Patch Management Hands-on Exercise

Background Story

You have been hired as the lead IT Administrator at the Florida International University (FIU) to manage the computers at the School of Computing and Information Sciences (SCIS), the Machine Room (MR), the Green Library (GL), and the College of Engineering and Computing (CEC). As shown in Fig. 5.1, SCIS, MR, GL, and CEC are physically located in four buildings. SCIS maintains about 200 desktop workstations in its instructional lab, MR maintains about 5 servers, GL maintains about 50 open access guest desktops, and CEC maintains about 500 PCs and laptops. The exact number and configurations of computers are not well documented. Typically, the servers run Windows 2003 and the desktop workstations, PCs, and laptops all run Windows XP. Active Directory is implemented in one of the servers, named dc, and is assigned to all computers in SCIS and GL, but not to those in CEC. As the lead IT Administrator of the organization you are responsible for ensuring that all systems run efficiently with minimal disruption of computing services to the users.

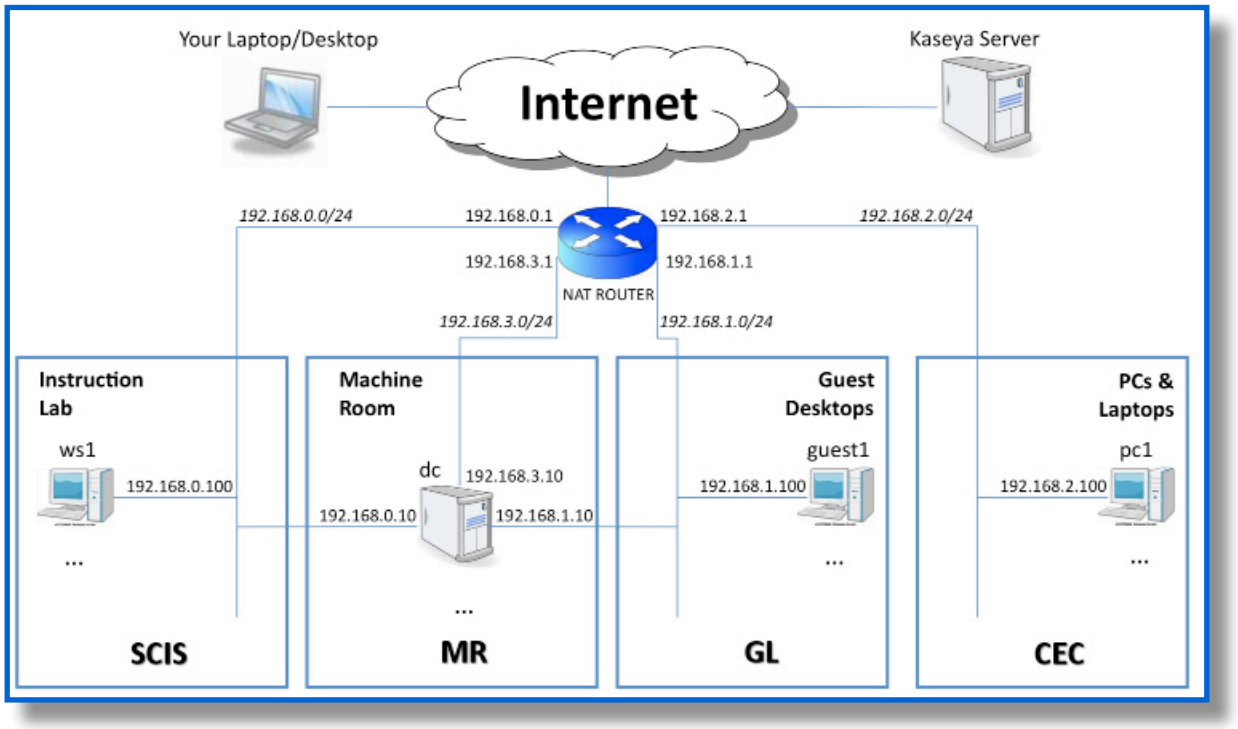


Fig. 5.26 A logical diagram of FIU's network.

You have decided to employ a Kaseya server to help you manage all computers at SCIS, MR, GL, and CEC. Your Kaseya server is now installed and is fully operational. In addition, you have successfully deployed agents on some of the machines under your management.

At this time, operating system patches are applied on an individual basis, one computer at a time, leading into a chaotic situation where 1) since all the computers are directly obtaining their updates from the internet, each patch is downloaded multiple times resulting in an artificially high network traffic, 2) unnecessary patches are being installed which in turn consumes large amounts of disk space, and 3) the potential for bugs and security risks are increased because it's unknown if all the computers are being patched on time, or if at all.

An organized and closely monitored method is needed to facilitate and monitor distribution and application of all necessary patches to the managed computers. Kaseya's Patch Management module will allow you to accomplish all these tasks and monitor patch activities.

Technical Information

Your dedicated virtual environment includes the computers and network devices depicted in Fig. 5.26 and further described below:

- NAT Router: 192.168.0.1 & 192.168.1.1 & 192.168.2.1 & 192.168.3.1
- SCIS: ws1.scis.fiu.edu - 192.168.0.100
- MR: dc.scis.fiu.edu - 192.168.0.10 & 192.168.1.10 & 192.168.3.10
- GL: guest1.gl.fiu.edu - 192.168.1.100
- CEC: pc1.cec.fiu.edu - 192.168.2.100 & laptop1: laptop1.cec.fiu.edu - 192.168.2.200

Note: This virtual environment includes only a limited number of representative servers and workstations physically housed in the four buildings.

Exercise

It is now time to implement policies that will keep the computers updated and avoid potential security risks by having non-patched computers within the environment. Setting up Kaseya to scan all the computers, with agents, will allow the VSA to keep a detailed record as to which patches have been installed. This detailed information will lead into informed enforcement of patch policies that which patches to automatically install (for example all security patches) and which patches to apply only after obtaining user approval (for example all optional patches). You also would like to configure Kaseya to download the patches from one central server to save bandwidth and decrease redundant network traffic. To be prepared for future deployment of computers, it would be best to set the policies to the agent templates.

Part 1

To keep an accurate record of all the patches installed on each computer, it would be best to schedule a scan, through Kaseya's VSA, to all the computers. While this is not a heavy process, it would still be best to schedule the scan during a time when the computer is otherwise idle.

-Using *Scan Machine*, schedule a scan to run every day at 3:00am on all the agent templates.

1. Open the Patch Management module. Go to *Manage Machines* > *Scan Machine*.

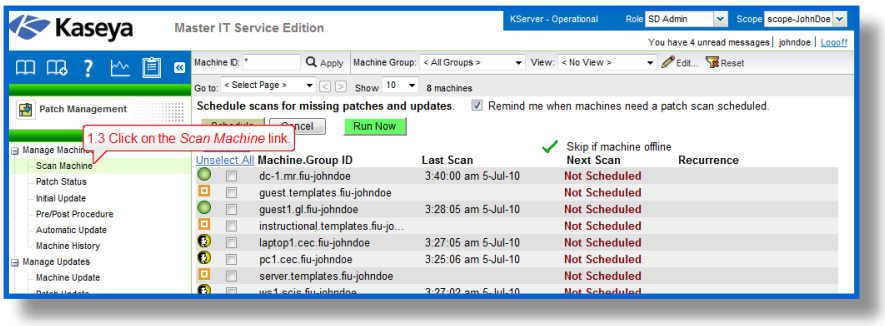
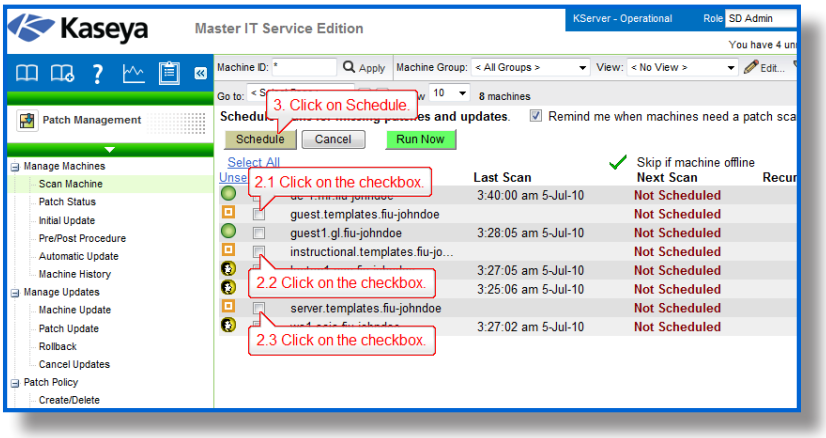


