the following command to download the certificate file:

```
wget -O /tmp/RHN-ORG-TRUSTED-SSL-CERT http://suse.manager.hostname/pub/RHN-ORG-TRUSTED-SSL-CERT
```

If you need proxy access to SUSE Manager server, you can export the `http_proxy` environment variable and the `wget` command will use the exported value.

### Installing the self-signed certificate in SA trust store

1. Open the downloaded file, copy the following text appearing at the end of the file:

```
-----BEGIN CERTIFICATE-----  
MIIE4TCCA8mgAwIBAgIJANwa50FPkBHMA0GCSqGSIb3DQEBCwUAMIGGMQswCQYD  
haXhmbq+5pEkpxGAactW+t0RsJmpgTdAXeq2rreYtgZ2/vCwdM0iwSVakGNFAvni
```

```
T9lnSVrADc0/S8V/DzcH30RzSpIS44beE23zag82019fCrsZg9VkyJER4Fn0tRq4
6U9I40gBSPSU34MXc1G1d0BAN+mANWHQYacZ7hHQJtMRP+mc8ZgHIvsKNnKR0H0d
Rh1a7cP7GYrXn/piQAxRW66f0YJ0eVIsAWJvgUb+A8ecwb+s6k56cQdLkkm0wKD0
2zUFMAg=
-----END CERTIFICATE-----
```

2. Open the `/opt/opsware/openssl/cert.pem` file in an editor and paste the copied text at the end of the file.

The certificate will be installed in the SA trust store. Ensure that the openssl tool verifies the SUSE Manager server certificate.

### Verifying that OPSWopenssl is validating the server certificate

After the CA certificate is installed in SA trust store, verify if openssl validates the SUSE Manager certificate before running the importer:

```
/opt/opsware/bin/openssl s_client -connect suse.manager.hostname:443 -verify 3
```

If the verification process is successful, the following message will be displayed at the end of the output:

```
Verify return code: 0 (ok)
```

If the verification fails, a non-zero value will be returned:

```
Verify return code: 21 (unable to verify the first certificate)
```

## Configuring the SA SUSE Manager Importer

To run SA SUSE Manager Importer with a default configuration file, you have to create a configuration file at

**`/etc/opt/opsware/sles_import/suse_manager.conf`**.

A configuration file template is available at `/etc/opt/opsware/sles_import/suse_manager.conf-sample`.

To create a configuration file:

1. Copy the sample configuration file to **`suse_manager.conf`**  

```
cp /etc/opt/opsware/sles_import/suse_manager.conf-sample /etc/opt/opsware/sles_import/suse_manager.conf
```
2. Provide write permission to the **`Suse_manager.conf`** file:  

```
chmod u+w /etc/opt/opsware/sles_import/suse_manager.conf
```
3. Edit the **`/etc/opt/opsware/sles_import/suse_manager.conf`** file:
  - a. In the **`host`** option, provide the hostname/IP address of your SUSE Manager Server.

**Note:** If you have a custom port you can append `!:<port number>` to the IP address or hostname. If port number is not provided, the importer uses the default HTTPS port which is 443.

- b. In the **`user`** and **`pass`** options, provide the user name and password of your SUSE Manager Server.
- c. Provide values to the **`opsware_user`** and **`opsware_password`** fields for configuring the SA credentials.

- d. In the channel option, you can list the channels you want to import. If you are unsure what values are valid, you can save the configuration file and run the following command:

```
/opt/opsware/sles_import/bin/suse_manager_import --show_labels
```

At this stage, the importer can access SA and your SUSE Manager to determine the default supported labels. Later, you can come back and fill the channels option with valid values.

Channel labels can also be specified in the command line, provided that all required options (that is SUSE Manager hostname, user and password) are defined in the configuration file. If no label is provided in the command line or in the configuration file, then all default supported parent channels will be imported.

## Working of SUSE Manager Importer tool

The basis for SUSE Manager is the channel. A channel is a grouping of one or more packages associated with a product repository. A patch released by SUSE is called as an erratum in SA and a collection of these patches is called errata in SA.

Channels are of two types:

- Parent channels
- Child channels

Parent channels are usually, but not necessarily, associated with Pool repositories, whereas the Updates repositories are considered as child channels of a Pool repository. In addition, there are other types of child channels that are not Updates repositories.

