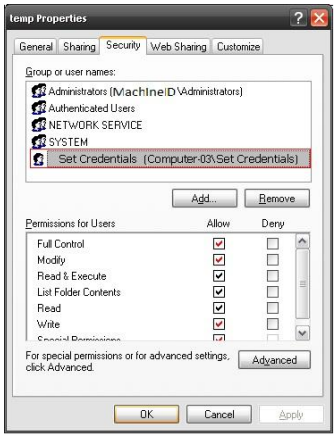
Kaseya: Patch Management Best Practices

Working (Temp) Directory permissions:

Setting the correct permissions on an endpoint is a must. The permissions that are needed for a successful patch is as follows:



If Set Credentials are used, the account must be a member of the Local Administrators Security Group and have explicit membership to the Working (temp) Directory. It cannot just be a member to the Local Administrators Security Group. Set Credentials, under Agent, must pass and so must the Patch Test on the Patch Status page.

If you set the File Source under Patch Management to download 'To temp directory on drive with most free space', you must verify that the Set Credential permissions to all other Working Directory folders on the partitions exist. Whether Set Credentials is used or not, you must still add System and Network Services accounts to the temp folder with full write access.

*NOTE: Do not us Windows protected folders: Neither Microsoft recommend nor Kaseya supports using these locations (e.g.: [Drive]:\Windows\, [Drive]:\Program Files\, [Drive]:\Documents and Settings\ but especially [Drive]:\windows\system32\.

Scan Machine:

On the Scan Machine page, patch scans can be scheduled to search for missing patches on selected managed machines.

Microsoft typically releases security/critical updates on the second Tuesday of each month (Patch Tuesday) and non-security/non-critical patches on the third and/or fourth Tuesdays of each month. (Occasionally security updates are released more often.)

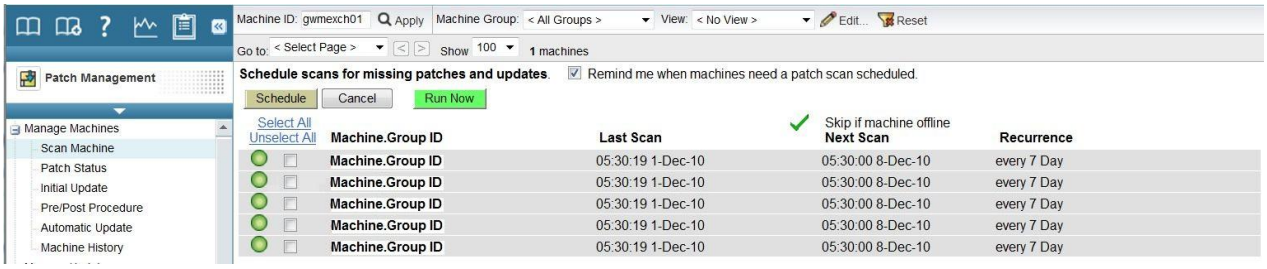
With that in mind, it's usually not necessary to run patch scan more than once a week. (For weekly patch scans, it is recommended to schedule scans on late Tuesdays or Wednesdays to be able detect new patches as soon as they are available.)

However, there are occasional out-of-band security updates. In order to detect these update as soon as they are available, daily patch scan is recommended. Note that the scan results are only processed if the results have

actually changed. So while there's a load caused by running scans on machines, there's typically little or no load for processing scan results since results will only change 3~4 times a month.

When scheduling scans on a large group of machines, stagger feature (for K1) or distribution window (for K2) should be used to distribute the load on the kserver especially following Patch Tuesday.

Also, since patch scan runs silently (no reboot required), it is not necessary to set the "Skip if machine offline" flag. This is important especially for machines with non-daily scans. (Consider weekly patch scan on Tuesdays and automatic update on Wednesdays scenario. If a machine went offline on Tuesday and online Wednesday, automatic update will not install any new patches published the day before if “Skip if machine offline” flag is set for patch scan since patch data would be at least a week old.)