Fig 5.27

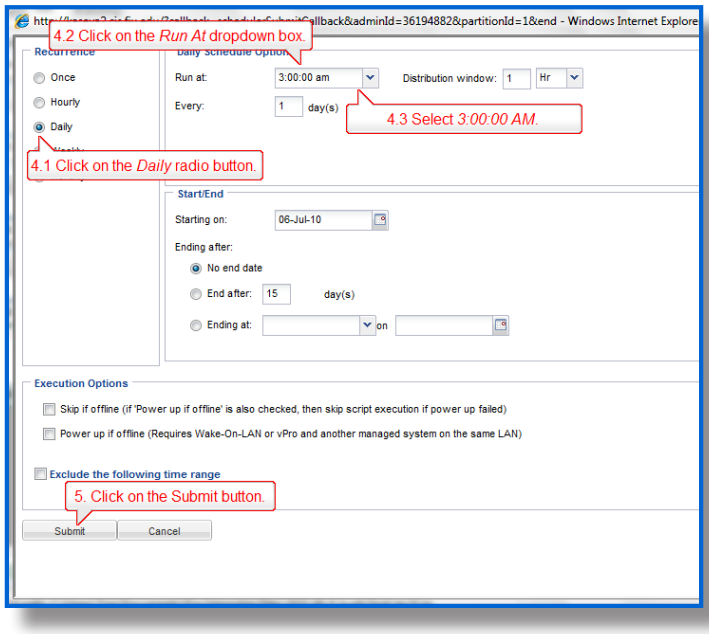
2. Select all the agent templates.
3. Click on the *Schedule* button.

Fig 5.28



4. Set the scan to run *Daily* at *3:00am* with a Distribution window of 1 hour.
5. Click on *Submit.*

Fig 5.29



Part 2

Policies are like templates in which you can approve/deny a group of patches, or an individual patch. Two policies can be created, one for all the XP machines and the other for the Windows 2003 Server machines. The policies should automatically apply all Security Updates by default on all machines and the optional updates should be set to Pending Approval. Once the patch policies are created and configured, they can be set within the designated agent templates.

Note: We are creating a W2K3 template since we only have Windows 2003 in our environment. Of course, if there are Windows 2008 servers or other servers in the environment, it would be better to name the policy for all the Windows servers as just “Servers”, and for all workstations as just “Workstations”.

- Create a patch policy, W2K3-PM-Policy-***<USERNAME>***, and set it to apply all future Security Updates by default. Everything else should be set to *Pending Approval*. Use a filter to deny patches that are optional and have not been superseded by other updates.

6. Open the Patch Management module. Go to *Patch Policy* > *Create/Delete*.
7. Type “W2K3-PM-Policy-***<USERNAME>***” under *Enter name for a new patch policy.*
8. Click on *Create.*

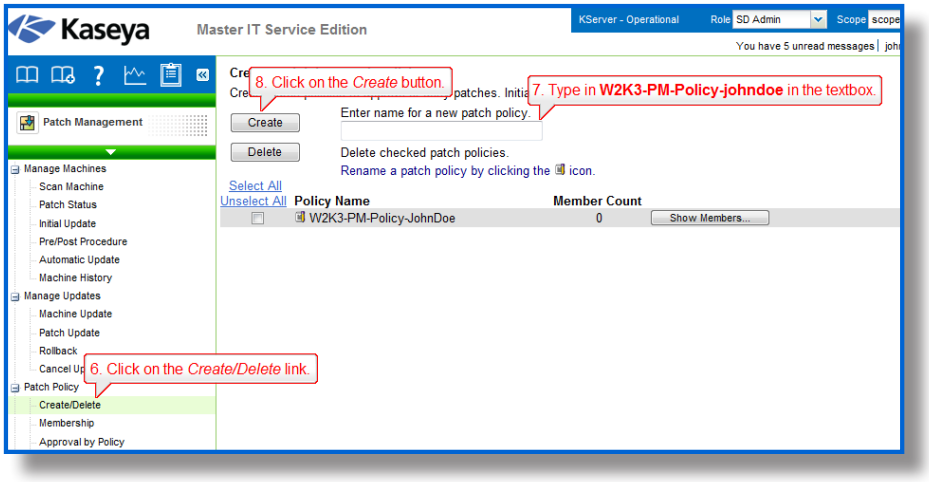
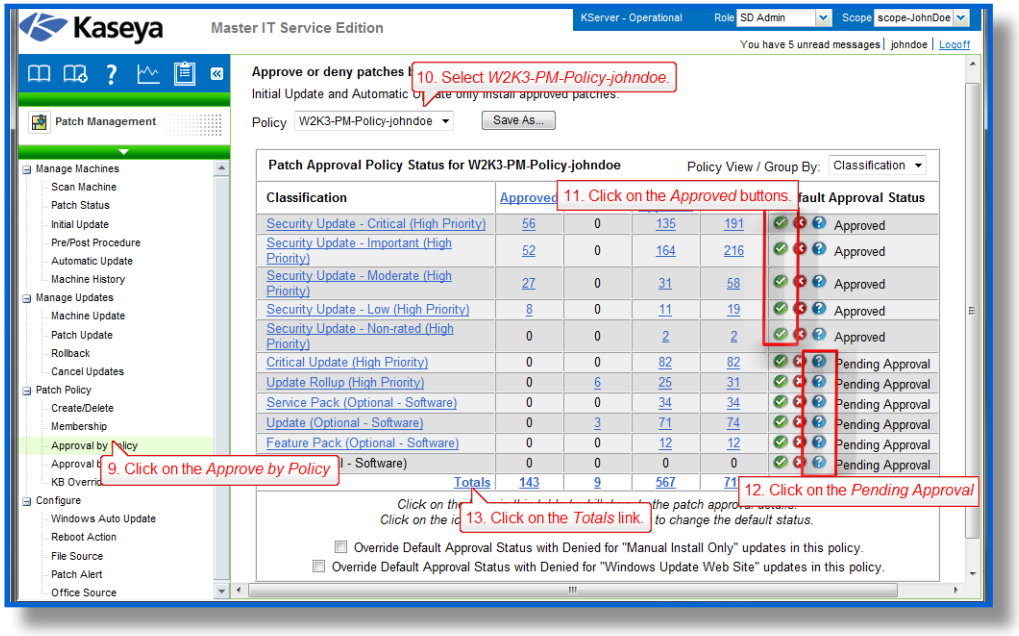


Fig 5.30

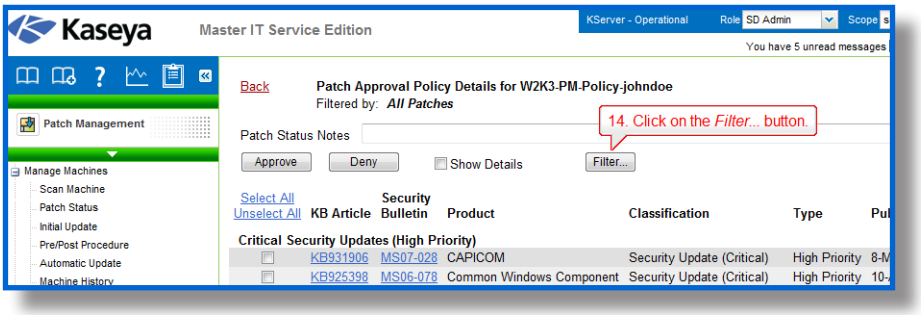
9. Go to *Patch Policy* > *Approval by Policy.*
10. Select “W2K3-PM-Policy-***<USERNAME>***” under the *Policy* dropdown list.
11. Click on the green checkmark for all the *Security Update* rows. The Green checkmark is under the column *Default Approval Status*.
12. Make sure the other rows’ *Default Approval Status* is set to *Pending Approval*.
13. Click on *Total* at the bottom of the table. A new page will load up.