**Note:** If you import a label into SA that is associated with the Pool channel, no erratum or errata will be imported because Pool channels do not have patches associated with it. If you import a label associated with the Updates channel, a channel software policy is created that contains all packages from errata.

The SA SUSE Manager Importer supports both parent and child channels. The command line options allow you to group all imported errata for a particular channel into a single software policy.

## Usage of SUSE Manager Importer tool

The new importer binary (`suse_manager_import`) for SUSE Manager is located at `/opt/opsware/sles_import/bin`.

Run the importer binary to group all imported erratum policies into a single errata policy:

```
/opt/opsware/sles_import/bin/suse_manager_import --mode=all [CHANNEL_LABEL...]
```

The `--mode` option specifies what to import. The `all` value specifies that you want to import packages of a channel, create a Channel Software Policy in SA, import errata, and create Software Policies for each erratum.

You can also choose:

- Channel imports packages from a repository and then creates a Software Policy
- Erratum imports patches and create software policies
- Errata imports all erratums and group them into a single software policy

By default, `suse_manager_import` uses a configuration file located at `/etc/opt/opsware/sles_import/suse_manager.conf`.

You can also specify another location for the configuration file using the `--conf=FILE` option.

To get the list of platforms supported by SA, run `./suse_manager_import --show_platforms`.

To get the list of labels that are supported by default in SA and on your SUSE Manager Server, run `./suse_manager_import --show_labels`.

## SMT Importer tool

Subscription Management Tool (SMT) is a package proxy system that is integrated with Novell Customer Center/SUSE Customer Center (NCC/SCC). It provides a repository and registration target that is synchronized with the NCC/SCC, allowing a more secure centralized deployment.

A repoindex file listing all the available repositories provided by SMT will be published in a public location such as `https://smt.hostname/repo/repoindex.xml`. This file can be protected by a user name and a password specified in `/etc/smt.conf` by `mirrorUser` and `mirrorPassword` attributes.

Following is an example of an `repoindex.xml` file, listing all the available repositories:

```
<repoindex>
<repo name="SLES12-Pool" alias="SLES12-Pool" description="SLES12-Pool for sle-12-
x86_64" distro_target="sle-12-x86_64" path="SUSE/Products/SLE-SERVER/12/x86_
64/product/" priority="0"pub="0" autorefresh="0" enabled="0"/>
<repo name="SLE10-SDK-SP4-Updates" alias="SLE10-SDK-SP4-Updates"
description="SLE10-SDK-SP4-Updates for sles-10-x86_64" distro_target="sles-10-x86_
64" path="$RCE/SLE10-SDK-SP4-Updates/sles-10-x86_64/" priority="0" pub="0"
autorefresh="1" enabled="0"/>
<repo name="SLES11-SP1-Pool" alias="SLES11-SP1-Pool" description="SLES11-SP1-Pool
for sle-11-i586" distro_target="sle-11-i586" path="$RCE/SLES11-SP1-Pool/sle-11-
i586/" priority="0"pub="0" autorefresh="0" enabled="0"/>
<repo name="SLE10-SDK-SP4-Pool" alias="SLE10-SDK-SP4-Pool" description="SLE10-SDK-
SP4-Pool for sles-10-x86_64" distro_target="sles-10-x86_64" path="$RCE/SLE10-SDK-
SP4-Pool/sles-10-x86_64/" priority="0" pub="0" autorefresh="0" enabled="0"/>
<repo name="SLES11-SP2-Updates" alias="SLES11-SP2-Updates" description="SLES11-SP2-
Updates for sle-11-ppc64" distro_target="sle-11-ppc64" path="$RCE/SLES11-SP2-
Updates/sle-11-ppc64/"priority="0" pub="0" autorefresh="1" enabled="0"/>
</repoindex>
```

where, `path` represents the relative location of a repository to `https://smt.hostname/repo/`. The `path` tag can be configured per repository.

The `repoindex` file publishes both SCC and NCC synced repositories. Each repository path can be protected by a user name and password. The `requiredAuthType` attribute from `/etc/smt.conf` enables or disables the authentication.

## Installing the SMT server certificate

By default, the importer binary `smt_import` validates the SMT server certificate. The remote server certificate is self-signed, therefore there is no CA bundled with SA `OSPWopenssl` component. To enable access for `smt_import` to SMT server, you must install the self-signed server certificate in the `OSPWopenssl` trust store.

To install the SMT server certificate:

1. Download the self-signed certificate from SMT server.
2. Install the self-signed certificate in SA trust store.
3. Verify `OSPWopenssl` is validating the server certificate.

