

Brink App Upgrade Policy Guide

Cloudbrink Hybrid Access as a Service administrators can define the Brink App upgrade policy from the admin portal of Cloudbrink. The Brink App Upgrade Policy infrastructure provides highly flexible and granular controls for admins to define upgrade policies that meet their organizational needs.

This document covers the admin portal policy for management of the Brink App.

Overview

This document provides a comprehensive guide to the configuration settings and policy options available for Cloudbrink's Zero-Trust Access solution, ensuring optimal user and device authentication practices. It outlines steps to monitor device postures and respond to any security policy violations effectively.

Note: Admins can define a “minimum client version” criteria so that all the users of the organization are mandatorily at the certain minimum software version. This helps in avoiding any user using a very older version of the Brink App that can lead to security risks.

The upgrade policy provides support for defining a scheduled date-time in future from which the policy will become activated. This helps the admins to define the policy at any time of their convenience but triggering the upgrade policy at another time which is most suitable for upgrades.

The configuration section provides details of each configuration parameter in the upgrade policy.

Configuration

Brink App upgrade policy config is available under below path.

Cloudbrink Management Portal (admin.cloudbrink.com) -> Configure -> System -> Brink App Upgrade Policy

Configuration - Continued

By clicking the “ADD” button, administrators can define the upgrade policy using below configuration window.

Configuration Parameters Table

Parameter	Description
Upgrade Policy Name	Name for this policy.
Minimum Client Version	The minimum Brink App version that is allowed to connect to Cloudbrink service. Any user using a Brink App that is lower the minimum client version will be forcefully upgraded.
Upgrade-To Version	<p>When a user is upgraded, the version to which they will be upgraded is decided based on this parameter. It can take two values</p> <ol style="list-style-type: none"> 1. Latest Version: Brink App will be upgraded to whatever is the latest version that Cloudbrink has released at that time 2. Release version: admin explicitly selects this version from the drop-down. Brink App will be upgraded to this version. <p>Note: Admin can't select both latest-version checkbox and a value for release-version at the same time</p>

Upgrade Policy Type	<p>Default:</p> <p>When “Override” checkbox is unchecked, it is called as default policy.</p> <ul style="list-style-type: none"> The default policy can be applied to the overall organization-level or security-group level. This policy will be Active perpetually (until admin deletes/modifies the policy) The default policy ensures that the upgrade policy is applied to any endpoints that are registered in the future as well. For example, a new employee joins after one month of defining the upgrade policy and connects to Cloudbrink from the new laptop. This laptop (Brink App) will be checked against default policy. 	<p>Override:</p> <p>When “Override” policy is checked, it is called as override policy.</p> <ul style="list-style-type: none"> Override policy can be used to specify a different behaviour other than that is specified in the default policy When override option is checked, admin can specify a different minimum client version and upgrade-to version for the security-group or specific users (list of email IDs) or platforms (operating system) <p>Note: Default policies remain active indefinitely, while override policies only apply to pre-existing endpoints. Once these endpoints are upgraded, the override policy is marked as “Completed” and won't apply to new devices.</p>
Device user groups	<p>List of device-user-groups (security groups) to which the policy is application.</p> <p>If none of the device-user-groups are specified (empty list), the policy is applicable for the overall organization.</p>	
Platforms	<p>Available only “Override” option is checked</p> <p>The policy is applicable for only those platforms (operating systems) specified in this parameter</p>	
Override users	<p>Available only “Override” option is checked</p> <p>The policy is applicable for only those users (list of email IDs) specified in this parameter</p>	
Upgrade schedule	<p>The time at which the policy will be activated.</p>	

Summary table

All the configured Brink App upgrade policies will be displayed in the summary table. The summary table provides the “Status” information of each of the policy.

Brink Agent Upgrade Policies

Brink Agent Upgrade Policies 1 ADD DELETE

<input type="checkbox"/>	POLICY NAME	MINIMUM CLIENT VERSI...	UPGRADE-TO VERSION	TYPE	OVERRIDE GROUPS	STATUS
<input type="checkbox"/>	Latest-Version-Availability		release_12.2.428	Default	All groups	active

Support

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