Patch Management

Table of Contents:

Introduction

As new operating system and software updates are released in an ever increasing pace to address system security vulnerabilities and provide enhanced functionalities, the task of applying the updates uniformly and correctly to all managed machines becomes more and more complex and challenging. The application of operating system and software updates is not a simple installation process. Some operating system and software patches must be uniformly deployed to all managed machines to maintain their inter-operability and some must be avoided to prevent conflicts with existing system and software requirements. In addition, the managed machines and the underlying networks span multiple locations, include multiple domains, traverse multiple firewalls, and include remote and home users. Obviously, maintaining a consistent and up-to-date system on all managed machines in such a complex environment is a mundane and time consuming task and an automated Patch Management tool to assist the system administrators to systematically track applied patches and automatically apply new patches based on pre-defined policies is a much needed tool.

Kaseya's Patch Management is a secure and comprehensive patch management solution providing the infrastructure to address the complexities of operating system and software patch deployment and enforce policies that describe how and when updates must be applied on a per machine basis.

An important aspect of automated patch management is the ability to quickly determine the patch status of each managed machine. In Kaseya, you can determine the patch status of each managed machine using the following pages:

- **Patch Management > Scan Machine** provides information on available patches that are not applied on managed machines**.**
- **Patch Management > Patch Status** provides a summary view of installed, missing and denied patches for each managed machine**.**
- **Patch Management > Patch History** provides a detailed view of historical patch management activities for each managed machine using **.**

After performing the initial assessments of managed machines using the above methods, you can install the necessary patches using one of five different methods. They are explained in detail in the following section.

Methods of Updating Patches

The VSA provides **five** methods of applying Microsoft patches to managed machines:

- **Initial Update:** This method provides a *one-time* processing of all approved Microsoft patches applicable to a managed machine based on patch policies. Patch policies describe how and when patches are to be applied. An active patch is defined as a patch that has been reported by a patch scan by at least one machine in the VSA. Any machine can be made a member of one or more patch policies. For example, you can create a patch policy named *servers* and assign all your servers to be members of this patch policy and another patch policy named *workstations* and assign all your workstations to be members of this policy. This way patch approvals can be configured differently for servers and workstations. **Initial Update** ignores the **Patch Management > Reboot Action** policy and reboots the managed machine **without warning the user** as often as necessary until all patches are applied. **Initial Update** should only be performed during non-business hours and is typically performed over a weekend on newly added machines.
- **Automatic Update:** This method is the *preferred* method of updating managed machines on a *recurring* basis. It obeys both the **Patch Policy** and the **Patch Management** > **Reboot Action** policy.

• **Patch Update**: If you're using **Automatic Update**, then **Patch Update** is occasionally used to apply individual patches to multiple machines or for patches that originally failed on certain machines. This overrides the **Patch Policy** but obeys the **Patch Management** > **Reboot Action** policy.

• **Machine Update**: **This method** is used to apply patches to individual managed machines. It overrides the **Patch Policy** but obeys the **Patch Management** > **Reboot Action** policy. **Machine Update** is often used to test a new patch prior to approving it for general release to all machines.

• **Patch Deploy**: This method enables you to develop a user-defined procedure to install a Microsoft patch using **Agent Procedures > Patch Deploy**. Microsoft releases many hot fixes as patches for very specific issues that are not included in the Microsoft Update Catalog or in the Office Detection Tool, the two patch data sources that the **Patch Management** module uses to manage patch updates. **You can use this method** to create a patch installation procedure for these hot fixes, via this wizard, that can be used to schedule the installation on any desired machine.

Patch Processing

When a patch installation is scheduled using one of the above methods, the following occurs:

1. The agent on the managed machine is told to start the update process at the scheduled time.

2. The patch executable is downloaded to the managed machine from the location set in **the Patch Management > File Source** for that machine ID.

3. The patch file is executed on the managed machine using the parameters specified in **Patch Management > Command Line**. You should never have to set these switches yourself, but just in case, this capability is there.

4. After all the patches have been installed, the managed machine is rebooted. *The time of the reboot* for a machine ID depends on the **Patch Management > Reboot Action** assigned to that machine ID. Reboots in response to an Initial Update always occur immediately and without warning the user.

5. The managed machine is rescanned automatically. It takes several minutes after the rescan is complete for this data to show up on the VSA. Wait several minutes before checking the patch state after a reboot.

5.1 Manage Machines

5.1.1 Scan Machine

The **Scan Machine** page schedules scans to search for missing patches on each managed machine. Scanning takes very little resources and can be safely scheduled to run at any time of day. The scanning operation does not impact users at all.

Scanning Frequency
System and network security depends on all your machines having the latest security patches applied. Microsoft typically releases patches on Tuesdays. Security and critical patches are typically released on the second Tuesday of the month (Patch Tuesday), and non-security and non-critical patches are typically released on the third and/or fourth Tuesdays of the month, but these schedules are not guaranteed. To ensure your machines are updated you should scan all managed machines on a daily basis.

Scanning the KServer

To scan the KServer, you must install an agent on the KServer. Once installed, you can scan the KServer just like any other managed machine.

View Definitions
You can filter the display of machine IDs on any agent page using the following options in View Definitions.

- Machines that have no patch scan results (unscanned)
- Last execution status for patch scan (success / failed)

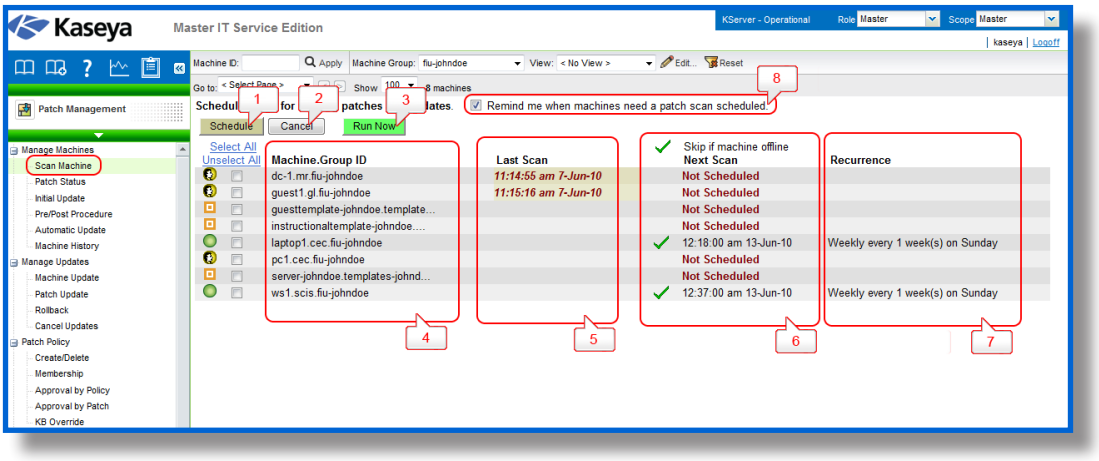


Fig. 5.1: *Scan Machine*

- Patch scan (schedule / not schedule)
- Patch scan (has / has not executed in the last <N> <periods>)

Notes

Note: *View Definitions was discussed in the Agents chapter. Please refer the Agents chapter.*

The generic view of the Scan Machine page is shown in Fig. 5.I below. The list of available options are:

1. **Schedule:** Click *Schedule* to display the Scheduler window, which is used throughout the VSA to schedule a task. Schedule a task once or periodically. Each type of recurrence (Once, Hourly, Daily, Weekly, Monthly, Yearly) displays additional options appropriate for that type of recurrence. Periodic scheduling includes setting start and end dates for the recurrence.

2. **Cancel:** Click *Cancel* to cancel execution of this task on selected managed machines.

3. **Run Now:** Click *Run Now* to run this task on selected machine IDs immediately.

4. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to see using **System > User Security > Scopes.**

5. **Last Scan:** This timestamp shows when the last scan occurred. When this date changes, new scan data is available to view.

6. **Skip if Machine Offline:** If a green checkmark is displayed and the machine is offline, skip and run the next scheduled period and time. If no checkmark displays, perform this task as soon as the machine connects after the scheduled time.This timestamp shows the next scheduled scan. Overdue date/time stamps display as red text with yellow highlight.

7. **Recurrence:** If recurring, displays the interval to wait before running the task again.

8. **Remind me when machines need a patch scan scheduled:** If this option is checked, a warning message displays the number of machine IDs not currently scheduled. The number of machine IDs

reported depends on the Machine ID / Group ID filter and machine groups the user is authorized to see using **System >** Scope.

5.1.2 Patch Status

The **Patch Status** page (Fig. 5.2) provides a summary view of the patch status for each of your managed machines. You can quickly identify machines that are missing applicable patches either because they were never installed or their installations failed.

View Definitions
You can filter the display of machine IDs on any agent page using the following options in View Definitions.

- Machines with Patch Test Result
- Machines missing greater than or equal to N patches
- Use Patch Policy

Fig. 5.2 below shows the generic view of the Patch Status page. The options available are:

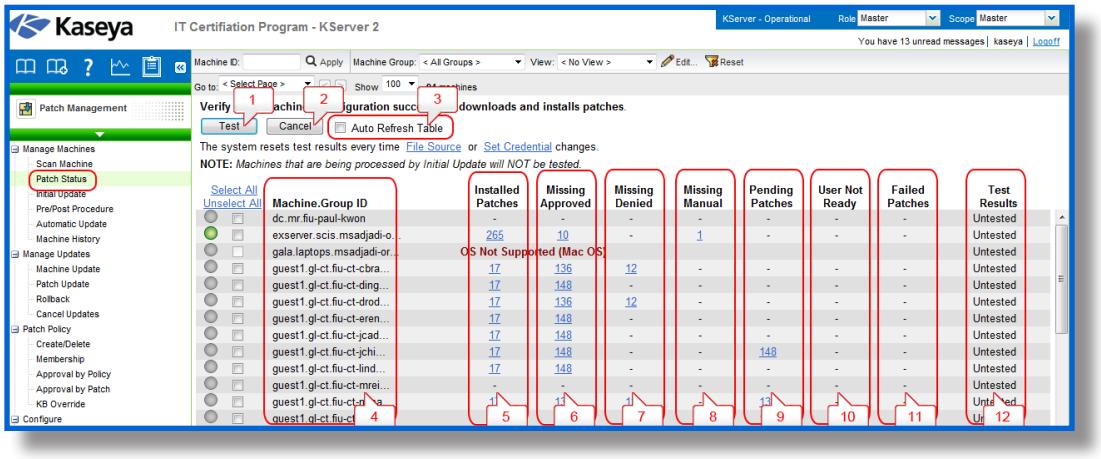


Fig. 5.2: *Patch Status*

1. **Test:** The test function exercises the entire patch deployment process without actually installing anything on the target machine or causing a reboot. If a machine ID's operating system does not support patching, the operating system is displayed. Click *Test* to verify patches can update selected machine IDs. Does not actually install any patches.

2. **Cancel:** Click *Cancel* to stop the test.

3. **Auto Refresh Table:** If checked, the paging area is automatically updated every five seconds. This checkbox is automatically selected and activated whenever *Test* is clicked.

4. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

5. **Install Patches:** Displays the number of patches installed. Clicking on the link displays the list of all patches that are installed.

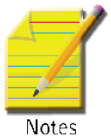
6. **Missing Approved:** Displays the number of approved patches that are not installed.

7. **Missing Denied:** Displays the number of unapproved patches missing.

8. **Missing Manual:** The number of approved patches missing that must be installed manually. These patches cannot be processed by **Patch Management>Automatic Update**, **Patch Management>Initial Update**, **Patch Management>Machine Update**, or **Patch Management>Patch Update**.
9. **Pending Patches:** Displays the number of patches scheduled to be installed.
10. **User Not Ready:** Displays the number of patches not installed because the patch requires:
    - The user to be logged in, or
    - The user to take action and the user declined or did not respond.
11. **Failed Patches:** Displays the number of patches that attempted to install but failed.
12. **Test Results:** The status returned after clicking the Test button:
    - Untested
    - Pending
    - Passed
    - Failed

5.1.3 Initial Update

Initial Update is a *one-time* processing of all approved Microsoft patches applicable to a managed machine based on Patch Policy. **Initial Update** ignores the **Patch Management > Reboot Action** policy and reboots the managed machine **without warning the user** as often as necessary until the machine has been brought up to the latest patch level. **Initial Update** should only be performed during non-business hours and is typically performed over a weekend on newly added machines.



Note: *The agent for the KServer is not displayed on this page.* Initial Update *cannot be used on the KServer.*

Patch Update Order
Service packs and patches are installed in the following order:

- Windows Installer
- OS related service packs
- OS update rollups
- OS critical updates
- OS non-critical updates
- OS security updates
- Office service packs
- Office update rollups
- All remaining Office updates

Note: *Reboots are forced after each service pack and at the end of each patch group* without warning. *This is necessary to permit the re-scan and installation of the subsequent groups of patches.*

Pre/Post Procedures
Agent procedures can be configured to be executed just before an Initial Update or Automatic Update begins and/or after it completes. For example, you can run agent procedures to automate the preparation and setup of newly added machines before or after Initial Update. Use **Patch Management > Pre/Post Procedures** (see Section 5.1.4) to select and assign these agent procedures on a per-machine basis.

