android

Simplifying Password Quality in Android 12

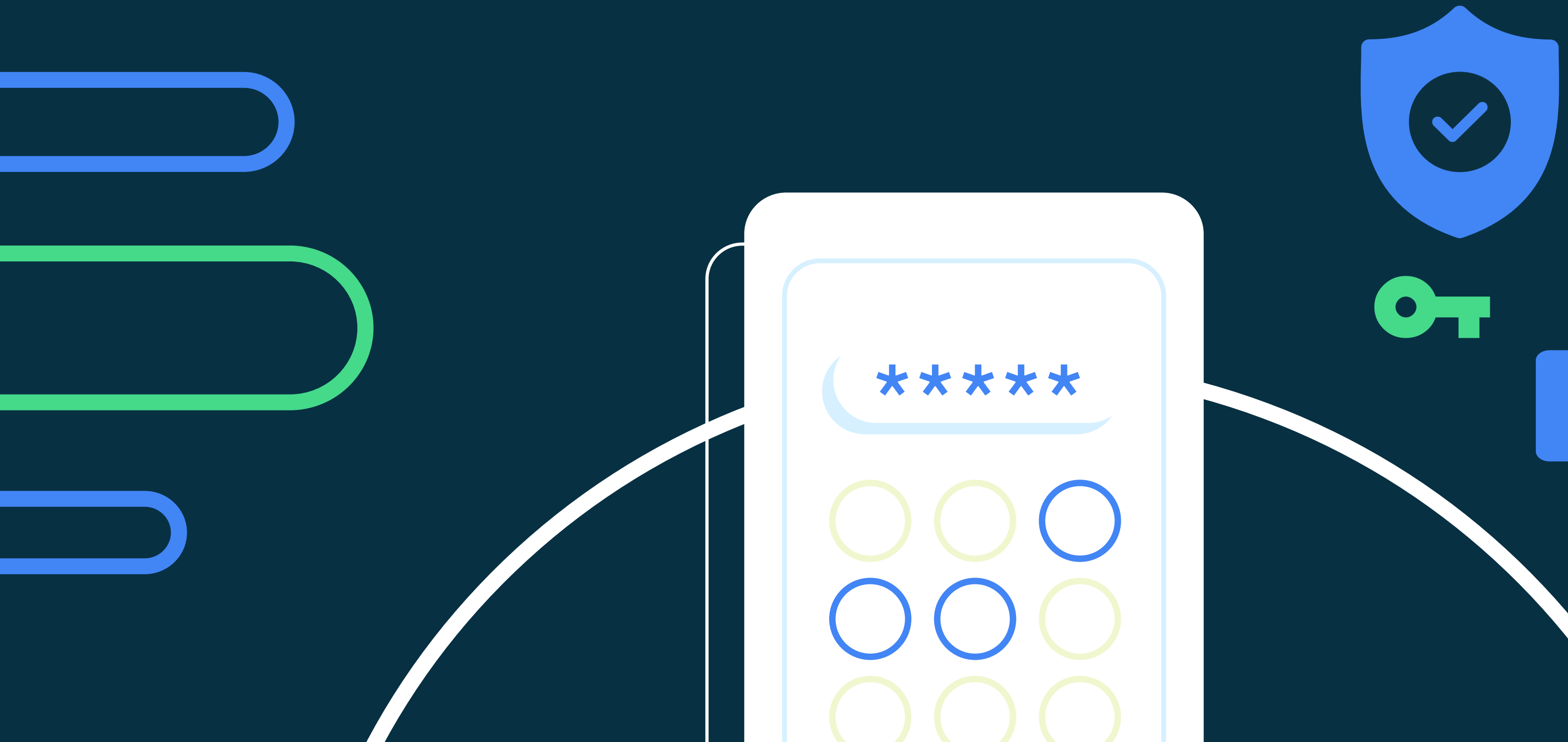

Table of contents

Simplifying Password Quality in Android 12

EMM Solutions using Android Management API

Why is Google replacing the password quality APIs on devices with a work profile?

