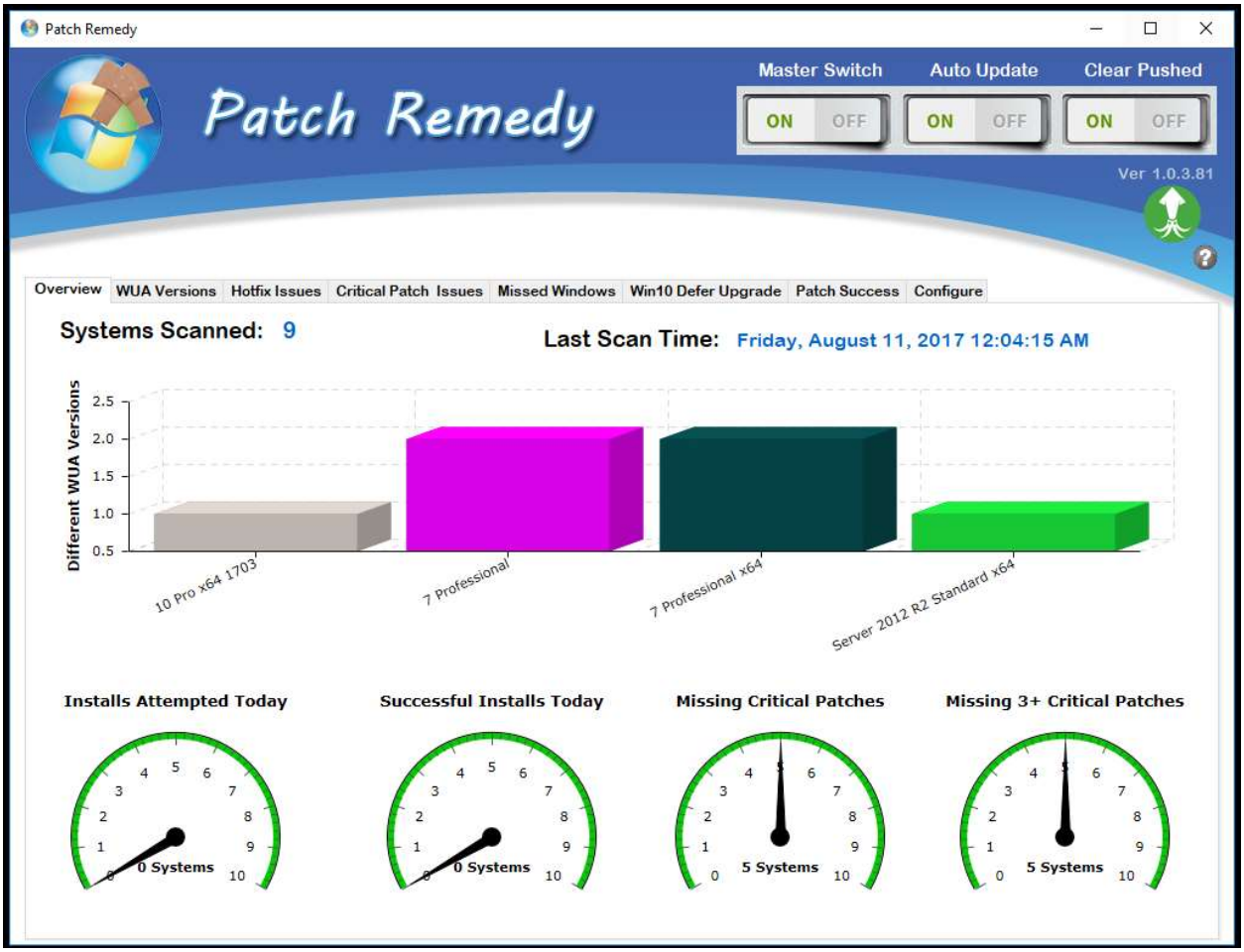
Patch Remedy Plugin

Document Project
Date: 05/07/2018
Revision: 1.0.3

Patch Remedy is a ConnectWise Automate plugin that monitor and updates the WUA services for all current versions of Windows. This in turn, allows ConnectWise Automate to better manage approved patching.

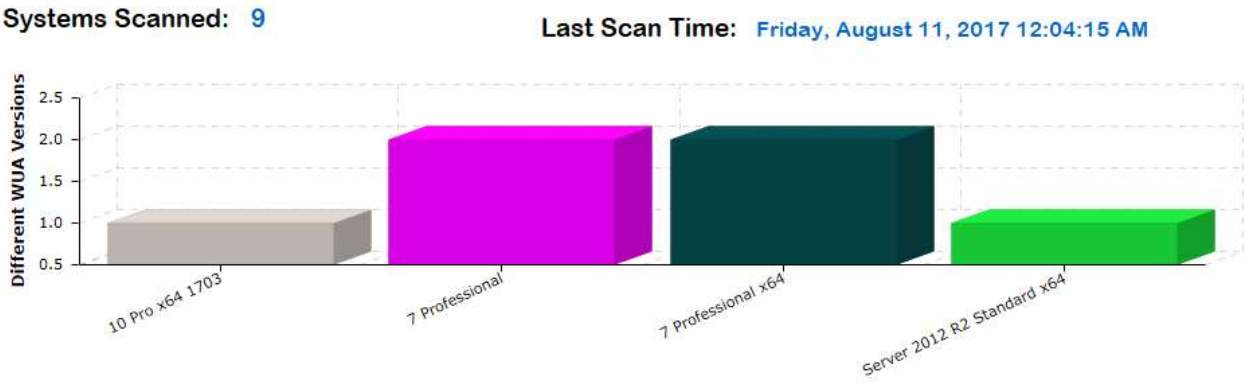
Patch Remedy plugin is launched from the [View] main menu in the Automate Control Center

Overview Tab



The **Overview** tab, there are several graphs and gauges that provide information about the current state of updates and patching stats. You will also find the number of systems reporting to the WUA database as **Systems Scanned** and the last time the scans were run.

The main bar graph shows the number of different versions of **WUA** seen across the scanned environment. Ideally you as a MSP would want to see all versions of Windows only be 1 brick high. MSPs showing a high count on a given OS type denotes several WUA versions reported back for that OS type. This means there are several outdated WUAs in the environment that should be found and updated.



