

HP Server Automation

Version: SA 9.14 (only)

Whitepaper

SA 9.14: SA Server Patching Updates

Software Release Date: December 17, 2012

Document Release Date: December 18, 2012



Contents

| | |
|--|----|
| SA Server Patching—Windows | 3 |
| Windows Patching Support for Multibinary Patches | 4 |
| Windows Patch Policy Remediation Job Option—Windows Patch Installation Order | 5 |
| Windows Patch Database Conflict Report—“Last Import Summary” Field..... | 7 |
| Windows Patching Support of All Products in the Microsoft Patch Catalog | 8 |
| Requirements | 8 |
| Default Selected Products | 8 |
| About Unsupported Products..... | 8 |
| Identifying Product Names for Missing Recommended Patches | 9 |
| Steps | 9 |
| Enabling/Disabling Windows Server 2008 Itanium (IA64) Patches | 15 |
| Importing Patch Contents from the Managed Servers View..... | 16 |
| Adding Items to a Windows Patch Policy Using the Object ID | 17 |
| SA 9.14 Upgrades Only | 19 |
| Patch De-duplication Steps for Windows Patching | 19 |
| Additional Functionality Added in the 9.1x Branch | 20 |
| Oracle Enterprise Linux (OEL) Patching Support | 20 |
| Solaris 11 Patching Support..... | 20 |
| Additional Information | 21 |

SA Server Patching Updates

This document describes new SA Server Patching functionality introduced in the SA 9.14 release of Server Automation.

SA Server Patching—Windows

A number of enhancements and bug fixes were made to provide predictable and reliable SA Windows Server Patching functionality. There were three priorities in this effort:

1. Resolving and preventing duplicate patches in the SA database and improving remediation reliability:
 - [Windows Patching Support for Multibinary Patches](#)
 - [Windows Patch Policy Remediation Job Option—Windows Patch Installation Order](#)
 - [Windows Patch Database Conflict Report—“Last Import Summary” Field](#)
2. Increasing the products supported in the Microsoft Patch Catalog and giving you greater control of the products selected in your environment:
 - [Windows Patching Support of All Products in the Microsoft Patch Catalog](#)
 - [Enabling/Disabling Windows Server 2008 Itanium \(IA64\) Patches](#)
3. Giving you greater control of the patches selected in your Windows Patch Policies
 - [Importing Patch Contents from the Managed Servers View](#)
 - [Adding Items to a Windows Patch Policy Using the Object ID](#)

Windows Patching Support for Multibinary Patches

Windows multibinary patch support is enabled by default in SA 9.14.

The ability to import and install Windows multibinary patches—including those traditionally blocked by SA or requiring `fixit` scripts—was introduced in 9.06 and 9.11. In 9.14, it is made available by default.

SA Agent Requirement: To support the Windows multibinary patching functionality, the SA Agent must be from SA release 9.06 or 9.11 or later within those branches. After **updating the agent, you should be able to scan and remediate the servers with the Windows Multibinary Patches.**

IMPORTANT: The SA Agent must be updated before you scan and remediate the servers.

Caution: *Do not* apply any SA-provided `fixit` scripts after upgrading to SA 9.11 or later.


The `fixit` scripts are only applicable to previous versions of SA. If you encounter an issue with a patch for which there have been `fixit` scripts in the past, contact SA Customer Support.

Applying `fixit` scripts after applying this SA update will not resolve the issue and could cause an error.

Tip: If you are installing Windows OS Service Packs (SPs), hotfixes, and update rollups, HP recommends that you remediate the server with the desired SP *before* installing the hotfixes and update rollups. Hotfixes are usually quickly released refinements that are eventually rolled up into the subsequent SP. Isolating the SP into its own policy before running the remainder of the vendor-recommended policy can prevent errors that might result from installing unnecessary hotfixes that are rolled up into the subsequent SPs.

Windows Patch Policy Remediation Job Option—Windows Patch Installation Order

Starting in 9.14, the new **Windows Patch Installation Order** setting in the Remediate job window enables you to control patch installation sequence in a given Windows Patch Policy remediation job. Selecting this option prevents the collision of Windows patch data derived from disparate sources.

 **Best Practice Tip:** This setting is strongly recommended for Windows Patch Policy remediation jobs.

SA Windows Patching installs patches from two different sources, Microsoft Offline Catalog (`wsusscn2.cab`) and HPLN Microsoft Patch Supplement. 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.

How it works:

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

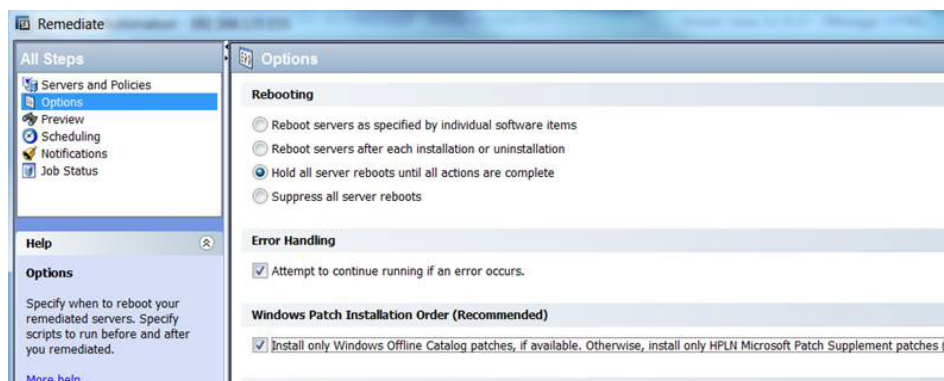


Figure: Windows Patch Installation Order setting in the Remediate window

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.