### Downloading the self-signed certificate from SMT server

You can download the certificate from the browser using the URL, `http://<smt_host>/smt.crt`. You can also download the certificate from `/srv/www/htdocs/smt.crt` of the SMT server.

### Installing the self-signed certificate in SA trust store

1. Open the downloaded file, copy the text appearing at the end of the file.

The following is an example of the text that appears at the end of the downloaded file:

```
-----BEGIN CERTIFICATE-----  
MIIE4TCCA8mgAwIBAgIJANwa50FPkBHMA0GCSqGSIb3DQEBCwUAMIGGMQswCQYD  
haXhmbq+5pEkpxGAactW+tORsJmpgTdAXeq2rreYtgZ2/vCwdM0iwSVakGNFAvni  
T9lnSVrADc0/S8V/DzcH30RzSpIS44beE23zag82019fCrsZg9VkyJER4Fn0tRq4  
6U9I40gBSPSU34MXc1G1d0BAN+mANWHQYacZ7hHQJtMRP+mc8ZgHIvsKNnKR0H0d  
Rh1a7cP7GYrXn/piQAxRW66f0YJ0eVIsAWJvgUb+A8ecwb+s6k56cQdLkkm0wKD0  
2zUFMAg=  
-----END CERTIFICATE-----
```

2. Open the `/opt/opsware/openssl/cert.pem` file in an editor and paste the copied text at the end of the file.

The certificate will be installed in the SA trust store. Ensure that `openssl` tool verifies the SMT server certificate.

### Verifying that `OSPWopenssl` is validating the server certificate

After the CA certificate is installed in the SA trust store, verify if `openssl` validates the SMT server certificate before running the importer:

```
/opt/opsware/bin/openssl s_client -connect smt.hostname:443 -verify 3
```

If the verification process is successful, the following message will be displayed at the end of the output:

```
Verify return code: 0 (ok)
```

If the verification fails, a non-zero value will be returned:

```
Verify return code: 21 (unable to verify the first certificate)
```

## Configuring the SMT Importer

To run SMT Importer with a default configuration file, you have to create a configuration file at

/etc/opt/opsware/sles\_import/smt\_import.conf.

A configuration file template is available at /etc/opt/opsware/sles\_import/smt\_import.conf-sample.

To create a configuration file:

1. `cp /etc/opt/opsware/sles_import/smt_import.conf-sample /etc/opt/opsware/sles_import/smt_import.conf`
2. `chmod u+w /etc/opt/opsware/sles_import/smt_import.conf`
3. Edit the `/etc/opt/opsware/sles_import/smt_import.conf` file:
  - a. Provide values to the `opsware_user` and `opsware_password` fields for configuring the SA credentials.
  - b. In the `host` option, provide the hostname/IP address of your SMT Server .

**Note:** If you have a custom port, you can append ':<port number>' to the IP address or hostname. If the port number is not provided, the importer can use the default HTTPS port which is 443.

- c. In the `User` and `Password` options, provide the user name and password of your SMT Server.
- d. In the `content_labels` option, you can list the channels you want to import. If you are unsure what values are valid, you can save the configuration file and run the following command:

```
/opt/opsware/sles_import/bin/smt_import --show_labels
```

At this stage, the importer can access SA and your SMT Server to determine the default supported labels. Later, you can come back and fill in the content labels option with valid values.

Content labels can also be specified in the command line, provided that all required options (that is, the SMT hostname, user, and password) are defined in the configuration file. If no label is provided in the command line or in the configuration file, then all default supported content labels will be imported.

## Working of SMT Importer

The basis for SMT is the content label. A content label is a grouping of one or more packages associated with a product repository. A content label is just another name for a channel – content label, which describes a repository sitting on a content deliverer (SMT in this case), while a channel is the official descriptor (based on a remote official portal). Whatever the case, channel-based policies will be created, one for each content label chosen. A patch released by SMT is called as an erratum in SA and a collection of these patches is called errata in SA.

**Note:** If you import a label into SA that is associated with Pool channel, no erratum or errata will be imported. This is because Pool channels do not have patches associated with them. If you import a label associated with Updates channel, SA creates a channel software policy containing all the packages from errata.

