

Device Security Posture Assessment Guide

Cloudbrink's [Device Security Posture Assessment](#) enables organizations to provide a robust Zero-Trust Access solution, emphasizing the continuous assessment of user device postures for compliance with corporate security standards. Through the admin portal, administrators can seamlessly define and manage the Device Security Posture Assessment (DSPA) feature.

This document provides an overview and basic configurations for the DSPA feature.

Overview

Device Posture Assessment comprises of two main categories:

- DSPA **Profile** - Defines what device checks to query
- DSPA **Policy** - Determines actions to take based on profile criteria

The table below highlights key DSPA Profile configurations with extensive options in each category.

OS Level Categories		
Windows	MacOS	Linux
Firewall	Firewall	Firewall
OS	OS	OS
Disk Encryption	Disk Encryption	Disk Encryption
File	File	File
Blacklisted Processes	Blacklisted Processes	Blacklisted Processes
Certificates	Certificates	
Patch	Trust Domain	
Registry		
Anti-Virus/Spyware		

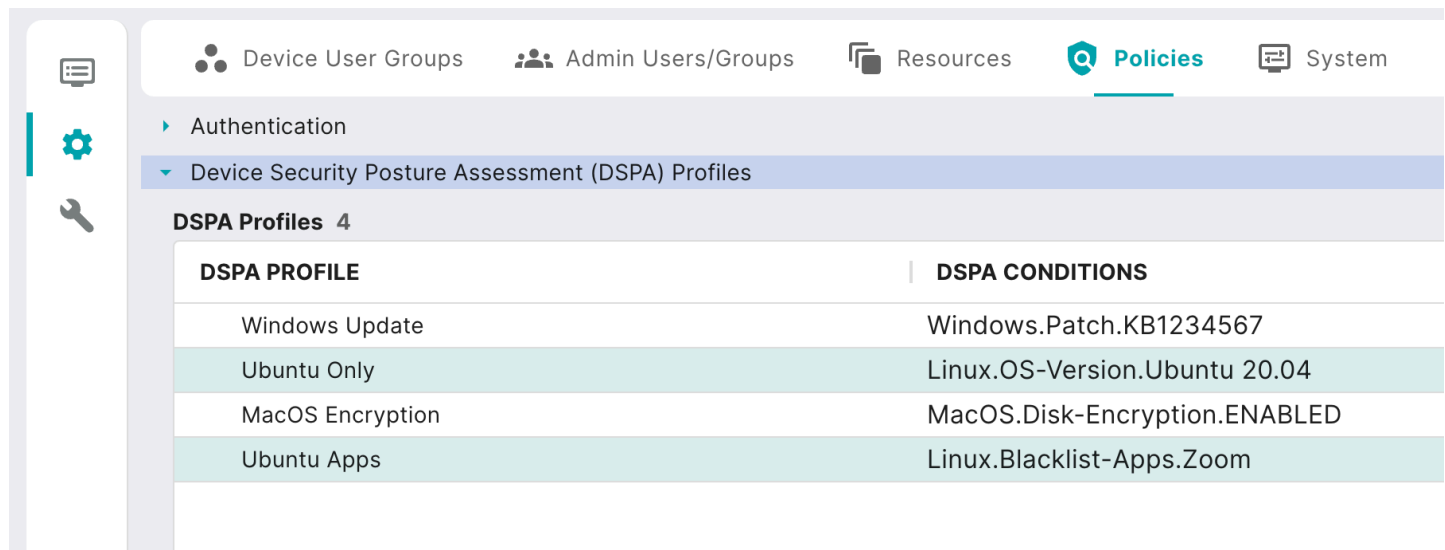
Configuration

In order to configure the DSPA feature, first log in with an account with administrative privileges at admin.cloubrink.com

- Select the “Configuration” gear on the left, followed by the “Policies” tab at the top.