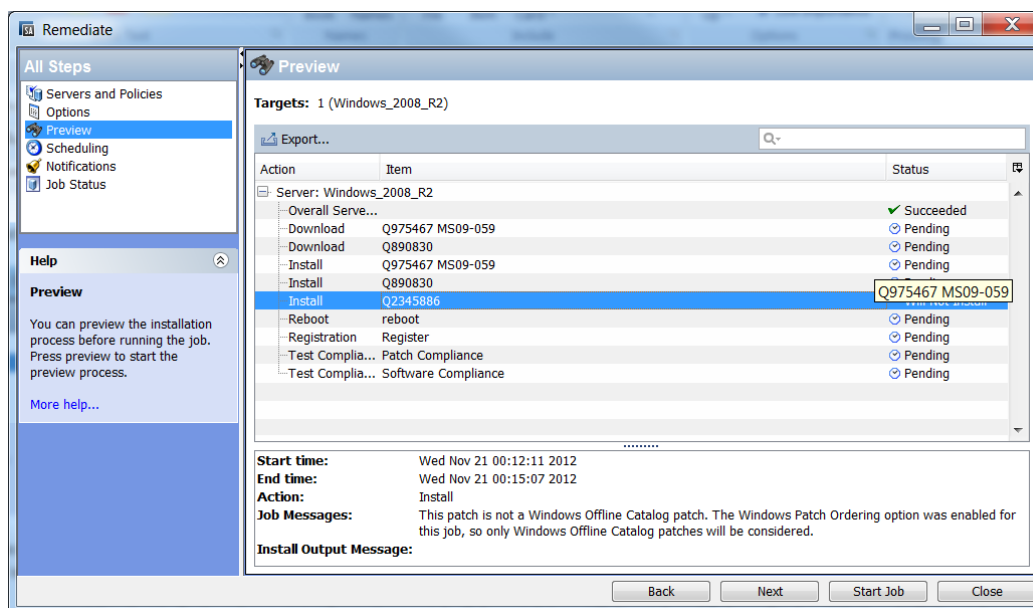
Warning: When this option is not selected, the default order is by KB #, which can cause problems if you are installing patches from both sources: Windows Offline Catalog (`wsusscn2.cab`) and HPLN Microsoft Patch Supplement.

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

IMPORTANT: 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.



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.

Known Issue—the error message above is not displayed. Instead, the following cryptic message is displayed. This will be corrected in a future release:


This non-WSUS patch was not installed because the job contains WSUS patches and remediation is set to `WSUS_EXCLUSIVE_OR` mode

'WSUS patches' refers to the patches from the Microsoft Offline Catalog (`wsusscn2.cab`). 'WSUS_EXCLUSIVE_OR mode' refers to the **Windows Patch Installation Order** option in the remediate job.

Windows Patch Database Conflict Report—“Last Import Summary” Field

Starting in 9.14, the patch database has a new field, Last Import Summary, which reports if any duplicates were found in your database. In the SA Client, navigate to **Administration > Patch Settings > Patch Database** to view this field.

Initially, this field will appear blank. However, after performing a patch import, this field will be updated to reflect the state of the imported database:

| Field Value | Description |
|--|---|
| Finished | The import operation completed. |
| Warning: <number> duplicates found. See SA Release Notes | <p>There is a conflict discovered in the patch database due to duplicate patches.</p> <p>If you encounter the warning, you should remove the duplicates before performing a compliance scan or remediation operation.</p> <p>IMPORTANT—To remove the duplicates, see the Patch De-duplication Steps for Windows Patching section of this document, (which is also provided in the <i>SA 9.14 Release Notes</i>). The De-duplication topic explains the underlying cause of this event and provides instructions on how to remove the duplicates from the database.</p> <p> Best Practice Tip: These steps are strongly recommended.</p> |

Note: If the Last Import Summary field continues to appear blank after running an import, it may be because of a known issue where the import is taking a long time and has not finished updating the patch library, or there is a rendering delay and SA Client cache needs to be reloaded (from the SA Client menu, go to **Tools > Options**, and click **Reload Cache**).

Windows Patching Support of All Products in the Microsoft Patch Catalog

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

Previously, SA Windows Patching only supported OS patches; however 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 the cab file was imported.

Now, when the `wsusscn2.cab` file is imported, all product-specific patches are imported according to the products selected under the Edit Products setting.

Requirements


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

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

Default Selected Products

At the time of this release, the default selected products in the `wsusscn2.cab` are:

- Exchange 2000 Server
- Exchange Server 2003
- Internet Security and Acceleration Server 2004
- Office 2003
- Visual Studio 2005
- Visual Studio 2008
- Visual Studio 2010
- Windows 2000
- Windows Server 2003
- Windows Server 2008
- Windows Server 2008 R2
- Windows Server 2012
- Windows XP

 **Best Practice Tip:** You can modify the list according to the products in your environment. If there are products in the default selected list that you do not want, they should be deselected before you run the Patch Import. This will minimize the data storage issues in the SA Core and Software Repository (word). Instructions for selecting products and using this new functionality are provided in the [Steps](#) section of this topic.