## Content labels

When importing from SMT, `smt_import` uses content labels to identify the CDN content to import. The format of the content label is the following:

```
<entitlement_content_name>:<distro_target>
```

where:

- `<entitlement_content_name>` is the repository's name as specified in the `repoindex.xml`
- `<distro_target>` is the attribute for `<entitlement_content_name>` present under the same tag of the **repoindex.xml** file.

To determine the label of the CDN content to import, run the following command: `smt_import --show_labels`

## Usage of SMT Importer

The new importer binary (`smt_import`) is located at `/opt/opsware/sles_import/bin`.

Run the following importer binary to group all imported erratum policies into a single errata policy:

```
/opt/opsware/sles_import/bin/smt_import --mode=all [CHANNEL_LABEL...]
```

The `--mode` option specifies what to import. The **all** value specifies that you want to import packages of a channel, create a Channel Software Policy in SA, import errata, and create Software Policies for each erratum.

You can also choose:

- Channel imports packages from a repository and then create a Software Policy.
- Erratum to import patches and create software policies.
- Errata to import all erratums and group them into a single software policy.

By default, `smt_import` uses a configuration file located at `/etc/opt/opsware/sles_import/smt_import.conf`.

You can also specify another location for the configuration file using the `--conf=FILE` option.

To get the list of platforms supported by SA, run `./smt_import --show_platforms`.

To get the list of labels that are supported by default in SA and on your SMT Server, run `./smt_import --show_labels`.

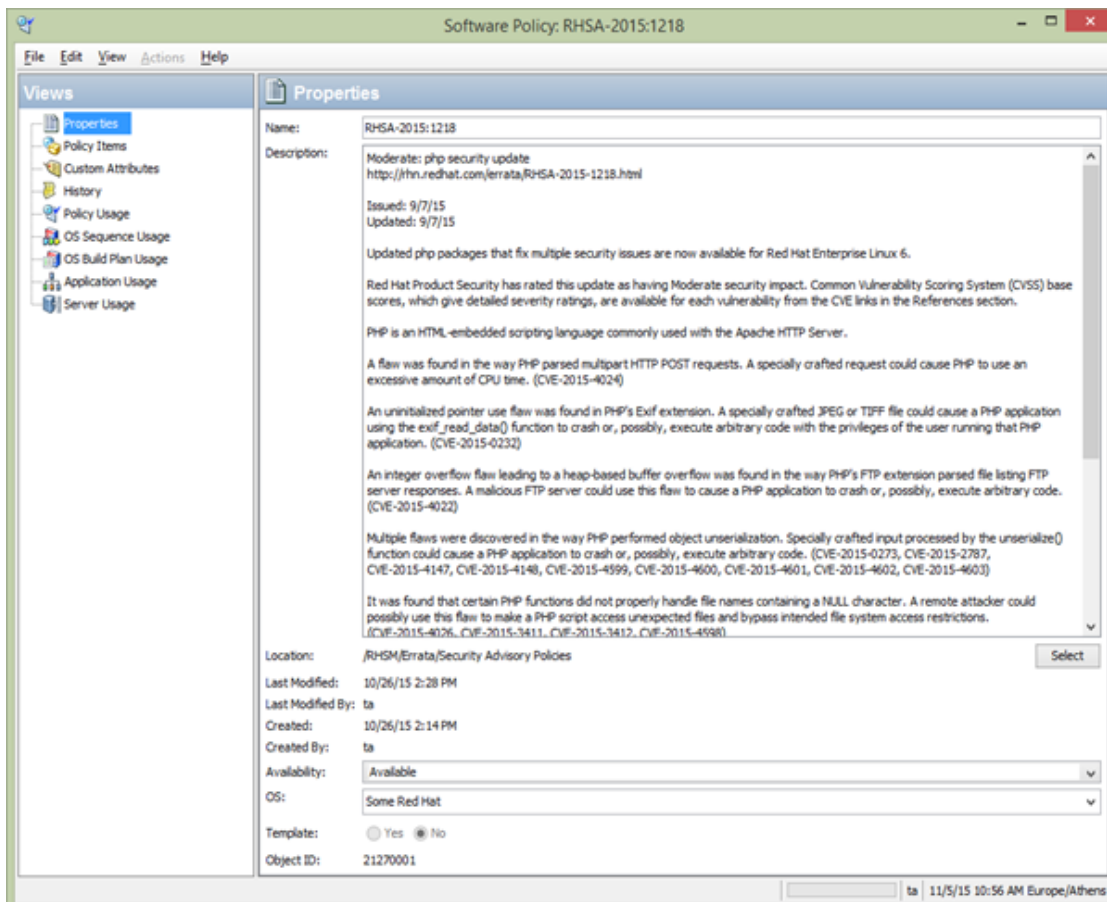
## View errata-based and channel-based policies in the SA Client

