ProactiveWatch 2.0
Patch Management and Reporting
Purpose of this Guide............................................................................................................... 1
II. Patching View .................................................................................................................. 1
   Main Patching Screen....................................................................................................... 2
   Filtering by Patch Attribute............................................................................................. 2
   Filtering by Customer and Title....................................................................................... 3
   Patch Details.................................................................................................................... 3
   Apply, Decline or Ignore (Multiple) Patches................................................................. 4
III. Managing an Individual Computer........................................................................... 5
IV. Configure Patching Variables with the Monitoring Template............................. 6
V. Troubleshooting ........................................................................................................ 7
   Run Error (Invalid Manifest)....................................................................................... 7
   Patches are not showing as available ........................................................................... 7
VI. Reporting .................................................................................................................. 8
Purpose of this Guide

This document will guide the ProactiveWatch VAR or Service Provider in the use and configuration of the Patch Management and Reporting features in Version 2.0. This guide assumes that the person following these instructions is familiar with ProactiveWatch, the Windows environments from an Administrator’s perspective and understands the mechanisms for updating Windows OS with Microsoft Patches.

I. Overview

ProactiveWatch’s patch management utilizes the standard built-in Microsoft update mechanism found on all Windows devices to centralize the management of Windows OS patches across all of your customers. This way, you are able to rely upon the robustness of the Microsoft processes, while taking advantage of the ability to easily deploy patches across all of your clients, just certain clients, or even manually selected machines.

ProactiveWatch does not interface with WSUS. So you are able to use the ProactiveWatch patching features in environments that do not have WSUS, including peer-to-peer networks, laptops and home offices, as well as locations that do have a WSUS server in place.

You assign the Windows Update Enhanced “Monitoring Extension” (or a clone of it) to the servers and workstations that you wish to perform patch actions upon. The Windows Update extension, during a timeframe defined by you (in the monitoring template, see section IV), sends the list of available patches to the ProactiveWatch backend servers. You are then able to perform broad or selective patch approval of these identified “available” patches across your customer base. Patches that you approve for installation are then enabled on the target machines by the ProactiveWatch Windows Update Extension for installation during a timeframe you determine. In the case of failed patches, ProactiveWatch will attempt multiple tries, and you will be alerted to failed attempts, as well as have the ability to run reports based upon the patch actions.

II. Patching View

Select the Patching Tab in the ProactiveWatch Explorer Console. From this view, you are able to work with available patches from the perspective of the patch or patches; that is, you can approve, decline, or ignore patches for each patch, and the actions can be applied across all machines at all of your customer sites, or can be approved, declined or ignored on a filtered basis: by customer, by individual machine, or by any of the other relational columns available, even your custom defined columns (see Settings->Manage Columns in the Admin Guide). For instance, it is useful to consider adding a ProactiveWatch column called ServerType, and using assignments like Exchange, Sharepoint, SQL, etc., to be able to manage patches for similar machines across all of your customers.
Main Patching Screen
Below is an example of the main Patching screen. The top portion of the panel provides filtering options on the left side, and a graph on the right that provides Patching Status Summary information for all of the machines across all of your customer sites. The bottom panel displays the available patches that conform to the selected filters. Patches that have not been approved, declined or ignored are shown in bold, similar to the way Outlook displays “unread” emails.

Filtering by Patch Attribute
ProactiveWatch provides powerful filtering to present just the patches you wish to work with.

The default filter selection presents a list of the patches most important for your review, showing only patches marked “Critical” by Microsoft, and only those patches that still need your review (i.e. - not already Declined or Ignored). It also will display any “Failed” patches in Red.

A count of the number of Patches matching your criteria is displayed in the bottom right.

Notes:
- The top two rows are logical “ORs” and should be read as “Not Reviewed” as well as “Approved” as well as “Mandatory,” etc.
- To see patches that Failed, it is necessary to check both “Failed” and “Approved”
- Applying “Critical Only” and/or “KB Articles Only” is a logical “AND” to the top two rows and further limits the filters.
Filtering by Customer and Title

You can further refine the list of available patches by selecting a specific customer, or by typing text into the “Title Filter.”

Enter text in the “Title Filter” field to return patches where the text is found anywhere in the description. This is very handy to find specific KB patches. For instance, enter “kb955” to find all patches that have the string “kb955” as part of their description; or “Vista” to find all Vista-related patches.

Patch Details

ProactiveWatch pulls information from the Microsoft Update Catalog to aid you in determining the actions you want to take for a specific patch. Double-click the patch or select, right-click and choose “Details” to bring up the “Patch Detail” screen, as shown here:

It is often useful to research a patch on the internet, and ProactiveWatch provides a “Web Search” tab that automatically searches for this patch. It is particularly useful when there is not any information from the Microsoft Update Catalog - in which case that tab will be blank.