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 Offline Catalog, `wsusscn2.cab`, may include patches for Windows OS or OS-specific products that SA does not support. These unsupported patches may still appear in the Patch Products selection list under SA Patch Settings. However, unsupported Windows patches will still be excluded 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 a subdued gray font. To determine the MS product necessary to import these missing patches, a KB#-to-Product Mapping script is available. Please contact HPSA Customer Support for details.

Steps

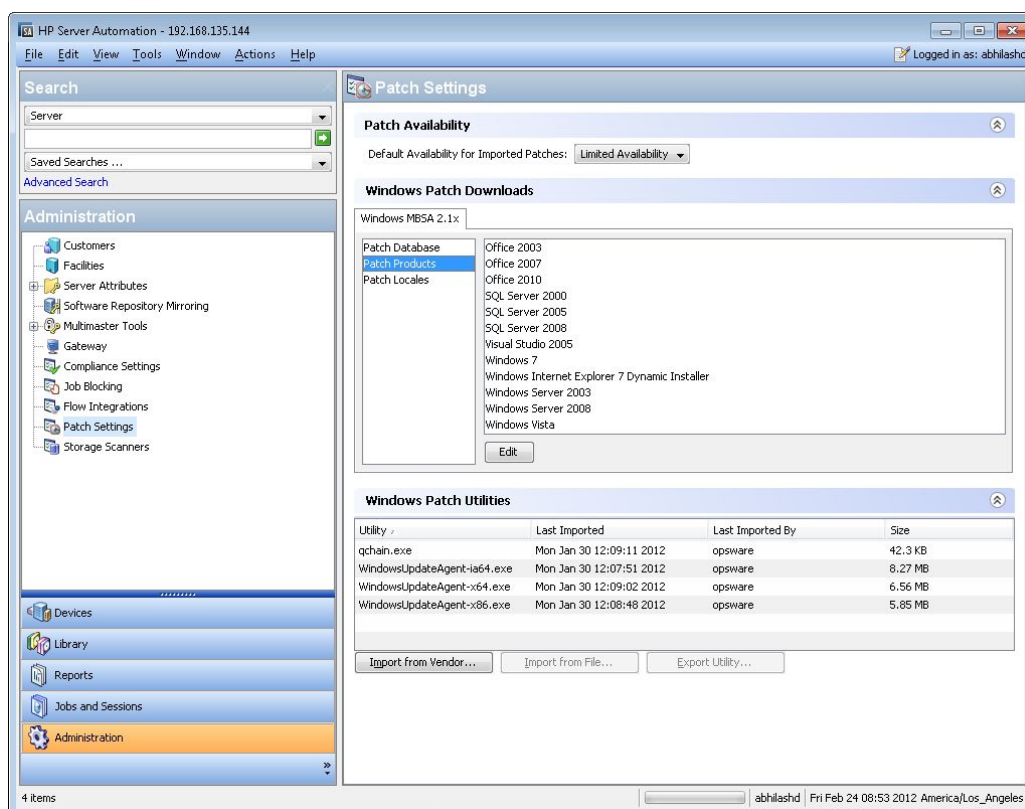
The following steps instruct how to get started with the new Windows All Products Support functionality.

- [Step 1 – Selecting Microsoft Products from the SA Client](#)
- [Step 2 – Import Windows Patches for Additional Products](#)
- [Step 3 – Scan and Remediate Servers](#)

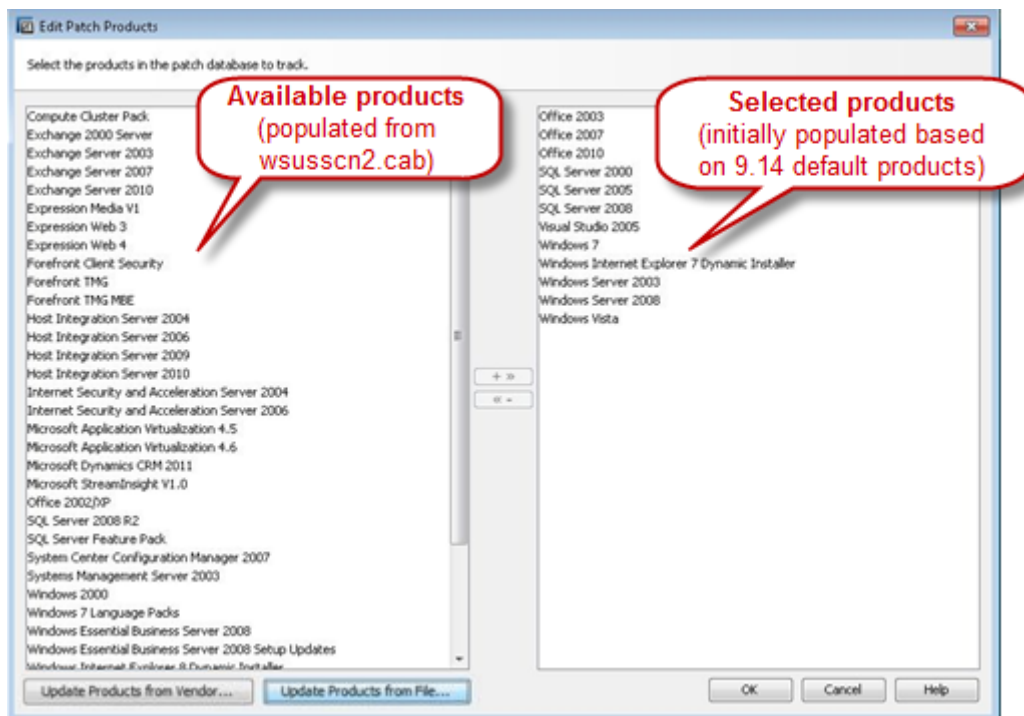
Step 1 – Selecting Microsoft Products from the SA Client