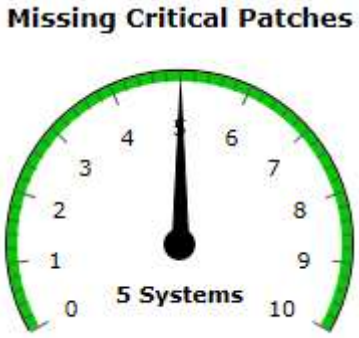
Install Attempted Today

This gauge is created by a query of the `commands` table in the LabTech database where the command ID of 100 and has a status of 3

Successful Installs Today

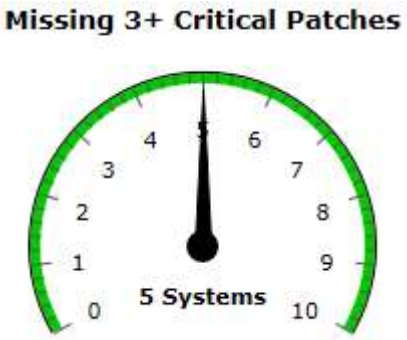
This gauge is created by a query of the `commands` table in the LabTech database where the command ID of 100 and has a status of 3

We then inspect the output for
`downloaded and installed successfully`
to be present.



Missing Critical Patches

This gauge is created by a query of the LabTech database table v_hotfixes. We examine this table for agents reporting a patch not installed that has a severity level set to critical.



Missing 3+ Critical Patches

This gauge is created by a query of the LabTech database table v_hotfixes. We examine this table for agents reporting 3 or more patches not installed that has a severity level set to critical.

Master Switch

This controls the Patch Remedy scanner, turning this off shuts all Patch Remedy automated functions down.

Auto Update

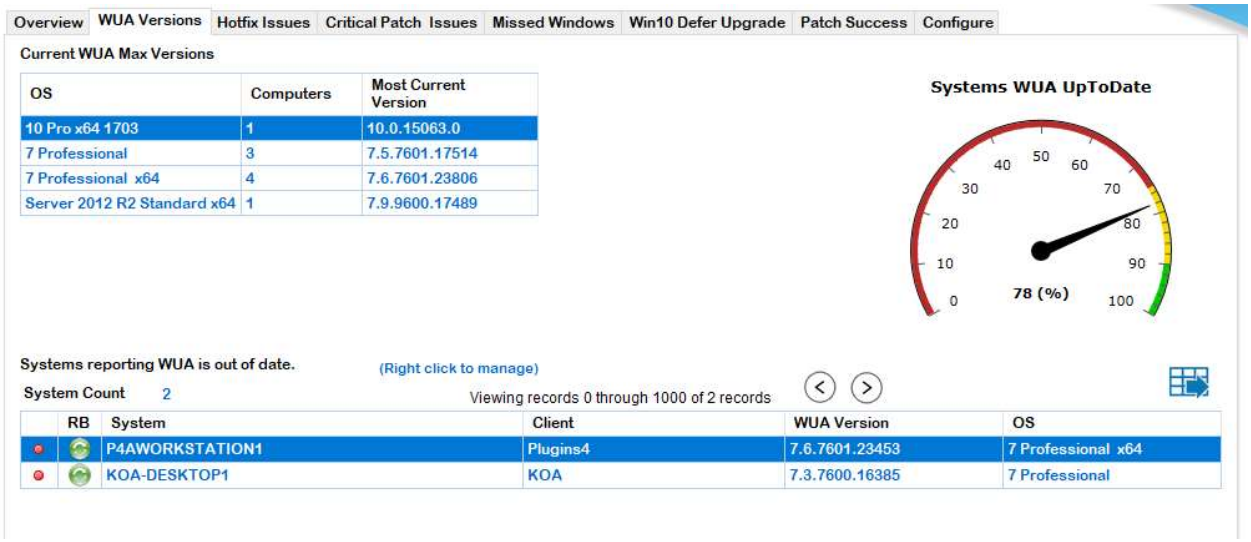
This control turns on and off the automated updating of WUA from Patch Remedy. If Master switch is on and this is off you will be in scan only mode. Turn this on to start updating agents.

Clear Pushed

This is a database function only. During a scan cycles Patch remedy will look for patches in the hotfix table where the push flag is one and installed flag is 0. The reason for this change is, LabTech will attempt a install of a patch, if it fails the push flag is set. Labtech skips this patch in future attempts until the flag is set back to 0. By setting this back to 0 Labtech patch engine will reattempt the installs.

WUA Versions

This is the primary tab for managing WUA inside of Patch Remedy. From this tab you will be able to see the different current WUA versions per OS type. There is a gauge to show the current WUA up to date percentage across the environment and a table of agents that are currently not at the most current levels of WUA.



WUA Out Of Date Table View

This table allows you to see the current online / offline status of the agent and if the agent is reporting a pending reboot. You can select the RB column image to launch a prompt to reboot the agent from inside Patch Remedy.

Common Controls

Excel Export Tool

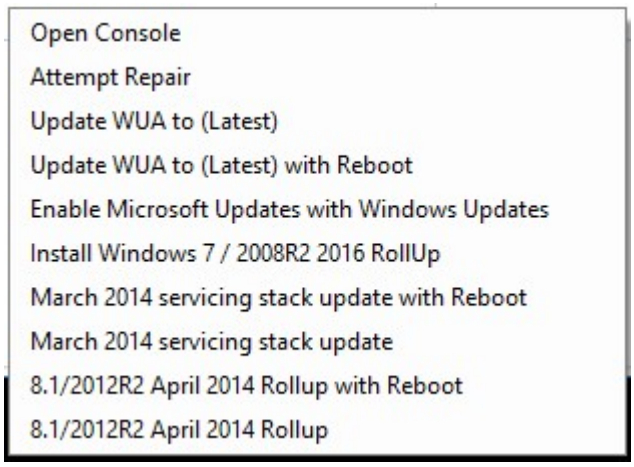
This tool exports a CSV of the current data to a local file on the tech's computer.

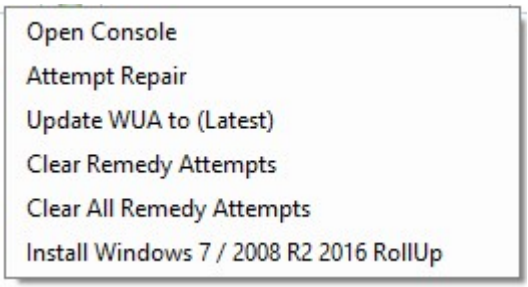
Data Table Paging

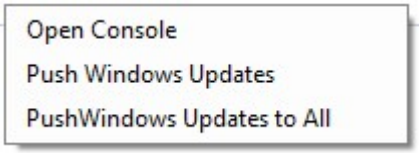
This control allows you to page through list that have more than 1000 records to display. Move forward and back through the data available.