Fig 5.31



14. Click on *Filter...* A new window will open up.

Fig 5.32

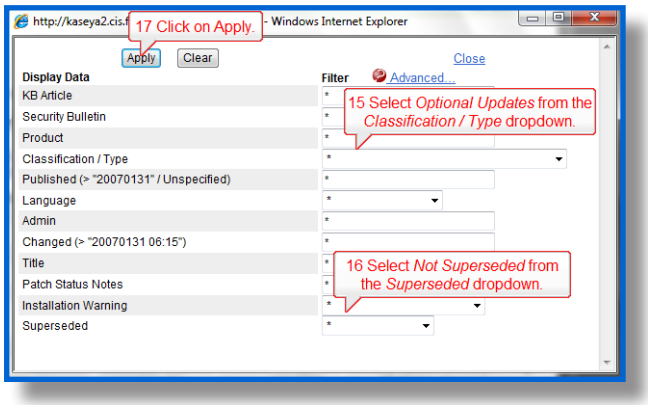


15. Select *Optional Updates* from the *Classification / Type* dropdown.

16. Select *Not Superseded* from the *Superseded* dropdown.

17. Click on *Apply.*

Fig 5.33



18. Click on *Select All*.
19. Click on *Deny*.

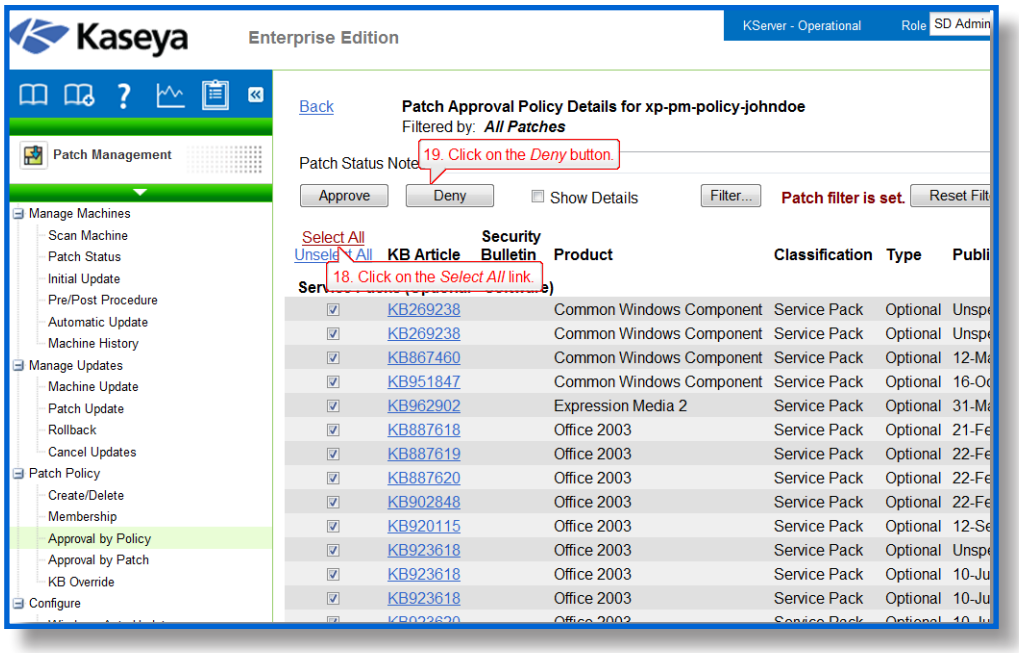


Fig 5.34

- Create a patch policy, XP-PM-Policy-***<USERNAME>***, and set it to all future Security Updates by default. Everything else should be set to *Pending Approval*.

20. Open the Patch Management module. Go to *Patch Policy* > *Create/Delete*.
21. Type "XP-PM-Policy-***<USERNAME>***" under *Enter name for a new patch policy.*
22. Click on *Create.*

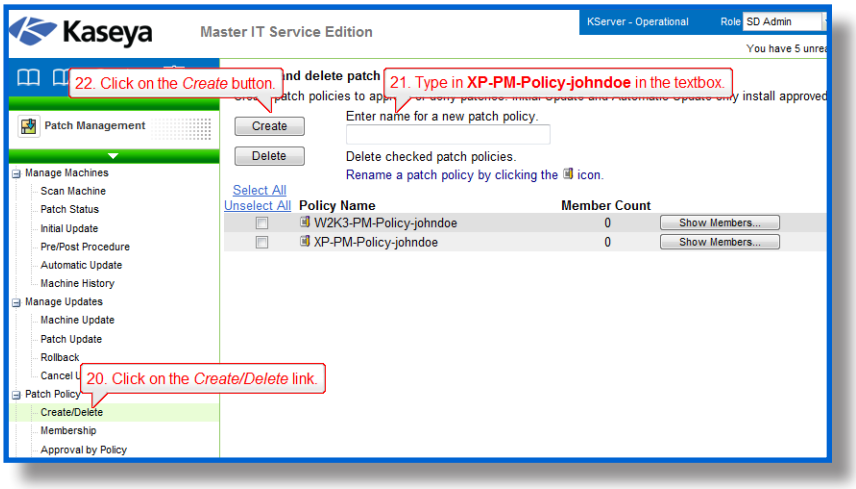


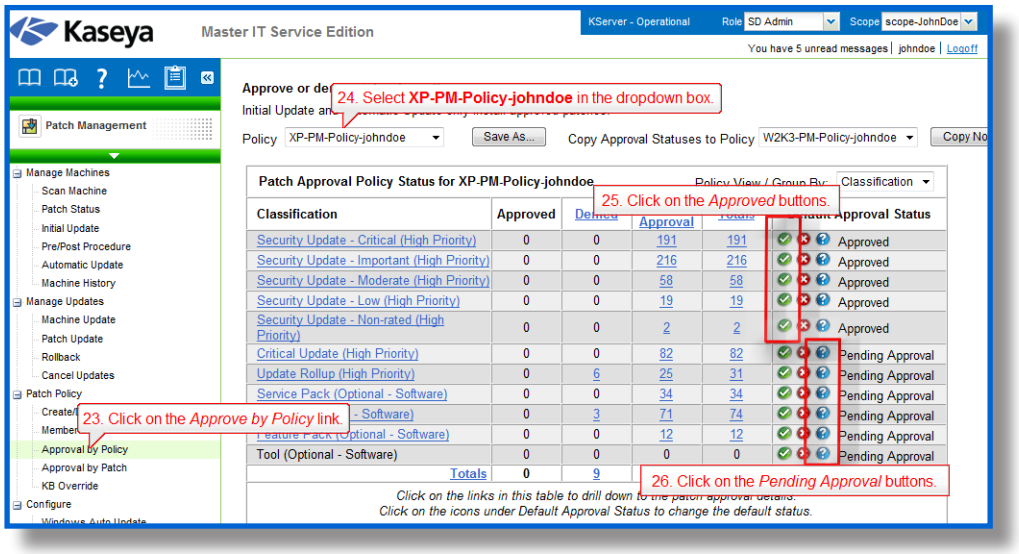
Fig 5.35

23. Go to *Patch Policy* > *Approval by Policy.*
24. Select "XP-PM-Policy-***<USERNAME>***" under the *Policy* dropdown list.

25. Click on the green checkmark for all the *Security Update* rows. The Green checkmark is under the column *Default Approval Status*.