To import product-specific patches, select the pertinent MS products:

1. Navigate to the Administration > Patch Settings.
2. Select **Patch Products** from the list of Windows Patch Download settings.



3. Click **Edit** to open the Edit Patch Products window.



Available products are on the left and selected products are on the right.

Note: Upon first usage, the initial set of selected products depends on which version of the Microsoft Product Catalog, `wsusscn2.cab`, is in your system. If your system does not already have `wsusscn2.cab` imported, the left panel will be empty.

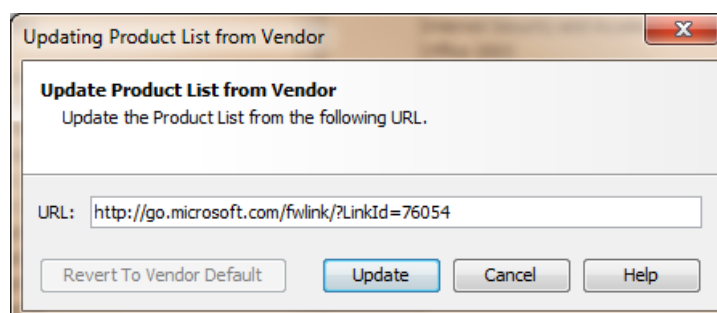
4. To populate the list of available products, click one of the **Update** action buttons:

Update Products from Vendor...: Use this option to update the list of products directly from the vendor site. The vendor site URL is the default URL for the database on the Microsoft web site.

Update Products from File...: Use this option to update the list of products from the `wsusscn2.cab` file on your local machine.

- a. **Updating Product List from Vendor**

The new Updating Product List from Vendor window allows you to update the available products list directly from the vendor's web site.

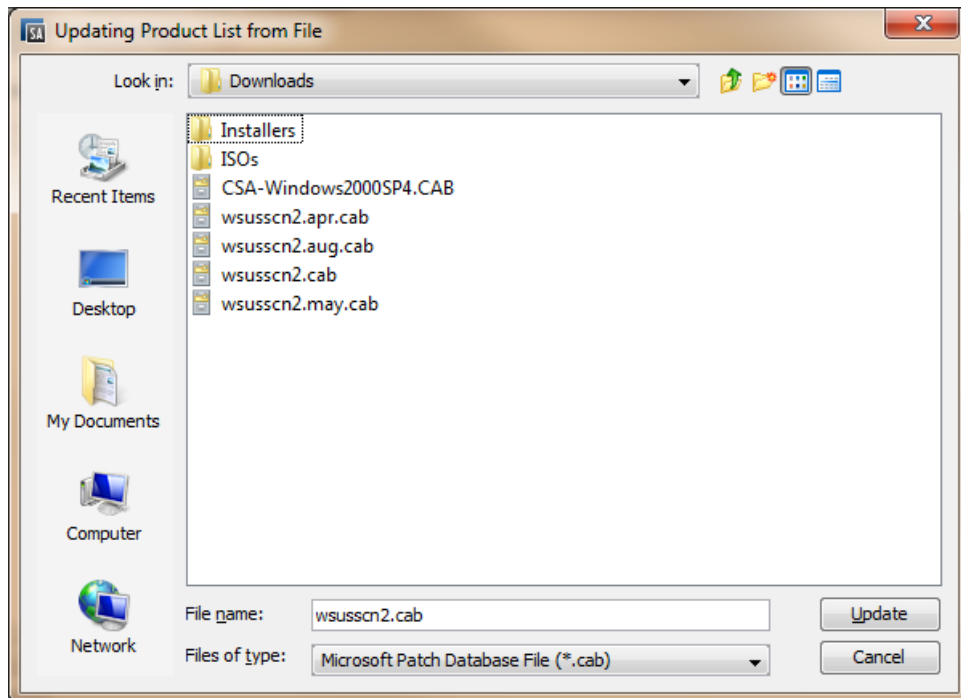


- **URL:** The location of the patch database with the product list on the vendor's web site. This value is auto-populated based on your system implementation settings, but it can be modified.
- **Revert to Vendor Default:** If you modify the URL, you can select this button to revert to the default URL for the vendor's patch database defined in your system implementation settings.