Device Profiles

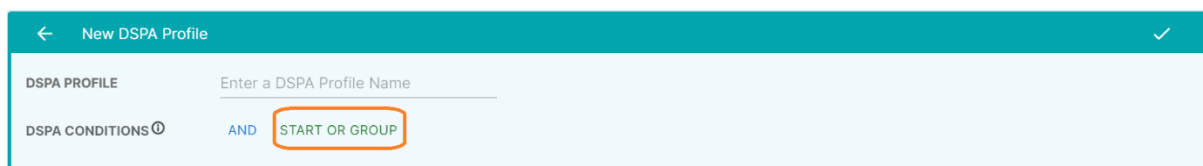
- Select the “Device Security Posture Assessment (DSPA) Profile” option.
- The drop down will list any already created profiles, their conditions, and the option to create new profiles.



The screenshot shows the Cloudbrink interface with the 'Policies' tab selected. On the left sidebar, there are icons for a list, settings (gear), and a wrench. The top navigation bar includes 'Device User Groups', 'Admin Users/Groups', 'Resources', 'Policies' (active), and 'System'. Under 'Policies', there is a dropdown menu with 'Authentication' and 'Device Security Posture Assessment (DSPA) Profiles' (selected). Below this, a section titled 'DSPA Profiles 4' contains a table with two columns: 'DSPA PROFILE' and 'DSPA CONDITIONS'.

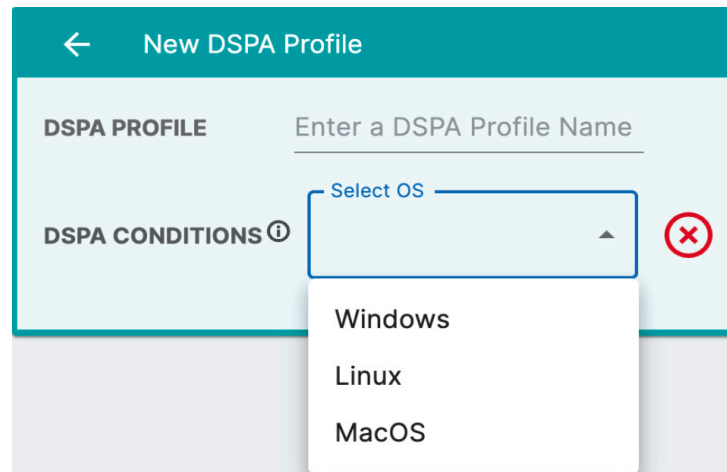
DSPA PROFILE	DSPA CONDITIONS
Windows Update	Windows.Patch.KB1234567
Ubuntu Only	Linux.OS-Version.Ubuntu 20.04
MacOS Encryption	MacOS.Disk-Encryption.ENABLED
Ubuntu Apps	Linux.Blacklist-Apps.Zoom


- Click the  logo in the bottom right to create a new profile.
- Enter a DSPA Profile name, and select if want the conditions to be “AND” or “OR”.
 - “AND” statements require all compounding conditions to be true.
 - “OR” statements require only one of the conditions to be true.
- A set of OR conditions can be grouped along with other checks with an implicit AND operation across them.
 - For example, expressions are possible such as
 - {(A OR B) AND C}
 - {(A OR B) AND (C OR D) AND E}



The screenshot shows the 'New DSPA Profile' form. It has a teal header with a back arrow, the title 'New DSPA Profile', and a checkmark. The form has two main sections: 'DSPA PROFILE' and 'DSPA CONDITIONS'. The 'DSPA PROFILE' section has a text input field labeled 'Enter a DSPA Profile Name'. The 'DSPA CONDITIONS' section has a radio button for 'AND' (selected) and a button labeled 'START OR GROUP' which is highlighted with an orange border.

- After selecting the condition type, select the OS for the first condition you want to configure.




