Creating a Patch Policy

Patch policies are used to patch some or all of the software that Automox natively supports.

From the main console, click Manage > Policies. Click Create Policy. The following types of patch policies are available and are described here.

**Note**: For information about configuring user notifications or setting a patching schedule, refer to Managing End-User Notifications and Setting a Patching Schedule.

Patch All

Use this policy type to patch all supported software. This includes all operating system patches and supported third-party software.

To create a Patch All policy, follow these steps:

1. From the Policy page, click Create Policy.
2. From the Create Policy page, click Patch > All.
3. Click Next.
   **Note**: You can use the Type menu to switch between patch policy types.
4. In the Info area of the Create Patch All Policy page, configure the following:
   - In the Policy Name field, enter a unique name for the policy. This field is required.
   - In the Notes field, enter any notes, if required.
5. Switch the Policy Status to Active or Inactive. This will enable or disable patching. If you want to pause patching, select Inactive.
6. To automatically install any Windows updates, choose Yes for the Install Optional and Recommended Windows Update. The default is No.
7. (Optional) Set filters under Device Targeting, as needed.
8. Set the patching schedule.
9. (Optional) From the User Notifications section, select what kind of notifications you want.
10. To assign this policy to a group, click Associate Groups. Select a group or groups that you want associated.
Patch Only

For this type of policy, you can select all packages that you want patched. Use the filter options to find these packages. Select the checkbox next to each package that you want to include in the patch. Your selections will appear on the right.

To create a Patch Only policy, follow these steps:

1. From the Policy page, click **Create Policy**.
2. From the Create Policy page, click **Patch > Only**.
3. Click **Next**.
4. In the Info area of the Create Patch Only Policy page, configure the following:
   - In the Policy Name field, enter a unique name for the policy. This field is required.
   - In the Notes field, enter any notes, if required.
5. Switch the Policy Status to Active or Inactive. This will enable or disable patching. If you want to pause patching, select Inactive.
6. To automatically install any Windows updates, choose Yes for the Install Optional and Recommended Windows Update. The default is No.
7. (Optional) Set filters under **Device Targeting**, as needed.
8. Use the **Package Targeting** area to identify and select specific packages that you want to patch.
   - Select the Automox Supported checkbox to filter the list for only software packages that are managed by Automox.
   - Use the filter field or scroll through the list of packages associated with this device.
   - Select the checkbox next to each package that you want to include in the patch.
   - Your selections will appear on the right.
   - See the information tip in the console for further guidance.
9. Set the patching schedule.
10. (Optional) From the User Notifications section, select what kind of notifications you want.
11. To assign this policy to a group, click **Associate Groups**. Select a group or groups that you want associated with this policy. Click **OK**.
12. Click Create Policy.

**Patch All Except**

For this type of policy, you can select all packages that you do not want patched. Use the filter options to find these packages. Select the checkbox next to each package that you want to exclude from the patch. Your selections will appear on the right.

To create a Patch All Except policy, follow these steps:

1. From the Policy page, click **Create Policy**.
2. From the Create Policy page, click **Patch > Except**.
3. Click **Next**.
4. In the Info area of the Create Patch All Except Policy page, configure the following:
   - In the **Policy Name** field, enter a unique name for the policy. This field is required.
   - In the **Notes** field, enter any notes, if required.
5. Switch the **Policy Status** to Active or Inactive. This will enable or disable patching. If you want to pause patching, select Inactive.
6. To automatically install any Windows updates, choose **Yes** for the **Install Optional and Recommended Windows Update**. The default is No.
7. (Optional) Set filters under Device Targeting, as needed.
8. Use the **Package Targeting** area to identify and select packages that you do not want to patch.
   - Select the **Automox Supported** checkbox to filter the list for only software packages that are managed.
9. Set the patching schedule.

10. (Optional) From the User Notifications section, select what kind of notifications you want.

11. To assign this policy to a group, click **Associate Groups**. Select a group or groups that you want associated with this policy. Click **OK**.

12. Click **Create Policy**.

---

### Manual Approval

A manual approval policy is used to only install patches that are approved by an administrator. This policy type can be activated to run on a schedule at the frequency of your choice.

To create a manual approval policy, follow these steps:

1. From the Policy page, click **Create Policy**.
3. Click Next.
4. In the Info area of the Create Manual Approval Policy page, configure the following:
   - In the Policy Name field, enter a unique name for the policy. This field is required.
   - In the Notes field, enter any notes, if required.
5. Switch the Policy Status to Active or Inactive. This will enable or disable patching. If you want to pause patching, select Inactive.
6. To automatically install any Windows updates, choose Yes for the Install Optional and Recommended Windows Update. The default is No.
7. Click Associate Groups and select the group(s) that should be associated with this policy. Click OK.
8. (Optional) Set filters under Device Targeting, as needed.
9. Set the patching schedule.
10. (Optional) From the User Notifications section, select what kind of notifications you want.
11. Click Create Policy.

Managing Approvals

After the policy is created, you can view and manage packages that are ready for approval, or save the policy and manage approvals at a later time.

**Note:** The policy must be associated with at least one group for any packages to be available for approval.

1. To view the packages that are ready for approval, click Manage Approvals.
2. From the Packages Ready For Approval page, use the filters and search options to sort the list of packages.
3. Select the checkbox of packages that you want to approve or reject. Click Approve or Reject for each package, or for a group of selected packages.
   **Note:** When you approve a patch, the software is applied on the policy’s next scheduled update.
4. Click Edit Policy to return to the Manual Approval Policy page.