26. Make sure the other rows' *Default Approval Status* is set to *Pending Approval*.

Fig 5.36

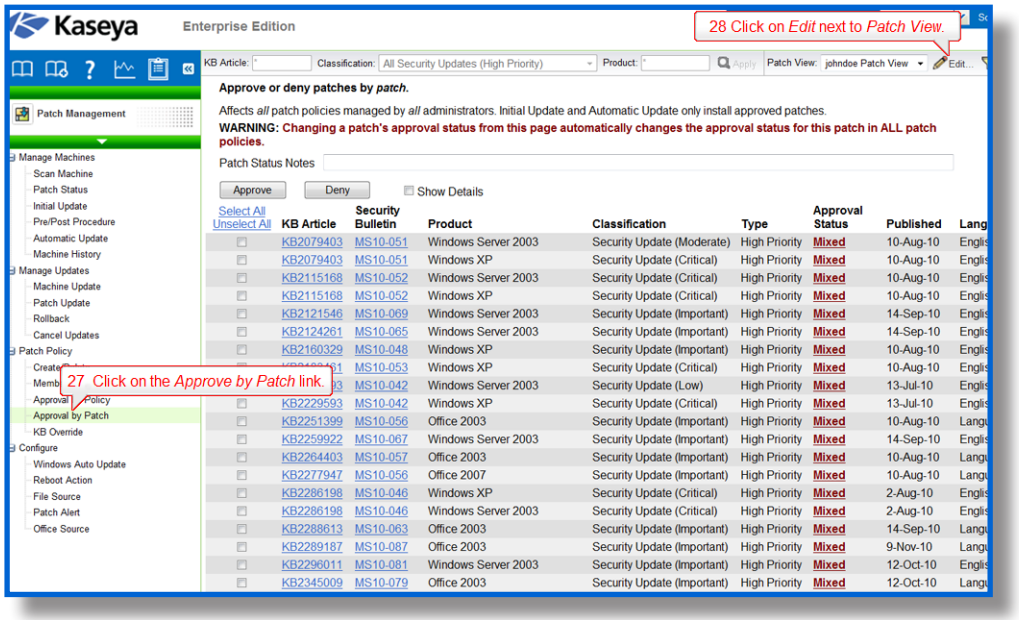


-Approve all Security Updates that have been released already for all patch policies.

27. Open the Patch Management module. Go to *Patch Policy* > *Approve By Patch*.

28. Click on *Edit* next to *Patch View*. A new window will open up.

Fig 5.37



29. Select *All Security Updates (High Priority)* from the *Classification / Type* dropdown.

30. Select *Not Superseded* from the *Superseded* dropdown.

31. Type "<***USERNAME***> *Patch View*" in the *View Name* textbox. Click on *Save.*

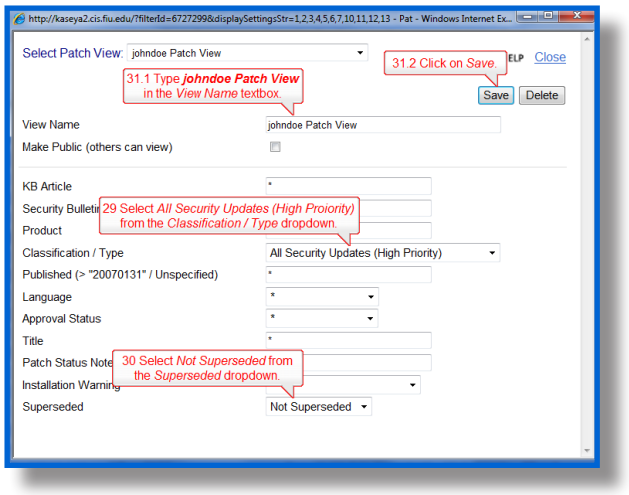


Fig 5.38

32. Click on *Select All*.

33. Click on *Approve.*

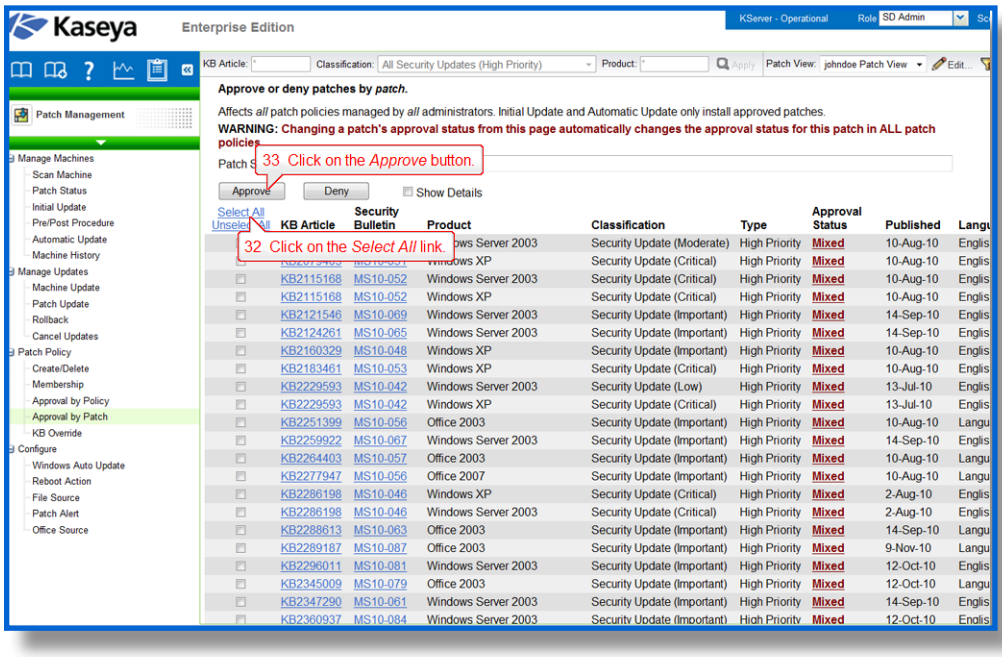


Fig 5.39

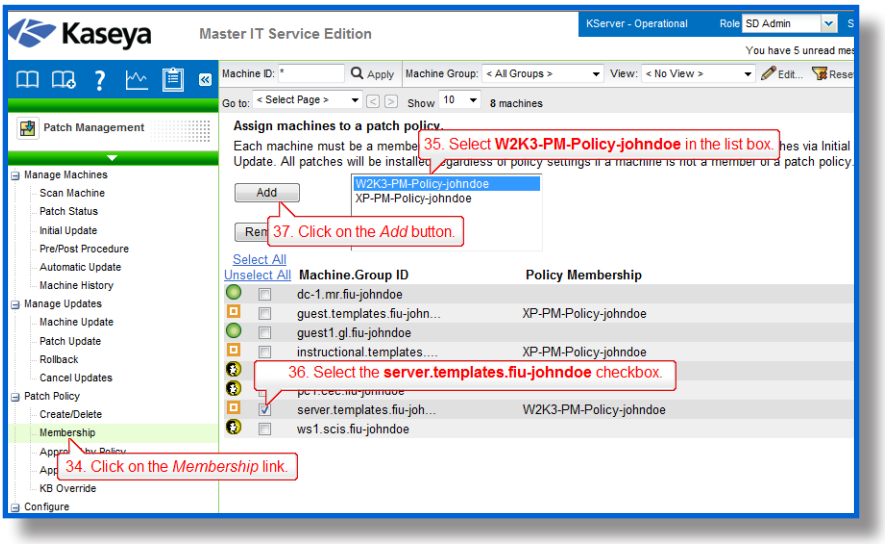
-Set the *Policy Membership* of W2K3-PM-Policy-***<USERNAME>*** to the Server machine template then set the *Policy Membership* of XP-PM-Policy-***<USERNAME>*** to the Instructional and Guest templates.

34. Open the Patch Management module. Go to *Patch Policy* > *Membership.*

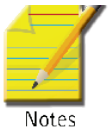
35. Select "W2K3-PM-Policy-***<USERNAME>***" in the list box.

36. Select the checkbox next to “server.templates.fiu -<***USERNAME***>”.
37. Click on *Add.*

Fig 5.40



38. Repeat steps 34-37 for the Instructional and Guest templates.



Note: This is only one way of setting up Patch Management. The number of different configurations are endless and you should set it up to best fit your needs. There is no “right way” of setting up Patch Management, only efficient or inefficient ones.

Part 3

Downloading all the patches to a file server and distributing it to all the machines on network will allow you to save bandwidth. Configure all the templates to pull from the file server using the UNC path “\\dc\PatchTemp” from the DC, then set the temporary directory to “C:\PatchTemp” on the dc server. The UNC path is used to point to the local address, on the DC, where the patch files are stored. If the computer cannot access DC, it should then download from the internet.

-Using File Source set up all the machines so that they download their updates from the DC. If the DC is unreachable, the machine should then download it from the Internet. The UNC path should be “\\dc\PatchTemp” while the local directory should be “C:\PatchTemp”.