The `suse_manager_import` and `smt_import` tools allow you to create errata-based, erratum-based, and channel-based policies in the SA Client. After successfully running them, you can view the properties of errata-based, erratum-based, and channel-based policies in the SA Client. You can view properties such as the SA user who created the software policy, the date when it was created, the name, the description, the availability, the location of the policy in the Library, the operating systems applicable to the policy and the SA Client ID of the software policy. We recommend that you do not edit the policies created by the `suse_manager_import` and `smt_import` tools.

To view the properties of a software policy:

1. From the navigation pane, select **Library > By Folder**.
2. Select the **SLES** folder.

3. From the content pane, select the errata, channel, or content-based policy and open it. The policy window appears.
4. From the **Views** pane, select **Properties**. You can view the properties for the policy in the content pane.



- **Name:** Contains the errata reference for the errata based software policy.
- **Description:** Includes all the errata documentation for the errata.
- **Location:** Specifies the location of the policy in the folder hierarchy. To change the location, click **Select** to specify the location for the policy in the folder hierarchy. The **Select Location** window appears. Select a folder in the Library to specify the location of the policy and then click **Select**.
- **Created:** Corresponds to the time when the errata was downloaded by SA to create the software policy.
- **Last Modified:** Corresponds to the time when the errata based policy was modified.
- **Availability:** Contains the SA server life cycle values for the errata based software policy. The default value for an errata-based policy is set to Available.



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

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

## Errata caching

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

A cache file is created for each channel (SUSE Manager Importer) and content label (SMT Importer).

The cache files are kept in the `/var/opt/opsware/sles_import` folder on the SA core server. The file name uses the `prev_import_ch_<label>.dat` pattern, where `<label>` is the SUSE Manager Importer channel label or the SMT content label.

Here are some sample file names:

- `prev_import_ch_SLES12-SP1-Updates:sle-12-x86_64.dat`
- `prev_import_ch_sles12-pool-x86_64.dat`

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

- An erratum is imported into the SA Library and then it is removed, renamed, or moved to another folder. When `suse_manager_import` and `smt_import` are run the next time, the erratum will not be re-imported into the SA Library. This is because the erratum details are present in the cache file, so it is skipped during the import.
- The errata roll-up policy is created and then it is removed, renamed, or moved to another folder (for example, by using the SA Client). When `suse_manager_import` or `smt_import` are run the next time, the errata roll-up policy will be recreated but it will contain only the errata that has been previously published by SUSE.

## Manage SUSE patches

The second phase of the SUSE Patching mechanism – although optional, sometimes can be very important in the patching process. Since SUSE patches are just normal RPM packages, you can do all the operations that SA Client allows you to do on SUSE packages:

- Open the package
- Viewing and editing package properties
- Viewing package contents
- Viewing all software policies associated with a package
- Deleting a package
- Renaming a package
- Locating packages in folders

## Restricting access to RPM folders

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

The repository that SA downloads to a managed server before actually scanning the server for recommended patches is built as follows:

- Packages whose platform set does not include the server platform are excluded from the RPM repository.
- Packages in folders whose customer constraints do not include the customer of the server are excluded from the RPM repository.
- If one or more `repo.restrict` custom attributes are defined for a particular server, only packages in the folders specified by these custom attributes are included in the RPM repository.

In SA, you can specify in a custom attribute, the folders in the SA Library that the server has access to. All other folders will be inaccessible to the server. This gives you folder-level control over which versions of RPMs can be applied to a given server, allowing you to precisely manage platform update versions, for example SLES 11 SP4 versus SP5.

**Note:** This is not intended as a user-level access control mechanism, but rather to restrict the library and folder view of a managed server from access to the full set of RPMs in the SA Library.

# Send Documentation Feedback

If you have comments about this document, you can [contact the documentation team](#) by email. If an email client is configured on this system, click the link above and an email window opens with the following information in the subject line:

**Feedback on User Guide: Server Patching (Server Automation 10.23.007)**

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to [hpe\\_sa\\_docs@hpe.com](mailto:hpe_sa_docs@hpe.com).

We appreciate your feedback!