Does the new password complexity API allow me to set strong enough requirements to protect my work data?

What if I want to set my own granular password requirements?

— For company-owned devices with a work profile

— For personally-owned devices with a work profile

— For fully-managed devices

Why can't I reset the device password if my user forgets?

What will happen to password quality policies I have already set on my devices when the devices are upgraded to Android 12?

Can I use the new password complexity API to set a password policy on my company-owned devices?

What is the timeline for when the password quality API will no longer function?

— For a work profile on personally-owned devices

— For a work profile on company-owned devices

Simplifying Password Quality in Android 12

In Android 12, the password settings have been simplified to make it much easier for admins as well as for users, all while ensuring the requisite level of security. Implementing industry best practices and with guidance, SP 800-63, from the National Institute of Standards and Technology (NIST), the password policies on a personally-owned device with a work profile will be changed from “password quality” to “password complexity” APIs. It’s important to note that existing policies are not impacted, only policies set from Android 12 onwards. This change consists of four simple options for setting the device level passcode which are High, Medium, Low or None. The two goals of this change are to simplify configuration and reduce the risk of users forgetting their device level passcodes.

Customers deploying devices with a work profile on company-owned and fully-managed devices will have the option to continue using the password quality policies, but we advise using the new password complexity APIs. The password quality APIs are not recommended for use in Android 12 for work profile devices and may be removed in releases beyond Android 12. Keep in mind that if the password quality APIs are used on work profile devices in Android 12, an exception will be logged.

For a simpler migration, customers using the Android Management API will have their password policies on personally-owned work profile devices automatically translated to the new APIs where appropriate. Legacy PasswordQuality values are mapped against the corresponding quality values in Android 12, preferring the stricter option where direct mapping is not possible (with exception: the old ALPHANUMERIC value maps to the new High value, which now permits a 6-digit PIN, and the old COMPLEX value maps to the new Medium value, which may permit less complex passwords according to the minimum letters, symbols, and length values specified).

For all devices, regardless of the deployment model, existing password policies already enforced on a device will not be impacted upon upgrading to Android 12. The EMM Partners can continue to support the current password policies, but can also enforce a migration to the new password complexity policy with their DPCs as they choose. Admins will be able to set any requirements they like for the work challenge, which will have improved UX to make it easier during the user enrollment process and for the device on fully-managed mode.

EMM solutions using Android Management API

Customers with personally-owned devices using a work profile and upgrading to Android 12 will have their device password policies translated automatically. For customers using a compliance rule set by passwordPolicies, a device may become non-compliant if the user's current password does not meet the new password complexity policy mapping. Users will be asked to set a stronger password if a new compliance rule is set, otherwise, they will be prompted when trying to set a new screen lock that they can no longer set one with the previous quality.

Why is Google replacing the password quality APIs on devices with a work profile?

Modern advancements in technology and services built into Android no longer require a complicated set of granular settings to prevent brute force attacks against locked devices. The password quality APIs were outdated and no longer aligned with industry standards, for example, NIST Special Purpose 800-63 series documents. Complex device passwords are often forgotten by users which results in unnecessary factory resets and personal data loss.

Modern Android devices are required to use the Gatekeeper subsystem. It performs device pattern/password authentication in a Trusted Execution Environment (TEE). Gatekeeper enrolls and verifies passwords via a hash-based message authentication code (HMAC) using a hardware-backed secret key. Additionally, Gatekeeper throttles consecutive failed verification attempts and refuses to service requests based on a given timeout and a given number of consecutive failed attempts. Therefore, it is not feasible to brute-force a device's password due to the significant amounts of time required.

Managed Android devices (both fully-managed and devices with a work profile) allow the IT admin to require complex device level passwords to protect sensitive company data. These varying levels of complexity included:

- Requirements including numeric, complex numeric, alphabetic or alphanumeric.
- Minimal length, number of letters, non-letters, lower-case letters, symbols and upper-case letters.
- Password expiration timeout settings.
- Password history length (prevent reuse of passwords)

These fine grained controls made sense when the API was first introduced, in Android 2.2 (Froyo), as hardware-backed security was not as ubiquitous as it is today. Originally, complex passwords were used to make it difficult for an attacker to brute-force a device's lock screen.