The figure below (Fig. 5.3) shows the generic view of the Initial Update page with all the functions listed below:

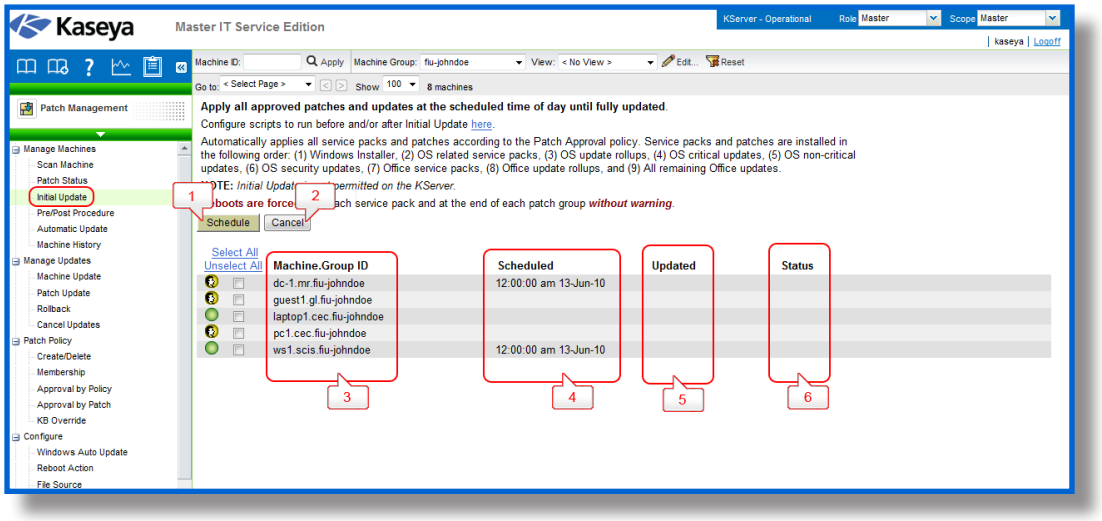


Fig. 5.3: *Initial update page*

1. **Schedule:** Click *Schedule* to display the Scheduler window, which is used throughout the VSA to schedule a task. Options include:

   • **Distribution Window** - Reschedules the task to a randomly selected time no later than the number of periods specified, to spread network traffic and server loading.

2. **Cancel:** Click *Cancel* to cancel execution of the initial update on selected managed machines.

3. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

4. **Scheduled:** This timestamp shows the scheduled Initial Update.

5. **Updated:** If checked, an Initial Update has been performed successfully on the machine ID. The timestamp shows when the Status being reported was completed.

6. **Status:** During the processing, the *Status* column is updated to display a message describing the current status of the initial update. The following is the list of available status messages:

   • Started

   • Processing Windows Installer

   • Processing operating system service packs

   • Processing operating system update rollups

   • Processing operating system critical updates

   • Processing operating system non-critical updates

   • Processing operating system security updates

   • Processing Office service packs

- Processing Office update rollups

Processing Office updates

- Completed - fully patched
- Completed - remaining patches require manual processing

For the last status message above, select the appropriate machine ID in **Patch Management > Machine Update** to determine why all patches were not applied. Some patches might require manual install or for the user to be logged in. In the case of patch failures, manually schedule failed patches to be reapplied. Due to occasional conflicts between patches resulting from not rebooting after each individual patch, simply reapplying the patches typically resolves the failures.

5.1.4 Pre/Post procedure

Pre/Post Procedure page (Fig. 5.4) can be used to run procedures either before and/or after **Patch Management>Initial Update** or **Patch Management>Automatic Update.**
For example, you can run procedures to automate the preparation and setup of newly added machines before or after **Initial Update.**

Note: *Post procedures will run even if there are patch installation failures.*

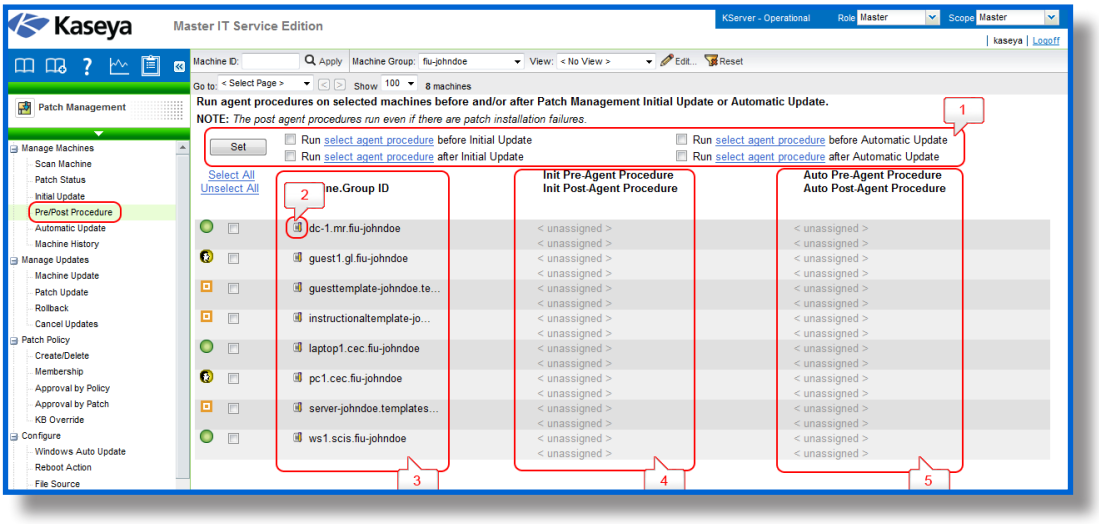


Fig. 5.4: *Pre/Post Procedure*

1. **To Run a Pre/Post Procedure**

- Select machine IDs or machine ID templates displayed on the page.
- Select one of the options listed as shown in Fig. 5.4 and select an agent procedure for each option selected.
  - Run select agent procedure before Initial Update
  - Run select agent procedure after Initial Update
  - Run select agent procedure before Automatic Update
  - Run select agent procedure after Automatic Update

- Click *Set*.

2. Edit icon: To edit the selection for a machine or to copy a machine's selection to other machines, click the edit icon next to a machine ID to populate its selected options in the header part of this page (refer to label one in Fig. 5.4). Now you can edit the selected options and / or set them to other machines.

3. Machine.Group ID: The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

4. Init Pre-Agent Procedure / Init Post-Agent Procedure: This column lists the procedures set to run before and/or after an **Initial Update**.

5. Auto Pre-Agent Procedure / Auto Post-Agent Procedure: This column lists the procedures set to run before and/or after an **Automatic Update**.

5.1.5 Automatic Update

The **Automatic Update** page (Fig. 5.5) is the *preferred* method of updating managed machines with Microsoft patches on a *recurring* basis. **Automatic Update** obeys both the Patch Policy and the **Patch Management > Reboot Action** policy. **Patch Management > Initial Update** needs to be used if you are installing patches for the first time on a managed machine.

- Patches that require manual intervention are not included in **Automatic Updates**. These are shown in the **Missing Manual** column of the Patch Status page and on the individual **Patch Management > Machine Update** pages.
- Patch installation only occurs when a new missing patch is found by **Patch Management > Scan Machine.**
- **Automatic Update** is disabled for a machine while **Initial Update** is being processed. **Automatic Update** is automatically enabled when **Initial Update** completes.

Fig. 5.5 below shows the generic view of the Automatic page. The functions supported are:

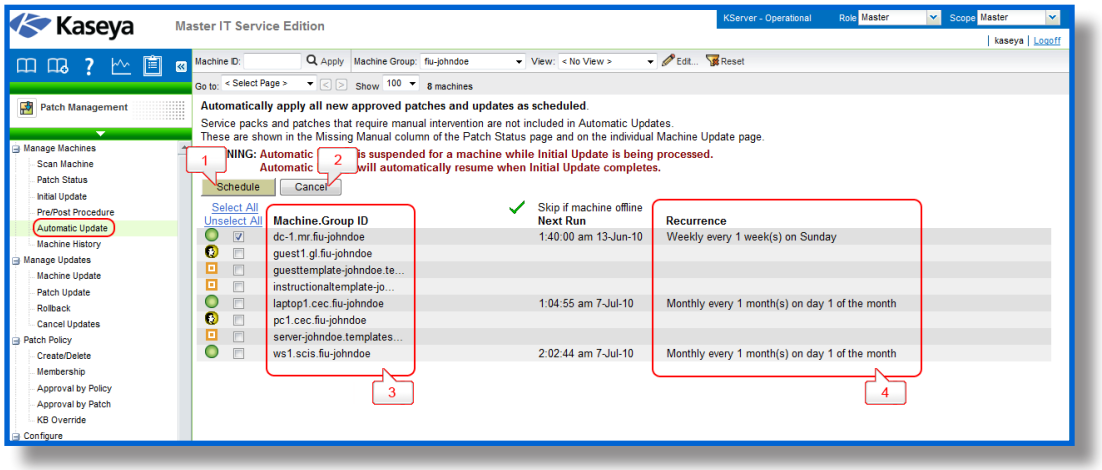


Fig. 5.5: *Automatic Update*

1. **Schedule:** Click *Schedule* to display the Scheduler window, which is used throughout the VSA to schedule a task.

2. **Cancel:** Click *Cancel* to cancel execution of this task on selected managed machines.

3. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

4. **Recurrence:** Depending on the option selected in Schedule, it displays the interval to wait before running the task again. All the options selected are recurring unless it is specified as *Once* in the scheduler window.

5.1.6 Machine History

The **Machine History** page (Fig. 5.6) displays the results from the most recent patch scan of managed machines. All installed and missing patches applicable to a managed machine are listed, regardless of whether the patch is approved or not.

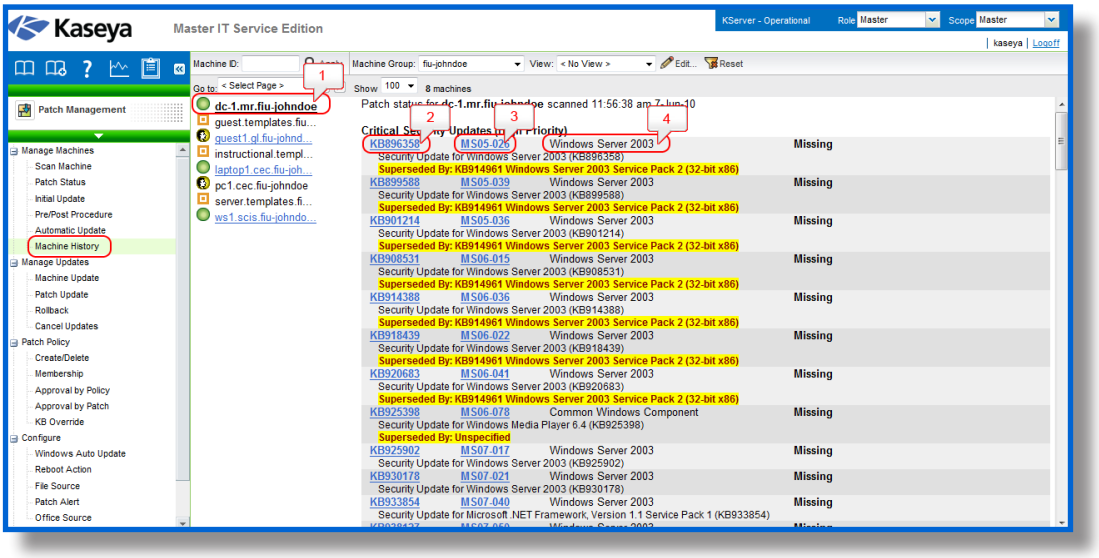


Fig. 5.6: *Machine History*

1. Click a *machine ID link* to display its patch history as shown in Fig. 5.6.

2. Click the *KB Article link* to display a Details page about the patch. The Details page contains a link to display the knowledge base article.

3. Patches classified as security updates have a security bulletin ID (MSyy-xxx). Clicking this link displays the security bulletin.

4. The Product column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (*i.e.,* Windows XP, Windows Server 2003, Vista, etc.), the product category is Common Windows Component else the specific operating system name is displayed. Examples include Internet Explorer, Windows Media Player and so on.

Superseded Patches

A superseded patch is a patch that doesn't have to be installed because a later patch is available. A typical example is a service pack, which bundles many other patches that have been released before the service pack. If you install the service pack, you don't have to install all the earlier patches. **Patch Management** only reports patches superseded by a service pack. Superseded patches have a string appended to the title of the patch that indicates that it is superseded by Service Pack X. This string is displayed as dark red text with yellow background to make it stand out.

The installation process installs superseded updates *only if* the service pack that supersedes these updates *is not* selected for installation. If the superseding service pack is selected for installation, the superseded updates *are not* downloaded or installed. A procedure log entry is added to indicate the update was skipped because it was superseded.