39. Open the Patch Management module. Go to *Configure* > *File Source.*

40. Select all the agent templates.
41. Select *Pulled from file server using UNC path.*
42. Type “\\dc\PatchTemp” next to *Pulled from file server using UNC path*.
43. Select “fiu-**<USERNAME>**.mr” next to *Machine Group Filter.*

44. Select “dc.mr.fiu-***<USERNAME>***” next to *File share located on.*

45. Type in “C:\PatchTemp” next to *in local directory*.

46. Select the *Download from Internet if machine is unable to connect to the file server checkbox*..Click on *Apply.*

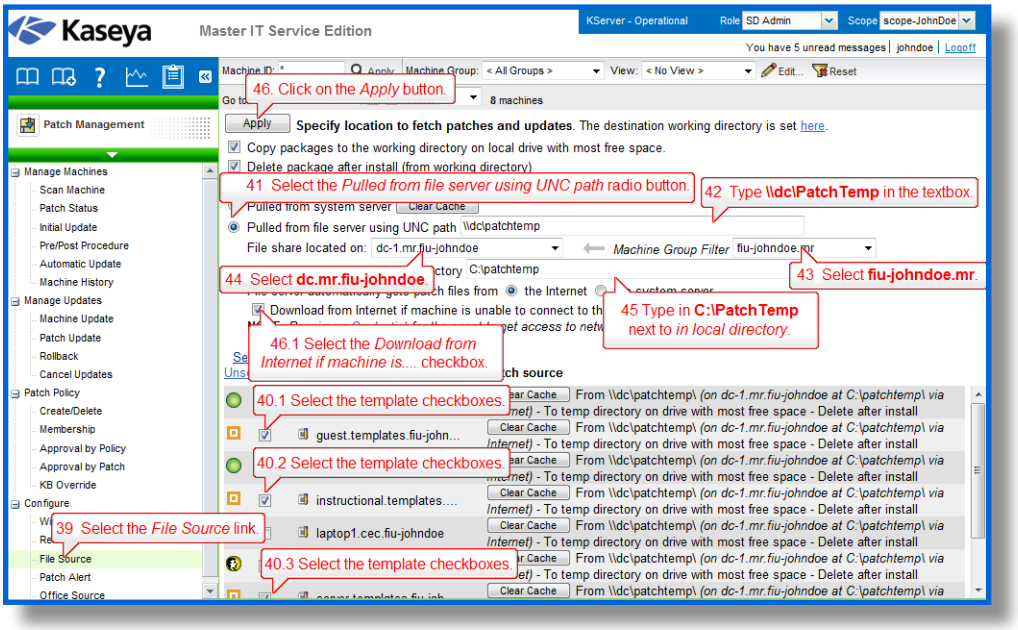


Fig 5.41

Part 4

Certain updates require the Windows OS to restart to finish installation. It would be best to set up the XP machines so that they restart only when a user is not online. As for the server machines, set up an email notification so that you can plan the restart and notify in advance the users of the server maintenance.

-Use Reboot Action to set the Guest and Instructor templates to Skip reboot if user logged in immediately after applying new patches and updates. Then, set the Server template to notify you immediately, via email, when a reboot is required after applying new patches and updates.

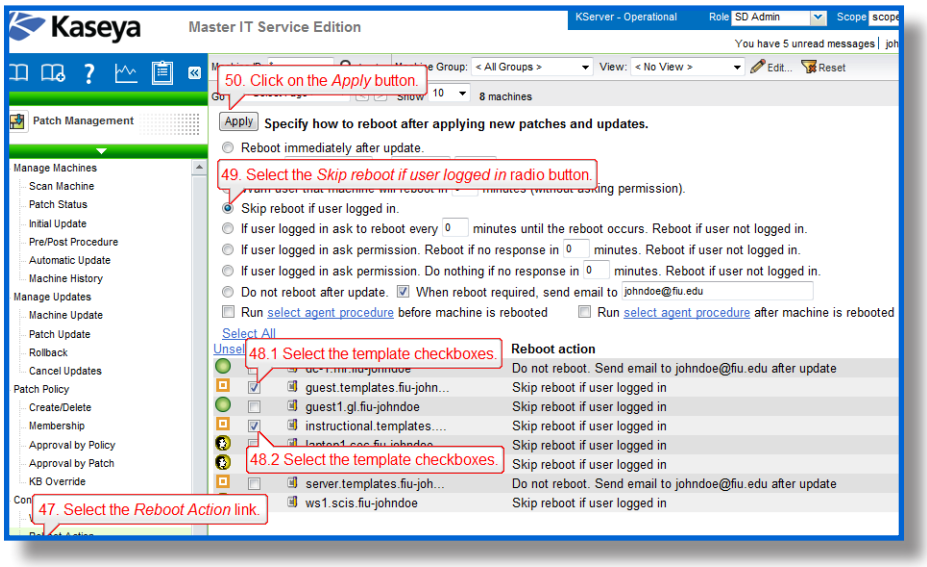
47. Open the Patch Management module. Go to *Configure* > *Reboot Action.*

48. Select the Guest and Instructor templates.

49. Click on *Skip reboot if user logged in*.

50. Click on *Apply.*

Fig 5.42



51. Repeat steps 47-50 for the Server template. Set the Server template to send the reboot notification to your personal email.


Notes

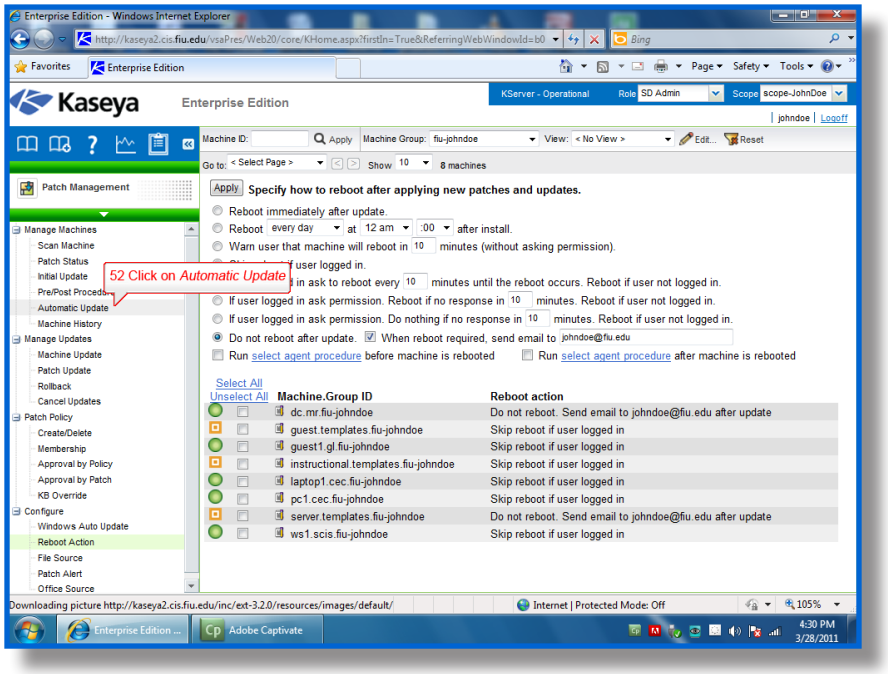
Note: Setting to *skip* reboot means it may take longer for the patch to take effect, thus increasing the risk of vulnerability. Therefore, it is best if all the instructional computers would be set to reboot at night automatically after an install, since these are not real user machines and we do not worry about losing open files. However if the target machines were end user machines, the best policy would be to set the workstations to "ask" and reboot if not logged in.

Part 5

Now that we have setup the patch policies to our liking, we need to setup Kaseya to apply the patches automatically to the machines.

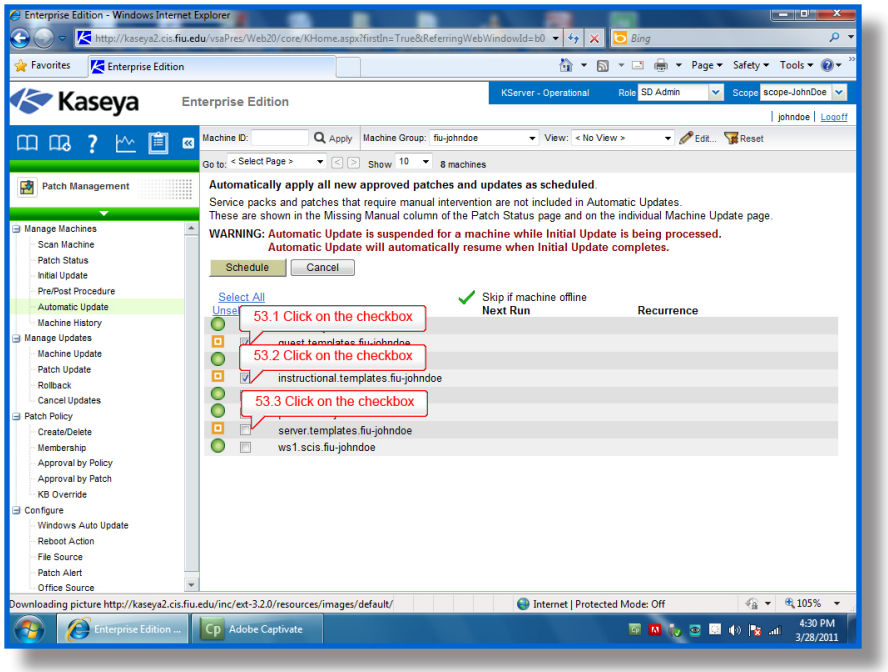
52. Open Patch Management module. Go to Manage Machines > Automatic Update.