An illustrative example

The password rate limiting feature of Android allows the first five password attempts in under one second. Attempts 5 through 10 require an additional 30 seconds in between each attempt. After the 10th guess, the factor for each subsequent attempt increases by a factor of 10.

Example of attempts:

30 guesses	10 min and 30 seconds
100 guesses	10 hours, 45 minutes, and 30 seconds
200 guesses	67 days, 2 hours, 45 minutes, and 30 seconds

There is no longer a need to enforce complex pass codes at the device level to protect data. Brute force techniques applied on a simple six-digit password could take years to execute. In addition, a recommended configuration for a managed Android device is to configure a limit of 10 guesses before auto wiping the device. In this case, there would be no opportunity to get past attempt number 10. This configuration is resident on the device and is enforced even if the device is offline.

Does the new password complexity API allow me to set strong enough requirements to protect my work data?

Yes, the password complexity API is in line with the latest security guidance from NIST's SP 800-63. A password is meant to protect against unauthorized use of a device and the prevention of data exfiltration from a lost or stolen device.

Research shows that passcode entry on a mobile device is difficult for an attacker to view by "shoulder-surfing". Therefore, even a medium password complexity policy is sufficient to protect against attackers spying:

Towards Baselines for Shoulder Surfing on Mobile Authentication

Swipe Authentication: Exploring Over-the-Shoulder Attack Performance

Literature review of relevant research

What if I want to set my own granular password requirements?

Admins can still utilize a more granular password, if they prefer, through the work security challenge to manage access to business apps in the work profile. The work security challenge enables an IT-approved password for access to data in the work profile, separate from a simplified password for the device.

We've improved the work profile setup process to prompt employees if their device password doesn't meet complexity requirements set by their admin, and allow them to easily set up a work security challenge to access apps in the work profile.

For company-owned devices with a work profile

- Continue using the password quality API until you are ready to migrate to the new password complexity API
- Use the work challenge

For personally-owned devices with a work profile

- Use the work challenge

For fully-managed devices

- Continue using the password quality API until you are ready to migrate to the new password complexity API

Why can’t I reset the device password if my user forgets?

Admins cannot reset the device level passcode when there is a work profile present, this feature is only available on a fully-managed device. This protects a user’s personal profile data from unintentional or intentional wipe and eavesdropping on a user’s personal privacy. These limitations apply to any device that has a work profile, whether personally-owned or company-owned.

An illustrative scenario:

A rogue admin or malicious actor seeks to gain access to the user’s personal profile data so they use a device passcode reset to change the password on the user’s device. They are now able to access the personal profile of the user on that device, allowing them to view private messages, documents, images, and contacts. In addition, it could expose a company to additional liability risks from the exposure of personal banking and health information stored in personal applications.

What will happen to password quality policies I have already set on my devices when the devices are upgraded to Android 12?

For all devices with a work profile, including personally-owned or company-owned, no existing password requirements will be impacted. The currently applied policies on these devices will remain in effect until the EMM chooses to switch to the new complexity API. Please work with your EMM Partner to determine when that may take effect in their solutions.

Can I use the new password complexity API to set a password policy on my company-owned devices?

Yes, you can choose to use the new password complexity API when you are ready to migrate. Please check with your EMM Partner for timing on their release.

What is the timeline for when the password quality API will no longer function?

For a work profile on personally-owned devices

When the EMMs DPC targets Android 12, the ability to use the password quality API will no longer be available at the device level and you must use the new password complexity API. However, the password quality API will still be available for use when configuring the work challenge if desired. Please check with your EMM Partner on timing.

For a work profile on company-owned devices

When the EMMs DPC targets Android 12, the ability to use the password quality API will still be available for the device passcode, but it is recommended to use the password complexity API, as the password quality API might be removed in the future. It is recommended that migrating to the new password complexity API be done promptly as further releases may remove support for the password quality API and thus force migration.