In addition:

- Patch titles in the Patch Management report include `Superseded By: Service Pack X`, when applicable.
- The patch filter on the patch approval pages now include the ability to filter on `superseded/not superseded`.
- Occasionally, the `Superseded By` warning displays as `Superseded By: Unspecified`. This is typically caused by a cross-operating system patch that is superseded by one or more service packs. This is likely to be seen on updates dealing with Media Player.

Patch
Patches are grouped by update classification first and knowledge base article number second.

Status
The following status messages can appear next to a patch:

- **Installed (date unknown)** – Displays the date of the patch installed as unknown
- **Installed (<datetime>)** – Displays the date and the time the patch was installed.
- **Missing** – This is displayed if the patch is missing as Kaseya compares the patch list with the Windows Update service list.
- **Denied by Patch Approval** – This is displayed if the patch was denied
- **Denied (Pending Patch Approval)**
- **Manual install to VSA database server only** - Applies to SQL Server patches on the database server where the KServer database is hosted
- **Manual install to KServer only** - Applies to Office or any “install-as-user” patches on the KServer
- **Patch Location Pending** - Applies to patches with an invalid patch location.
- **Missing Patch Location –** The location of the installed patch file is missing.
- **Ignore**

5.2 Manage Updates

5.2.1 Machine Update

The **Machine Update** page is used to manually install Microsoft patches on individual machines. **Machine Update** overrides the **Patch Approval Policy** but obeys the **Patch Management > Reboot Action** policy. **Machine Update** is often used to test a new patch prior to approving it for general release to all machines.

The generic view of the Machine Update page is show in Fig. 5.7 below. The options available on this page are:

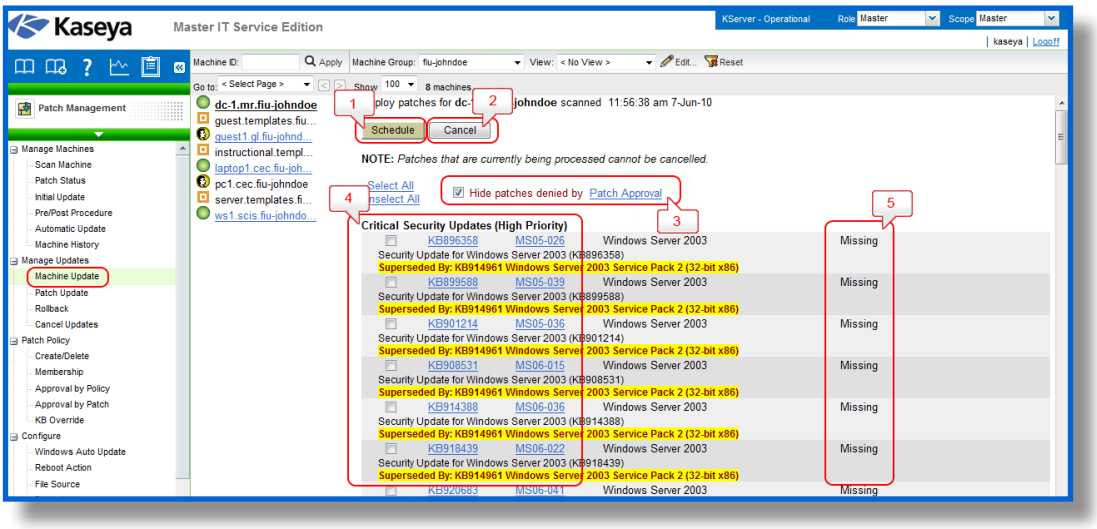


Fig. 5.7: *Machine Update*

1. **Schedule:** Click the *Schedule* button to display the **Scheduler** window, which is used throughout the VSA to schedule a task. All tasks are scheduled only *once*.

2. **Cancel:** Click *Cancel* to cancel execution of this task on selected managed machines.

Note: *Patches that are currently being processed (status of Pending - Processing Now) cannot be cancelled.*

3. **Hide patches denied by Patch Approval:** If checked, hides patches that are denied patch approval. Patches with the status Pending Approval are considered denied by **Machine Update**.

4. **Patch:** Patches are grouped by update classification first and knowledge base article number second.

5. **Status:** A status message maybe displayed next to a patch which shows the current status of the patch. For more information regarding Patch failures and error messages, refer to Patch Failure section at the end of this chapter.

5.2.2 Patch Update

The **Patch Update** page updates missing Microsoft patches on all machines displayed in the paging area. **Patch Update** overrides the **Patch Approval Policy** but obeys the **Patch Management > Reboot Action** policy. If you're using **Patch Management** > **Automatic Update**, then **Patch Update** is occasionally used to manually apply individual patches to multiple machines or to re-apply patches that originally failed on certain machines.

Duplicate Entries
Microsoft may use a common knowledge base article for one or more patches, causing patches to appear to be listed more than once. **Patch Update** displays patches sorted by **Update Classification** or **Product** first and knowledge base article number second. Check the **Product** name or click the **KB Article** link to distinguish patches associated with a common knowledge base article.

Patch update page provides a lot of options as shown in Fig. 5.8. The options available are:

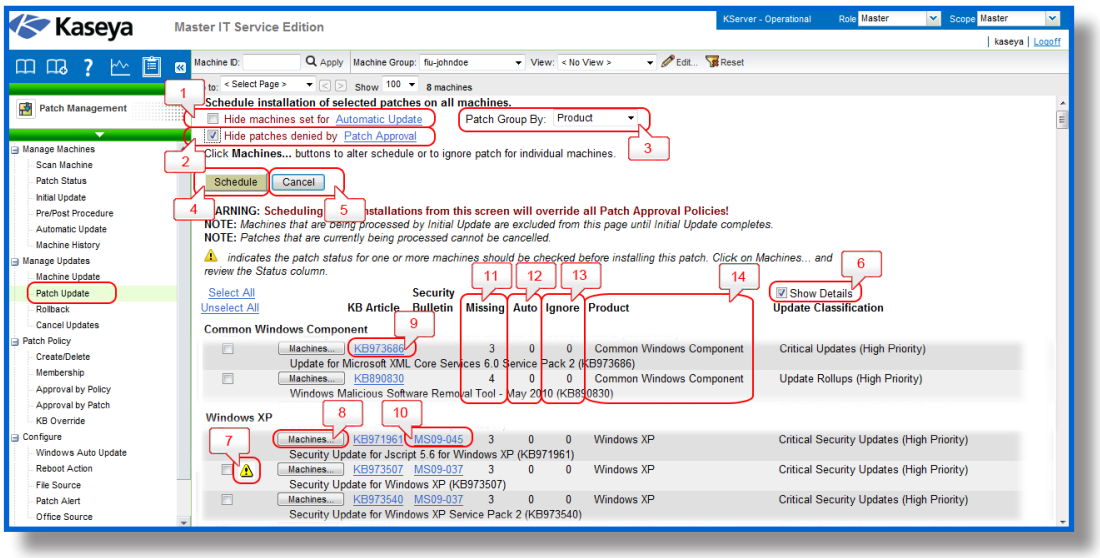


Fig. 5.8: *Patch Update*

1. t**Hide machines set for Automatic Update:** If checked, hides patches missing from machine IDs set to **Patch Management > Automatic Update.**

2. **Hide patches denied by Approval Policy:** If checked, hides patches denied by Patch Approval Policy.

3. **Patch Group By:** Displays patch groups by either **Classification** or **Product**.

4. **Schedule:** Click this button to display the **Scheduler** window, which is used throughout the VSA to schedule a task. Schedule this task *once*.

5. **Cancel:** Click *Cancel* to cancel execution of this task on selected managed machines.

Note: Patches that are currently being processed (status of Pending - Processing Now) cannot be cancelled.

Notes

6. **Show Details:** Click the *Show Details* checkbox to display the expanded title and installation warnings, if any, of each patch.

7. **Status Warning Icon:** A warning icon indicates the patch status for one or more machines should be checked before installing this patch. Click the *Machines* button and review the **Status** column for each machine missing this patch.

8. **Machines:** Click *Machines* to list all machines missing this patch. On the details page, status messages can appear next to a patch which indicates the current status of the patch. For more information regarding the status message of the patch, refer the Patch Failure section at the end of the chapter.

9. **KB Article:** The knowledge base article describing the patch. Click the *KB Article link* to display all the details page about the patch.

10. **Security Bulletin:** Patches classified as security updates have a security bulletin ID (MSyy-xxx). Clicking this link displays the security bulletin.

11. **Missing:** The missing column shows the number of machines missing this patch.

12. **Auto:** Displays only if the *Hide machines set for Automatic Update* box is *not* checked. The number of machines scheduled to install this patch by **Automatic Update**.

13. **Ignore:** This option shows the number of machine set to ignore a patch using the **Machines** button. The **Ignore** setting applies to the selected patch on the selected machines. If **Ignore** is set, the patch is considered Denied. Patches marked as **Ignore** on the selected machines cannot be installed by any of

the installation methods. To be installed, the **Ignore** setting must be cleared.

14. **Product:** The **Product** column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (*i.e.*, Windows XP, Windows Server 2003, Vista, etc.), the product category is Common Windows Component. Examples include Internet Explorer, Windows Media Player, MDAC, MSXML, and so on.

5.2.3 Rollback

The **Rollback** page removes patches after they have been installed on a system. Not all patches may be uninstalled when Rollback is performed. This is because the system only lists patches supporting the rollback feature.

Warning: *Removing Windows software in the wrong order may cause the operating system to stop functioning.*

The generic view of the Rollback page is shown in Fig. 5.9 below. The options available in this module are:

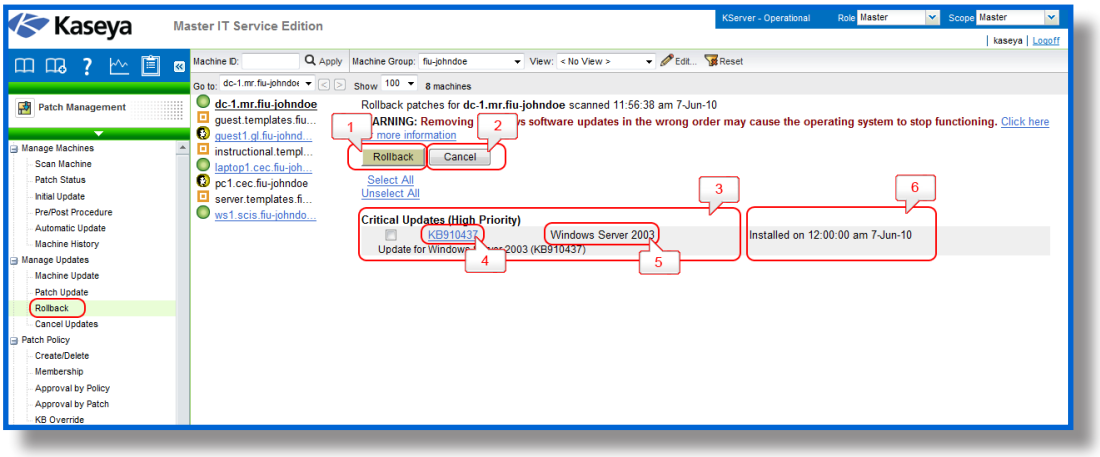


Fig. 5.9: *Rollback page*

1. **Rollback:** Click this button to display the **Scheduler** window, which is used throughout the VSA to schedule a task. Schedule this task *once*.

2. **Cancel:** Click *Cancel* to cancel a scheduled rollback.

3. **Patch:** Patches are grouped by update classification first and knowledge base article number second.

4. **KB Article:** The knowledge base article describing the patch. Click the *KB Article link* to display the entire details page about the patch.

5. **Product:** The **Product** column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (*i.e.,* Windows XP, Windows Server 2003, Vista, etc.), the product category is Common Windows Component. Examples include Internet Explorer, Windows Media Player, MDAC, MSXML, and so on.

6. **Install Date:** This column displays the date the patch was installed, if available.

To Remove a Patch from a Managed Machine

1. Click the machine ID that you want to remove a patch from.

2. Check the box to the left of the patch you want to uninstall.

3. Click the *Rollback* button.

5.2.4 Cancel Updates

The **Cancel Updates** page clears *all manually scheduled* patch installations on selected machine IDs.

The **Cancel Updates** page can also *terminate* currently running patch installation processes. The time a patch installation is being processed, a *Terminate* button is displayed next to the machine name. Clicking this Terminate button deletes existing patch installation procedures for the selected machine, and the installation process ends after deletion of the patch installation procedure.