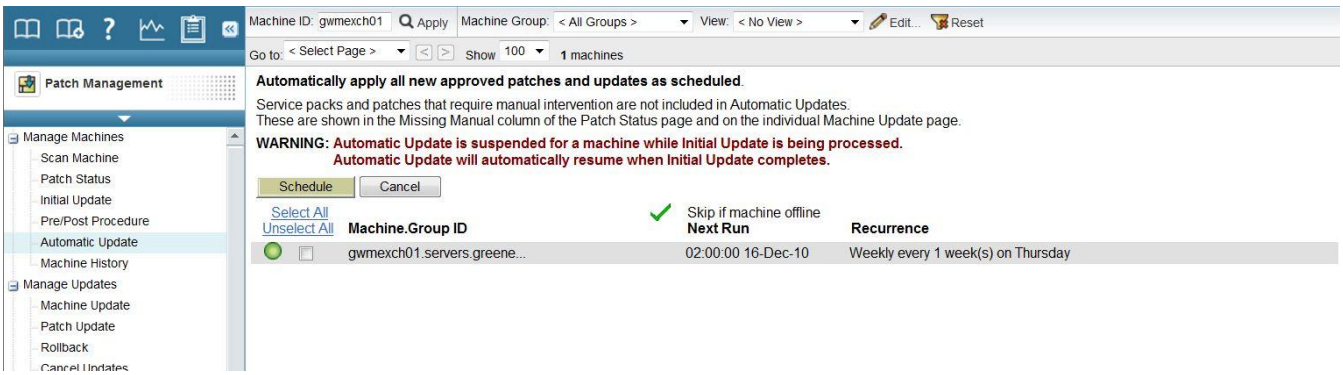
Automatic Updates:

Automatic Update (AU) should be used to apply Microsoft patches on a recurring basis. AU schedule depends on how patch scan is scheduled on the machine.

For machines with weekly scans, it is recommended to run Automatic Update weekly following patch scan. (ie. If the scan is scheduled on Tuesdays, automatic update can be scheduled on Wednesdays.)

For a machine with daily scans, daily automatic update should be scheduled following patch scan. (Note: Applying patches requires a reboot.)

When scheduling scans on a large group of machines, stagger feature (for K1) or distribution window (for K2) should be used to distribute the load on the kserver especially following Patch Tuesday.



Patch Policy:

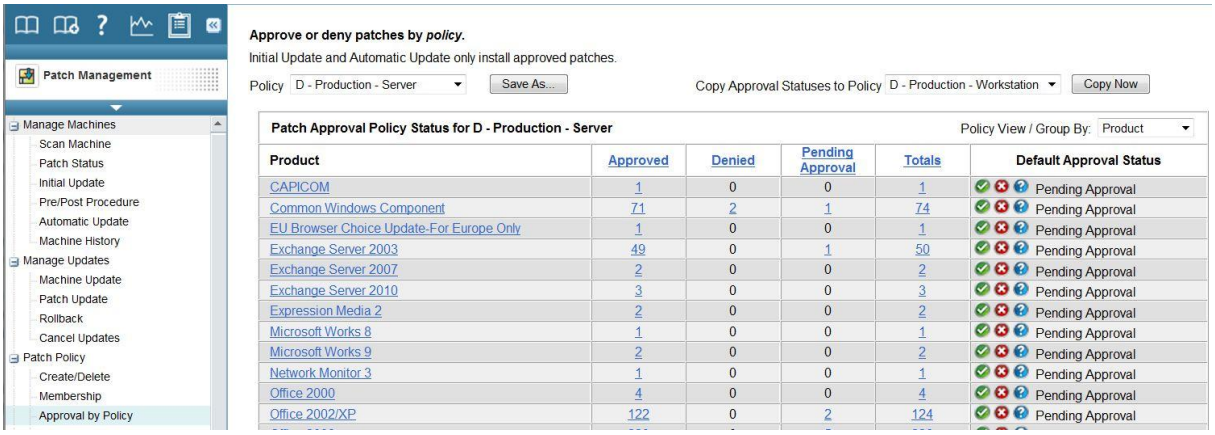
Patch Policy defines approval status of all active patches. Automatic Update (as well as Initial Update) will only install approved patches defined in the approval policy that the machine belongs to. (Note that machines that are not a member of any patch policy will install all missing patches.)

It's recommended that the default approval status for **Security** and **Critical updates** are set to *approved*. This will ensure that all security/critical updates get installed on machines as soon they are published.