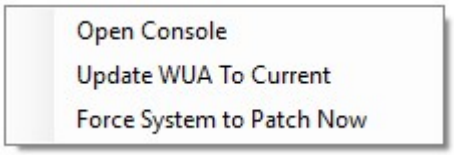
Table Menus

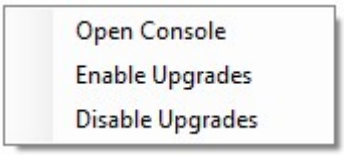
There are several menus available throughout the Patch remedy plugin. A lot of them carry the same controls and others have controls specific to that data table. Below are the different menu items and what they do inside of Patch Remedy.

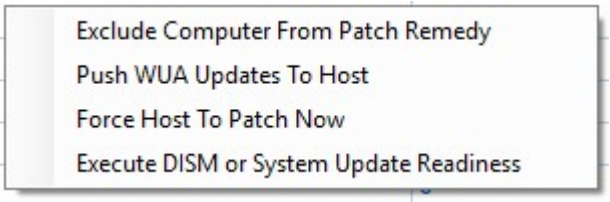


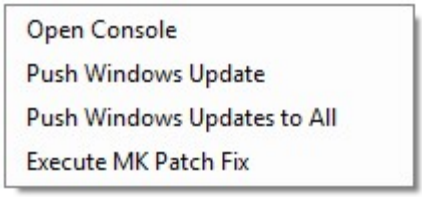












Attempt Repair

Based on KB971058 https://support.microsoft.com/en-us/kb/971058, Attempt Repairs will try to reset all Windows Update components for the agent.

Update WUA to (Latest)

This function is the same function the automation attempts during a scan if **Auto Update** is turned on. This is the manual control that will only update WUA to the next level in the ladder of updates. You may require to run this repeatedly to walk extremely out of date systems through all the required updates.

Update WUA to (Latest) with Reboot

Same as the function **Update WUA to (Latest),** The difference is the function is not told to include the **/no restart** command line switch when executing an update. This does not mean that the update will

reboot the system after update. It means we do not tell it to not reboot after install. It will be up to the update to determine if it will force the reboot or not.

Enable Microsoft Updates with Windows Updates

This executes a small VB script from the Maintenance script that adds a new service to the service manager with a ID of "7971f918-a847-4430-9279-4a52d1efe18d". This will cause Microsoft software updates to also take place.

Install Windows 7 and 2008 RS 2016 Rollup

This function executes the maintenance script instructing it to install the KB3172605. See https://support.microsoft.com/en-us/help/4009440

March 2014 service stack update (with Reboot)

This function installs KB2919442 to Windows 8.1 and 2012 agents. See https://support.microsoft.com/en-us/help/2919442/march-2014-servicing-stack-update-for-windows-8-1-and-windows-server-2

8.1/2012 April 2014 Roll Up

This function installs several updates in a row and all at the same time. The following updates are applied to agents

- KB2919355
- KB2932046
- KB2934018
- KB2937592
- clearcompressionflag.exe

This function schedules the maintenance script to perform the tasks.

Clear All Remedy Attempts

This function clears the counters **for all agents** under Patch Remedy control. The counters are seen on the **HotFix Issues** tab as the (RT) column in the top data table. Agents showing more than 3 attempts will stop attempting to apply updates through automation.

Clear Remedy Attempts

This function clears the counters **for just the agent selected**. The counters are seen on the **HotFix Issues** tab as the (RT) column in the top data table. Agents showing more than 3 attempts will stop attempting to apply updates through automation.

Force System To Patch Now

This function tells the agent to execute the LabTech Patch Now command followed by executing at the agent `wuauclt.exe /detectnow /updatenow` having the WUA service on Windows update its catalogue. The LabTech patch command tells Labtech to patch based on the policies you have set and the approvals made in the LabTech Patch Manager.

Open Console

This function will cause the computer console in LabTech to open for the agent selected.

Push Windows Updates

This function tells the agent to execute the LabTech Patch Now command followed by executing at the agent `wuauclt.exe /detectnow /updatenow` having the WUA service on Windows update its catalogue. The LabTech patch command tells Labtech to patch based on the policies you have set and the approvals made in the LabTech Patch Manager.

Push Windows Updates to All

This function **tells all agent under Patch Remedy management** to execute the LabTech Patch Now command followed by executing at the agent `wuauclt.exe /detectnow /updatenow` having the WUA service on Windows update its catalogue. The LabTech patch command tells Labtech to patch based on the policies you have set and the approvals made in the LabTech Patch Manager.

Execute MK Patch Fix

This patch fix process was conceived of by Martyn Keigher (MK) to assist in systems that are continuously failing patching. This command assigns the Patch Remedy maintenance script to run that will execute several commands.

1) **Reimports a Certificate** associated with the (97817950D81C9670CC34D809CF794431367EF474) fingerprint.
2) **Stops** the **wuauserv** service and the **cryptsvc** service
3) **Removes** the C:\windows\softwaredistrobution folder
4) **Removes** the c:\windows\system23\catroot2 folder
5) **Restarts** the stopped **services**
6) **Resets Windows Updates** to Default
7) **Resends** all installed **patches** for system
8) **Pushes** an install of **all approved patches**

Enable / Disable Upgrades

Windows 10 editions let you defer upgrades to your PC. When you defer upgrades, new Windows features won't be downloaded or installed for several months. Deferring upgrades doesn't affect

security updates. Note that deferring upgrades will prevent you from getting the latest Windows features as soon as they're available.

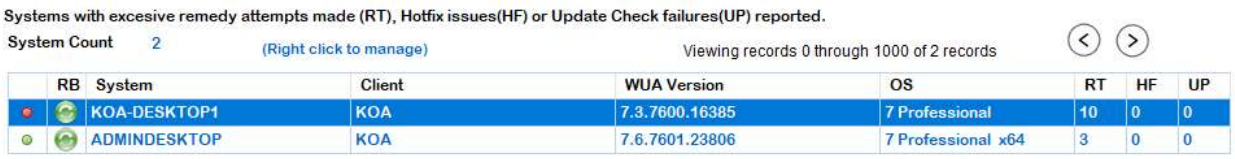
DISM or System Update Readiness tool

Windows updates and service packs may fail to install if there are corruption errors. For example, an update might not install if a system file is damaged. The **DISM** or **System Update Readiness tool** may help you to fix some Windows corruption errors. Windows 8, 2012 and 10 use the inbox Deployment Image Servicing and Management (DISM) tool where Windows 7, 2008 and 2008 R2 use System Update Readiness tool.