Note: *Installed Patches can be removed from managed machines using Rollback.*

Notes

The options supported by the Cancel Updates page are shown in Fig. 5.10 below:

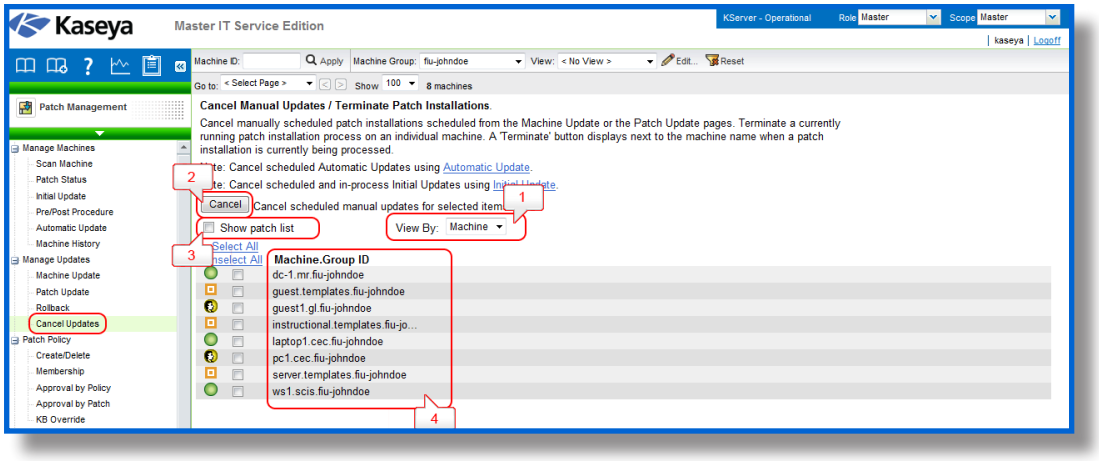


Fig. 5.10: *Cancel Updates*

1. View By: This option allows you to view patches sorted by machine or by patch first. Depending on the option selected here option (3. Show patch list) changes.

2. Cancel: Click *Cancel* to clear all scheduled patch installations scheduled by either **Machine Update** or by **Patch Update** on selected machine IDs.

3. Show patch list: *Show patch list* is displayed only if View by Machine is selected fropm option (1. View by). If both *View by Machine* and *Show patch list* are checked, all *scheduled patch IDs* for each machine ID are listed. If *Show patch list* is blank, the *total number of scheduled patches* is listed for each machine ID.

Show machine list: If *View By Patch* is selected and *Show machine list* is checked, all *scheduled patch IDs* for each machine ID are listed. If *Show machine list* is blank, the *total number of scheduled patches* is listed for each machine ID.

Note: *This option is displayed only if View by Patch is selected.*

Notes

Machine.Group ID: The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

KB Article: Displays the knowledge base article describing the patch. This column is displayed only if *View by patch* is selected. Click the *KB Article link* to display a Details page about the patch. The

Details page contains a link to display the knowledge base article.

5.3 Patch Policy

5.3.1 Create/Delete

The **Create/Delete** page creates or deletes patch policies. Patch policies contain all active patches for the purpose of approving or denying patches. An active patch is defined as a patch that has been reported by a patch scan by at least one machine in the VSA. Any machine can be made a member of one or more patch policies.

For example, you can create a patch policy named servers and assign all your servers to be members of this patch policy and another patch policy named workstations and assign all your workstations to be members of this policy. This way, you can configure patch approvals differently for servers and workstations.

- The patches of machines that are not a member of any patch policy are treated as if they were *automatically approved*.
- When a new patch policy is created the default approval status is *pending approval* for all patch categories.
- The default approval status for each category of patches and for each product can be individually set.
- If a machine is a member of multiple patch policies and those policies have conflicting approval statuses, the most restrictive approval status is used.
- **Patch Management > Initial Update** and **Patch Management > Automatic Update** require patches be approved before these patches are installed.
- **Approval by Policy** approves or denies patch by *policy*.
- **Approval by Patch** approves or denies patches by *patch* and sets the approval status for that patch in all patch policies.
- KB Override overrides the default approval status by *KB Article* for all patch policies and sets the approval status for patches associated with the KB Article in all patch policies.
- **Patch Management > Patch Update** and **Patch Management > Machine Update** can install denied patches.
- Non-Master role users can only see patch policies they have created or patch policies that have machine IDs the user is authorized to see based on their scope.

Fig. 5.11 shows the general view of the Create/Delete page. The options supported are:

1. **Create:** Enter a new machine patch policy name in the edit field and click *Create* to define a new patch policy.
2. **Delete:** Click *Delete* to delete selected patch policies.
3. **Policy Name:** Lists all machine patch policies defined for the entire system.
4. **Member Count:** Lists the number of machines that are members of each patch policy.
5. **Show Members:** Click *Show Members* to list the members of a patch policy.

6. **Edit Icon:** Click the edit icon to the left of a patch policy to rename it.

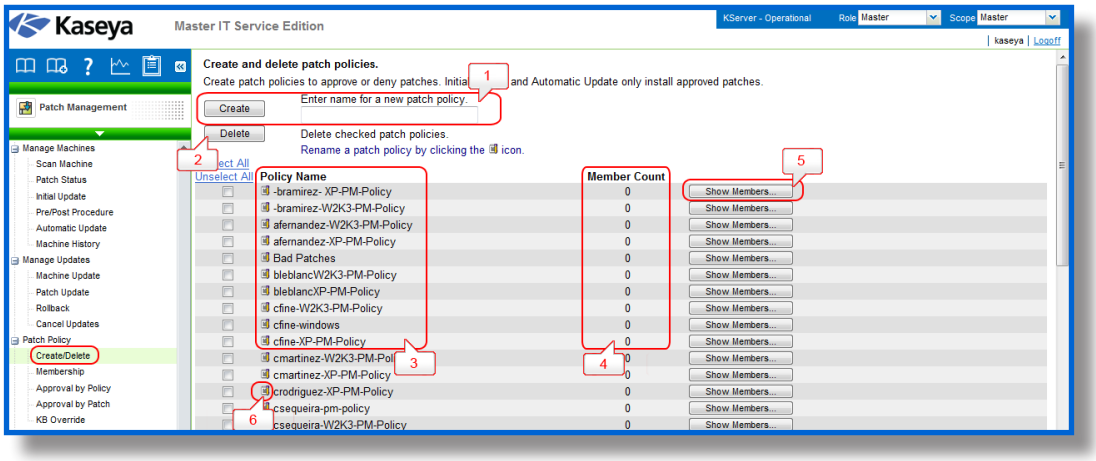


Fig. 5.11: *Create/Delete Page*

5.3.2 Membership

The **Membership** page assigns machine IDs to one or more patch policies.

Fig. 5.12 below shows the generic view of the Membership page. The options supported by this page are listed below.

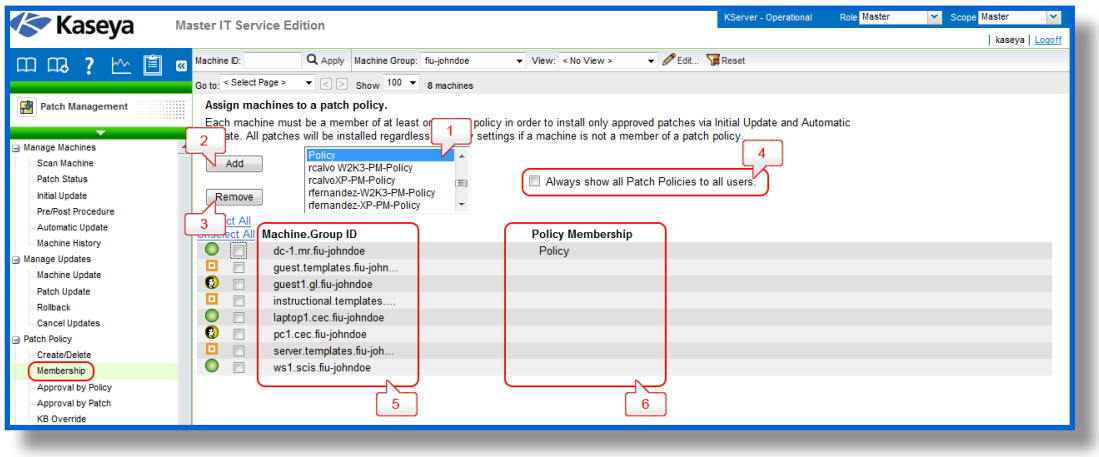


Fig. 5.12: *Membership*

1. **Policy:** Select one or more patch policy names to mark them for adding or removing from selected machine IDs.

2. **Add:** Click *Add* to add selected machine IDs (5. Machine.Group ID below) to selected patch policies (1. Policy above).

3. **Remove:** Click *Remove* to remove selected machine IDs (5. Machine.Group ID below) from selected patch policies(1. Policy above).

4. **Always show all Patch Policies to All Users:** If checked, always show all patch policies to all users. This allows all non-master role users to deploy patch policies, even if they did not create the patch policies and don't have machines yet that use them. If blank, only master role users can see all patch policies. If blank, non-master role users can only see patch policies assigned to machines within their

scope or to unassigned patch policies they created. This option only displays for master role users.

5. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

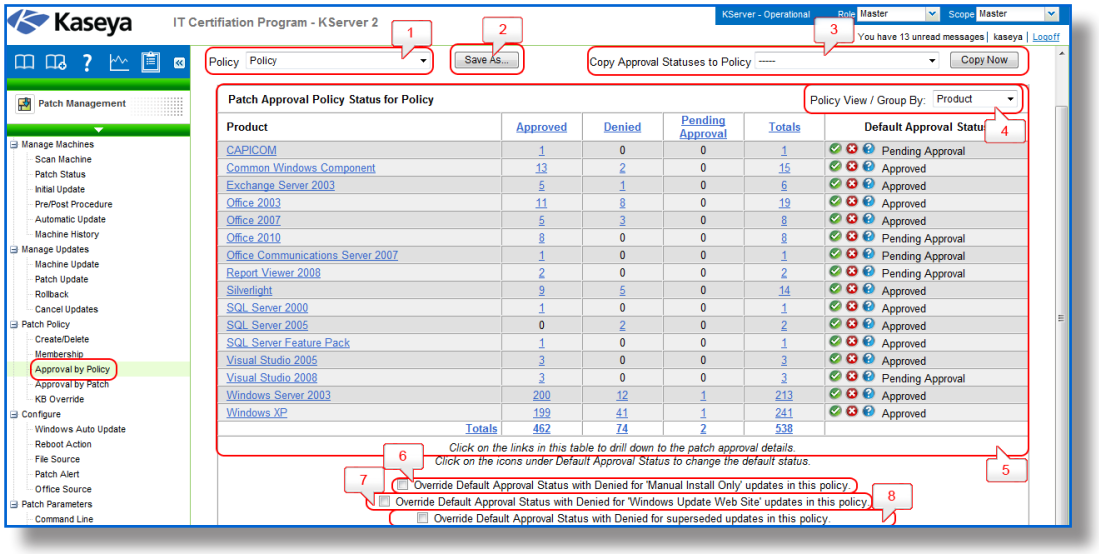
6. **Policy Membership:** Displays a comma separated list of patch policies that each machine ID is a member of.

5.3.3 Approval by Policy

The **Approval by Policy** page approves or denies the installation of Microsoft patches on managed machines by *patch policy*. Patches pending approval are considered denied until they are approved. This gives you the chance to test and verify a patch in your environment before the patch automatically pushes out.

The features supported by Approval by Policy page (Fig. 5.13) are:

Fig. 5.13: *Approval by Policy*



1. **Policy:** Select a patch policy by name from the drop-down list.

2. **Save As:** To save a patch policy under a different name click *Save As* and it is saved to a new policy with identical settings. All patch approval/denial statuses are copied as the default approval statuses for the policy.

3. **Copy Approval Statuses to Policy <Policy Name>:** Select a policy to copy approval statuses *to*, from the currently selected policy. Then click *Copy Now*. This feature enables you to perform patch testing against a group of test machines using a test policy. Once testing has been completed and the patches have been approved or denied, use the copy feature to copy only the approved or denied statuses from the test policy to a production policy.

4. **Policy View / Group By:** Displays patch groups by classification or product.

5. **Patch Approval Policy Status:** This table displays the approval status of patches by update classification or product group. *Approved, Denied, Pending Approval*, and *Totals* statistics are provided for each update classification or product group.

Select a **Default Approval Status** for any category for this patch policy. Newly identified patches for this patch policy are automatically set to this default value. Choices include:

Approved Denied Pending Approval

6. Override Default Approval Status with Denied for "Manual Install Only" updates in this policy: If this option is checked, all existing and future Manual Install Only updates are set to *Denied* for this policy.

7. Override Default Approval Status with Denied for "Windows Update Web Site" updates in this policy: If this option is checked, all existing and future Windows Update Web Site updates are set to *Denied* for this policy.

8. Override Default Approval Status with Denied superseded updates in this policy: If this option is checked, it automatically denies superseded patches that has been added. This functions in the similar manner as the above described options.

Note: *If the same patch is assigned two different* Default Approval Status *settings then the more restrictive of the two defaults has precedence: Denied over Pending Approval over Approved.*

Notes

Clicking any link on the *Patch Approval Policy Status* table takes you the *Patch Approval Policy Details* page (Fig. 5.16) where patches can be approved or denied individually.