- **Update:** Updates the Microsoft Products List in SA based on the vendor's patch database at the specified URL.

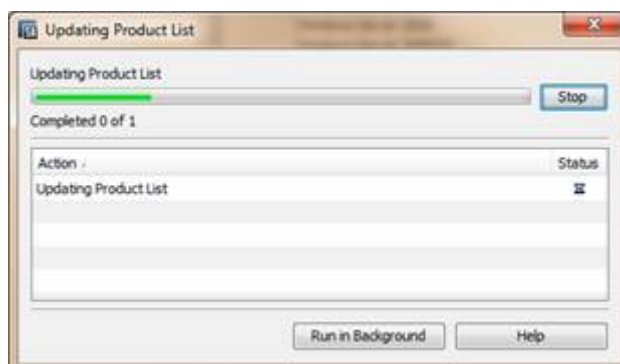
b. **Updating Product List from File**

The new Updating Product List from File window allows you to update the available products list from a file on your local machine. This method is useful for *air-gapped* environments, where the managed servers do not have internet access.

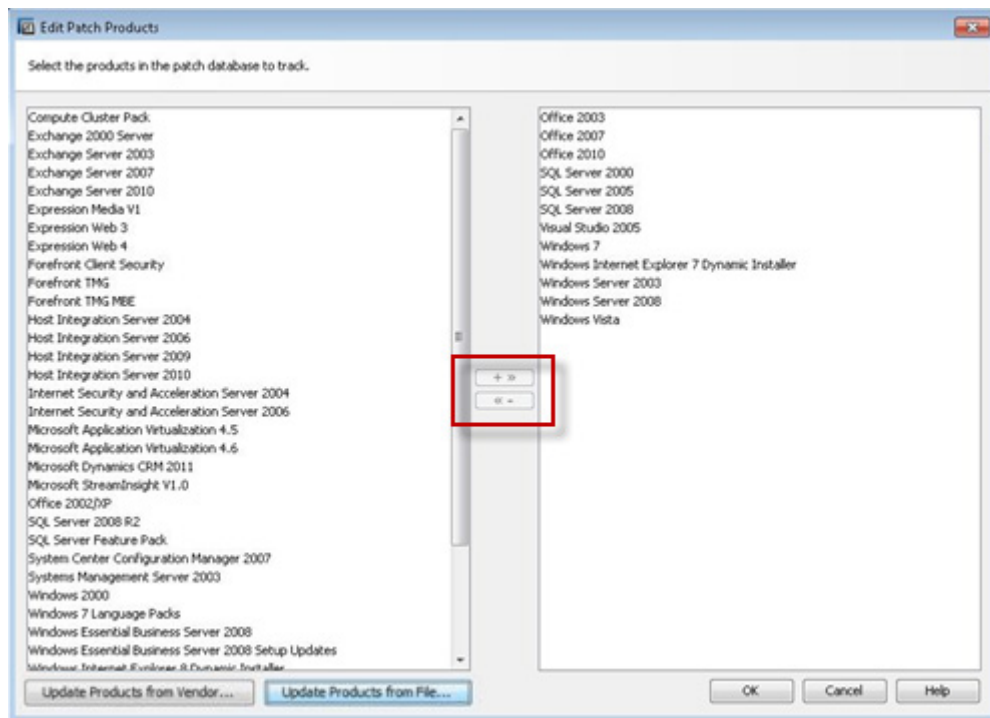


- **Filename:** Navigate to the location of the Microsoft Offline Catalog (`wsusscn2.cab`) file on your local machine.
- **File of Type:** Accept the default, Microsoft Patch Database File (`*.cab`).
- **Update:** Updates the Microsoft Products List in SA based on the selected file.

As the update is taking place, you can click **Run in Background** to minimize the Update window.



5. After the list is updated, modify the selected products list as needed for your environment:



- a. **To add a product:** select it from the list of available products in the left-side pane, and click + >> to move it to the selected products list on the right.
 - b. **To remove a product:** select it from the list of selected products in the right-side pane and click <<- to move it to the available products list on the left.
6. Click **OK** to save your selection.

The next time you run import Windows patches, patches for the selected products will be included in the download.