When you select ***DISM*** *or* ***System Update Readiness*** from the drop-down menu we will schedule the Patch Remedy Maintenance script to process the DISM functions needed based on OS Type automatically. For more information of repair process please visit https://support.microsoft.com/en-us/kb/947821

Hotfix Issues

Systems with Update Check or Hot Fix Issues Reported



RB	System	Client	WUA Version	OS	RT	HF	UP
	KOA-DESKTOP1	KOA	7.3.7600.16385	7 Professional	10	0	0
	ADMINDESKTOP	KOA	7.6.7601.23806	7 Professional x64	3	0	0

This table displays agents that have excessive remedy attempts or have shown through data queries into the hotfix and commands tables in LabTech to have had issues during common tasks. This does not necessarily mean that the agent is in trouble or that the failure still exists, just that there were issues seen in the data recently. This might denote a larger issue with any given agent.

Systems that have had errors during installation of patches

System	Client	Last Error	Error

This table displays agents that have shown errors in the returns of the patch commands LabTech is sending during normal patch cycles. This view looks back over 30 days and reports any agent and how many times that agent is seen with an error in this table. An agent having one or two errors is not uncommon, what you should be looking for is agents that have several or excessive failures. This tends to denote a larger issue with that agent and a more detailed look at agent is warranted.

Critical Patch Issues

Systems that have not patched in 30+ days

This table displays agents that have not shown to have had any patches installed by LabTech in over 30 days. We query the `h_patching` table looking at last date of any install, if we cannot find at least one install inside the last 30 days then agent is reported here.

Systems missing critical patches

Patch Remedy queries the `v_hotfixes` view in the LabTech database and counts the number of critical patches that show that they have not been installed per agent. Agents must be missing at least 1 critical patch to be in the list.

Missed Windows

Systems that have missed 1 or more ignite patch windows

This table displays the agents that have shown to have missed resent Ignite patch windows. This typical shows agents that are offline when the LabTech patching services can run. Labtech will skip the system

and wait till the next windows to try patching again. Excessive missed windows denote out of date systems that may need interventions.

Windows 10 Upgrades

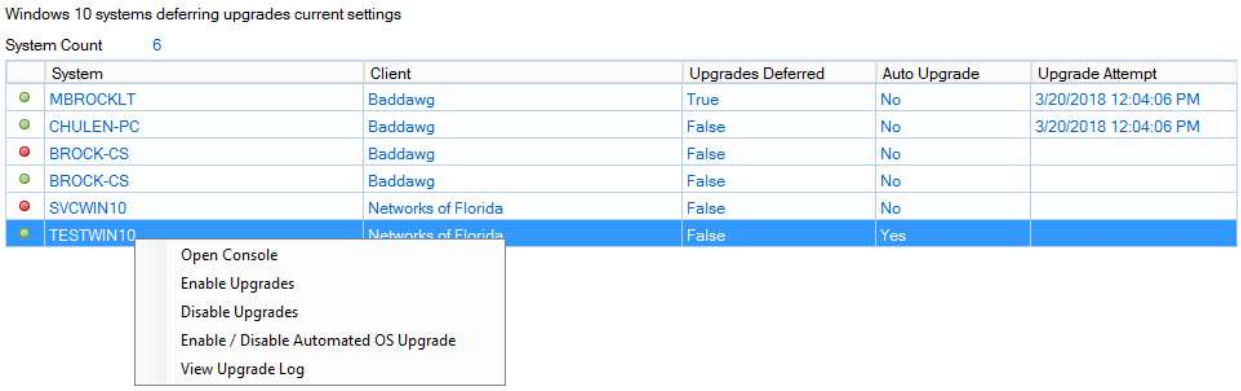
Windows 10 systems upgrades services

Deferring

This table displays all the windows 10 systems you have and what their current deferred upgrades settings are set to. Patch Remedy scans Windows 10 systems to see if the system is set to defer upgrades. You can also use Patch Remedy to enable or disable this option on the remote Windows 10 agent that support this option.