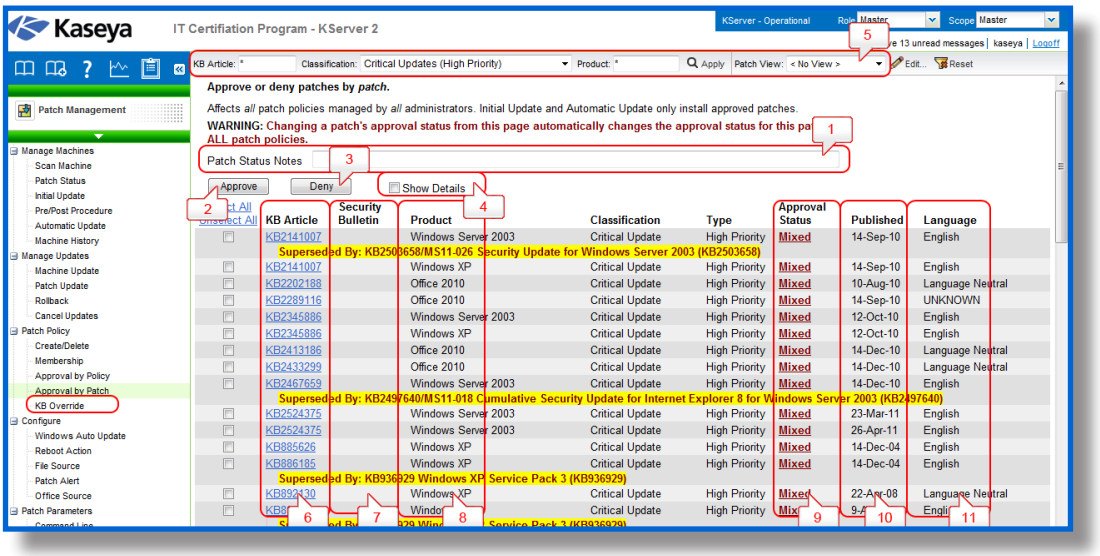


Fig. 5.14: *Patch Approval Policy Details*

In the *Patch Approval Policy Details* (Fig. 5.14) page you can:

1. Approve or deny approval of patches individually.

2. Click the *KB Article link* to display a Details page about the patch. The Details page contains a link to display the knowledge base article.

Note: *Microsoft may use a common knowledge base article for one or more patches, causing patches to appear to be listed more than once. Check the* Product *name or click the* KB article *link to distinguish patches associated with a common knowledge base article.*

Notes

3. Click the *Security Bulletin link* to review the security bulletin, if available. Patches classified as security updates have a security bulletin ID (MSyy-xxx).

4. The **Product** column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (*i.e.,* Windows XP, Windows Server 2003, Vista, etc.), the product category is Common Windows Component. Examples include Internet Explorer, Windows Media Player, MDAC, MSXML, and so on.

5. Click the *Show Details* checkbox to display the expanded title, patch status notes and installation warnings, if any, of each patch.

6. Click *Filter* to restrict the amount of data displayed. You can specify a different advanced filter for each column of data displayed.

7. Optionally add a note, up to 500 characters, using **Patch Status Notes**. The note is added when the *Approve* or *Deny* buttons are selected. If the text box is empty when the *Approve* or *Deny* buttons are selected, the note is removed for selected patches.

5.3.4 Approval by Patch

The **Approval by Patch** page allows for approving or denying the installation of all Microsoft patches on managed machines on a patch by patch basis. Changes made here affect patches installed by all users thereby avoiding the need for approving pending patches separately for each patch policy.

The features supported by Approval by Patch page (Fig. 5.15) are:

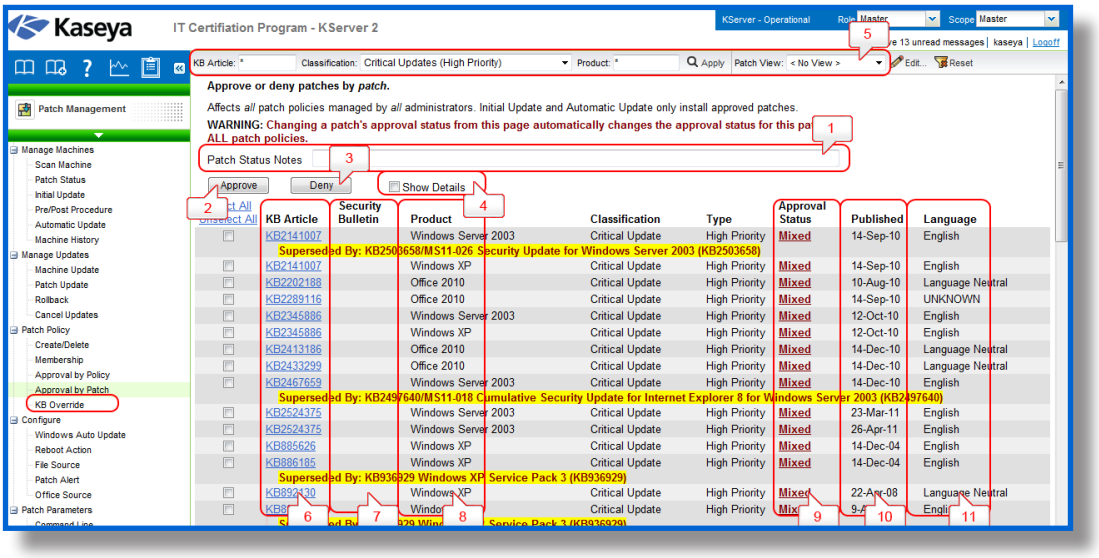


Fig. 5.15: *Approval by Patch*

1. **Patch Status Notes:** Optionally add a note, up to 500 characters, using *Patch Status Notes*. The note is added when the *Approve* or *Deny* buttons are selected. If the text box is empty when the *Approve* or *Deny* buttons are selected, the note is removed for selected patches.

2. **Approve:** Click *Approve* to approve selected patches for all patch policies.

3. **Deny:** Click *Deny* to deny selected patches for all patch policies.

4. **Show Details:** Check *Show Details* to display multiple rows of information for all patches. This includes the title of a patch, the number of patch policies that have been approved, denied, or are pending approval for a patch, patch status notes, and installation warnings, if any.

5. **Patch Data Filter Bar:** You can filter the data displayed by specifying values in each field of the Patch Data Filter Bar at the top of the page. Enter or select values in the KB Article, Classification or Products fields. You can also click the Edit button to filter by additional fields and save the filtering selections you make as a view. Supports advanced filtering logic. Saved views can be shared using the Make

Public (others can view) checkbox when editing the view.

6. **KB Article:** Click the *KB Article link* to display a Details page about the patch. The Details page contains a link to display the knowledge base article.

7. **Security Bulletin:** Click the *Security Bulletin link* to review the security bulletin, if available. Patches classified as security updates have a security bulletin ID (MSyy-xxx).

8. **Product:** The **Product** column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (*i.e.,* Windows XP, Windows Server 2003, Vista, etc.), the product category is Common Windows Component. Examples include Internet Explorer, Windows Media Player, MDAC, MSXML, and so on.

9. **Approval Status:** The approval status for this patch in *all* policies. Displays *Mixed* if even 1 policy differs from all other policies. Clicking the Approval Status link displays a page displaying the approval status assigned to this patch by each policy.

10. **Published:** The Published column displays the date the patch was released.

11. **Language:** The Language column displays the language the patch applies to.

5.3.5 KB Override

The **KB Override** page **(Fig. 5.18)** overrides the *default* approval status of patches set using **Patch Management > Approval by Policy** by *KB article* for *all* patch policies. It also sets the approval status for *existing* patches by KB Article for all patch policies. Changes affect patches in *all* patch policies installed by *all* users.

Example: The KB890830, "The Microsoft Windows Malicious Software Removal Tool", is released monthly. If you decide to approve all patches associated with this KB Article using KB Override, then not only are existing patches approved but all *new* patches associated with this KB article are automatically approved each time the new patch is released.

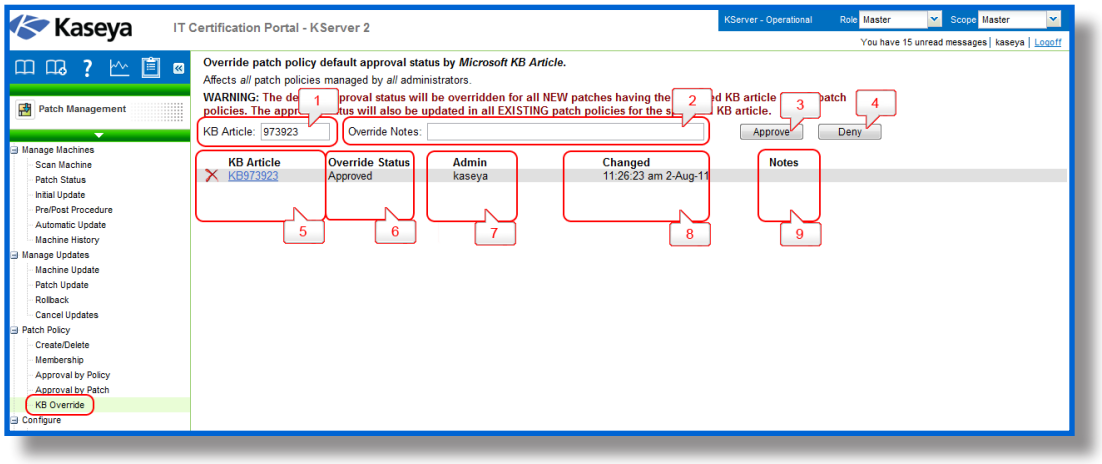


Fig. 5.16: *KB Override*

Fig. 5.16 shows the KB Override page. The functions supported by this module are listed and explained below.

1. **KB Article:** Enter the *KB Article* to approve or deny.

2. **Override Notes:** Enter a note to remind VSA users why the override was set.

3. **Approve:** Click *Approve* to approve patches associated with this KB Article. Multiple patches can

be associated with a KB Article.

4. **Deny:** Click *Deny* to deny patches associated with this KB Article. Multiple patches can be associated with a KB Article.
5. **KB Article:** Click the *KB Article link* to display the KB article.
6. **Override Status:** Approved or Denied. Applies to all patches associated with this KB Article.
7. **Admin:** The user who approved or denied patches associated with this KB Article.
8. **Changed:** The date and time the user approved or denied patched associated with this KB Article.
9. **Notes:** Reminds VSA users why the override was set.

5.4 Configure

5.4.1 Windows Auto Update

The **Windows Auto Update** page determines whether **Windows Automatic Updates** on managed machines is disabled, is controlled by the user, or configured according to the requirements.

Windows Automatic Updates
Windows Automatic Updates is a Microsoft tool that automatically delivers updates to a computer. Windows Automatic Updates is supported in the following operating systems: Windows 2003, Windows XP, Windows 2000 SP3 or later and all operating systems released after these versions. Patch Management > Windows Auto Update can enable or disable this feature on managed machines. While Windows Millennium Edition (Me) has an Automatic Updates capability, it cannot be managed as the above operating systems.

Windows Automatic Update Cannot Use Template Accounts
Windows Automatic Updates is one feature that cannot be preconfigured in a machine ID template. This is because Windows Automatic Updates is only supported on Windows 2000 SP3/SP4, Windows XP, Windows Server 2003, and later operating systems. Since a machine ID template cannot specify an operating system, a setting for this feature cannot be stored in the machine ID template. Also, a machine's current settings must be known before they can be overridden. The current settings are obtained when a Patch Management > Scan Machine is performed.

Fig. 5.17 shows the generic view of the Windows Auto Update page. The functions supported by this module are listed and explained below:

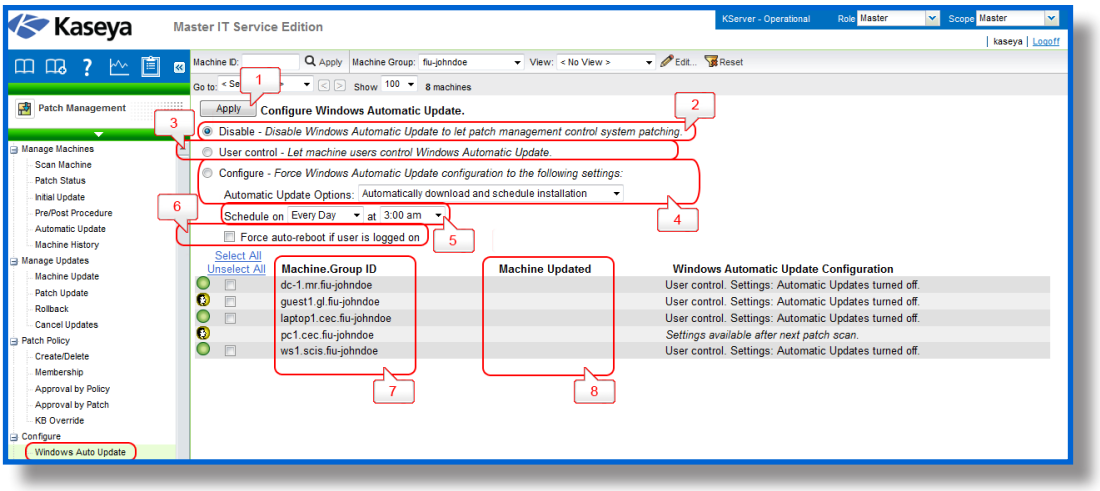


Fig. 5.17: *Windows Auto Update*

1. **Apply:** Click *Apply* to apply parameters to selected machine IDs.