Fig 5.43



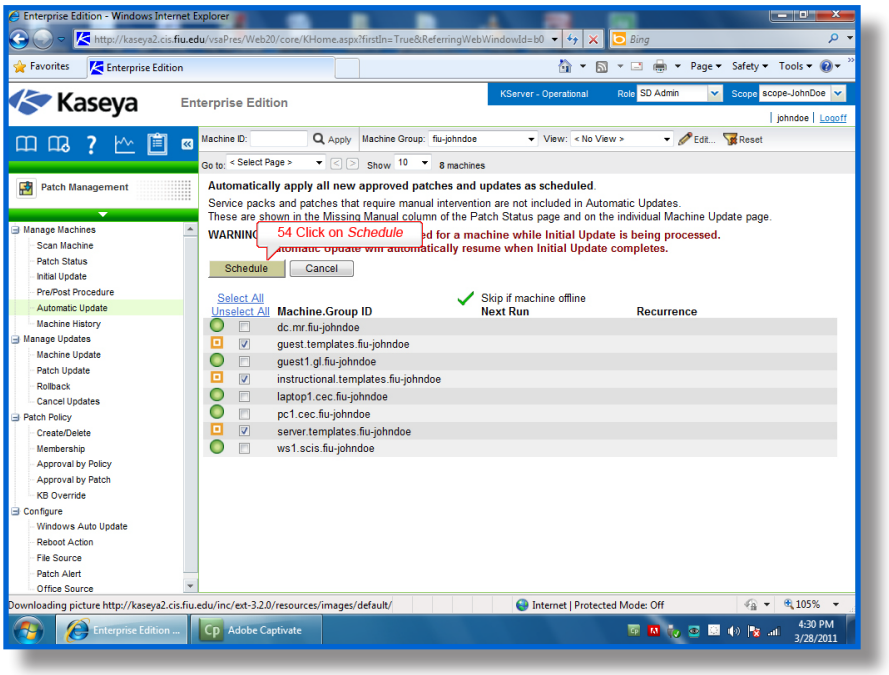
53. Select all the template agents in the list.

Fig 5.44



54. Click on Schedule

Fig 5.45

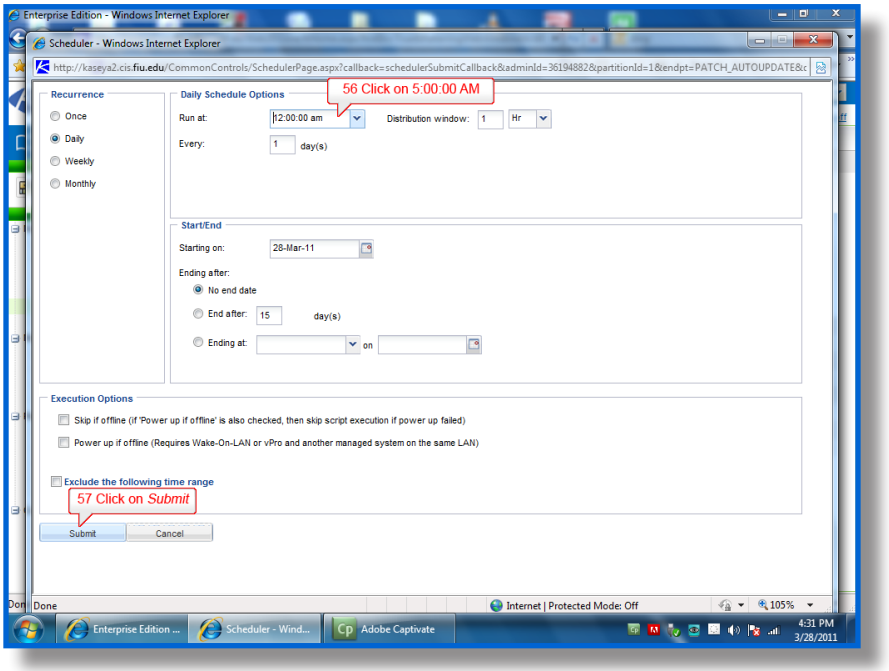


55. Click on Daily

56. Set the run time to 5:00 AM with a distribution window of 1 hour.

57. Click on Submit

Fig 5.46



Part 6

Now that all three agents templates contain all the patch management settings, it is time to push the settings captured in the templates to all the currently deployed agents with the similar roles.

-Copy the settings from the templates to the specified computers on the network. Server template will be used for the MR building. Instructional template will be used for the SCIS and CEC buildings. Guest template will be used for the GL building.

58. Open the Agent module. Go to *Configure Agents* > *Copy Settings*.
59. Click on *select machine ID* link and a new window will open up.

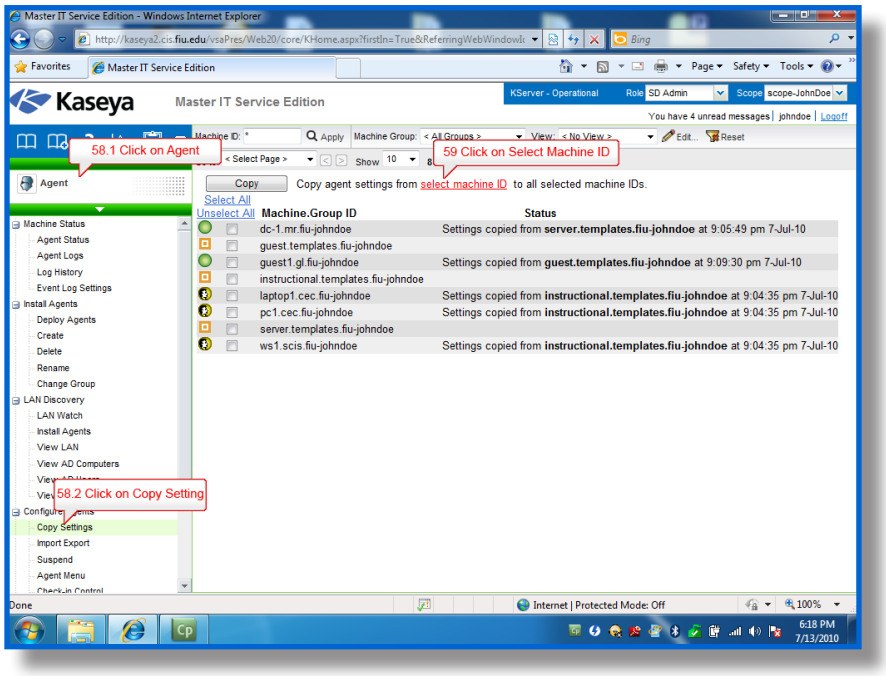
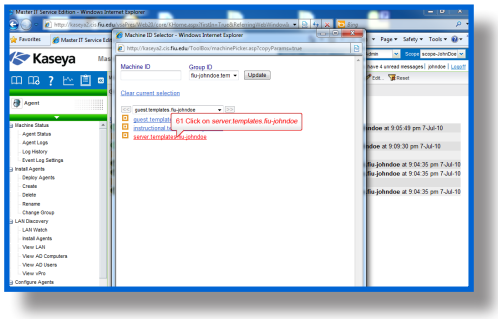


