Configure Clients in a Non–Active Directory Environment

In a non-Active Directory environment, you can configure Automatic Updates by using any of the following methods:

* Using Group Policy Object Editor and editing the Local Group Policy object
* Editing the registry directly by using the registry editor (Regedit.exe)

**Editing the Local Group Policy object**

For a listing of the entries and the values to set, see [Configure Clients Using Group Policy](http://technet.microsoft.com/en-us/library/d7d4c391-f707-4257-8987-e40705e097e7) earlier in this guide.

**Using the registry editor**

Administrators who do not wish to use Group Policy may set up client computers using the registry. Registry entries for the WSUS server are located in the following subkey:

**HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate**.

The keys and their value ranges are listed in the following table.

**Windows Update registry keys**

|  |  |  |
| --- | --- | --- |
| **Entry name** | **Data type** | **Values** |
| **AcceptTrustedPublisherCerts** | Reg\_DWORD | Range = 1|0  1 = Enabled. The WSUS server will distribute signed third-party updates if available.  0 = Disabled. The WSUS server will not distribute third-party updates. |
| **ElevateNonAdmins** | Reg\_DWORD | Range = 1|0  1 = Users in the Users security group are allowed to approve or disapprove updates.  0 = Only users in the Administrators user group can approve or disapprove updates. |
| **TargetGroup** | Reg\_SZ | Name of the computer group to which the computer belongs, used to implement client-side targeting (for example, "TestServers.") This policy is paired with **TargetGroupEnabled**. |
| **TargetGroupEnabled** | Reg\_DWORD | Range = 1|0  1 = Use client-side targeting.  0 = Do not use client-side targeting. This policy is paired with **TargetGroup**. |
| **WUServer** | Reg\_SZ | HTTP(S) URL of the WSUS server used by Automatic Updates and (by default) API callers. This policy is paired with **WUStatusServer**; both must be set to the same value in order for them to be valid. |
| **WUStatusServer** | Reg\_SZ | The HTTP(S) URL of the server to which reporting information will be sent for client computers that use the WSUS server configured by the **WUServer** key. This policy is paired with **WUServer**; both must be set to the same value in order for them to be valid. |
| **DisableWindowsUpdateAccess** | Reg\_DWORD | Range = 1|0  1 = Disables access to Windows Update.  0 = Enables access to Windows Update. |

**Automatic Update configuration options**

The registry entries for Automatic Update configuration options are located in the following subkey:

**HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\AU**

The keys and their value ranges are listed in the following table.

