

Cloudbrink Mobile Access Policy and Mobile Device Posture Assessment

Cloudbrink's [Mobile Access Policy](#) enables administrators to customize accessible applications distinctly for mobile and desktop platforms, accommodating the variance in application usage across devices. [Mobile Device Posture Assessment](#) enables administrators to strengthen their security posture by ensuring only trusted devices are used by the users to access business applications.

Overview

With 13.1, Cloudbrink supports two new features that will augment the Brink Apps on mobile iOS/iPadOS and Android platforms.

- Mobile Access Policy
- Mobile Device Posture Assessment

Mobile Access Policy

Mobile access policies are a new configuration entity on the Cloudbrink administration portal that allows administrators to define separate sets of applications accessible over mobile platforms and desktop platforms.

The applications that users typically access over laptops are different than applications over mobile devices, though there are a subset of common applications. For example, users access datacenter servers (e.g., SSH, RDP) on laptops but not mobiles whereas an e-mail client is a common application on both platforms.

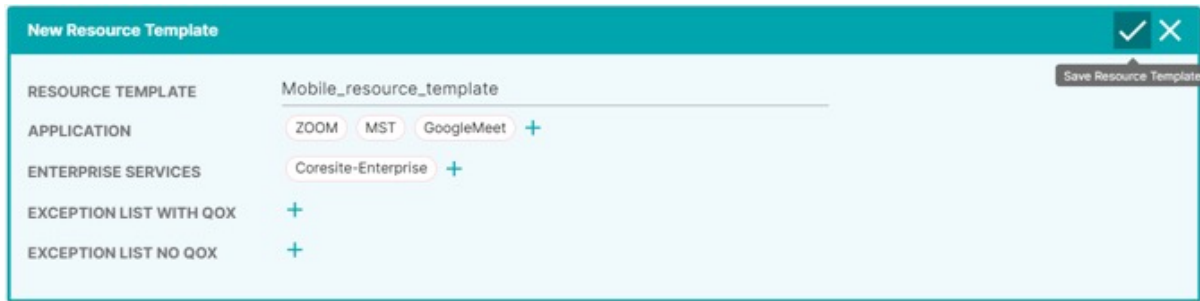
To provide the flexibility for administrators to define application sets for laptops and mobiles, a Cloudbrink mobile access policy configuration can be implemented.

NOTE: If a Mobile Access Policy configuration is not used, mobile platforms also will use same application set (resource-template) as that of the laptops.

Configuration

1. Log into the Cloudbrink Administrator portal with Administrative privileges
2. Create a new resource-template for mobile platforms

Configure > Resources > Resource Templates



The 'New Resource Template' dialog box is shown. It has a teal header with a checkmark and an 'X' icon. A 'Save Resource Template' button is in the top right. The form contains the following fields:

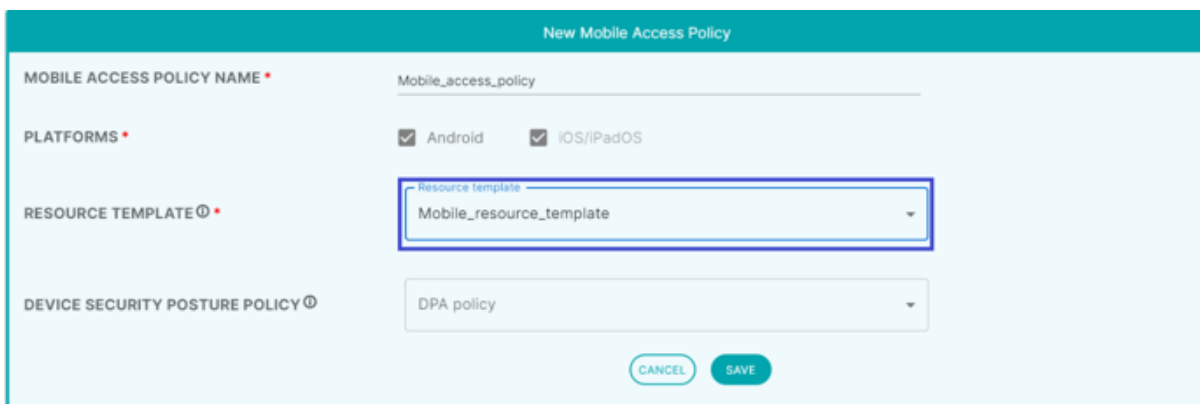
Field	Value
RESOURCE TEMPLATE	Mobile_resource_template
APPLICATION	ZOOM MST GoogleMeet +
ENTERPRISE SERVICES	Coresite-Enterprise +
EXCEPTION LIST WITH QOX	+
EXCEPTION LIST NO QOX	+

3. Create a new mobile access policy

Configure > Policies > Mobile Access Policies > Add

4. Select the newly created resource-template for mobile platforms from the drop-down

Configure > Policies > Mobile Access Policies



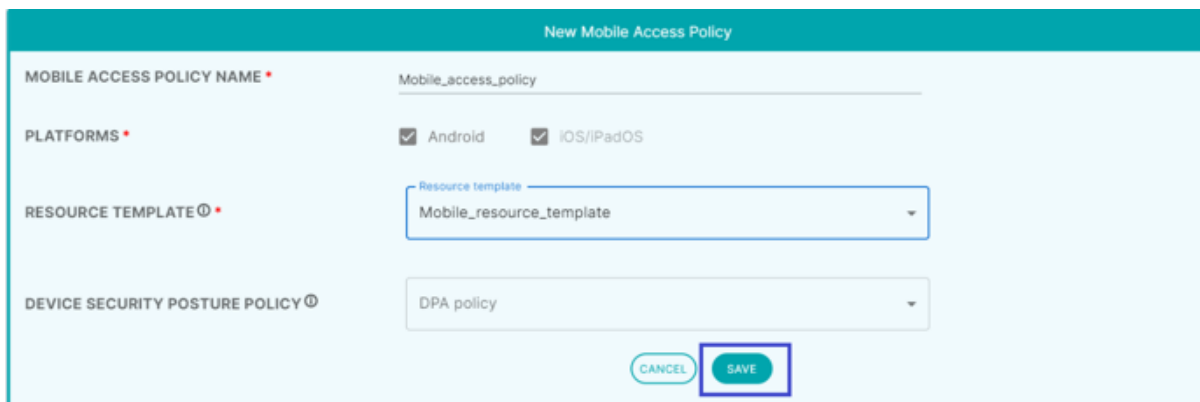
The 'New Mobile Access Policy' dialog box is shown. It has a teal header. The form contains the following fields:

Field	Value
MOBILE ACCESS POLICY NAME *	Mobile_access_policy
PLATFORMS *	<input checked="" type="checkbox"/> Android <input checked="" type="checkbox"/> iOS/iPadOS
RESOURCE TEMPLATE ⓘ *	Mobile_resource_template
DEVICE SECURITY POSTURE POLICY ⓘ	DPA policy

At the bottom are 'CANCEL' and 'SAVE' buttons. The 'RESOURCE TEMPLATE' dropdown is highlighted with a blue border.

5. Save the newly created mobile access policy

Configure > Policies > Mobile Access Policies



This is the same 'New Mobile Access Policy' dialog box as above, but the 'SAVE' button at the bottom right is highlighted with a blue border.

6. Assign mobile access policy to a device-user-group

Configure > Device User Groups > Device User Group Policies

The screenshot shows the 'VPN Template' configuration interface. It includes a header bar with a checkmark and a trash icon. Below the header, there's a 'Save Device User Group Policies' button. The main form has five rows, each with a label and a dropdown menu. The 'DEVICE USER GROUP' dropdown is set to 'VPN_ODBT'. The 'RESOURCE TEMPLATE' dropdown is set to 'VPN Template'. The 'DSPA POLICY' dropdown is empty. The 'DEVICE SESSION POLICY' dropdown is empty. The 'MOBILE ACCESS POLICY' dropdown is set to 'Mobile_access_policy'.

With the above sample configuration, users belonging to “VPN_ODBT” device-user-group will be able to access apps defined in resource-template “VPN Template” from their laptops and apps defined in resource-template “Mobile_resource_template” which is selected in the Mobile_access policy from their mobile devices.

Mobile Device Posture Assessment

Administrators can strengthen their security posture by ensuring only trusted devices are used by the users to access business applications. As part of the Cloudbrink Zero-Trust Security stack, Cloudbrink now supports device posture assessment for mobile platforms.

The advantages of the current device posture assessment feature for laptops are extended to mobile platforms as well.

1. Continuous device posture assessment: The device posture checks that an administrator has defined are executed periodically (the interval is configurable, default is 30 minutes) even if the user is not logged out of Cloudbrink. This will ensure that Cloudbrink can detect out-of-compliance devices in the shortest time possible.
2. Quarantine/Deny/Log_and_Allow actions: Administrators may choose to treat non-compliance devices in different ways. Administrators can either block the non-compliance device completely (Deny action) or put the device in a quarantine state with limited app access (Quarantine action) or simply allow full access but notify the administrator about non-compliance state (Log_and_Allow action)

Configuration

1. Create a new Device Posture Assessment profile with Mobile DPA checks

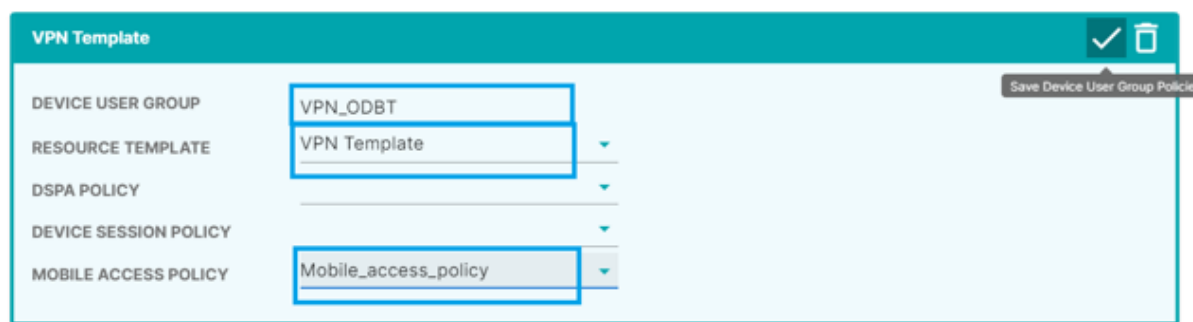
Configure > Policies > Device Security Posture Assessment (DSPA) Profiles

2. Create a new Device Posture Assessment policy by using the profile created in step-1, and set continuous check to 30 minutes

Configure > Policies > Device Security Posture Assessment (DSPA) Policies

3. Update the existing Mobile Access Policy (or create a new mobile access policy if one does not exist) and select the newly created Device Posture Assessment policy from the drop-down

Configure > Policies > Mobile Access Policies



VPN Template

✓ [trash icon]

Save Device User Group Policies

DEVICE USER GROUP	VPN_ODBT
RESOURCE TEMPLATE	VPN Template
DSPA POLICY	
DEVICE SESSION POLICY	
MOBILE ACCESS POLICY	Mobile_access_policy

With the above configuration, users can access business apps defined in the Mobile_resource_ template only if their device is not jailbroken (iOS/iPadOS) or rooted (Android). If the device is jailbroken/rooted, access will be denied (Deny action) to these business apps.

Support

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