2. **Disable:** Select *Disable* to disable Windows Automatic Updates on selected machine IDs and let **Patch Management** control patching of the managed machine. Overrides the existing user settings and disables the controls in Windows Automatic Updates so the user *cannot* change any of the settings. Users can still patch their systems manually.

3. **User Control:** Let machine users enable or disable Windows Automatic Updates for selected machine IDs.

4. **Configure:** Forces the configuration of Windows Automatic Updates on selected machine IDs to the following settings. Overrides the existing user settings and disables the controls in Windows Automatic Updates so the user cannot change any of the settings. Users can still patch their systems manually.

   - **Notify user for download and installation** - Notifies the user when new patches are available but does not download or install them.
   - **Automatically download and notify user for installation** - Automatically downloads updates for the user but lets the user choose when to install them.
   - **Automatically download and schedule installation** - Automatically downloads updates and installs the updates at the scheduled time.

5. **Schedule every day / <day of week> at <time of day>:** Applies only if **automatically download and schedule installation** is selected. Perform this task every day or once a week at the specified time of day.

6. **Force auto-reboot if user is logged on:** Optionally check the box next to **Force auto-reboot if user is logged on**. By default, **Windows Auto Update** does *not* force a reboot. **Patch Management > Reboot Action** settings do not apply to **Windows Auto Update**.

7. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

8. **Machine Updated:** Displays the status of configuring Windows Automatic Updates on selected machine IDs using this page.

   - Pending - Windows Automatic Updates is being configured on the selected machine ID.
   - Timestamp - The date and time Windows Automatic Updates was configured on the selected machine ID.

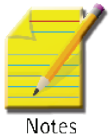
5.4.2 Reboot Action

The **Reboot Action** page defines how reboots are performed after a patch install. Patch installs do not take effect until after a machine is rebooted. The **Reboot Action** policy applies to Machine Update, Patch Update and Automatic Update. It does *not* apply to Initial Update.

Warning: *Automatic rebooting of the KServer or database server can have adverse effects on other KServer processes!*

Patch Process
The patch installation procedure runs at the scheduled time and performs the following steps:

- Downloads, or copies from a shared folder, all the patch files to a local drive, typically the same drive the agent is installed on.
- Executes each patch file, one at a time.
- Performs a reboot of the machine, as specified by this page.



Note: *After all the patches have been installed the machine reboots once.*

Note: If you are installing a service pack with other patches you will see a reboot after the service pack install and then another single reboot after all the other patches are installed.

View Definitions
You can filter the display of machine IDs on any agent page using the following options in View Definitions.

- **S**how machines that have/have not rebooted in the last N periods
- Machines with Reboot Pending for patch installations

The generic view of the Reboot Action page is shown in Fig. 5.18 and all the supported functions on this page is listed and explained below.

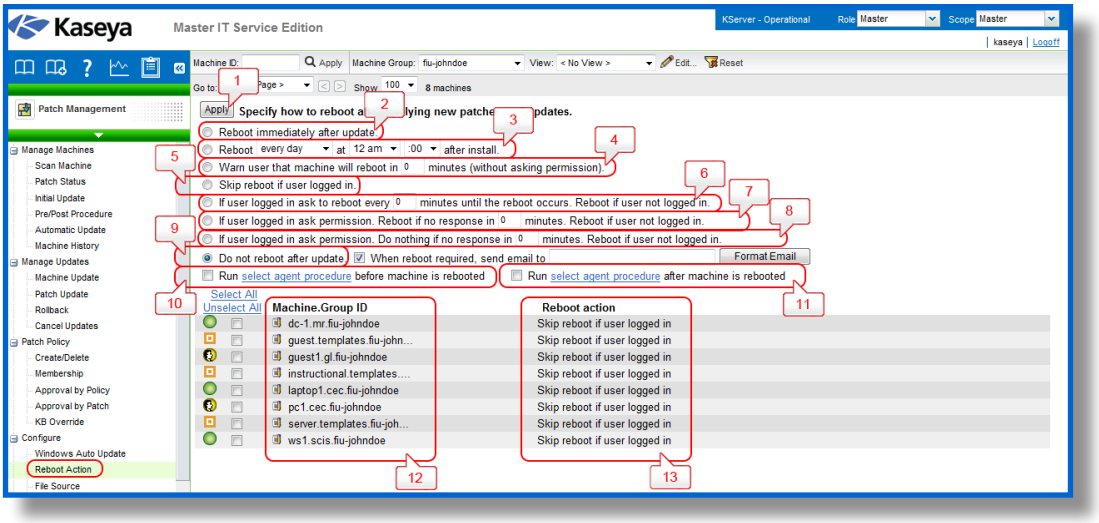


Fig. 5.18: *Reboot Action*

1. **Apply:** Click *Apply* to apply parameters to selected machine IDs.
2. **Reboot immediately after update:** Reboots the computer immediately after the install completes.
3. **Reboot <day of week> at <time of day> after install:** After the patch install completes, the computer is rebooted at the selected day of week and time of day. Use these settings to install patches

during the day when users are logged in, then force a reboot in the middle of the night. Selecting **every day** reboots the machine at the next specified time of day following the patch installation.

4. **Warn user that machine will reboot in <N> minutes (without asking permission):** When the patch install completes, the message below pops open warning the user and giving them a specified number of minutes to finish up what they are doing and save their work. If no one is currently logged in, the system reboots immediately.

5. **Skip reboot if user logged in:** If the user is logged in, the reboot is skipped after the patch install completes. Use this setting to avoid interrupting your users. This is the default setting.

6. **If user logged in ask to reboot every <N> minutes until the reboot occurs:** This setting displays the message below, asking the user if it is OK to reboot now. If no one is at the computer or they answer no, the same message appears every N minutes repeatedly, until the system has been rebooted. If no one is currently logged in, the system reboots immediately.

7. **If user logged in ask permission. Reboot if no response in <N> minutes. Reboot if user not logged in:** This setting displays the message below, asking the user if it is OK to reboot now. If no one is at the computer, it reboots automatically after N minutes **without saving** any open documents. If no one is currently logged in, the system reboots immediately.


Notes

8. **If user logged in ask permission. Do nothing if no response in <N> minutes. Reboot if user not logged in:** This setting displays the message below, asking the user if it is OK to reboot now. If no one is at the computer, the reboot is skipped. If no one is logged in, reboot immediately.

9. **Do not reboot after update:** Does not reboot. Typically used if the machine is a server and you need to control the reboot. You can be notified via email when a new patch has been installed by checking **Email when reboot required** and filling in an email address. You can also format the email message by clicking the **Format Email** button. This option only displays for master role users.

The following types of patch reboot emails can be formatted:

- Patch Reboot

Note: *Changing the email alarm format changes the format for all* Patch Reboot *emails.*

The following variables can be included in your formatted email alerts and in procedures.

Within an Email	Description
<at>	alert time
<db-view.column>	Include a view.column from the database. For example, to include the computer name of the machine generating the alert in an email, use <db-vMachine.ComputerName>
<gr>	group ID
<id>	machine ID

10. **Run select agent procedure before machine is rebooted:** If checked, the selected agent proce-

dure is run just *before* the machine is rebooted.

11. Run select agent procedure after machine is rebooted: If checked, the selected agent procedure is run just *after* the machine is rebooted.

12. Machine.Group ID: The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

13. Reboot Action: The type of reboot action assigned to each machine ID.

5.4.3 File Source

The **File Source** page defines where each machine gets executable patch files from, prior to installation, and where these patch executables are copied to the local machine. File source locations include:

- The Internet
- The KServer
- A shared folder

Note: *Patch download links with a* `cab` *extension are always downloaded directly from the internet regardless of the* File Source *setting.*

The figure below shows the generic view of the File Source page (Fig. 5.19). The supported functions on this page are listed and explained below.

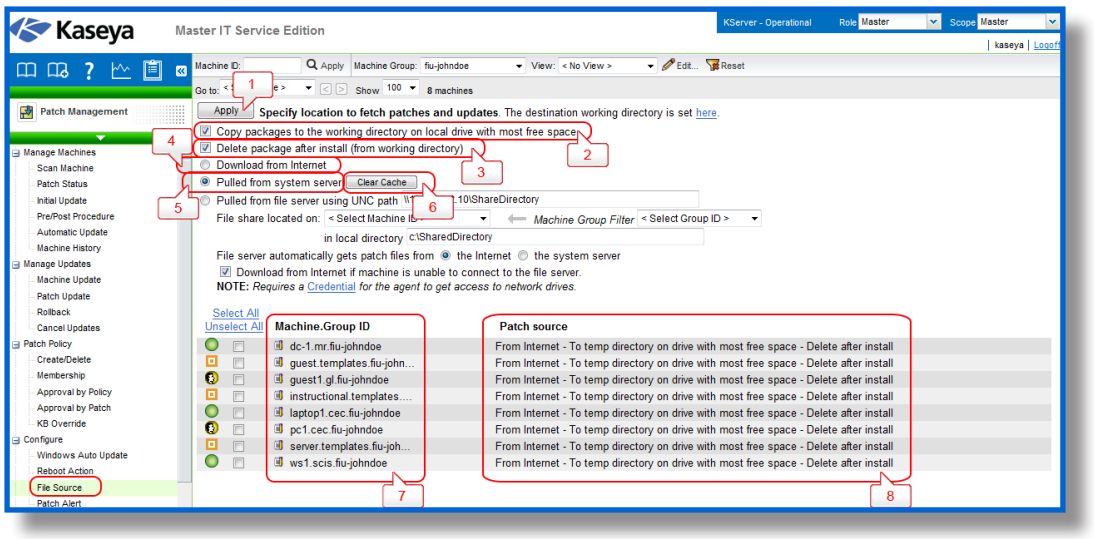


Fig. 5.19: *File Source*

1. Apply: Click *Apply* to apply the selected patch source option to selected machine IDs.

2. Copy packages to working directory on local drive with most free space: Patches are downloaded, or copied from a shared folder, to the managed machine's hard disk. Several patches, especially service packs, may require significant additional local disk space to completely install. Check this box to download patches to the **Agent > Working Directory**, but use the drive on the managed machine with the most free disk space. Uncheck this box to always

3. use the drive specified in **Working Directory** for the machine ID.

4. Delete package after install (from working directory): The install package is typically deleted after the install to free up disk space. Uncheck this box to leave the package behind for debugging pur-

poses. If the install fails and you need to verify the **Patch Management > Command Line** switches, do not delete the package so you have something to test with. The package is stored in the **Agent > Working Directory** on the drive specified in the previous option.

5. **Download from Internet:** Each managed machine downloads the patch executable file directly from the internet at the URL specified in **Patch Management > Patch Location.**

6. **Pulled from system server:** First the KServer checks to see if it already has a copy of the patch file. If not, the new patch executable is downloaded automatically and stored on the KServer, then used for all subsequent distributions to managed machines. When a patch needs to be installed on a managed machine, this patch file is pushed to that machine from the KServer.

7. **Clear Cache:** Click *Clear Cache* to clear all downloaded patches stored on the KServer.

8. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

9. **Patch Source:** Lists the patch source selected for each machine ID. A *Clear Cache* button displays in this column if the *Pulled from file server using UNC path* option is selected for a machine ID. Clicking this *Clear Cache* button clears patches from the specified file server UNC path. The *Clear Cache* button is *not* machine specific. All patches stored on that file server for the specified path will be deleted.

Pulled from file server using UNC path: This method is recommended if you support many machines on the same LAN. Patch files are downloaded to the local directory of a selected machine ID. The local directory on the machine ID is configured to be shared with other machine IDs on the same LAN. All other machine IDs on the same LAN use a UNC path to the shared folder located on the first machine ID. All other machines on the same LAN require a credential to access the shared folder on the first machine and install the patch files. A credential is specified for the first machine with the shared directory using **Agent > Set Credential.**

Setup:

1. Enter a UNC path in the *Pulled from file server using UNC path* field.

Example: "\\computername\sharedname\dir\" or "\\192.168.2.10\ShareDirectory" as shown in Fig. 5.20.

2. Use the *Machine Group Filter* drop-down list to select a group ID.

3. Select a machine ID from the *File share located* **on** drop-down list.

4. Enter a shared local directory in the **in** *local directory* field.

Note: *The value in the* local directory *field must be in full path format, such as* c:\shareddir\dir

First the KServer checks to see if the patch file is already in the file share. If not, the machine ID with the file share automatically loads the patch file either directly from the internet or gets it from the KServer. In either case, the managed machine with the file share **must have an agent** on it.