**Automatic Updates Configuration Registry Keys**

|  |  |  |
| --- | --- | --- |
| **Entry name** | **Data type** | **Value range and meanings** |
| **AUOptions** | Reg\_DWORD | Range = 2|3|4|5  2 = Notify before download.  3 = Automatically download and notify of installation.  4 = Automatically download and schedule installation. (Only valid if values exist for **ScheduledInstallDay** and **ScheduledInstallTime**.)  5 = Automatic Updates is required, but end users can configure it. |
| **AutoInstallMinorUpdates** | Reg\_DWORD | Range = 0|1  0 = Treat minor updates as other updates are treated.  1 = Silently install minor updates. |
| **DetectionFrequency** | Reg\_DWORD | Range = n, where n = time in hours (1–22).  Time between detection cycles. |
| **DetectionFrequencyEnabled** | Reg\_DWORD | Range = 0|1  1 = Enable DetectionFrequency.  0 = Disable custom DetectionFrequency (use default value of 22 hours). |
| **NoAutoRebootWithLoggedOnUsers** | Reg\_DWORD | Range = 0|1  1 = Logged-on user gets to choose whether or not to restart his or her computer.  0 = Automatic Updates notifies user that the computer will restart in 5 minutes. |
| **NoAutoUpdate** | Reg\_DWORD | Range = 0|1  0 = Enable Automatic Updates.  1 = Disable Automatic Updates. |
| **RebootRelaunchTimeout** | Reg\_DWORD | Range = n, where n = time in minutes (1–1,440).  Time between prompting again for a scheduled restart. |
| **RebootRelaunchTimeoutEnabled** | Reg\_DWORD | Range = 0|1  1 = Enable **RebootRelaunchTimeout**  0 = Disable custom **RebootRelaunchTimeout**(use default value of 10 minutes) |
| **RebootWarningTimeout** | Reg\_DWORD | Range = n, where n = time in minutes (1–30).  Length, in minutes, of the restart warning countdown, after installing updates with a deadline or scheduled updates. |
| **RebootWarningTimeoutEnabled** | Reg\_DWORD | Range = 0|1  1 = Enable **RebootWarningTimeout**  0 = Disable custom **RebootWarningTimeout** (use default value of 5 minutes) |
| **RescheduleWaitTime** | Reg\_DWORD | Range = n, where n = time in minutes (1–60).  Time, in minutes, that Automatic Updates should wait at startup before applying updates from a missed scheduled installation time.  Note that this policy applies only to scheduled installations, not deadlines. Updates whose deadlines have expired should always be installed as soon as possible. |
| **RescheduleWaitTimeEnabled** | Reg\_DWORD | Range = 0|1  1 = Enable **RescheduleWaitTime**  0 = Disable **RescheduleWaitTime** (attempt the missed installation during the next scheduled installation time). |
| **ScheduledInstallDay** | Reg\_DWORD | Range = 0|1|2|3|4|5|6|7  0 = Every day.  1 through 7 = The days of the week from Sunday (1) to Saturday (7).  (Only valid if **AUOptions** = 4.) |
| **ScheduledInstallTime** | Reg\_DWORD | Range = n, where n = the time of day in 24-hour format (0–23). |
| **UseWUServer** | Reg\_DWORD | Range = 0|1  1 = This machine gets its updates from a WSUS server.  0 = This machine gets its updates from Microsoft Update.  The **WUServer** value is not respected unless this key is set. |

**Automatic Updates scenarios**

The following scenarios illustrate specific issues

**RescheduleWaitTime**

If a scheduled installation is missed (because the client computer was turned off) and **RescheduleWaitTime** is not set to a value between 1 and 60, Automatic Updates waits until the next scheduled day and time to perform the installation. If a scheduled installation is missed and **RescheduleWaitTime** is set to a value between 1 and 60, then Automatic Updates reschedules the installation to occur at the Automatic Updates service start time plus the number of minutes specified in **RescheduleWaitTime**.

There are 3 basic rules for this feature:

1. When a scheduled installation is missed, it will be rescheduled for the system startup time plus the value of **RescheduleWaitTime**.
2. Changes in the scheduled installation day and time via the Control Panel or Group Policy are respected over the rescheduled time.
3. The rescheduled time has precedence over the next calculated scheduled day and time if the “next calculated scheduled day and time” is later than the rescheduled time. The “next calculated scheduled day and time” is calculated as follows:
   1. When Automatic Updates starts, it uses the currently set schedule to calculate the “next calculated scheduled day and time”.
   2. The resulting day and time value is then compared to the **ScheduledInstallDate**.
   3. If the values are different, Automatic Updates performs the following actions:
   4. sets a new “next calculated scheduled day and time” within Automatic Updates.
   5. writes this new “next calculated scheduled day and time” to the **ScheduledInstallDate** registry key.
   6. logs an event stating the new scheduled installation day and time.

The following examples show the use of the **RescheduleWaitTime** value.

**Example 1: Installation must occur immediately following system startup**

This example shows the consequences of **RescheduleWaitTime** set to 1.

1. Update installations are scheduled to occur every day at 3:00 A.M.
2. The **RescheduleWaitTime** registry value is set to 1.
3. Automatic Updates finds an update, downloads it, and is ready to install it at 3:00 A.M.
4. The logged-on user does not see the “ready to install” prompt because the user does not have administrative privileges on the computer.
5. The user shuts down the computer.
6. The user restarts on the computer after the scheduled time has passed.
7. When Automatic Updates starts, it recognizes that it missed its previously set scheduled installation time and that **RescheduleWaitTime** is set to 1. It therefore logs an event with the new scheduled time (one minute after the current time).
8. If no one logs on before the newly scheduled time (1 minute interval) the installation begins. Since no one is logged on, there is no delay and no notification. If the update requires it, Automatic Updates will restart the computer.
9. The user logs on to the updated computer.

