Selecting Devices to Update

https://campus.barracuda.com/doc/89620980/

In order to use Advanced Software Management to apply updates, you must purchase an additional license. Contact your Barracuda sales representative.

You can select devices that are eligible for Advanced Software Management two ways:

- Automatically, by creating rules that include devices that match specific criteria. See To create rules that automatically apply devices to Advanced Software Management policies. If you select devices and groups using automatic application rules, the devices are not under Advanced Software Management until the Advanced Software Management policy is added to an active Service Plan or a Service in an active Service Plan. See Adding an Advanced Software Management policy to a Service.
- Manually, by selecting individual devices and groups. See Adding Devices or Groups to a Patch Policy Manually. If you select devices and groups manually, the selected devices and groups are under Advanced Software Management from the time you select them.

Working with Rules to Automatically Include Devices in Advanced Software Management Policies

Automatic application rules are one method to determine which devices are eligible to have the Advanced Software Management policy applied. For example, if you are creating a policy for workstations only, you can set up an automatic application rule to exclude devices with the word “server” in the OS name.

When adding devices using auto-application rules, you can create multiple rules that add devices when those devices meet those criteria. If you use the And operator, devices are added when they meet all the criteria you set up. If you use the Or operator, devices are added when they meet any of the criteria.

If you want to exclude devices from the Advanced Software Management policy even though they meet the criteria, you can identify them using the To exclude devices from an Advanced Software Management policy procedure.

Automatic application rules do not come into effect until the patch policy has been added to an active Service Plan or by adding it to a Service in an active Service Plan.

The process for setting up automatic application rules is the same for Advanced Software Management policies as it is for all other policy types (i.e, patch, monitoring, automation, and Avast Antivirus).

You can test the automatic application rules you have created to see which devices will be included when the policy is added to an active Service Plan or a Service in an active Service Plan by following the To preview automatic application rules for Advanced Software Management policies procedure.

To create rules that automatically apply devices to Advanced Software Management policies

Automatic application rules do not come into effect until the Advanced Software Management policy has been added to an active Service Plan or by adding it to a Service in an active Service Plan.

1. In Service Center, click **Configuration** > **Policies** > **Advanced Software Management**.
2. Click the name of the patch policy in which you want to create an automation inclusion rule.
3. Click the **Automatic Application** tab.
4. Click **Add**.
5. Do any of the following:
    - Select an option in the **Type** box.
    - Select the criteria to search in the **Rule** box.
    - Select an operator in the **Operator** box.
    - Select an option in the **Value** box.
6. Click **Add**.
7. Repeat steps 4-6 until the rule is complete.
8. Click **Save**.

When you apply Advanced Software Management policies to devices using automatic application rules, those devices are not under Advanced Software Management until the policy is added to an active Service Plan or a Service in an active Service Plan. See Adding an Advanced Software Management policy to a Service.

To preview automatic application rules for Advanced Software Management policies

After creating the automatic inclusion rules and defining a scope, you can preview the devices that the rules will include. Previewing lets you verify that the automatic application rules you created will add all the devices you want included.

The Auto-Application Preview page displays a list of devices, including information such as the site, IP Address, a description, and a green check mark to indicate whether it is SNMP- or WMI-enabled.

1. In Service Center, click **Configuration** > **Policies** > **Advanced Software Management**.
2. Click the policy name.
3. Click the **Automatic Application** tab.
4. Click **Preview**.
5. When you are finished previewing, click **Close**.

To exclude devices from an Advanced Software Management policy

You can exclude specific devices from a patch policy. When you add a device to the exclusion list, it will not have this Advanced Software Management policy applied, even if the device meets the criteria outlined in the automatic application rules and the patch policy is applied to the site or group to which the device belongs.

1. In Service Center, click **Configuration** > **Policies** > **Advanced Software Management**.

2. Click the name of the patch policy from which you want to exclude devices.
3. Click the **Excluded Devices** tab.
4. Click **Add**.
5. Use the filters at the top to narrow your selection, and click **Filter**.
6. Select the check box beside each device you want to exclude from the policy.
7. Click **OK**.
8. Click **Save**.

You can exclude multiple devices in a site or group by selecting Site or Group from the Filter By list, and then selecting the check box at the top of the list of returned devices to exclude all devices listed.

Adding Devices or Groups to a Patch Policy Manually

1. In Service Center, click **Configuration** > **Policies** > **Advanced Software Management**.
2. Click the name of the patch policy to which you want to add devices or groups.
3. Click the **Manual Application** tab.
4. Do one of the following to apply the patch policy to a group or device:
    - In the **Applied Groups** area, click **Add**. Filter on the **Group Type**, if desired. Click the group and click **OK**.
    - In the **Applied Devices** area, click **Add**. Filter the list of devices. Select the check box beside the device and click **OK**.

You can view the Advanced Software Management policies applied to service and site groups on the Groups page, by going to **Configuration** > **Groups**, clicking the group name, and then clicking the Policies tab. For more information, see Viewing the Policies Applied to a Group.

Removing Devices or Groups from an Advanced Software Management policy

1. In Service Center, click **Configuration** > **Policies** > **Advanced Software Management**.
2. Click the name of the patch policy you want to add to devices or groups.
3. Click the **Manual Application** tab.
4. Do one of the following:
    - To select one device or group at a time, select the check box that corresponds with each device you want to remove.
    - To select all the devices or groups at once, select the check box at the top of the column.
5. Click **Remove**.