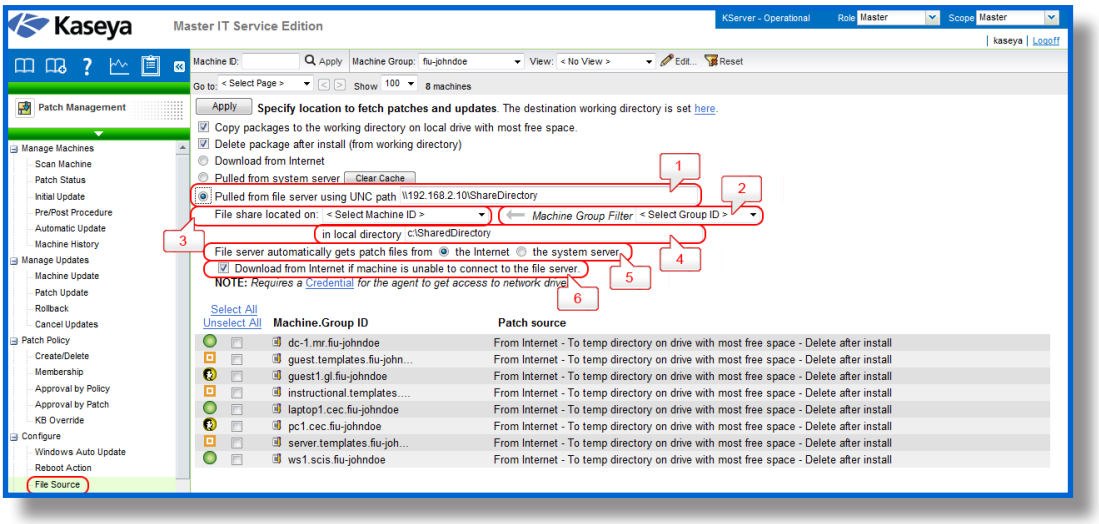
5. **File Server automatically gets patch files from** - Select one of the following options:

   • **the Internet** - Use this setting when the managed machine running the file share has full internet access.

   • **the System server** - Use this setting when the managed machine running the file share is blocked from getting internet access.

6. **Download from Internet if machine is unable to connect to the file server** - Optionally check this box to download from the internet. This is especially useful for laptops that are disconnected from the company network but have internet access.

Fig. 5.20: *Setup*



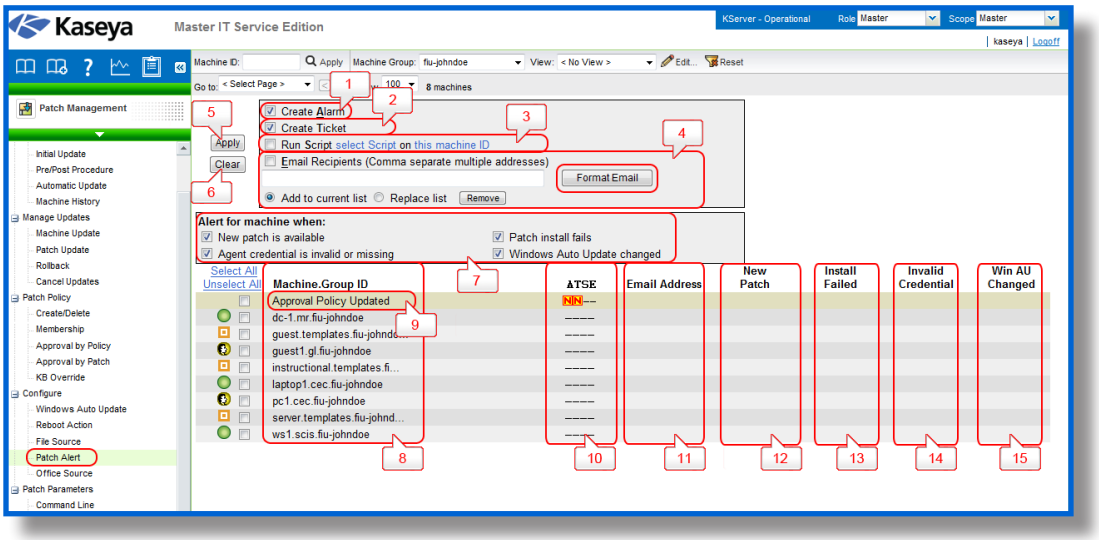
5.4.4 Patch Alert

The **Patch Alert** page triggers an alert for patch management event on managed machines.

- A new patch is available for the selected machine ID.
- A patch installation failed on the selected machine ID.
- The agent credential is invalid or missing for the selected machine ID.
- Windows Auto Update changed.

Fig. 5.21 shows the generic view of the Patch Alert page. The functions supported by this page are listed and explained below.

Fig. 5.21: *Patch Alert*



1. **Create Alarm:** If checked and an alarm condition* is encountered, an alarm is created. Alarms are

displayed in **Monitor > Dashboard List**, **Monitor > Alarm Summary** and **Info Center > Reports > Logs > Alarm Log**.

Note: *An alarm condition exists when a machine's performance succeeds or fails to meet a pre-defined criteria.*

Notes

2. **Create Ticket:** If checked and an alarm condition is encountered, a ticket is created.

3. **Run Script:** If checked and an alarm condition is encountered, an agent procedure is run. You must click the *select script* link to choose an agent procedure to run. You can optionally direct the agent procedure to run on a specified range of machine IDs by clicking *this machine ID* link. These specified machine IDs do not have to match the machine ID that encountered the alarm condition.

4. **Email Recipients:** If checked and an alarm condition is encountered, an email is sent to the specified email addresses.

   • The email address of the currently logged on user displays in the *Email Recipients* field. It defaults from **System >Preferences.**

   • Click *Format Email* to display the *Format Alert Email* popup window. This window enables you to format the display of emails generated by the system when an alarm condition is encountered as shown in Fig. 5.22.

   • If the *Add to current list* radio option is selected, when *Apply* is clicked alert settings are applied and the specified email addresses are added without removing previously assigned email addresses.

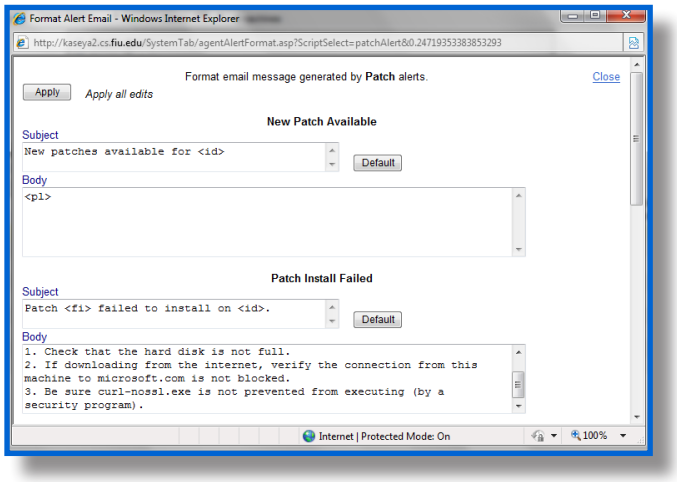


Fig. 5.22: *Format Alert Email*

   • If the *Replace list* radio option is selected, when *Apply* is clicked alert settings are applied and the specified email addresses replace the existing email addresses assigned.

   • If *Remove* is clicked, all email addresses are removed without modifying any alert parameters.

   • Email is sent directly from the KServer to the email address specified in the alert. Set the *From Address* using **System > Outbound Email.**

5. **Apply:** Click *Apply* to apply parameters to selected machine IDs. Confirm the information has been applied correctly in the machine ID list.

6. **Clear:** Click *Clear* to remove all parameter settings from selected machine IDs.

7. **Patch Alert Parameters:** The system can trigger an alert for the following alarm conditions for a selected machine ID:

    - **New patch is available**
    - **Patch install fails**
    - **Agent credential is invalid or missing**
    - **Windows Auto Update changed**

8. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

9. **Approval Policy Updated:** Displays as the first row of data. If selected and the *Apply* button clicked, an alert is generated when a new patch is added to all patch policies.

10. **ATSE:** The ATSE response code assigned to machine IDs:

    - A = Create **A**larm
    - T = Create **T**icket
    - S = Run Procedure
    - E = **E**mail Recipients

11. **Email Address:** A comma separated list of email addresses where notifications are sent.

12. **New Patch:** If checked, an alarm is triggered when a new patch is available for this machine ID.

13. **Install Failed:** If checked, an alarm is triggered when a patch installation has failed for this machine ID.

14. **Invalid Credential:** If checked, an alarm is triggered when the credential is invalid for this machine ID.

15. **Win AU Changed:** If checked, an alarm is triggered if the group policy for Windows Automatic Update on the managed machine is changed from the setting specified by **Patch Management > Windows Auto Update.**

Note: *A log entry in the machine's Configuration Changes log is made regardless of this alert setting*

To Create a Patch Alert

1. Check any of these checkboxes to perform their corresponding actions when an alarm condition is encountered:

    - *Create* A*larm*
    - *Create* T*icket*
    - *Run* S*cript*
    - *Email Recipients*

2. Set additional email parameters.
3. Set additional patch alert specific parameters.
4. Check the machine IDs to apply the alert to.
5. Click the *Apply* button.

To Cancel a Patch Alert

1. Select the machine ID checkbox.
2. Click the *Clear* button. The alert information listed next to the machine ID is removed.

Passing Alert Information to Emails and Procedures
The following types of patch alert emails can be sent and formatted:

- New Patch Available
- Patch Install Failed
- Patch Approval Policies Updated
- Agent Credential Invalid
- Windows Auto Update Configuration Changed

Note: *Changing the email alarm format changes the format for all* Patch Alert *emails.*

5.4.5 Office Source

The **Office Source** page sets *alternate* source locations for installing Office and Office component applications. The source location can be changed from the default CD-ROM, which is the typical installation source, to a shared folder or a directory on a local hard drive. By changing the installation source to a network share or a local directory, patches that require the Office installation source for installation can get access **without prompting the user for the installation media**. This alternate source location can be configured to be read-only. It must contain an exact copy of the installation media contents including all hidden files and/or directories.

An Office source for a managed machine is only available after you have run **Patch Management > Scan Machine** at least once for the managed machine. Machine IDs are displayed on this page only if they:

- Currently match the Machine ID / Group ID filter.
- Have Office or Office component applications installed for Office 2000, XP, or 2003.

Note: *Office 2007 installs a full set of source installation files on a machine and an alternate source location is not required.*

Multiple Entries
Multiple entries may be displayed for a machine because the machine contains one or more Office component applications, such as FrontPage or Project, that were installed separately from their own installation source and were not part of the Office installation.

Credential Required
Managed machines must have a credential set (refer Agent > Set credential) to use the Office Source page. The agent must have a credential to use the alternate Office source location.

Validation

The specified location is validated to be sure that the location is accessible from the machine and that the installation source in the specified location contains the correct edition and version of Office or the Office component application. The machine's registry is modified to use the specified location only after the validation .

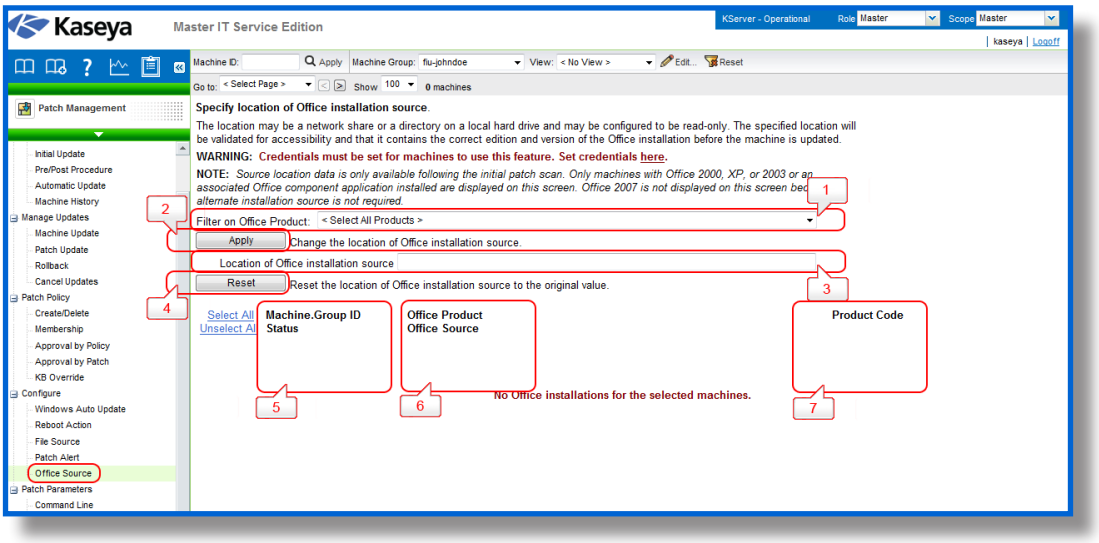
Installing Office Products

Some patches—particularly Office service packs—still display progress dialogs even though the silent installation switch (/Q) is included using **Patch Management > Command Line**. These progress dialogs do not require any user intervention. Some patches and service packs display a modal dialog indicating the update has completed, again even though the silent installation switch (/Q) is used. This requires the user to click on the OK button to dismiss the dialog. Until this happens, the patch installation procedure appears to be hung and will not complete until this dialog is dismissed.