Fig 5.47

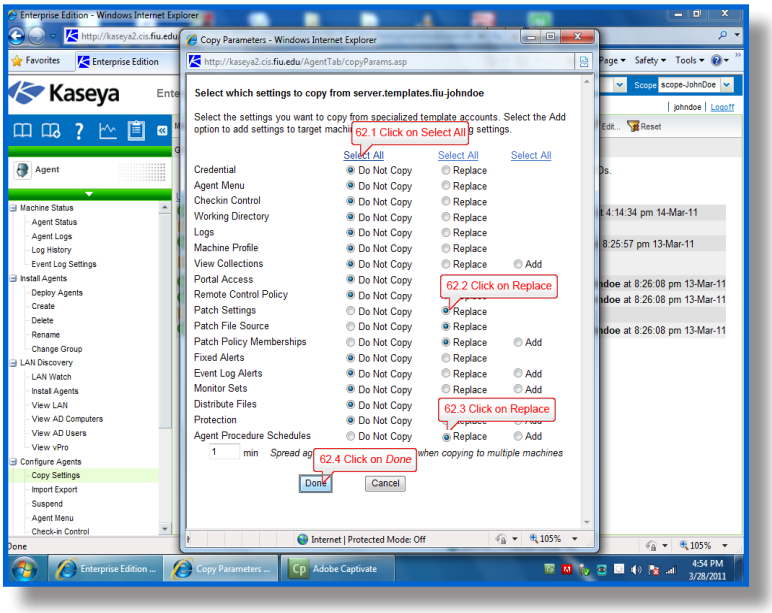
60. Select “fiu-<***USERNAME***>.templates” from the *Group ID* dropdown list.
61. Click on “Server” from the list of templates shown.

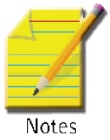
Fig 5.48



62. Click the Select All under the Do Not Copy column and then select replace for Patch Settings, Patch File Source and Patch Policy Memberships, Agent Procedure Schedules and click on *Done*.

Fig 5.49





Note: When you have a schedule in Agent Procedures activity on an agent template, you need to make sure *Agent Procedure Schedules* is selected in copy settings.

63. Select all the computers in the MR building and click on the *Copy* button.

64. Repeat steps 52-57 for the Instructional and Guest templates.

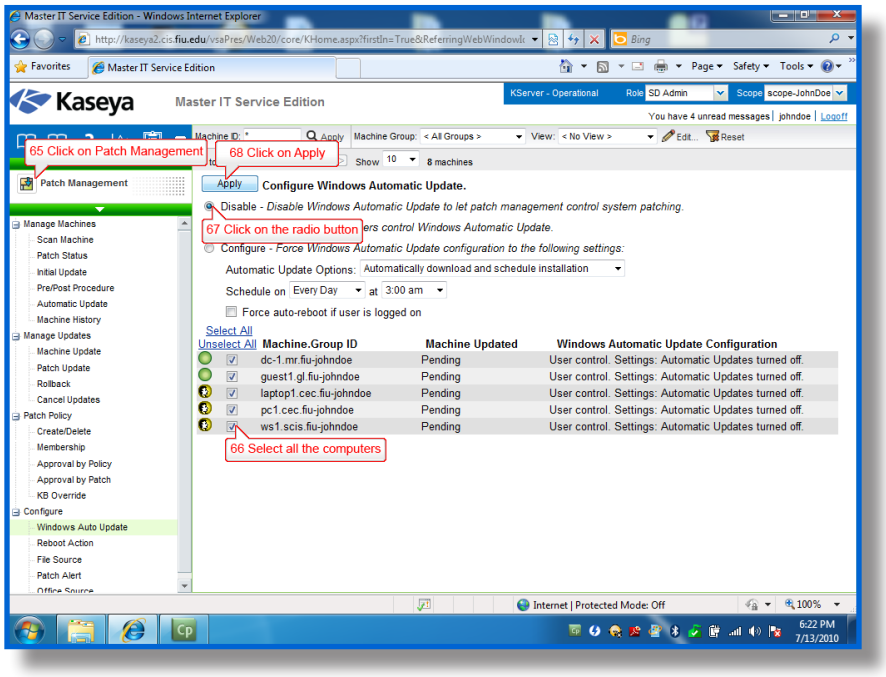
Part 7

Windows Automatic Update can interfere with the functionality of Kaseya's Patch Management and must be disabled. While Kaseya allows you to disable Windows Automatic Update from within the Patch Management module this option cannot be implemented in a template and must be implemented by selecting agent(s) that check in.

-Disable Windows Automatic Update for all computers.

65. Open the Patch Management module. Go to *Configure* > *Windows Auto Update*.
66. Select all the computers.
67. Select *Disable – Disable Windows automatic Update to let patch management control system patching*.
68. Click on *Apply*.

Fig 5.50



Note: If the checkboxes are missing, please wait 5-10 minutes and refresh the page as the Patch Scan is not completed yet. Checkboxes will not display for any machine that either has an operating system that does not support Windows Automatic Updates, or for which an initial Scan Machine has not been completed.

Part 8

Microsoft has just released a new KB article and it entails a new version of Internet Explorer; however, management has asked you not to install it and to prevent future installations of it via Windows Updates. KB Override is the best choice to accomplish this task since it will override all current patch policies and future patches. Using KB Override prevent Internet Explorer from being installed using the KB article (KB944036).

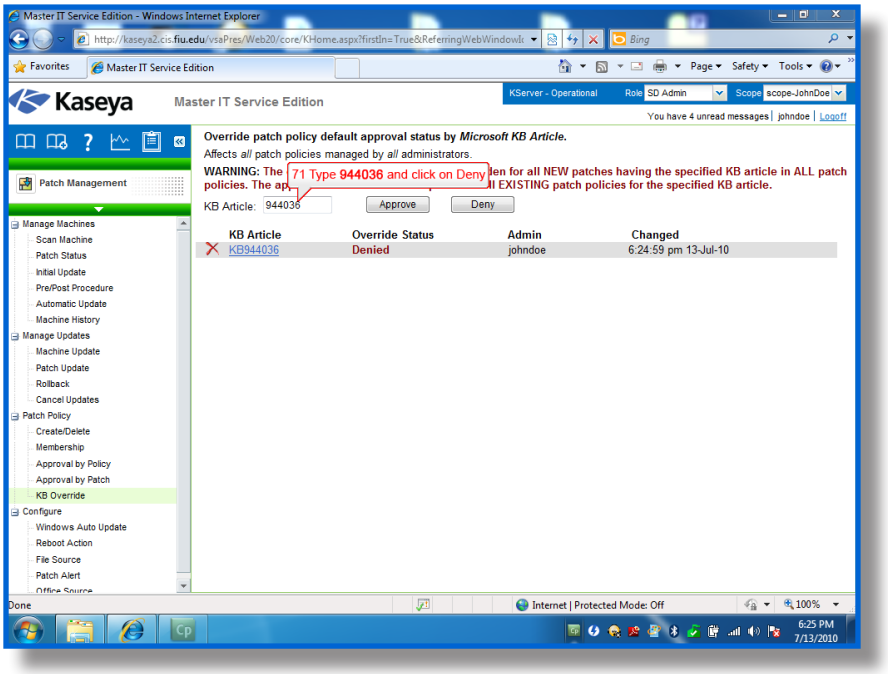
-Prevent Internet Explorer from installing by using *KB Override*.

69. Open the Patch Management module. Go to *Patch Policy* > *KB Override*.

70. Type in “944036” in the *KB Article* textbox.

Fig 5.51

71. Click *Deny*.



Note: If this patch has already been denied, it means that another administrator who shares this Kaseya server with you have already performed this task. If this is the case, you can first remove it, by clicking on the X icon, and add this setting by going through the above steps. This way, you will make sure that your work is reflected in the system logs for future reference.