**Example 2: Installations must occur fifteen minutes after the Automatic Updates service starts**

This example shows the consequences of **RescheduleWaitTime** set to 15.

1. Update installations are scheduled to occur every day at 3:00 A.M.
2. The local administrator of the client computer sets the RescheduleWaitTime registry value to 15.
3. Automatic Updates finds an update, downloads it, and is ready to install it at 3:00 A.M.
4. The local administrator ignores the prompt to install the update.
5. The local administrator shuts down the computer.
6. The local administrator restarts on the computer after the scheduled time has passed.
7. When Automatic Updates starts, it recognizes that it missed its previously set scheduled install time, and that **RescheduleWaitTime** is set to 15. It therefore logs an event with the new scheduled time (fifteen minutes after the current time).
8. The local administrator logs on before the newly-scheduled time.
9. After Automatic Updates has been running for 15 minutes, it starts the scheduled installation.
10. The local administrator is notified five minutes before installation begins by the countdown timer.
11. The timer expires and the installation proceeds.

**NoAutoRebootWithLoggedOnUsers**

To prevent Automatic Updates from restarting a computer while users are logged on, the administrator can create the NoAutoRebootWithLoggedOnUsers registry value in s. The value is a DWORD and must be either 0 (false) or 1 (true). If this value is changed while the computer is in a restart pending state, it will not take effect until the next time an update requires a restart.

When the admin creates and sets the **NoAutoRebootWithLoggedOnUsers** registry key to 1, the restart countdown dialog that pops up for the logged on user (active and inactive) will change in the following ways:

|  |  |
| --- | --- |
| **Users with administrator credentials** | **Users without administrator credentials** |
| The **No** button will be active. | The **No** button will be inactive. |
| The **Yes** button will be active if the logged-on user is the only administrator logged on at the time the restart dialog appears. | The **Yes** button will now be active only if the logged-on user is the only non-administrator logged on at the time the restart dialog appears. However, the **Yes** button will be inactive if the user’s local security policy prohibits restarting. |
| The restart countdown progress bar and the text underneath the progress bar will not display. | The restart countdown progress bar and the text underneath the progress bar will not display. |

**Example 1: Non-administrator user on a workstation**

In this scenario the network has been set up with the following conditions:

* Updates are scheduled to be installed every day at 3:00 A.M.
* Users must run as non-administrative users.
* **NoAutoRebootWithLoggedOnUsers** is set to 1.
* The user is assigned **Shut down the system** privileges via Group Policy.

Resulting client behavior:

1. Automatic Updates detects and downloads an update and sets the scheduled installation time to 3:00 A.M.
2. The logged on non-administrative user leaves the workstation locked at the end of the day.
3. The scheduled installation starts At 3:00 A.M.
4. This update requires a restart, so Automatic Updates pops up a dialog to the user's locked session saying that a restart is required.
5. At 9:00 A.M. the user unlocks the workstation and sees the restart prompt.
6. The user is unable to click **No** to dismiss the dialog, but can click **Yes** because no other users are logged on to the workstation. There is no timeout, so the user can accept the prompt to restart at a convenient time.

**Example 2: Non-administrator user on a server**

In this scenario the network has been set up with the following conditions:

* By default, users who do not have administrative privileges are not allowed to restart Windows Servers. This is enforced by the local security policies.
* Multiple non-administrator users are logged on at the time the scheduled installation begins.
* The installation requires that the computer be restarted.

Resulting client behavior:

1. Users are notified of the installation.
2. When the installation requires a restart, all logged-on users are notified that the computer must be restarted.
3. Event ID 21 is written to the system event log:
4. Non-administrator users are not allowed to dismiss the dialog by clicking **No**.
5. Since non-administrator users do not have permissions to restart the server, the **Yes** button is also disabled.
6. If new users log on, they also receive the notification that the server needs to restart.
7. Users log off.

Every time a user logs off, Automatic Updates tests to see if there are any users still logged on.