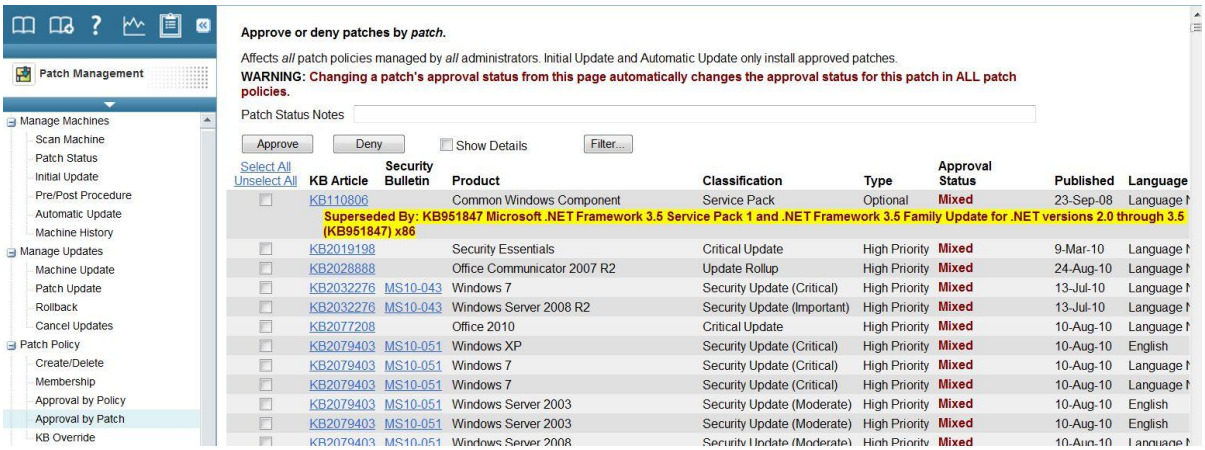
That said, we recommend that the default approval status for **Service Packs** be set to *denied*. This will exclude service packs being installed as part of recurring automatic updates. Service packs are usually very large in size so takes a long time to download and install. Also, they often cause failures due to various reasons (eg. Managed machines might not have enough disk space. Service packs might have prerequisite requirements.) Service packs can be installed using either Patch Update or Machine Update.

For all other classification, default approval policy can be set to *pending approval*.

To further granulate the patch management, you can approve or deny application patches by switching the view using *Policy View/Group By* dropdown.



Note that if a machine is a member of multiple patch policies and those policies have conflicting approval statuses, the most restrictive approval status is used. On the *Approval by Patch* page, a patch with different approval statuses among policies will show approval status of *Mixed*. On K2, approval status is a clickable link that pops up a window with a list of patch policies and approval status that the patch belongs to.



Patch deployment process

Machine Scan will scan the endpoint machine to see what patches apply to it based off what is discovered using Legecy scan/ WUA (WUA uses the Microsoft Update Catalog). Patch Mgmt will take that information and remove the patches that are denied in Patch by Policy. Automatic Updates will then schedule the patch installs. Once the install schedule runs WUA Patch Scan 1 script will run to see what is installed. The install script for the patch will then pull the patch from the File Source and save to the Working(temp) directory using the Set Credentials/System account. Once the patch finishes, if the reboot action restarts the system a WUA Patch Scan 2 script will scan the machine and verify the patch install. It will then write the results to the Patchscn.xml or Ptchscan2.xml in the Working(temp) folder and report the results to Patch Management. Patchscn.xml is the file used by the Kaseya legacy scan. Ptchscan2.xml is the file Patch saves all the patch install information (success, fail).

Initial Updates

When this is initiated the process will continue until all patches are deployed. Reboot Action will be ignores and if a reboot is required then the system will reboot and continue with the next patch. This assumes that the patch installed and reports correct. If a patch fails then the process will repeats until the patch reports installed. If a machine is powered off then this can further delay the complete patching of the system. Often users will report that a system rebooted for no reason that they can see and will report that there was no warning. Also, the user will not be able to delay the reboot.

Patch approval status

Whenever a patch is release by Microsoft whether it is a new or older patch if the installer, Update ID or other areas the Microsoft is modified these patches will report as new in the Microsoft Update Catalog (MUC). When Scan Machine runs a patch scan on a machine using the MUC, if any of these patches report as missing on that machine Kaseya will set the approval status for it to Pending Approval. This will require the approval status for this patch to be updated in order for installation.