Creating a Microsoft Patch Policy

https://campus.barracuda.com/doc/90440357/

A Microsoft patch policy is a collection of rules that manages Microsoft patches on devices.

What You Can Do

You can

- specify how frequently the patch managed device will check for new updates
- specify the time frame in which updates are installed after they are downloaded
- specify whether users are prompted for updates to be installed or if updates are installed automatically
- application rules, or by selecting specific devices and groups

Patch policies also determine to which devices the policy is applied. You can set up automatic inclusion rules, or manually apply a patch policy to devices and groups. Note that automatic inclusion rules only take effect when the patch policy is included as part of a service delivery model (i.e., added to a service or service plan that is then applied to a site or group).

You can create as many patch policies as you require.

- If a device is included in more than one Patch policy, the Patch policy with the lowest detection frequency is applied to the device. If both policies have the same detection frequency, the policy that was created first is applied.

To create a Microsoft patch policy

1. In Service Center, click **Configuration** > **Policies** > **Patching**.
2. Click **New**.
3. In the **Create New Policy** section, type a name and description for the policy.
4. Click **Create**.
5. Click the **Settings** tab, and click **Modify**.
6. From the **Detection Frequency** list, select how often you want the devices to check for new patches.
   The default 22 hours is good for almost all circumstances. You may want to have devices that receive definition updates check more frequently.
7. In the **Automatic Updates Options** section, select one of the following option buttons:
   Notify for download and install Local users will be notified in the notification area (**System Tray** or **Notification Area**) that updates are ready to be downloaded/installed.
   Auto download and notify for install Updates will be automatically downloaded and local users will be notified in the notification area (**System Tray** or **Notification Area**) that updates are ready to be installed.

Auto download and schedule the install Updates will be automatically downloaded. The install will be scheduled according to the applicable execution schedule.
Allow local admin to choose setting Local users with administration rights can adjust the update settings in Windows.

The **Allow local admin to choose setting** option is not permitted for managed devices with a Device Manager installed. When a Patch policy with this setting is applied to these devices, **Notify for download and install** is used instead.

8. If you selected the **Auto download and schedule the install** option, do the following:
    1. To have the Patch policy use an execution schedule to schedule patches, select the **Install as per applicable Execution Schedule** option button. For more information about execution schedules, see Setting Up Execution Schedules.
    2. To have the Patch policy override any execution schedules applied to a site or group, select the **Override Execution Schedules option** button. For more information about overriding the execution schedule, see To set up a schedule for Microsoft patches that overrides any applicable execution schedules.

    If you select the **Install as per applicable Execution Schedule** option, and there is no execution schedule applied, patch management will default to the **Notify for download and install** option.
9. Select the **Immediately install minor updates (updates that do not interrupt Windows services or require a restart)** check box to have updates installed immediately if they do not interrupt Windows services or require a restart.
10. Select the **Allow non-administrators to receive update notifications** check box to allow regular users to select updates to install.
11. Optionally, select the **Assign the newly added devices of this Patch Policy to the following Approval Group** check box to automatically add all devices that will get applied to this policy to an approval group that you select from the list. This option helps you facilitate the installation of patches by automatically approving patches for the devices in this policy. Then select an approval group.
12. Optionally, select the **Apply changes to existing devices in this policy** check box to add the existing devices in this policy to the approval group that you selected.
13. Click **Save**.

To set up a schedule for Microsoft patches that overrides any applicable execution schedules

When setting up a Microsoft patch policy, you can indicate that the policy uses the applicable execution schedule that was set up for the site or group to which the devices in the policy belong. If you do not want to use the applicable execution schedule, you can override it and create a custom patching schedule within the policy.

You may want to override execution schedules if you have special requirements for your patching schedule. For example, you may have set up an execution schedule for a customer site that takes place Friday evenings at 8 pm. However, for patching, you might want to set up your patching to occur the day after Microsoft releases patches, which typically occurs on the first Tuesday of every month. Overriding execution schedules grants you the flexibility to create a patching schedule that meets your specific patching requirements.

To set up a custom patching schedule, you must select the **Auto download and auto install** option when setting up the **Automatic Update Options** for the policy.

1. In Service Center, click **Configuration** > **Policies** > **Patching**.
2. Click **New** to create a policy, or click the name of an existing policy.
3. Click the **Settings** tab.
4. Click **Modify**.
5. In the **Automatic Update Options** area, select **Auto download and auto install** from the list.
6. Select the **Override Execution Schedules** option button.
7. In the **Start Time** box, type a start time for when patching will begin. Alternatively, you can click the clock icon to select a time from the list.
8. In the **Recurrence Pattern** area, select whether you want patches to run daily, weekly, or monthly.
9. In the **Reboot Options** section, select an option:
   - To allow the operating system to determine the reboot behavior, select **Use operating system default behavior**. The behavior will vary by operating system.
   - To wait until the user is logged off to reboot, select **Do not auto-reboot when a user is logged on**.
   - To reboot immediately when the update requires, select **Force a reboot when an update requires one**.

   Some Microsoft updates will cause a server to reboot, even if you choose **Do not reboot**. This behavior does not come from Barracuda Managed Workplace, but is native to Windows. We recommend reading all details of a patch before applying it to a server.
10. In the **Missed Installation Options** area, select **wait X minutes after the next system startup to install** and enter a value for X in minutes between 1 and 60, or select **wait until next scheduled time to install** to define how missed installations are handled.
11. Select **Immediately install minor updates** to automatically install updates that do not interrupt Windows services or require a restart.

    This option does not apply to Windows 10 or Windows Server 2016.
12. Select the **Allow non-administrative users to approve or disapprove deputes on clients managed by Onsite Managers** check box to allow end users do not have an administrative role to approve or disapprove updates on devices managed by Onsite Manager.

    This option does not apply to Windows 10 or Windows Server 2016.
13. Click **Save**.