When there are no logged-on users (therefore no opportunity for user data loss), Automatic Updates writes Event ID 22 to the system event log as shown below, and begins the restart procedure.

**Summary of behavior for NoAutoRebootWithLoggedOnUsers settings**

The following table shows the difference in behavior with **NoAutoRebootWithLoggedOnUsers** enabled (set to 1) or disabled/not configured (not set to 1).

|  |  |  |
| --- | --- | --- |
| **Scenario following a scheduled installation** | **With NoAutoRebootWithLoggedOnUsers enabled** | **With NoAutoRebootWithLoggedOnUsers disabled or not configured** |
| No users logged on | Automatic restart immediately following installation | Automatic restart immediately following installation |
| Single user with administrative privileges | Restart notification allows user to start or postpone restart. This notification does not have a countdown timer. Therefore the user must initiate the system restart. | Restart notification allows user to start or postpone restart. This notification has a 5 minute countdown timer. When the timer expires, the automatic restart begins. |
| Single user with restart privileges but no other administrative privileges | Restart notification that allows user to initiate the restart but not to postpone it. This notification does not have a countdown timer. Therefore the user must initiate the system restart. | Restart notification that allows user to initiate the restart but not to postpone it. This notification has a 5-minute countdown timer. When the timer expires, the automatic restart begins. |
| Single non-administrator without restart privilege | Restart notification that does not allow the user to initiate the restart or postpone it. This notification does not have a countdown timer. Therefore the user must wait for an authorized user to initiate the system restart. | Restart notification that does not allow the user to initiate the restart or postpone it. This notification has a 5-minute countdown timer. When the timer expires, the automatic restart begins. |
| Administrator while other users are logged on | Restart notification that does not allow the user to initiate the restart but does allow the user to postpone it. This notification does not have a countdown timer. Therefore the user must initiate the system restart. | Restart notification that does not allow the user to initiate the restart but does allow the user to postpone it. This notification has a 5 minute countdown timer. When the timer expires, the automatic restart begins. |
| Non-administrator with restart privilege while other users are logged on | Restart notification that does not allow the user to initiate the restart or postpone it. This notification does not have a countdown timer. Therefore the user must initiate the system restart. | Restart notification that does not allow the user to initiate the restart or postpone it. This notification has a 5 minute countdown timer. When the timer expires, the automatic restart begins. |
| Non-administrator without restart privilege while other users are logged on | Restart notification that does not allow the user to initiate the restart or postpone it. This notification does not have a countdown timer. Therefore, the user must wait for an authorized user to initiate the system restart. | Restart notification that does not allow the user to initiate the restart or postpone it. This notification has a 5 minute countdown timer. When the timer expires, the automatic restart begins. |

Note: After all users log off, Automatic Updates will restart the computer to complete the installation of the update.

**Interaction with other settings**

If the “Remove access to use all Windows Update features” setting (**HKEY\_CURRENT\_USER\Software\Microsoft\Windows\CurrentVersion\Policies\WindowsUpdate\DisableWindowsUpdateAccess**) is enabled, Automatic Updates will not notify that logged-on user. It makes a local administrator appear as a non-administrator, so that user will not be able to install updates. When this policy is enabled, the Automatic Updates service still runs, and scheduled installations will still occur if they were configured to run.

If the “Remove links and access to Windows Update” Group Policy setting (**HKEY\_CURRENT\_USER**\**Software\Microsoft\Windows\CurrentVersion\Policies\Explorer\NoWindowsUpdate**) is enabled, then Automatic Updates will continue to get updates from the WSUS server. Users with this policy set will not be able to get updates that the WSUS administrator has not approved on the WSUS server. If this policy is not enabled, the Microsoft Update icon will remain on the Start menu; local administrators will be able to visit the Microsoft Update Web site and install software that the WSUS administrator has not approved. This happens even if you have specified that Automatic Updates should get approved updates from the WSUS server. In Windows Vista, enabling this setting will gray out the **Check for updates** option in the **Windows Update** application.

The above settings can be overridden by the **HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\Windows\WindowsUpdate\ DisableWindowsUpdateAccess** setting.