Step 2 – Import Windows Patches for Additional Products

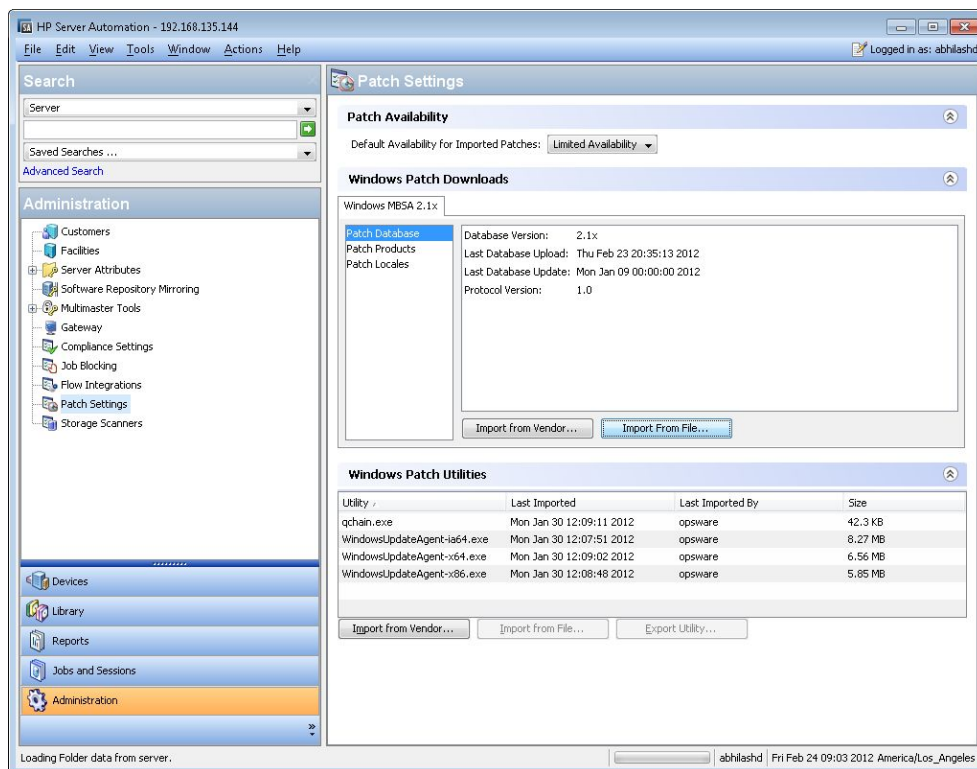
After you have specified the Windows products to include, you can run the patch import.

To import windows patches:

1. Navigate to the Administration > Patch Settings.
2. Select **Patch Database** from the list of Windows Patch Download settings.
3. Import the patch database by clicking one of the action buttons:

Import from File...: Use this option to import the Windows patch metadata for the selected products from the `wsusscn2.cab` file on your local machine.

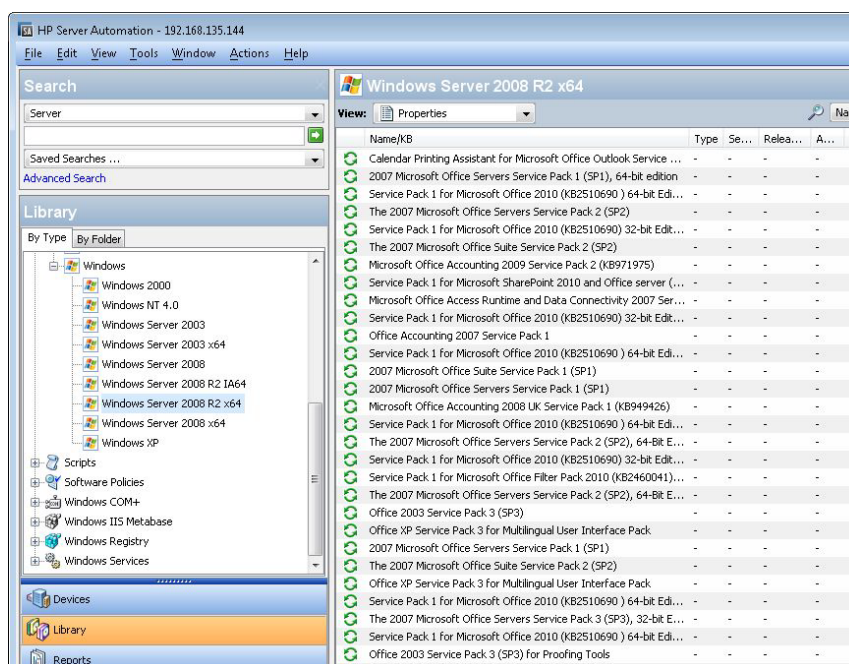
Import from Vendor...: Use this option to import the Windows patch metadata for the selected products directly from the vendor site. The vendor site URL is the default URL for the database on the Microsoft web site.



Tip: To stay current, re-import the patch database monthly, after Microsoft's patch Tuesday.

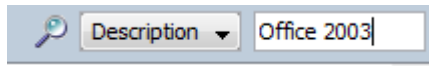
Warning: The more products that are selected, the longer the patch database import operation will take. If all products are selected, importing the Windows patch database -- and subsequently importing the corresponding binaries -- will take long time and will require a large disk space.

4. When the import is complete, go to the SA Windows Patch Library to verify that the patches for the selected products were uploaded:
 - a. Navigate to **Library > By Type > Patches > Windows.**



- b. Select one of the Windows operating systems to see the patches for products on that OS.

- c. 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.



The list will filter the patches to only display those that match the search criteria.

Step 3 – Scan and Remediate Servers

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 the *SA 9.10 User Guide: Server Patching* for instructions on attaching a patch policy to the server.

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

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

2. Remediate the recommended patches as you normally would. (See the *SA 9.10 User Guide: Server Patching* for instructions on remediating a server per a patch policy.)

Enabling/Disabling 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 9.14, 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 Web Client as an administrator with Opsware System Administrators privileges.
Note: SA configuration parameters are accessible only via the SA Web 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**.
3. 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

Warning: 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.

