Device Scout

Overview

Device Scout checks devices against a repository of recommended security controls or any custom controls to reflect security requirements needed for a school or district environment. The repository of rules for compliance are established by recommendations from many recognized cybersecurity agencies and are mapped to CIS and NIST frameworks, as well as a set of proprietary rules. Select any/all rules to apply to the devices and ensure they are in compliance. Enable auto-remediation so that non-compliant devices are automatically corrected to be in compliance with the specific security control.

For Mac computers, the agent is leveraged for compliance scans. Therefore, the Mosyle Manager app must be installed.

Click the Security tab and expand the Device Scout menu option in the left menu bar. Device Scout is organized into four sections:

- Overview
- Devices
- Security Controls
- Logs (macOS Only)

Overview

The Overview pane provides a quick summarized view of your device compliance status. You can view the following in this area:

Device Scout Score: The score is calculated based on the security controls applied and device compliance status. The higher the score, the more secure your devices are.

Based on your Security Controls (macOS): Use the dropdown menus to view the top controls or top devices that are compliant or not compliant.

Top Rules among All Schools (macOS): A list of the top rules activated across all Mosyle companies.

Evolution over Time / You vs All Schools: View the compliance average or max active rules over a period of time for your school and other Mosyle schools.

What changed?: View any recent changes in the compliance status.

device-scout.png

Security Controls

View a list or grid of all active Security Controls. To change views, use the dropdown on the right side of the screen to choose between “Grid View” or “List View”.

Each control will show the rule name, associated security benchmarks, the percentage of devices in compliance, as well as if remediation is turned on or not. Favorite any controls to make sure they show at the top of the list by clicking the star icon in the rule box. To refresh and update the controls to show the latest compliance status, click the refresh button within the rule. Device compliance status is checked every hour.

Using the filter, choose to view the rules based on: show only favorites, by security baselines, if remediation is available or unavailable, or if remediation is enabled or not enabled.

Search for specific Security Controls using keywords and sort based on the control name or compliance percentage.

Click + New Control at any time to add additional Security Controls. When adding controls, choose to use controls from Mosyle's Repository or by creating your own custom Security Control.

Use the Bulk Assignment or Bulk Remove buttons to assign controls to devices in bulk, or remove compliance checks for controls in bulk.

Devices that are not in compliance with the controls assigned will automatically be grouped into a “Security Group”, categorized by each control. Use these Security Groups when assigning management profiles as needed.

rules.png

Devices

View a list of devices assigned to security controls and their corresponding compliance status. Clicking on a device tile will bring up a detailed list of the security controls assigned, which are compliant, and give you the ability to automatically remediate controls not in compliance. Click the link to open a new tab to view additional device info.

Filter the list of devices by: serial number, device name, asset tag, deviceUDID, Wifi MAC Address, Ethernet MAC Address, user assigned, grade levels, and more.

Sort the list of devices by the device name or compliance percentage.

After filtering and sorting devices as needed, export a spreadsheet of the devices and security controls by clicking the button in the upper right corner that indicates X devices match filters. The spreadsheet will include a list of devices (device name and serial number) and all assigned controls along with the compliance status.

Logs

View logs to see detailed info for when a device became compliant or lost the compliance status. In addition to the compliance status, the control name, date/time stamp, device name and serial number are listed. The logs provide detailed reports containing necessary information for any potential internal and external audits.

To export a list of devices and the compliance status, go to the Security tab and click the Devices menu option under Device Scout. Filter the devices as needed and click the Export button in the upper right to export in a CSV or XLSX file format.

Configuring Controls

When first accessing the Device Scout Overview area under the Security tab, a list of controls available from the Mosyle repository will be displayed that can be activated. Select any controls to scan for compliance and assign the devices. When finished, click Start.

To add more controls to be checked for compliance, go to the Security tab > Device Scout > Security Controls > + New Control. Choose a rule from the Mosyle Repository or create your own custom control.

new-control.png

After checking the box for the rule, click the button to “Enable Tracking”. Select the users and/or devices to assign the control to and click “Enable”.

control-repository.png

Once controls are enabled, they'll be listed in the Security Controls area. Click any of the controls to view detailed information about the control, change assignments, and/or turn on auto-remediation.

Configuring Custom Controls

To configure a custom control, go to the Security tab > Device Scout > Security Controls > + New Control. Choose “Create a New Security Control”.

Name the control, choose an icon, add tags and/or framework mapping or reference. Enter the code that should be run on devices to check for compliance. Be sure to include specific output that can be used to define devices in compliance or not. Define what should be considered compliant under “Results for Compliance”, anything that doesn't meet the definition will be considered not in compliance. Add the assignment and save.

To remediate the custom control, go to the Management tab and use any of the Management profiles, including Custom Commands, to create the profile or configuration to remediate the control. When assigning the profile for remediation, assign it to the automatically created Security Group for devices not in compliance with the control.

Compliance Checks

Devices are checked for compliance during every device info update. The device info update is automatically requested every hour, so long as the device remains online and reachable. If the device is not online, the update of device info along with any compliance checks will be pending. Once the device is back online, the commands will go through and the compliance status as well as the device info will update. For Mac computers, the compliance checks rely on the Mosyle Manager app being installed on the Mac.

If a device has not responded to a compliance status check in over 5 days, the compliance will change to “Not compliant” until the device checks back in to confirm it's current status.

Auto-Remediation

Auto-remediation is completed using a combination of management profiles and/or customized commands created by our Developers. When auto-remediation is turned off, or the security configurations are unassigned, the remediations installed via profiles will be removed from the device and the security control will no longer be enforced. Any other remediations that were not applied via profiles, rather were processed using customized commands, will no longer be executed. Turning off auto-remediation does not revert any settings.

If auto-remediation is turned on, it's recommended to not duplicate any controls or policy configuration through Management profiles to avoid any unexpected side effects. For example, if passcode controls are configured in Device Scout with auto-remediation enabled, it's not recommended to also push a Passcode Policy payload.

Revision #1
Created 2025-10-08 00:44:46 UTC by joliveira
Updated 2025-10-08 00:45:53 UTC by joliveira