

# Guide: Apply a Baseline Configuration via Custom Policy

1 Navigate to <https://console.jumpcloud.com/#/configurations>

2 Click here.

The screenshot shows the JumpCloud console interface. On the left is a dark sidebar with navigation items: Users, User Groups, USER AUTHENTICATION (LDAP, RADIUS, SSO Applications, Password Manager), DEVICE MANAGEMENT (Devices, Device Groups, Policy Management (marked as NEW), Policy Groups, Commands, MDM). The main content area has two blue configuration cards: 'Disable USB mass storage devices' (prevents mounting of removable storage) and 'Lock Down Control Panel & Device Preferences' (selectively disables control panel options). Below these is a search bar with 'OS : darwin' and a table of policies:

<input type="checkbox"/>	Type	Name ^
<input type="checkbox"/>	Apple	<b>Allow Activation Lock</b> Allow Activation Lock
<input type="checkbox"/>	Apple	<b>Analytics</b> Analytics
<input type="checkbox"/>		<b>baseline</b>

### 3 Click "Mac"

The screenshot shows the 'New Policy' page in the Mac section. The page has a header with 'ement' and 'Product Tour' links. Below the header, there are tabs for 'Windows', 'Mac', 'Linux', 'iOS', 'Android', and 'Recommended'. The 'Mac' tab is selected and highlighted with an orange circle. A search bar is located below the tabs. The main content area is a table with two columns: 'Name' and 'Description'. The table lists three policies: 'Advanced: Custom Registry Keys', 'Allow System To Be Shutdown Without Having To Logon', and 'Allow The Use of Biometrics'. The 'Mac' tab is highlighted with an orange circle.

Name	Description
Advanced: Custom Registry Keys <i>Enterprise Settings, Configuration</i>	Utilize custom policies to enforce configurations already offer in our standard policies.
Allow System To Be Shutdown Without Having To Logon <i>Enterprise Settings</i>	This policy will ensure the system is able to be shutdown without having to logon.
Allow The Use of Biometrics	Help strengthen authentication and guard against unauthorized access to the Windows Hello service.

### 4 Click "configure"

The screenshot shows a list of policies on the 'New Policy' page. Each policy entry consists of a description and a 'configure' button. The 'configure' button for the 'Distribute custom MDM configuration profiles using this policy.' entry is highlighted with an orange circle.

This policy grants Full Disk Access permissions through a Privacy Preferences Policy Control (PPC) policy for the Malwarebytes' Nebula agent on macOS devices.	configure
This policy lets you manage login items for macOS devices based on their Bundle Identifier, launchd plist label, or Apple code signing Team Identifier.	configure
This policy allows admins to manage device behavior for Apple's Rapid Security Response security fixes on macOS 13 and later.	configure
Distribute custom MDM configuration profiles using this policy.	configure
This policy configures the device timezone and NTP Server.	configure
This policy manages the ability of non-JumpCloud users to change their password through System Preferences on selected machines.	configure
Control access to Shutdown, Restart, Sleep, and Power Off options at the login window and under the Apple menu.	configure

5 Click "upload file"

The screenshot shows a settings page for mobile configuration. On the left is a vertical navigation menu with letters A, b, C, C, C, D, F. The main content area has two sections: 'Policy Activation' with the text 'Applies the provided mobileconfig configuration to the device using the MDM protocol. You must set up an Apple MDM Certificate before this policy takes effect.' Below this is a 'Settings' section with a sub-section 'Mobile Configuration File' containing a teal 'upload file' button, which is circled in orange.

6 Click "Device Groups"

The screenshot shows a policy details page. At the top right are links for 'Product Tour', 'Pricing', and 'Alerts'. Below is a navigation bar with tabs: 'Details', 'Policy Groups', 'Device Groups' (circled in orange), and 'Devices'. On the left is a sidebar with an Apple logo shield icon, the text 'Policy', and a 'Learn more' link. The main content area displays the title 'Mac - MDM Custom Configuration Profile Policy' and fields for 'Policy Name' (MDM Custom Configuration Profile) and 'Policy Notes'.

7 Click this checkbox.

**NEW POLICY**

JumpCloud MDM enrollment [Learn more](#)

Type	Name	Count
Apple	Android	2
Apple	Android	0
Apple	Android	0
Apple	Android	1
Apple	Android	0
Apple	Android	1
Apple	Android	0

<input type="checkbox"/>	<b>All Systems</b> Group of Devices	0
<input type="checkbox"/>	<b>Android Devices</b> Group of Devices	2
<input type="checkbox"/>	<b>AutoGroup-Linux</b> Group of Devices	0
<input checked="" type="checkbox"/>	<b>AutoGroup-Mac</b> Group of Devices	1
<input type="checkbox"/>	<b>AutoGroup-Windows</b> Group of Devices	0
<input type="checkbox"/>	<b>CIS_machine</b> Group of Devices	1
<input type="checkbox"/>	<b>Commands in Bulk</b> Group of Devices	0

8 Click "save"

<b>p-Windows</b> ices	0	Static	
<b>hine</b> ices	1	Static	
<b>Is in Bulk</b> ices	0	Static	
<b>Test</b> ices	0	Static	
<b>ices</b>	1	Static	iOS/iPadOS Automated Device Enrollment
<b>es</b> ices	1	Static	iOS/iPadOS User Enrollment

cancel save

9

Click "Save"

