Enterprise WSUS Service Details and Application

April 2012

An enterprise Windows System Update Service (WSUS) is now available to all units and centers. The delivery of the service is designed to be the least invasive for end users and IT managers.

Benefits of the Enterprise WSUS service are that the unit IT manager will receive a weekly report showing the status of any workstation or Windows server's operating system update status. This report will come in handy as required by system and university policy to represent your unit's efforts in maintaining patch management for your workstations.

For the regional centers the benefit is a drastic reduction in bandwidth consumption by having the workstations obtain updates from the SUS server located on the local network vs. utilization of the limited WAN bandwidth.

Following are details about the service for unit IT managers to review and apply:

Active Directory Policy Model:

The WSUS service policies have been configured for three situations:

Option 1: Systems that will automatically download and install patches and auto reboot
Option 2: Systems that will automatically download and install patches but ***NOT*** auto-reboot
Option 3: Systems that will download patches but require that patches be manually approved and the system must be manually rebooted.

Default for all the above Policies:

- All computers would automatically be set to check for updates nightly at 3am
- If the system is not online at 3am, it will check for updates 3 hours after next connection to the network is made.
- Except for Option 3: Updates would be automatically applied after download and the user provided with an hourly prompt notifying that the system needs to be rebooted to apply the changes. The user can defer or the next time the system is rebooted the updates will be applied.

Example applications would be:

Option 1 applies to generic business and office systems.
Option 2 applies to lab systems that perform overnight data collection or data crunching
Option 3 would apply normally to a window server.

Application Model:

Following is information about how each option described above is applied to each windows workstation or server:

Option 1: All workstations by default in your "COMPUTERS" OU will be under Option 1 model also any subfolder under your "COMPUTERS" OU will have option 1 model applied.

Option 2: Workstations or servers that need to be on the Option 2 model must be manually added to the **WSUS–NoReboot-UnitName** group that has been created in your "GROUPS" folder in Active Directory. Even though the computer you add to this group will also be in your "COMPUTERS" OU the Option 2 policy will be applied as a priority. You can verify the WSUS policy in use by performing a GPRESULT command via the workstation command shell after it has been rebooted and received the policy update.

Option 3: Workstations or servers that need to be on the Option 3 model must be manually added to the **WSUS –Servers-UnitName** group that has been created in your "GROUP" folder in Active Directory. Even though the computer you add to this group will also be in your "COMPUTERS" OU the Option 3 policy will be applied as a priority. You can verify the WSUS policy in use by performing a GPRESULT command via the workstation command shell after it has been rebooted and received the policy update.

NOTE: Please DO NOT RENAME, DELETE OR REMOVE any of the above groups.
NOTE: Renaming a computer added to one of these groups for Option 2 or 3 will require you to re-add them to the appropriate group. (Not required if Option1 is in use)

WSUS Activation:

Upon the next reboot or local policy update the workstation will receive updates from the WSUS update service and be included in the automatic reports generated for each unit.

Reporting Service:

Automatic reports for each unit and center will be generated and delivered monthly via email to the unit IT Manager (where applicable). The report will provide a patch status for each computer within your OU and the status of any given patch (i.e. Installed, PendingReboot, Failed, etc.)