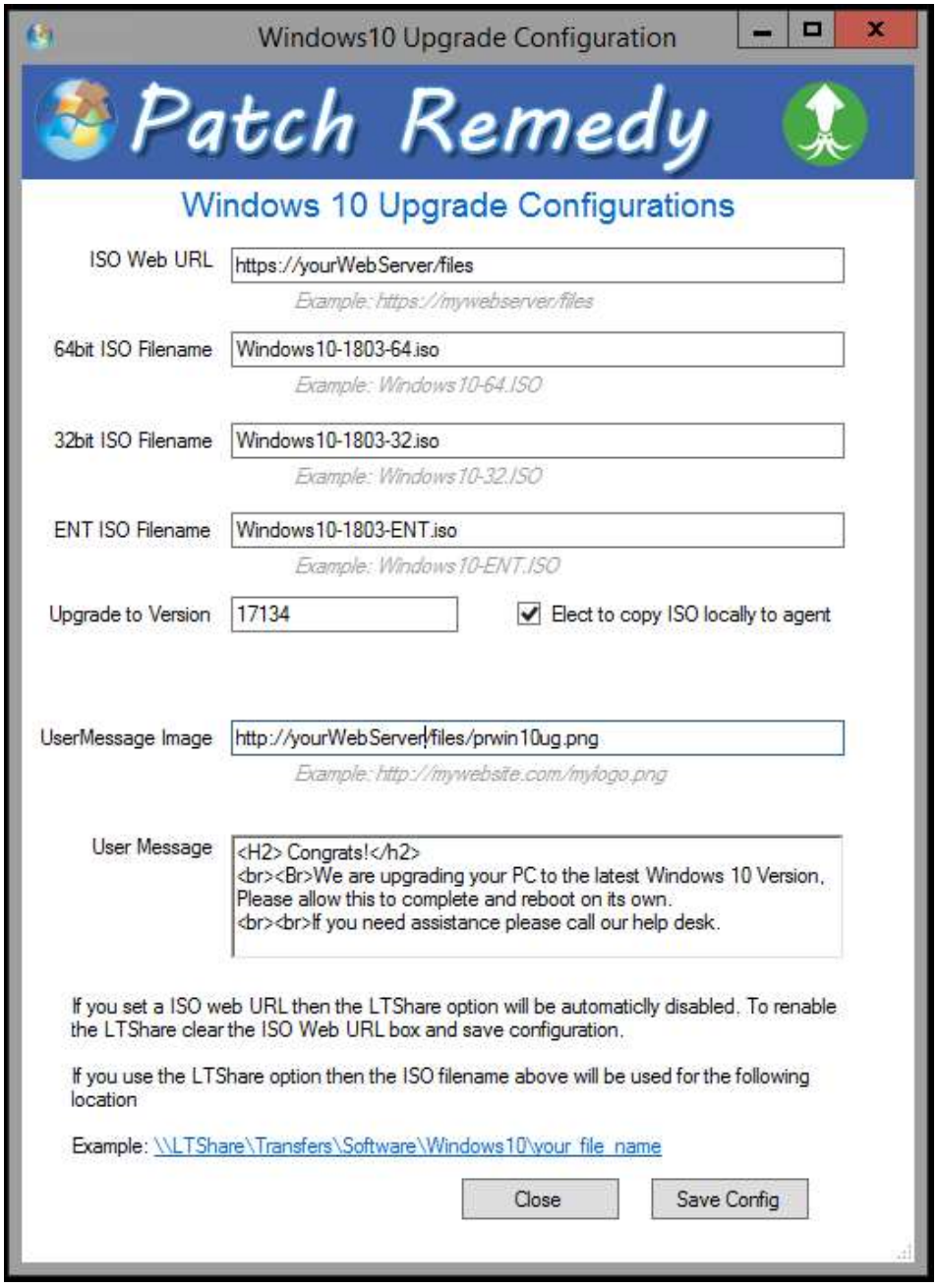
Auto Upgrade

Enabling this feature will set the Patch remedy services to attempt a Windows 10 OS version upgrade. Select an agent from the Windows10 view and select from the menu Enable / Disable Automated OS Upgrade. This will tell Patch Remedy to attempt an OS upgrade on this system on next scheduled upgrade cycle. If a user is logged in and using system, Patch Remedy will reach out to them and ask if the update can proceed. If the user agrees then the update continues else, it is logged that user rejected and we exit any installs. To view install logs and to reset agent for a second attempt use the View Upgrade Logs menu item.



To successfully complete Windows 10 Version upgrades there is a few prereq's needed. If any prereq is not met, then that information will show up in the install logs of any agent that has attempted an upgrade. Use log view to reset an agent for automation.

Windows ISO File Configuration



ISO Web URL allows you to **disable** the use of the [LTShare] and instead retrieve all ISO files directly from the Internet. This is the preferred way when not all Clients or Locations can reach the LTShare on the LTHost.

32/64bit/ENT ISO file tells Patch Remedy what files need to be downloaded based on OS type. If you are updating both 32 and 64 bit systems and Enterprise you will need all 3 ISOs.

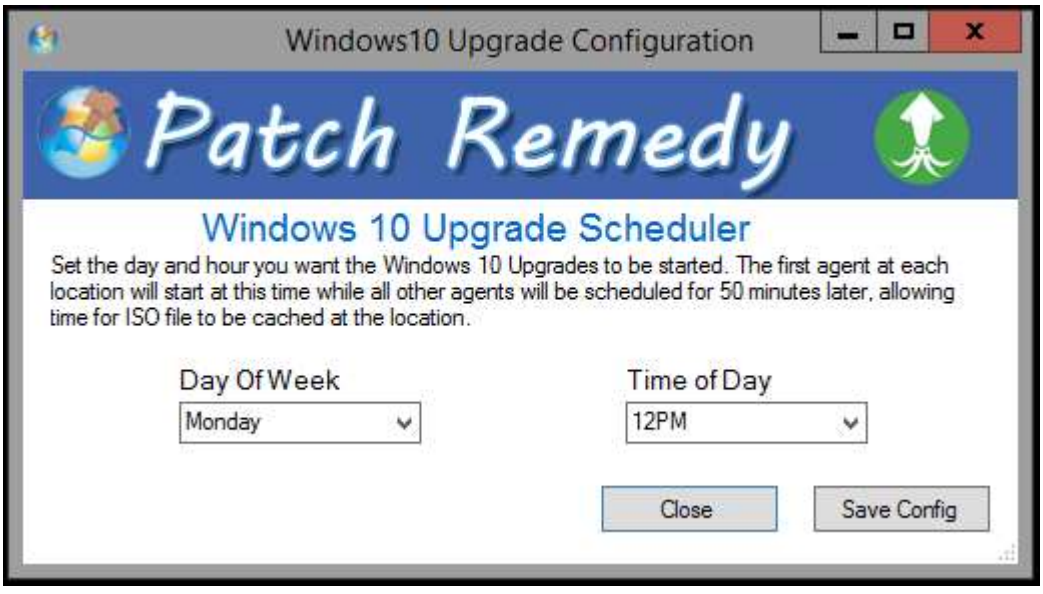
The **Upgrade to Version** sets the max build number an agent will upgrade to. This should correspond with the ISO made available.

The **Elect to copy ISO locally to agent** has the agent copy the ISO from the Location Drive to the local agents C drive before mounting the ISO. By default, the agent will mount the ISO from the network share saving 5 Gb of storage needed on the local agent for the ISO. Mounting from network may have issues if many agents are trying to mount ISO at same time.

The **User Message Image** allows you to place a custom logo in place of our default Patch Remedy logo when an user is logged in and an upgrade is pushed.

The **User Message** allows you to set a HTML message for any logged in user that may be using the system during a upgrade process. The user will be asked if upgrade can continue and then afterwards this message will pop up letting them know upgrade is in progress.

Schedule Windows 10 Upgrades



You can schedule a weekly window for the Windows 10 upgrades to be executed. When the schedule time arrives, Patch remedy will execute the install on (1) agent at each location where agents are set to upgrade. Then Patch Remedy will schedule all the other agents for 50 minutes later to allow the first agent to cache the ISO file from the web or LT host. Consider this when setting the scheduler.

What to consider when supporting plugin and using the media creation tool to create the ISO:

https://www.microsoft.com/en-us/software-download/windows10/

64-bit or 32-bit processor (CPU). You'll create either a 64-bit or 32-bit version of Windows 10. To check this on your PC, go to PC info in PC settings or System in Control Panel, and look for System type.