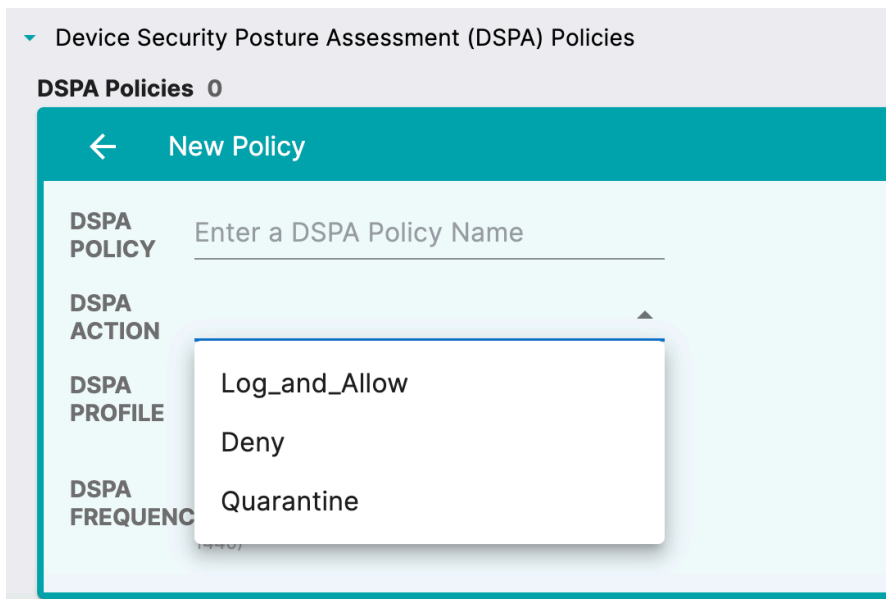
- Then, select the OS level category and it's value.
- When finished, select the  icon in the top right to save.
- Create as many profiles as needed, but one profile/policy can only apply to a single device user group.

Device Policies

Device Policies define what actions to take when the profile criteria is not met. The three actions available are:

1. **Log_and_Allow:** If profile criteria is not met, the user will still be permitted to sign on and provided the access defined by their device user group. The failure reasoning, and status will be logged in the portal for administrators to be aware or take action.
2. **Deny:** If profile criteria is not met, the user will be denied access. The failure reasoning, and status will be logged in the portal for administrators to be aware or take action.
3. **Quarantine:** If profile criteria is not met, the user will be placed into an admin defined resource template. This access can be at any required by your organization.
 - a. Example: If quarantined for not meeting an AV failure, quarantine resource template can be configured to only allow access to a subnet which the cyber security team can access the device from.
 - b. Example: If quarantined for not meeting patch level requirements, quarantine resource template can be configured to only allow access to a patch management server(SCCM, InTune, JAMF)

- Expand the DSPA policies, and click the  logo to create a new policy.
- Create a policy name, and select the action to take.



▼ Device Security Posture Assessment (DSPA) Policies

DSPA Policies 0

← New Policy

DSPA POLICY Enter a DSPA Policy Name

DSPA ACTION

DSPA PROFILE

DSPA FREQUENCY

Log_and_Allow

Deny

Quarantine

- Select the DSPA Profile to map to the DSPA Policy.
- In the DSPA Frequency field, select how often you want the DSPA profile criteria to be checked for.
 - DSPA Frequency of zero (0) will result in having the check run only at login.
 - Configuring an interval (in minutes) will result in the check being ran at login, and also on the interval configured
 - If the DSPA profile criteria are not met at any interval the policy states will change accordingly.

Apply

Apply the DSPA Policies to the desired device user group(s).

▼ Device User Group Policies

Device User Group Policies 3

DEVICE USER GROUP	RESOURCE TEMPLATE	DSPA POLICY
Engineering-Division	Engineering-Resource-Template	Ubuntu-Secure-Device
Marketing-Division	Marketing-Resource-Template	MacOS-Secure-Device
Sales-Division	Sales-Resource-Template	Windows-Secure-Device

Important Notes:

- File paths must be absolute. Do not use wildcards.
- Blacklist apps format based on the operating system:
 - c. Windows: <appName>.exe
 - d. Mac: <appName>.app
 - e. Linux: <appName>
- Patches must start with “KB” followed by numbers. Example: KB4487.
- Conditions are combined using “AND” by default unless specified in an “OR” group.
- “OR” groups must only contain conditions related to a single OS.

Support

We would love to hear from you! For any questions, concerns, or feedback regarding this feature, please reach out at support@cloudbrink.com

Corporate Headquarters Cloudbrink, Inc.
530 Lakeside Drive, Suite 190, Sunnyvale, CA 94085