Some Office service packs fail for no apparent reason. Checking the machine's application event log reveals that another Office component service pack failed. This has been observed with Office 2003 service pack 2 requiring the availability of FrontPage 2003 service pack 2. When the Office source location for the FrontPage 2003 is configured, the Office 2003 service pack 2 finally successfully installs.

Fig. 5.23 below shows the generic view of the Office source page. The functions supported by this page is listed and explained below.

Fig. 5.23



1. **Filter on Office Product:** Because each managed machine may be listed multiple times—once for each Office product or Office component application installed—you can filter the Office products/components displayed. This ensures selecting the same product code for multiple machines when setting the installation source location.

2. **Apply:** Click *Apply* to apply the Office source location specified in *Location of Office installation source* to selected machine IDs.

3. **Location of Office installation source:** Add the network share as a UNC path (*i.e.,* \\machinename\sharename) or a local directory as a fully qualified path (*i.e.,* C:\OfficeCD\Office2003Pro) in the installation source text box.

4. **Reset:** Click *Reset* to restore selected machine IDs back to their original installation source, typically the CD-ROM.

5. **Machine.Group ID:** The list of Machine.Group IDs displayed is based on the Machine ID / Group ID filter and the machine groups the user is authorized to view.

Status
Displays one of the following:

- Missing Credential
- Update Procedure Failed
- Validation Procedure Failed
- Original Source
- Pending Validation
- Updating Machine
- Incorrect Edition
- Processing Error
- Restoring Original
- Office Source Updated

6. **Office Product:** Displays the name of the Office product.
   Office Source: Displays the current installation source location for this Office product on this machine ID.
7. **Product Code:** Displays the Office product code.

5.5 Patch Parameters

5.5.1 Command Line

The **Command Line** page defines the command line switches used to silently install a specified patch. Occasionally a patch is released that does not use normal switch settings or the patch database has not been updated with the new switches. If you find a patch does not successfully install with its assigned switch settings, you can change them here. Locate patch switches by clicking the **KB Article** link and reading through the knowledge base article.

Warning: *Changes to the switches affect all users. This page is only displayed for master role users.*

Suppress Automatic Reboot
Usually you want to load a patch without requiring any user interaction at all. The system supports batch installs of multiple patches at the same time and reboots once at the end of all patch installations. Therefore, use switch settings to suppress automatic reboot wherever possible.

Switch Settings
Typical patch file switch settings for silent, unattended installs without reboot:

- /quiet /norestart - This is the standard setting for most patches in recent years.
- /u /q /z - Typical switch settings used to silently install older patches that do not use the Windows Installer technology.

- /m /q /z - Typical switch settings to silently install older patches released for Windows NT4.
- /q:a /r:n - Internet Explorer and other application switch settings to install in quiet user mode (/q:a) and not automatically reset (/r:n) when the install completes.
- Other switch settings found with Microsoft patch installations include:
- /? - Display the list of installation switches.
- /u - Use Unattended mode.
- /m - Unattended mode in older patches.
- /f - Force other programs to quit when the computer shuts down.
- /n - Do not back up files for removal.
- /o - Overwrite OEM files without prompting.
- /z - Do not restart when the installation is complete.
- /q - Use quiet mode (no user interaction).
- /l - List the installed hotfixes.
- /x - Extract files without running Setup.

Microsoft Office command line switches
The only switch permitted for use with Microsoft Office 2000 and Office XP related patches is /Q. If /Q is not specified, Microsoft Office 2000 and Microsoft Office XP switches will be automatically reset to /INSTALL-AS-USER. Microsoft Office 2003 patches may also include the /MSOCACHE switch used to attempt a silent install if the MSOCache exists on the machine. These settings are enforced by the application.

Server-side command line switches
Special server-side command line switches can be combined with patch specific switches:

- /INSTALL-AS-USER - Tells the system to only install this patch as a user. Some rare patches do not install successfully unless someone is logged onto the machine. Add this switch if you find a patch is failing to install if no one is logged in.

Warning: *This setting conflicts with the* Skip update if user logged in *setting found in* Reboot Action./INSTALL-AS-USER *requires that a user be logged in to install.*

- /DELAY-AFTER=xxx - After the install wait xxx seconds before performing the reboot step. The reboot step starts after the install package completes. Some rare installers spawn additional programs that must also complete before rebooting. Add this switch to give other processes time to complete after the main installer is done.

Fig. 5.24 below shows the generic view of the Command Line page. The supported options are explained below.

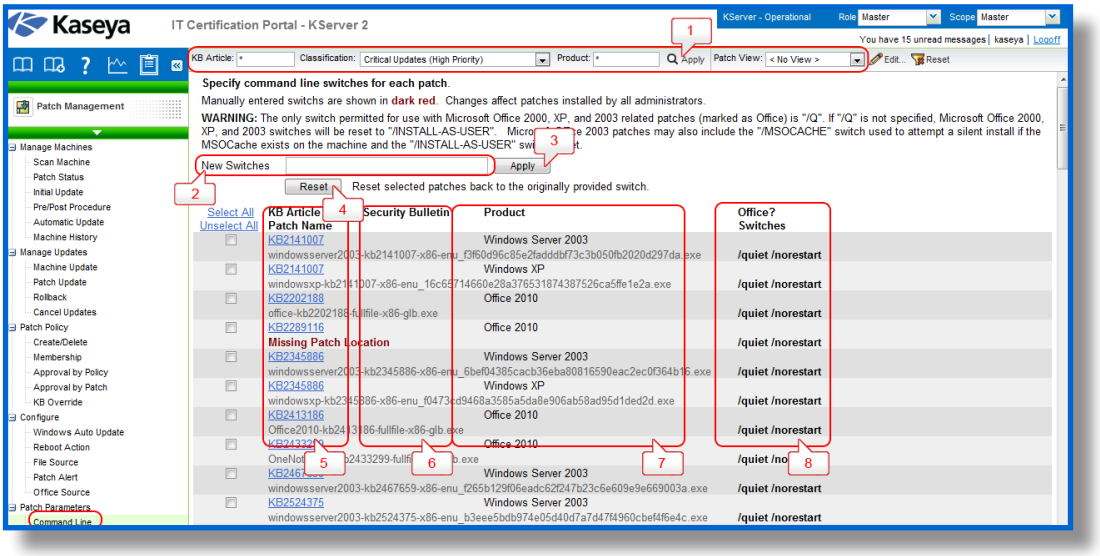


Fig. 5.24: *Command Line page*

1. **Patch data filter bar:** You can filter the data displayed by specifying values in each field of the Patch Data Filter Bar at the top of the page. Enter or select values in the KB Article, Classification or Products fields. You can also click the Edit button to filter by additional fields and save the filtering selections you make as a view. Supports advanced filtering logic. Saved views can be shared using the Make Public (others can view) checkbox when editing the view.

2. **New Switches:** Enter the command line switches you want to apply to selected patches.

3. **Apply:** Click *Apply* to apply the specified command line switches to selected patches.

4. **Reset:** Click *Reset* to reset the command lines of selected patches back to their default settings.

5. **KB Article:** The knowledge base article describing the patch. Click the **KB Article** link to display a Details page about the patch. The Details page contains a link to display the knowledge base article.

   Patch Name: The patch install filename.

6. **Security Bulletin:** Click the *Security Bulletin* link to review the security bulletin, if available. Patches classified as security updates have a security bulletin ID (MSyy-xxx).

7. **Product:** The *Product* column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (*i.e.,* Windows XP, Windows Server 2003, Vista, etc.), the product category isCommon Windows Component. Examples include Internet Explorer, Windows Media Player, MDAC, MSXML, and so on.

8. **Office?:** If the product displayed is an Office product, the version is displayed here.

   Switches: The command line switches used to install this patch is displayed.

5.5.2 Patch Location

The **Patch Location** page defines the URL from which each patch is downloaded. Only patches *missing* from machine IDs that currently match the Machine ID / Group ID filter are displayed here. You should consult this

page if, when attempting to install a patch, you are notified of a Path Missing.

The KServer maintains a list of each patch and the URL it should be downloaded from. In most cases the download URLs provided for patches are correct. Path Missing errors may occur for the following reasons:

- Each language may require a separate URL to download from.
- The URL may change for one or more patches.
- The KServer's record for the URL may be entered incorrectly or be corrupted.

In such cases, users can change the download path associated with a patch. Manually entered URLs are shown in dark red.

Note: *Changes affect patches installed by all users. This page is only displayed for master role users*

Fig. 5.25: *Patch Location*

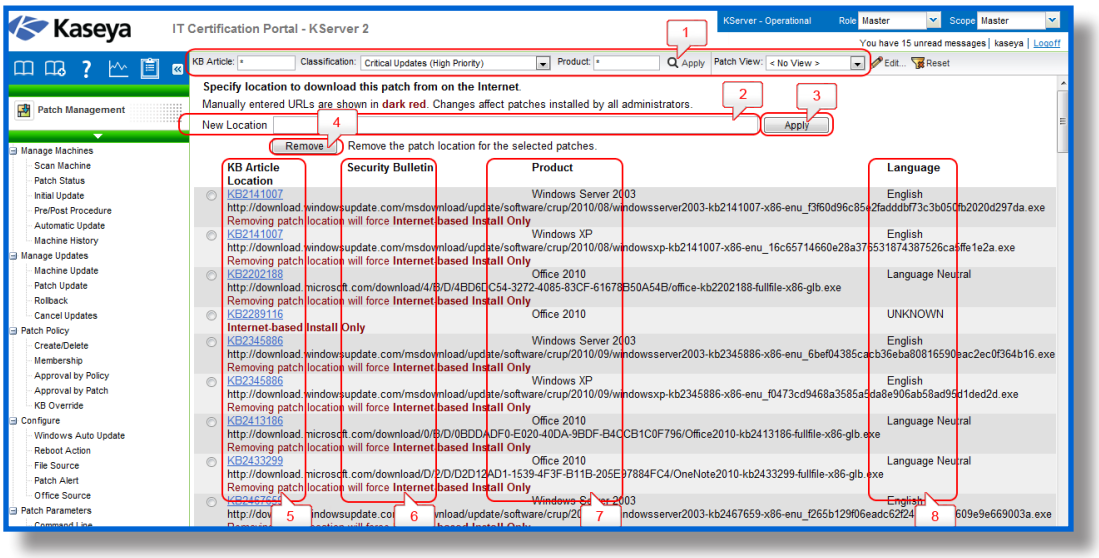


Fig. 5.25 below shows the generic view of the Patch Location page. The options supported by this module are listed and explained below.

1. **Patch data filter bar:** You can filter the data displayed by specifying values in each field of the Patch Data Filter Bar at the top of the page. Enter or select values in the KB Article, Classification or Products fields. You can also click the Edit button to filter by additional fields and save the filtering selections you make as a view. Supports advanced filtering logic. Saved views can be shared using the Make Public (others can view) checkbox when editing the view.

2. **New Location:** Enter a new URL.

3. **Apply:** Click *Apply* to apply the URL listed in the *New Location* field to the selected patch.

4. **Remove:** Click *Remove* to delete the download URL associated with a patch ID.

Warning: *Removing a path disables patching managed machines using this patch until the correct path is entered*

5. **KB Article:** The knowledge base article describing the patch. Click the **KB Article** link to display a Details page about the patch. The Details page contains a link to display the knowledge base article.

6. Security Bulletin: Click the **Security Bulletin** link to review the security bulletin, if available. Patches classified as security updates have a security bulletin ID (MSyy-xxx).

7. Product: The *Product* column helps identify the product category associated with a specific patch. If a patch is used across multiple operating system families (*i.e.,* Windows XP, Windows Server 2003, Vista, etc.), the product category isCommon Windows Component. Examples include Internet Explorer, Windows Media Player, MDAC, MSXML, and so on.

8. Language: The language associated with the patch location.

To find the URL to a missing path

1. Click the *KB Article* listed for the missing path.

2. Read through the knowledge base article and locate the download URL for the patch.

3. Click on the download link for your patch. If a different patch is available for each language, you will be prompted to select a language.

4. Select the appropriate language for the download, if applicable.

5. Click the *Download* link or button and download the patch file.

6. On your web browser, click the *History* icon to view your URL history.

7. Locate the file you just downloaded from your history list. Typically, the file will be in the *download.microsoft.com* domain.

8. Right- click the filename you just downloaded and select *Copy* from the menu. This copies the entire URL into your clipboard.

9. Return to the Patch Location page and:

   - Paste the URL into the *New Location* edit box.
   - Select the radio button to the left of the KB Article for which you are entering a new patch location.
   - Click the *Apply* button.