Creating Reports

You can create reports that provide information about the devices in your zone. The following reports are available from the Reports page. To view each type of report, click View.

The following reports are described here:

- Activity Log
- Overview Report
- Needs Attention Report
- Pre-patch Report

**Activity Log**

The activity log tracks all automated and manual actions taken over a given period of time on the devices in your zone.

- Use the filter options to create the desired report.
- Click the Export CVS button to export this information to a CSV file.
- Click the name of the device to view the Device Details page.
- Select Full Logs for more information.
Note: The logs that are generated represent complete and unfiltered data from your zone. The following filtering and searching options enable you to fine-tune and export the results you want.

Filtering and Searching in the Activity Log

The filter panel to the left of the activity log list is made up of different types of options to fine-tune your report. You can filter the list of activity logs by date, policy type, policy name, and device name. When you select any of the individual filters, the resulting log list automatically updates. You can clear selections individually, or select Reset Filters to clear all.

You can hide or show the filter panel, as needed. The filter panel shows by default.

Search by date

Use the Date Range options to find the desired activity log results. The last selection is saved in local storage and becomes the new default.
Note:

- Custom reports are limited to a maximum date range of 31 days.
- Data is filtered by UTC.

Select from the options or create a custom date range search by using the calendar options.

**Search by policy type**

Click the *All Policy Types* drop-down list to filter results by Patch, Worklet, or Required Software.

**Search by policy name**

Click the *All Policies* drop-down list to filter results by the name of any policy in your zone.

**Search by device name**

Use the *Device Name* field to search for a specific device or devices. This search will show all entries that match any of the individual search criteria you set.
Search by log details

Use the search box at the top to find logs for specific details listed in the Log Summary column such as package names and KBs. Click Full Logs for complete information about the logged activity.

By entering a string, the list populates with matching entries. You can use multiple strings to narrow your search results.

Sorting search results

You can sort the list of results by clicking the arrow at the column heading. This type of sort is available for Device Name, Policy Name, and Event Time columns.

Note: The search parameters you select are now stored in the page URL. The back button in your browser functions as expected and filter searches can now be bookmarked and shared.

Overview Report

The overview report provides a summary of the state of devices in your zone. This includes the device overview, history of patches applied, and patches by group. Total patches refers to all available patches and Pending updates are any scheduled patches based on the patch policies.

Click highlighted text to jump to a filtered list of devices.
Needs Attention Report

This report provides a list of devices that need attention. Any relevant information about the devices is listed here. This report can be run for an individual group or all groups.

Creating a Needs Attention report

1. From the Reports page, click View for Needs Attention Report.
2. Click Select Group from the drop-down menu. Scroll to select the group you want a report for.
   Note: You can select an individual group or All Groups.
3. The report opens in a new window.

4. To switch between groups, select Choose Group Option.

You can use the search bar to narrow down results
You can sort by clicking on the column heading
You can set the page view up to 500 rows

You can easily spot any devices that need attention. The report includes the following information:

<table>
<thead>
<tr>
<th>Needs Attention Report Details</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Endpoint Name</td>
<td>This is the name of the device in your zone. This name can be searched for on the Devices page.</td>
</tr>
<tr>
<td>Policy</td>
<td>This field lists any policies the device is associated with.</td>
</tr>
<tr>
<td>Status</td>
<td>This shows the connection status of the device.</td>
</tr>
<tr>
<td>Last Scanned</td>
<td>This shows the last time the system scanned the device.</td>
</tr>
<tr>
<td>Issue</td>
<td>The reason the device needs attention is listed here.</td>
</tr>
<tr>
<td>Severity</td>
<td>The severity level is provided here. See also the following severity codes table.</td>
</tr>
<tr>
<td>Days Exposed</td>
<td>Calculated based on the first time the package was detected.</td>
</tr>
</tbody>
</table>

CVE Severity Codes:

Severity levels are determined by Automox in the following manner:
This report shows you a list of all scheduled patches per device. The severity and exposure information allows you to effectively assess any internal impact to your zone. This report can be run for an individual group or all groups.

Creating a Pre-patch report

1. From the Reports page, click View for Pre-Patch Report.
2. Click Select Group from the drop-down menu. Scroll to select the group you want a report for.
   
   **Note**: You can select an individual group or All Groups.
3. The report opens in a new window.
4. To switch between groups, select Choose Group Option.
The report includes the following information:

<table>
<thead>
<tr>
<th>Pre-patch Report Details</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Software Name</td>
<td>Name of the available software</td>
</tr>
<tr>
<td>CVE</td>
<td>CVE associated with the scheduled patch</td>
</tr>
<tr>
<td>Severity</td>
<td>Severity level of the scheduled patch. See also Understanding Automox Severity Data.</td>
</tr>
<tr>
<td>Days Exposed</td>
<td>Calculated based on the first time the package was detected</td>
</tr>
<tr>
<td>Patch Window</td>
<td>The date and time that the update will start</td>
</tr>
</tbody>
</table>

Note: You must manually refresh the page to see any updated data.