



Centurion Technologies

Windows Updates

Updated 09/30/13

Technical Support Available

Monday to Friday hours: 8:30AM until 5:30PM CST/CDT

1-844-265-6055

support@centuriontech.com

Introduction

This module will explain how to best use Windows Updates on a SmartControl managed network as well as a SmartShield stand-alone setup. There are several approaches to using Windows Updates with SmartShield, all of which will be outlined in this document.

Windows Updates Using Schedules

This guide is for a SmartControl managed network using schedules to activate Windows Updates on a selection of computers. To start this process, go to "Scheduling" > "Scheduling" and click the "Schedule Tasks" tab. This area is where you determine what time the scheduled event occurs.

This screen allows you to name and say when a schedule will run. Determine the time, recurrence and start date of your schedules. All fields are mandatory except "Description". When you finish this section, click the "Targets and Fallback" tab.

Your targets are the machines that you want to run the schedule on. You can select an individual machine or a group folder. Please note that a machine can only run one schedule at a time. The scheduler will allow you to set up a machine to run several at once, but this can cause strange behavior and issues for your SmartShield machines. Be sure that they exist in one and only one schedule at a time. Your fallback options allow you to choose which areas of the computer are automatically locked if a schedule fails. Your fallback time will be determined based on how long it takes your schedule to run. You can set it now or let the scheduler automatically set it at the end. When you finish this section, click the "Action" tab.

The action tab allows you to put together a list of actions that you would like to perform. Here is our recommended set of actions in order:

- Wake On LAN
- Disable Protection
- Reboot
- Windows Update (Block Users) [40-400 minutes]
- Enable Protection
- Reboot/Shutdown (Whichever you would like to end with)

Finally, enter and confirm your SmartShield password and press "Save Schedule". The scheduler will automatically return you to any place where the scheduler has incomplete information.

Once your schedule is complete, it will run automatically at the time designated. The SmartControl computer must be turned on for a schedule to be pushed down to your SmartShield computers. Your SmartShield client either must be turned on or it must support Wake-On LAN and have the function enabled. This Windows Update set up is the most flexible because it allows you to determine whether the computer shuts down or restarts. It is the easiest to manage because the only machines they do their updates are the ones you specify.

Windows Updates feature

This feature can be set up by either the SmartShield client or the SmartControl. Activating this feature will enable the following steps:

- Disable Protection
- Reboot
- Windows Update (Block Users)
- Enable Protection
- Reboot

To set this feature up from a SmartControl, highlight the computers you would like to enable Windows Updates on. Navigate to "Client Control" > "Misc. Configuration" > "Client Windows Update".

To set this feature up from a SmartShield client, right click the SmartShield icon in the system tray and go to "Configure". Under the "Machine Control" tab, go to "Windows Updates".

Check the box to enable Windows Updating. In SmartControl the option will say "Enable Windows Updates". In SmartShield the option will say "Enable SmartShield Windows Update Management".

Once you have enabled the option, you must set the day of the week that you want your clients to connect to the Windows Update server (whether you use WSUS or the standard Windows Updates), what time updates will start, how long they will spend doing updates on that given day and what types of updates will be done.

To turn this feature off from SmartControl, go to "Client Control" > "Misc. Configuration" > "Client Windows Update", then send the command without ticking the box. This will clear the command and remove the feature.

To turn this feature off from SmartShield, right click the SmartShield icon in the system tray and go to "Configure". Under the "Machine Control" area, click the "Windows Updates" tab. Uncheck the box called "Enable SmartShield Windows Update Management".

If you want to check the status of whether Windows Updates are enabled in this way, in SmartControl there is a status tab called "Windows Update". If this tab is not showing, right click on the top bar and check the option called "Windows Update". Any machines that have the feature enabled will show "Client Configured".

Please note, this feature will decide when it will run Windows Updates based on the local machine time. Be sure that your machine time is correct or Windows Updates may run at unexpected times.

Using WSUS (Windows Server Update Services)

SmartControl is compatible for use with WSUS integration on a network that supports the feature. To set up your SmartShield clients to use a WSUS server, highlight the clients that you would like to point to your server computer for their updates and go to "Client Control" > "Misc. Configuration" > "Windows Update WSUS / SUS". Once you set this feature, any time Windows Updates are run, they will point to this location to download them.