Importing Patch Contents from the Managed Servers View

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

To import patch contents from the 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 patches.
5. Right-click and select **Import Contents** and select **From Vendor...** or **From File....**

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

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

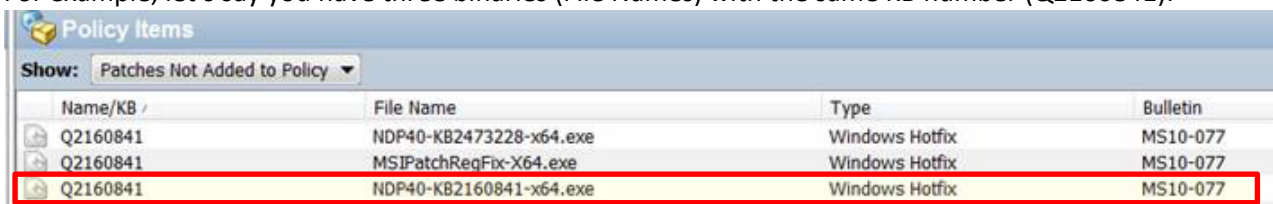
Adding Items to a Windows Patch Policy Using the Object ID

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.

Previous Behavior (before 9.14):

In pre 9.14 versions of SA, when you wanted to add or remove multiple Windows hotfix patches with the same KB number to or from a patch policy, you needed to right-click one of the items in the Policy Items screen and choose **Add Item to Patch Policy**. All the items with the same KB number in the window would be added. Setting, copying, or removing patch exceptions worked in a similar way. This method of multiple additions often resulted in duplicate inclusions or unwanted additions of multiple entries.

For example, let's say you have three binaries (File Names) with the same KB number (Q2160841):



| Name/KB | File Name | Type | Bulletin |
|----------|-------------------------|----------------|----------|
| Q2160841 | NDP40-KB2473228-x64.exe | Windows Hotfix | MS10-077 |
| Q2160841 | MSIPatchRegFix-X64.exe | Windows Hotfix | MS10-077 |
| Q2160841 | NDP40-KB2160841-x64.exe | Windows Hotfix | MS10-077 |

If you right-click on any one of the three binaries and click **Add Item to Patch Policy**, all the patches named Q2160841 will be added to the patch policy, even if they are different items with different Object IDs. These added items are shown in the 'Patches Added to Policy' view:

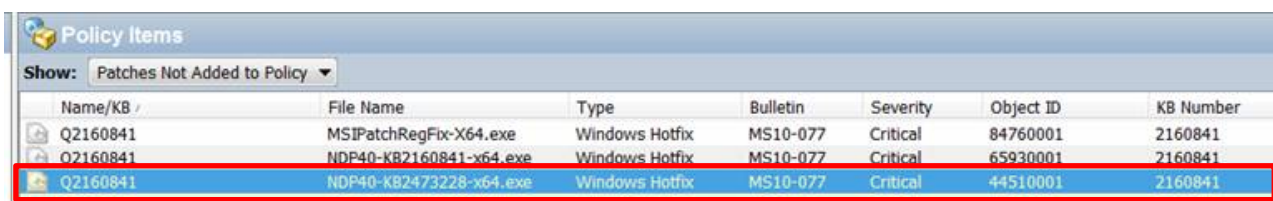


| Name/KB | File Name | Type | Bulletin | Severity | Object ID | KB Number |
|----------|-------------------------|----------------|----------|----------|-----------|-----------|
| Q2160841 | NDP40-KB2473228-x64.exe | Windows Hotfix | MS10-077 | Critical | 34480001 | 2160841 |
| Q2160841 | MSIPatchRegFix-X64.exe | Windows Hotfix | MS10-077 | Critical | 65300001 | 2160841 |
| Q2160841 | NDP40-KB2160841-x64.exe | Windows Hotfix | MS10-077 | Critical | 51020001 | 2160841 |

New Behavior (9.14):

Starting in SA 9.14, SA no longer identifies Windows hotfix patches or patch exceptions by their KB number. Instead, the Object ID is used. Therefore, you can no longer select a single item using one right-click and expect all items with the same KB number to be highlighted too; you must now right-click each individual item or multi-select the items that you want to add/remove/set/copy to the policy.

For example, using a similar data set as before, where you have three binaries with the same KB number, Q2160841:



| Name/KB | File Name | Type | Bulletin | Severity | Object ID | KB Number |
|----------|-------------------------|----------------|----------|----------|-----------|-----------|
| Q2160841 | MSIPatchRegFix-X64.exe | Windows Hotfix | MS10-077 | Critical | 84760001 | 2160841 |
| Q2160841 | NDP40-KB2160841-x64.exe | Windows Hotfix | MS10-077 | Critical | 65930001 | 2160841 |
| Q2160841 | NDP40-KB2473228-x64.exe | Windows Hotfix | MS10-077 | Critical | 44510001 | 2160841 |

Now, if you right-click on any one item and click **Add Item to Patch Policy**, only the selected item will be added. The other two items will not be added.