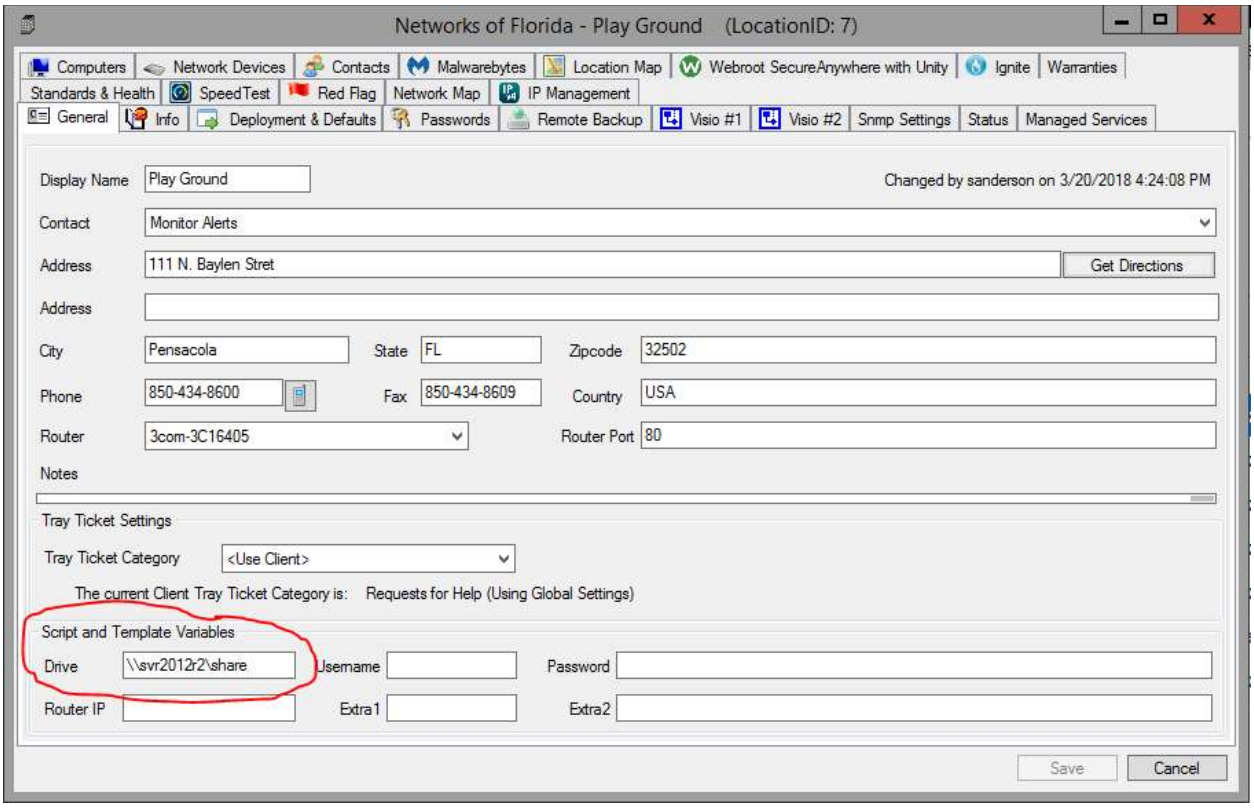
System requirements. Make sure the PC meets the system requirements for Windows 10. We also recommend going to the PC manufacturer's website for additional info about updated drivers and hardware compatibility.

Language in Windows. You'll need to choose the same language when you install Windows 10. To see what language you're currently using, go to Time and language in PC settings or Region in Control Panel.

Edition of Windows. You should also choose the same edition of Windows. To check what edition you're currently running, go to PC info in PC settings or System in Control Panel, and look for Windows edition. Windows 10 Enterprise isn't available in the media creation tool. For more info, go to the Volume Licensing Service Center.

The Patch Remedy Maintenance script will cache the 4+ GB ISO file to the locations share drive. You must have each Location's "Drive" populated with a share capable of saving the 4+ GB ISO file. Once the first agent downloads the ISO it will be placed here, all other agents will look here for ISO first. If ISO is missing they will attempt to download it and place it here. This will prevent large groups of downloads from attempting to download ISO and drowning out the bandwidth connection.

The Location Drive is located here for each location each client has:



If the network share requires authentication the use the “Username” and “Password” field.

Patch Success

Systems that have successfully installed patching (last 7 days)

Systems that have successfully installed patching

System Count 0 (last 7 days)

	System	Client	Last Patch Date

This tables displays agents that have reported back to Labtech during a Patching session that they have installed patches in the last 7 days.

System patch Percentages

This is a query of the Labtech database, depending on if the LabTech systems is a LT 10.5 or 11 system and if the "use LT view" is selected we will query 1 of 2 tables in the LabTech Database.
If the "Use LT View" is selected we query using the `v_xr_hotfixstats` view in LabTech. Otherwise we query the `hotfix` table to define the counts for each agent. Patching must be being reported to the Labtech database correctly for views to show accurate data.

Fully Patched This Month

This gauge shows the number of agents that have reported back to LabTech that reported back as a status to the LabTech patch command "`No Updates to Install`". This would denote that that agent is fully patched and has no new updated that need to be applied.

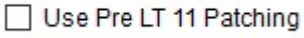
Configure

Scan Interval

The Scan interval sets how often the Automation will run against online agents.

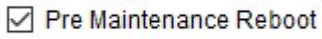
All times run at the top of the hour. (first 6 minutes)

- 24 = once at 1am
- 12 = twice at 12 am and 12 pm
- 8 = three runs at 12 am, 8 am and 4pm
- 4 = four runs at 12,4,8am and 12,4,8pm
- 2 = every 2 hours starting at 12 am
- 1 = every hour



Use Pre LT 11 Patching

This sets Patch Remedy queries to look for patching data using the older LT10.5 standards. If you moved to LT11 and have not migrated to the newer LT 11 patching services then this should be selected. This will tell the plugin to ignore that the host is LT 11 and to treat it as LT 10.5



Pre Maintenance Reboots

This tells the Patch Remedy automated service to look at each location's default maintenance windows selections and pull out the windows time frames that have the alerts set to off for maintenance. We then at that time scan that location for computers that are managed by Patch Remedy and are not on the Patch remedy exclude lists. When a Windows computer matches this profile, and has the "pending reboot" flag set, it then gets a reboot command sent to them.