**Note:** The package scope here is limited to only the devices associated with the group or groups associated with the policy.
Note: When you click Manual Approval from the dashboard, the Packages Ready For Approval page provides a list of all packages that fall under any manual approval policy that exists in the system.

By Severity

Use this policy type to select the severity level you want to have included in the patch update: Critical, High, Medium, Low, None, and Unknown. You can select multiple severities. The severity levels are defined by the CVE score. See also Understanding Automox Severity Data.

To create a By Severity policy, follow these steps:

1. From the Policy page, click Create Policy.
2. From the Create Policy page, click Patch > Severity.
3. Click Next.
4. In the Info area of the Create By Severity Policy page, configure the following:
   - In the Policy Name field, enter a unique name for the policy.
   - In the Notes field, enter any notes, if required.
5. Switch the Policy Status to Active or Inactive. This will enable or disable patching. If you want to pause patching, select Inactive.
6. To automatically install any Windows updates, choose Yes for the Install Optional and Recommended Windows Update. The default is No.
7. (Optional) Set filters under Device Targeting, as needed.
8. Use the Package Targeting area to select the severities that you want to have patched. You can select one or
all of the following severity types: Critical, High, Medium, Low, None, and Unknown.

9. Set the patching schedule.

10. (Optional) From the User Notifications section, select what kind of notifications you want.

11. To assign this policy to a group, click Associate Groups. Select a group or groups that you want associated with this policy. Click OK.

12. Click Create Policy.

---

**Advanced Policy**

Use the advanced patch policy to create custom patching configurations by choosing certain conditions that best match the desired compliance requirement for the device.

To create an advanced patch policy, follow these steps:

1. From the Policy page, click Create Policy.

2. From the Create Policy page, click Patch > Advanced.

3. Click Next.

4. In the Info area of the Create Advanced Policy page, configure the following:
   - In the Policy Name field, enter a unique name for the policy.
   - In the Notes field, enter any notes, if required.

5. Switch the Policy Status to Active or Inactive. This will enable or disable patching. If you want to pause patching, select Inactive.

6. To automatically install any Windows updates, choose Yes for the Install Optional and Recommended Windows Update. The default is No.

7. (Optional) Set filters under Device Targeting, as needed.

8. Use the Package Targeting area to select the conditions that you want to have patched. See Package Targeting for details.

9. Set the patching schedule.

10. (Optional) From the User Notifications section, select what kind of notifications you want.

11. To assign this policy to a group, click Associate Groups. Select a group or groups that you want associated with this policy. Click OK.
12. Click Create Policy.

Package Targeting

In addition to setting filters to target specific devices, you can add package targeting to your advanced policy. This is a custom patching configuration that targets packages according to the filter options that fit your requirements.

The following are the current options for package targeting:

- Patch Source (Microsoft, Apple, etc)
- Patch OS
- Type (Windows Only)
- Display Name
- Patch Severity
- Patch Age

Example for Package Targeting: Patch OS

- In the following example, we select Patch OS as the first condition which targets all patches based on the OS the device is running. This example is targeting any device that is running Microsoft Windows.
Example for Package Targeting: Patch Severity

- You can add as many conditions as desired. The policy will continue to refine the list of patches it will remediate it runs on the devices. In the following same example, you can see that Patch Severity was added as an additional condition, for which the severity is Critical.

Example for Package Targeting: Patch Age

- You can also add the option to target only packages that are over a certain number of days old. Use the option Patch Age and set a number between 1 and 180. Use this option if you want to only push a patch if the patch was released x number of days ago. This is useful if you do not want to push out brand new patches on your production devices until there has been a period of time that has passed.

Note: This option is currently only available for Advanced policies.

After you configure all of the conditions, to preview the patches that will be remediated by the policy, click Preview Package That Would Be Patched. This will show all of the packages that are targeted by the policy for remediation.
<table>
<thead>
<tr>
<th>OS</th>
<th>Package Name</th>
<th>Severity</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Security Update (KB5076334)</td>
<td>Critical</td>
</tr>
<tr>
<td></td>
<td>Security Update for Windows Server 2016 for x64-based Systems (KB4528344)</td>
<td>High</td>
</tr>
<tr>
<td></td>
<td>2019-05 Security Monthly Quality Rollup for Windows 7 for x64-based Systems</td>
<td>Critical</td>
</tr>
<tr>
<td></td>
<td>(KB4479164)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2020-05 Cumulative Update for Windows 10 Version 1909 for x64-based Systems</td>
<td>Critical</td>
</tr>
<tr>
<td></td>
<td>(KB4551357)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2020-04 Cumulative Update for Windows 10 Version 1909 for x64-based Systems</td>
<td>Critical</td>
</tr>
<tr>
<td></td>
<td>(KB4551357)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Security Update for Windows 7 for x64-based Systems (KB2738385)</td>
<td>Critical</td>
</tr>
<tr>
<td></td>
<td>Security Update for Windows 7 for x64-based Systems (KB3191103)</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>Security Update for Microsoft .NET Framework 3.5.1 on Windows 7 and Windows</td>
<td>Medium</td>
</tr>
<tr>
<td></td>
<td>Server 2008 R2 SP1 for x64-based Systems (KB2011990)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2020-04 Cumulative Update for Windows 10 Version 1903 for x64-based Systems</td>
<td>Critical</td>
</tr>
<tr>
<td></td>
<td>(KB4599017)</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2021-03 Cumulative Update for Windows 10 Version 2004 for x64-based Systems</td>
<td>Critical</td>
</tr>
<tr>
<td></td>
<td>(KB4506080)</td>
<td></td>
</tr>
</tbody>
</table>