The 'Patches Added to Policy' view will show a singular Q2160841 item added to the policy:



| Name/KB | File Name | Type | Bulletin | Severity | Object ID | KB Number |
|----------|-------------------------|----------------|----------|----------|-----------|-----------|
| Q2160841 | NDP40-KB2473228-x64.exe | Windows Hotfix | MS10-077 | Critical | 44510001 | 2160841 |

The 'Patches Not Added to Policy' view will display the two Q2160841 items that were not added:



| Name/KB | File Name | Type | Bulletin | Severity | Object ID | KB Number |
|----------|-------------------------|----------------|----------|----------|-----------|-----------|
| Q2160841 | MSIPatchRegFix-X64.exe | Windows Hotfix | MS10-077 | Critical | 84760001 | 2160841 |
| Q2160841 | NDP40-KB2160841-x64.exe | Windows Hotfix | MS10-077 | Critical | 65930001 | 2160841 |

Note: Object IDs are generated per SA Core server. This means that binaries with the same KB will have different Object IDs on different cores. The "New Behavior" example is taken from a different SA Core than the previous example, so the KB number is the same, but the Object IDs are different.

SA 9.14 Upgrades Only

Patch De-duplication Steps for Windows Patching

Duplicate patches can be inadvertently created in the SA database if you import the Microsoft Patch Supplement (MPS) and then run the SA Patch Import process using the Microsoft Offline Patch Catalog (`wsusscn2.cab`). These duplicates can cause conflicts during remediation and compliance checks.

How do I know if I have duplicates?

Starting in 9.14, the patch database has a new field, *Last Import Summary*, which reports if any duplicates were found in your database. In the SA Client, navigate to **Administration > Patch Settings > Patch Database** to view this field. If it displays a warning message after performing a patch import, then there are duplicates in your database. If duplicates are found, these de-duplication steps are strongly recommended.

Resolving Duplicates

To resolve this, a one-time de-duplication procedure is available that enables you to remove the duplicates and eliminate the source of these conflicts to prevent future duplication.

Step-by-step instructions are provided in the whitepaper, *Resolving Conflicts between SA Patching and the MS Patch Supplement*, which is available on the [HP Software Support Online site](#) under the 9.14 Server Automation release.

Note: These steps should only be performed after upgrading to SA 9.14 from a previous release. If you are installing SA for the first time in 9.14, these instructions do not apply.

IMPORTANT: The de-duplication procedure varies based on your version of SA. For this reason, there will be multiple versions of this whitepaper, each providing release-specific instructions.

To find the whitepaper:

1. Go to HP Software Support Online: <http://www.hp.com/go/hpsoftwaresupport>
2. Click the **Self-solve** tab.
3. Log in using your HP Passport credentials.
4. Complete the search criteria:
 - a. All of these words: duplicate patches
 - b. Product: Server Automation
 - c. Version: 9.14
 - d. Document types: Manuals and White Papers
 - e. Sort by: Relevance
5. Click **Search**.
6. Scroll down to see the results.
7. Find the file named: SA9.14_Windows_PatchingPatch_Supplement_wp.pdf

You can also do the same search directly from the SSO Product Manuals site:

<http://support.openview.hp.com/selfsolve/manuals>

Additional Functionality Added in the 9.1x Branch

SA Server Patching—Oracle Enterprise Linux (OEL)

Oracle Enterprise Linux (OEL) Patching Support

Introduced in 9.13, the HPSA Patch Importer for Oracle Enterprise Linux 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 HPSA. It can be run from the command line manually, or can be part of a `cron` job that performs the import on a recurring basis.

Documentation: OEL patching support has been available since 7.87, 9.04, and 9.13, on the respective SA release branches. For information about using the HPSA Patch Importer, download the whitepaper, *SA Patch Importer for Oracle Enterprise Linux*, from the HP Software Support Online at: <http://support.openview.hp.com/selfsolve/manuals>.

SA Server Patching—Solaris

Solaris 11 Patching Support

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.

Introduced in SA 9.13, 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.

Documentation: The *SA 9.14 Solaris 11 Patching Whitepaper* provides detailed instructions on setting up and maintaining the IPS Package database. This document also describes the Solaris 11 patch policy and remediation differences. This whitepaper is available via HP's Software Support Online at: <http://support.openview.hp.com/selfsolve/manuals>.

Additional Information

In this section:

- [Legal Notices](#)
- [Documentation Updates](#)
- [Support](#)

Legal Notices

Warranty

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

The information contained herein is subject to change without notice.

Restricted Rights Legend

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

Copyright Notices

© Copyright 2000-2012 Hewlett-Packard Development Company, L.P.

Trademark Notices

Adobe® is a trademark of Adobe Systems Incorporated.

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

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

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

UNIX® is a registered trademark of The Open Group.

Documentation Updates

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

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

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

This site requires that you register for an HP Passport and sign in. To register for an HP Passport ID, go to:
<http://h20229.www2.hp.com/passport-registration.html>, or click the **New users – please register** link on the HP Passport login page.

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

Support

Visit the HP Software Support Online web site at: <http://support.openview.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: <http://h20229.www2.hp.com/passport-registration.html>
- To find more information about access levels, go to: http://support.openview.hp.com/access_level.jsp

Support Matrices

For complete support and compatibility information, see the support matrix for the relevant product release. All support matrices and product manuals are available here on the HP Software Support Online web site:

http://support.openview.hp.com/sc/support_matrices.jsp

You can also download the HP Server Automation Support and Compatibility Matrix for this release from the HP Software Support Online Product Manuals web site:

<http://support.openview.hp.com/selfsolve/manuals>