Force Scan

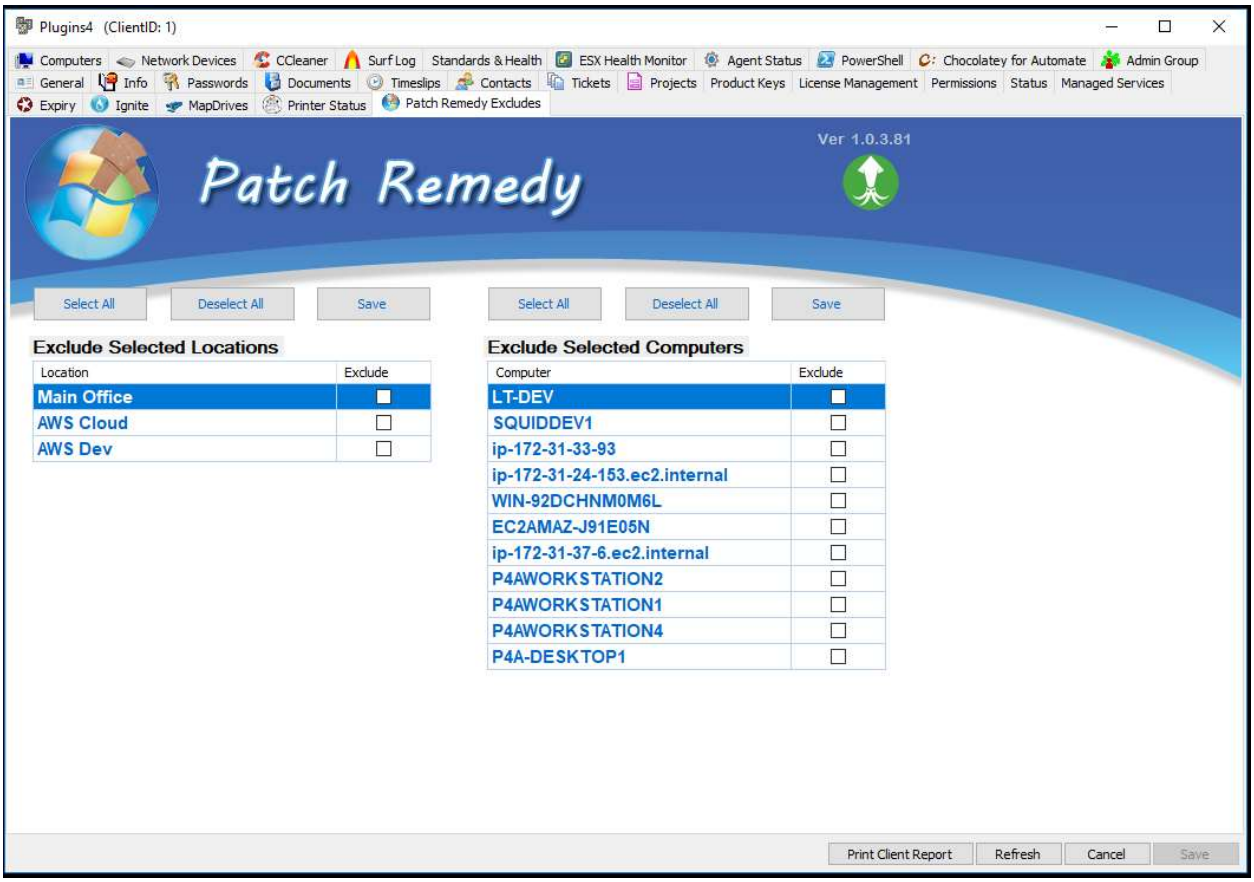
This will cause a full system scan to be started just as if the maintenance cycle was run. This can take several minutes to fully complete for larger agent counts. Once the scan box closes you should wait several minutes for all the scheduled scripts to complete before refreshing data. You may want to close and reopen the Patch Remedy console is data looks odd.

This attempts to reload the views inside Patch Remedy.

Scan only Selected Clients

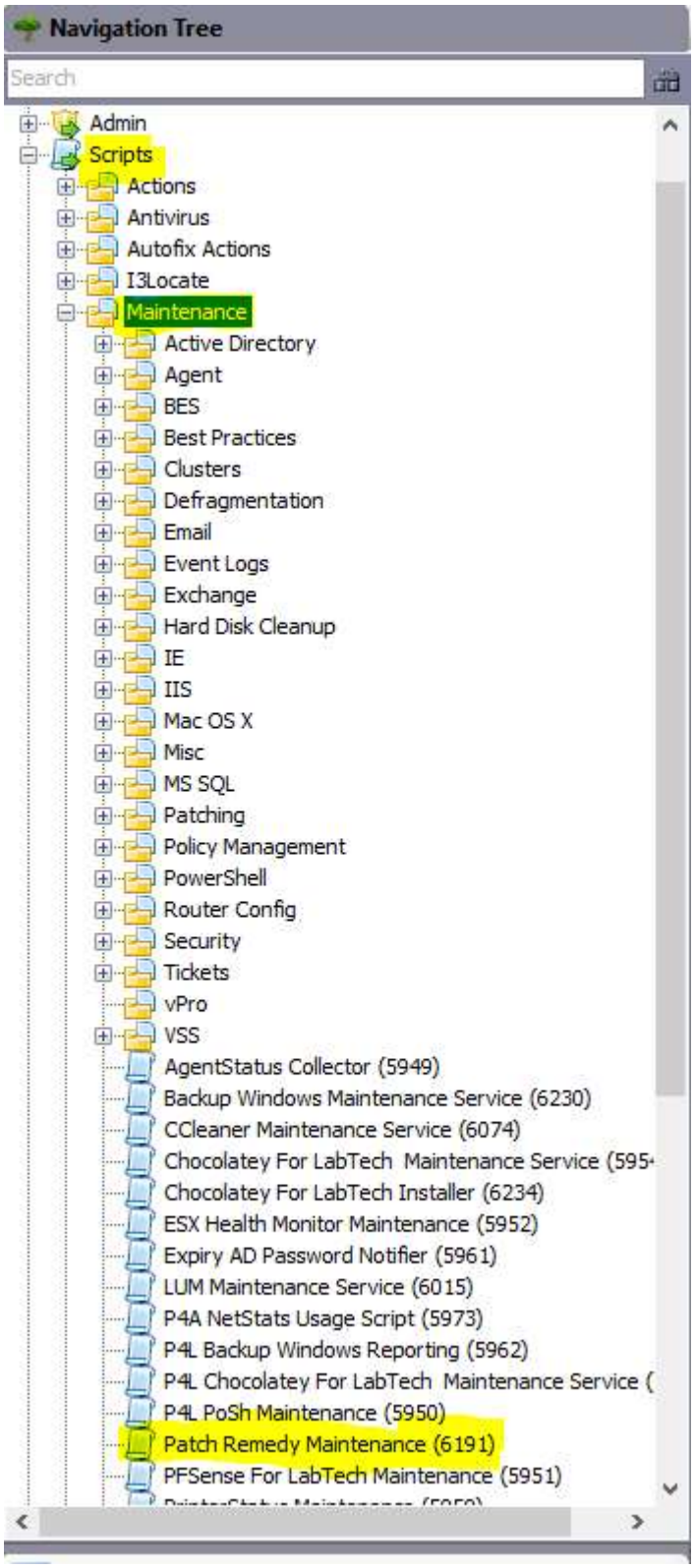
Use this tool to enable different clients for Patch Remedy management and reporting. Select the clients you want Patch Remedy to scan and run automation on.