You may also work the patches using the panel on the right. It will display a list of the machines for which this patch is applicable. You may multi-select (Ctl-Click), etc., and then Approve, Decline or Ignore the patch for those machines.
Apply, Decline or Ignore (Multiple) Patches

From the main Patching view, apply the appropriate filters (above) to see the patches you wish. Select all (using Shift-click from top to bottom) or use multi-select (ctl-click), click the approve, decline or ignore button (or right-click for those options) to perform that action upon the selected patches. That will bring up a dialog that allows you to further decide whether to apply that action for all machines, or choose to apply a filter by customer, specific computer, or any of the ProactiveWatch columns, including columns you may have added.
III. Managing an Individual Computer

You may also work patches on an individual computer basis. From the ProactiveWatch main grid, select the row, right-click and choose “Manage Computer....”

This will display a dialog similar to the main Patching view, but you will get the list of available patches just for this machine.

Perform filtering and patching actions as described above.

An important option is the “Patch Manually” checkbox. This prevents ProactiveWatch from performing any patches on this computer and takes precedent over the above patching actions. This feature allows you to return available patches to the system from this machine, but prevents accidentally patching a device you wish to [temporarily] patch by hand.
IV. Configure Patching Variables with the Monitoring Template

ProactiveWatch patching is performed by a monitoring extension that is pushed to the target machines, and controlled by a Monitoring Template. You may use the default “Windows Update Enhanced” template by assigning the template to one or more computers. To change default settings, clone the template (right-click, “Clone”), rename it, and open the Configure Extensions by clicking the Configure button to view and edit the patch settings:

**AutoApprove_All_Critical**, when set to TRUE, instructs ProactiveWatch to allow the Microsoft Update Mechanism to install all Critical patches automatically. This is useful to apply to client workstations if you prefer not to have to use the manual approval via the Explorer console.

Similarly, **AutoApprove_Critical_Security**, when set to TRUE, will automatically approve Critical Security patches.

The **Patch_Install_Window** and **Patch_Install_Duration** allow you to define a time for the beginning of patch installation, and the subsequent duration. The default setting is to install patches beginning at 2:00am (local machine time) for a period of 4 hours (i.e. to 6:00am). Of course, it is necessary that the target computers are running during this timeframe.

The **Patch_Sync_Window** and **Patch_Sync_Duration** allow you to define a timeframe for patch “synchronization.” This is the time that ProactiveWatch will determine available patches on the machine and send that information to the ProactiveWatch backend application for your management in the Patching view, described above. The default start time is 6:00am for a duration of 12 hours. This will occur just once per day during the “Synchronization” window, and we suggest that the timing is such that it is after Microsoft typically posts patches.
V. Troubleshooting

Run Error (Invalid Manifest)
Upon applying the “Windows Update Enhanced” template (or a clone of that template), it may take a few minutes for the new configuration to be pulled to the target machines, and depending upon timing, you may see a “Windows Update” alarm with the information “RUN ERROR: Monitor Error” with the information “Invalid Manifest…”

If you are running ProactiveWatch agents v1.6.0032 or later, this should clear itself within 3-5 minutes when the extension is downloaded and installed. If you are running an earlier version of the agent, please use Settings->Manage Updates and apply the updates to those machines. This will update both the agent to the latest version, and force the download and installation of the Patching extension. Please be patient - the update process can take several minutes to complete and the alarm will resolve itself.

Patches are not showing as available
There are several reasons why you might not see patches as available:

1. Make sure that you have assigned the “Windows Update Enhanced” template and allowed sufficient time (5-10 minutes) for it to be installed and for patches to be returned.

2. Ensure that the Patch Sync Window has been active for that machine.

3. Uncheck Critical Only - it is possible that there are not Critical Patches available for that machine.

4. It is possible that the “Automatic” mode of “Automatic Updates” is enabled and all patches are already installed. Change the setting to “Download…” or “Notify…”

5. Make sure that WSUS or Group Policies are not preventing Automatic Updates on the machine.

Before contacting support, please make sure that Automatic Updates is working correctly on the system, and that updates are available.
VI. Reporting

New Reporting in ProactiveWatch 2.0 includes Patching and Inventory reports that include:

- Critical Patches by Computer
- Pending KB Article Patches by Computer
- Failed Patches by Computer
- Inventory Reports

From the ProactiveWatch Explorer, Choose Report->Patching-> to select the report you wish:

You may then click “Generate” to run the selected report against all computers across all of your customers, or use Filter to select a sub-set based on any of the relational columns in your console, such as Customer, Location, Computer or any of your custom defined columns:

The report will run and display the results, which can then be printed or exported as either Excel or PDF:
A powerful and useful feature is the **Generate for each Customer** option, which will create a PDF report for each of your Customers. Simply select the folder where you want the reports saved and click OK.