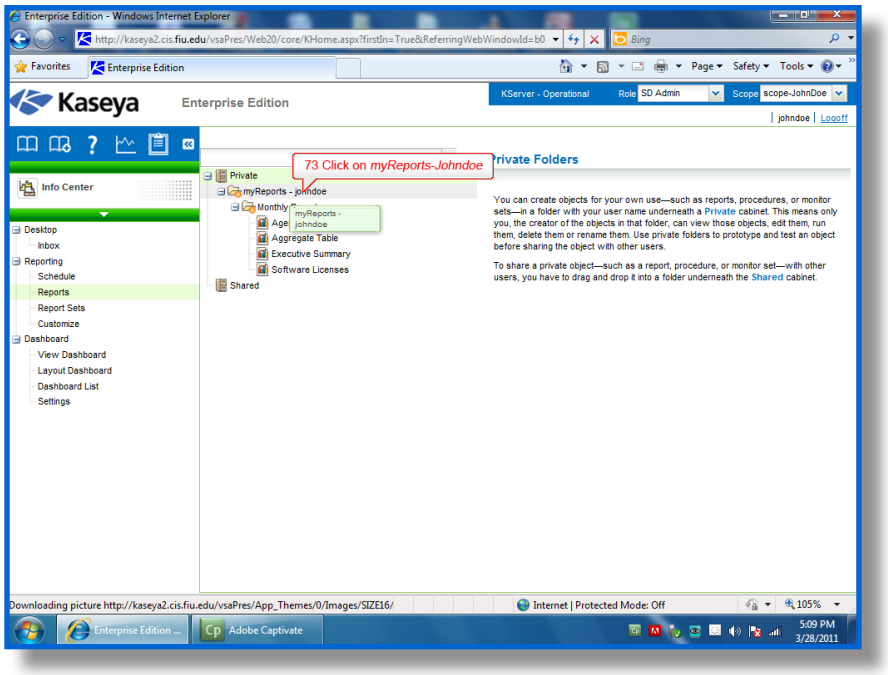
Part 9

Management still needs the patch management report by the end of the work day. The patch management report should contain a brief overview of the patches. To accomplish this, you will rely on the Info Center module to generate a patch management report.

72. Open the Info Center module. Go to *Reporting* > *Reports*.

73. Click on your Private folder, “myReports-<***USERNAME***>”, choose *New Report* and a new window will open up.

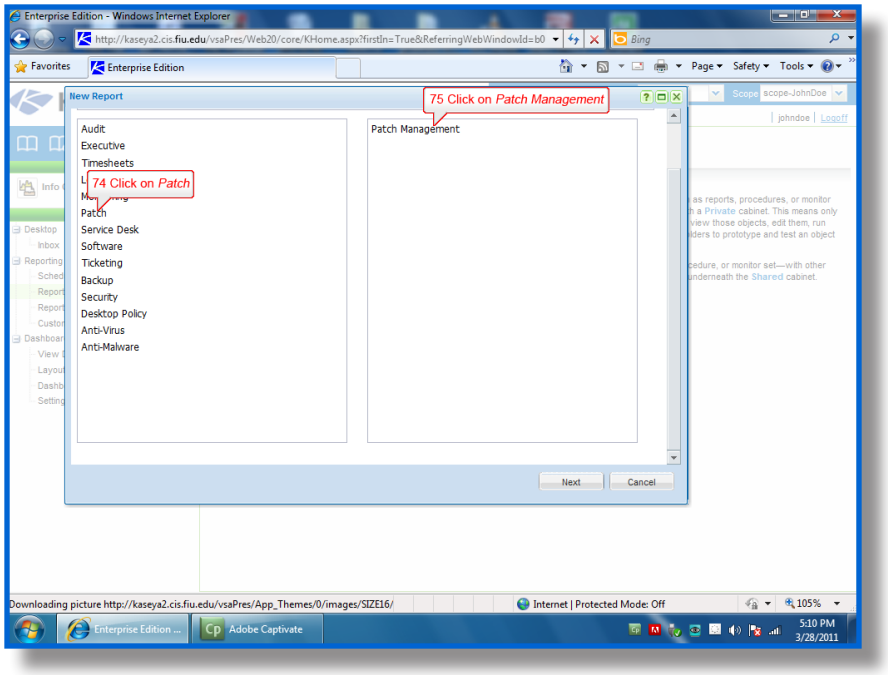
Fig 5.52



74. Choose *Patch* in the left column.

Fig 5.53

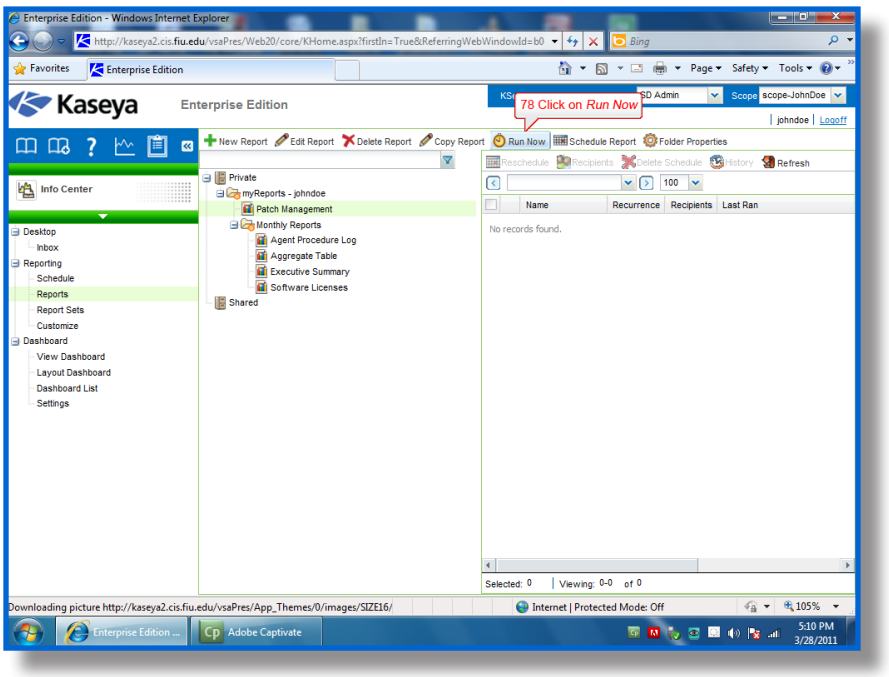
75. Choose *Patch Management* report template.



76. Click *Next*.

77. Leave all the default options and choose *Save*.
78. Select the newly created report under your folder then choose *Run Now*.

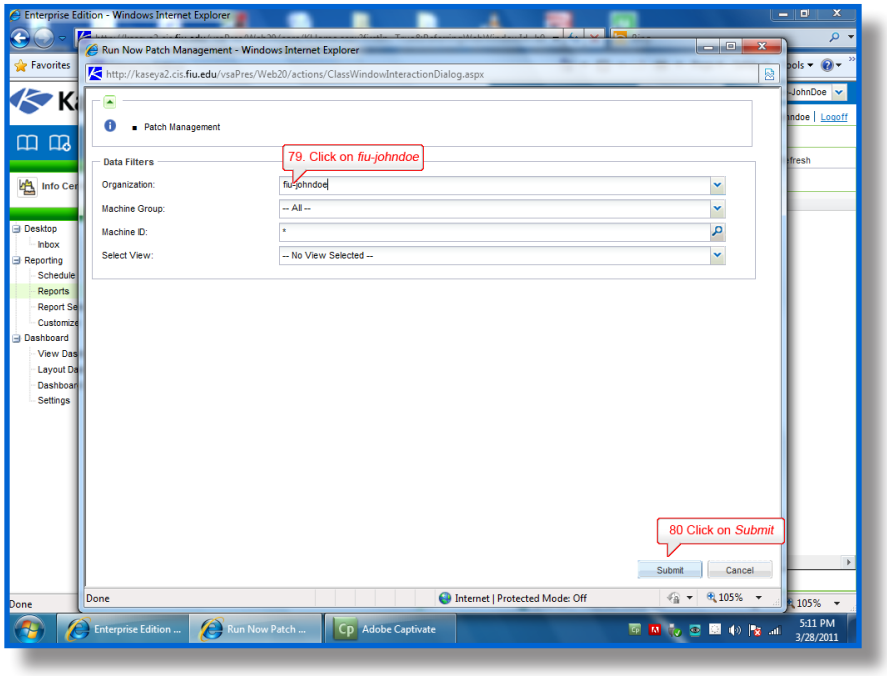
Fig 5.54



79. Choose "FIU-<***USERNAME***>" next to *Organization* in the new window.
80. Click on *Submit*.

Fig 5.55

81. Once the scheduled report is done, the report will open automatically.



Note: Use the report to check and see if the audit ran successfully. The report can be printed out for record keeping; however, this is not necessary for this exercise.

Notes

Note: If your report comes out incomplete, wait 15-20 minutes before running it again. This is due to the patch scan not being completed in time.

Notes