Client Console



Patch Remedy has a Client Console tab that allows you to exclude agents at the location level or individually. This allows you to enable a client but exclude agents inside the client that should not have any scans or updates applied. They will also be excluded from any table views inside Patch Remedy.

Patch remedy Maintenance Script



The Patch Remedy Maintenance script is located under the maintenance folder in the scripts directory.

This script is used widely in Patch Remedy to manage the processes needed to successfully update and manage the agents Patch Remedy controls.

It is not suggested that you edit this script as it could break Patch Remedy.

If you alter script then on next update of script any changes will be overwritten. If you need to repair the script just delete from the system and restart the Labtech DB agent to have it recreated.

Windows7 and 2008 R2 Auto Update process

The automation process for Windows 7 and 2008R2 systems may require multiple update intervals to complete. A interval is defined under the configure tab and should be set to 12 as a baseline. An interval of 12 will cause Patch remedy to look for agents online twice a day and will attempt to scan them. Based on the current WUA versions Patch Remedy will walk the systems up the "Security Rollup" path. This makes sure any prereqs that maybe needed are applied in the correct order to allow for the next update to complete. If you are not using the "Pre Maintenance reboot" functions
then you should craft a script that reboots Windows 7 agents when scheduled. Apply a liberal reboot schedule to allow the windows 7 agents to complete updates before moving on to the next update.

The Rollups that are applied are:

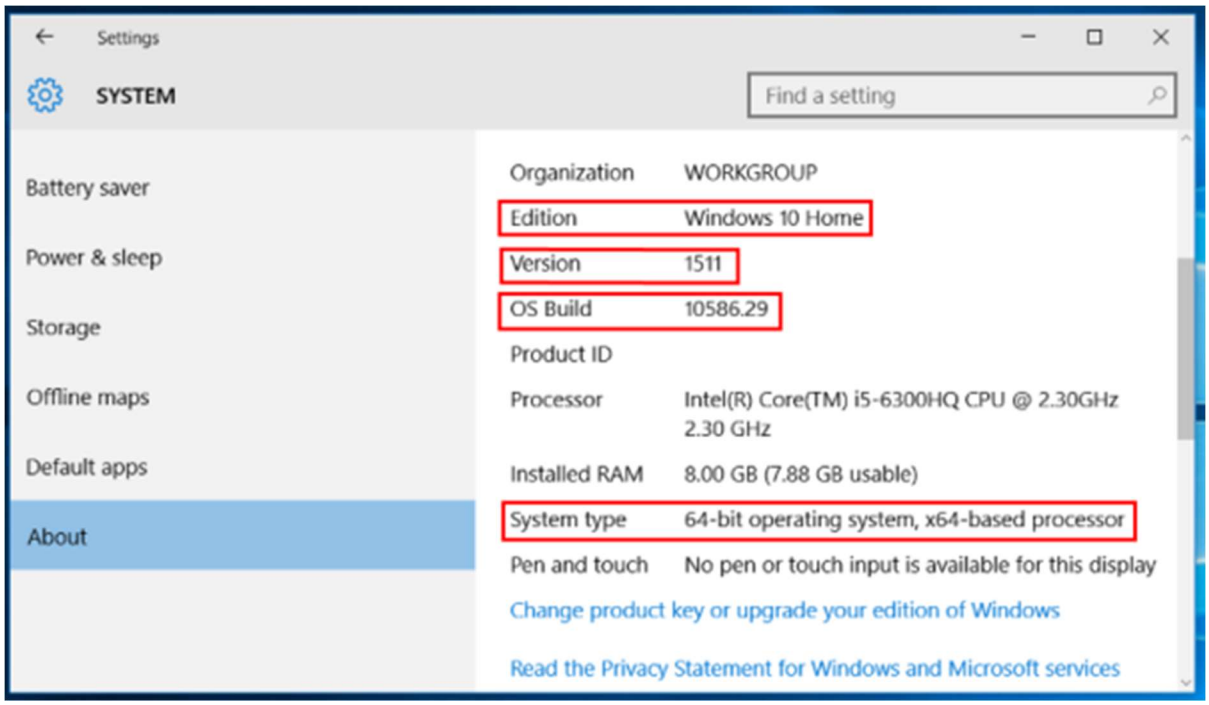
If WUA is pre 7.5.7601.17514 the Windows 7 SP1 has not yet been applied. Patch Remedy will attempt to apply Service Pack 1 with the no restart switch. This will allow the first step in installing the service pack to be silent and not affect the end user by rebooting. On next reboot, the update process will enter step 2 and cause the system to process the rest of the update and reboot several times on its own. During the 2nd step the system will not be useable and the end user will need to allow it to fully complete and reboot before the user can log in.

After Service Pack 1, Patch remedy will attempt in order the following updates one at a time (Scan Cycle). A reboot followed by a Patch Remedy scan will need to be completed between updates for the system to report updated WUA versions.

- KB3020369 < 7.6.7601.23453
- KB4012218 < 7.6.7601.23714
- KB4015549 < 7.6.7601.23735
- KB4019265 < 7.6.7601.23775
- KB4022722 < 7.6.7601.23806

Windows 10 / 2016 Automated Updates

Patch Remedy will poll each Windows agent prior to the update process to determine the Version and Build numbers for that system.



Patch Remedy will, if the systems is found not to meet the current standards in Patch Remedy, apply the latest updates for the version number of Windows 10. This includes Versions 1511, 1607 and the latest 1703 Creators Edition.

For **1511** the latest build pushed is **10586.1007**
For **1607** the latest build pushed is **14393.1532**
For **1703** the latest build pushed is **15063.483**

Windows 8 / 2012

Patch Remedy has added updates for Windows 8.1 and 2012 servers to the automation services. KB4022717 security rollups for Windows 8.1 and Windows Server 2012 are now included in the latest build of Patch Remedy (1.0.3.80).