Security

In this section, you can configure security-related policies.

Security risk actions

Choose what to do when a device reports a SecurityRisk in status reports.

Supported SecurityRisk types:

> **Unknown OS**: Play Integrity API detects that the device is running an unknown OS (basicIntegrity check succeeds but ctsProfileMatch fails).
>
> **Compromised OS**: Play Integrity API detects that the device is running a compromised OS (basicIntegrity check fails).
>
> **Hardware-backed evaluation failed**: Play Integrity API detects that the device does not have a strong guarantee of system integrity, if the MEETS_STRONG_INTEGRITY label doesn't show in the device integrity field.

Available actions:

> **Wipe corporate data (default)**: Disenroll and wipe work data (entire device if fully managed, or only work profile for profile-owned).
>
> **No action**: Leave the device enrolled and do nothing automatically.

When you select **Wipe corporate data**, you can also configure wipe options:

> **Preserve factory-reset protection**: Preserve Factory Reset Protection (FRP) data when wiping the device.
>
> **Wipe external storage**: Additionally wipe the device's external storage (such as SD cards) when performing the wipe.

Wipe eSIMs: For company-owned devices, this removes all eSIMs from the device when the device is wiped. In personally-owned devices, this will remove managed eSIMs (eSIMs which are added via the ADD_ESIM command) on the devices and no personally owned eSIMs will be removed.

1. Max time to lock

Maximum time (in seconds) for user activity until the device locks. A value of 0 means there is no restriction.

2. Stay on when charging

The battery plugged in modes for which the device stays on. When using this setting, it is recommended to clear **Maximum time to lock** so that the device doesn't lock itself while it stays on.

AC charger: Power source is an AC charger.

USB port: Power source is a USB port.

Wireless charger: Power source is wireless.

3. Keyguard disabled

If true, this disables the Lock Screen for primary and/or secondary displays. This policy is supported only in dedicated device management mode.

4. Password requirements

Password requirement policies.

Use **Configure Password Requirements** to add one or more password requirement blocks. Use **Clear All** to remove all configured password requirements.

Password requirements can use **Auto** scope (single requirement) or separate **Device**/**Work profile** scopes. Complexity-based requirements must be coupled with quality-based requirements for the same scope.

4.1. Scope

The scope that the password requirement applies to.

> **Auto**: The scope is unspecified. The password requirements are applied to the work profile for work profile devices and the whole device for fully managed or dedicated devices.
>
> **Device**: The password requirements are only applied to the device.
>
> **Work profile**: The password requirements are only applied to the work profile.

4.2. Password history length

The length of the password history. After setting this field, the user won't be able to enter a new password that is the same as any password in the history. A value of 0 means there is no restriction.

4.3. Max failed passwords for wipe

Number of incorrect device-unlock passwords that can be entered before a device is wiped. A value of 0 means there is no restriction.

4.4. Password expiration timeout (days)

This setting forces the user to periodically update their password, after the specified number of days.

4.5. Require password unlock

The length of time after a device or work profile is unlocked using a strong form of authentication (password, PIN, pattern) that it can be unlocked using any other authentication method (e.g. fingerprint, trust agents, face). After the specified time period elapses, only strong forms of authentication can be used to unlock the device or work profile.

> **Device’s default**: The timeout period is set to the device’s default.
>
> **Every day**: The timeout period is set to 24 hours.

4.6. Password quality

The required password quality.

> **Complexity high**: Define the high password complexity band as: On Android 12 and above: PIN with no repeating (4444) or ordered (1234, 4321, 2468) sequences, length at least 8; alphabetic, length at least 6; alphanumeric, length at least 6.
>
> **Complexity medium**: Define the medium password complexity band as: PIN with no repeating (4444) or ordered (1234, 4321, 2468) sequences, length at least 4; alphabetic, length at least 4; alphanumeric, length at least 4.

Complexity low: Define the low password complexity band as: pattern; PIN with repeating (4444) or ordered (1234, 4321, 2468) sequences.

None: There are no password requirements.

Weak: The device must be secured with a low-security biometric recognition technology, at minimum. This includes technologies that can recognize the identity of an individual that are roughly equivalent to a 3-digit PIN (false detection is less than 1 in 1,000).

Any: A password is required, but there are no restrictions on what the password must contain.

Numeric: The password must contain numeric characters.

Numeric complex: The password must contain numeric characters with no repeating (4444) or ordered (1234, 4321, 2468) sequences.

Alphabetic: The password must contain alphabetic (or symbol) characters.

Alphanumeric: The password must contain both numeric and alphabetic (or symbol) characters.

Complex: The password must meet the minimum requirements specified in passwordMinimumLength, passwordMinimumLetters, passwordMinimumSymbols, etc. For example, if passwordMinimumSymbols is 2, the password must contain at least two symbols.

4.7. Minimum length

The minimum allowed password length. A value of 0 means there is no restriction.

4.8. Minimum letters

Minimum number of letters required in the password.

4.9. Minimum lower case letters

Minimum number of lower case letters required in the password.

4.10. Minimum upper case letters

Minimum number of upper case letters required in the password.

4.11. Minimum non letter characters

Minimum number of non-letter characters (numerical digits or symbols) required in the password.

4.12. Minimum numerical digits

Minimum number of numerical digits required in the password.

4.13. Minimum symbols

Minimum number of symbols required in the password.

4.14. Unified lock

Controls whether a unified lock is allowed for the device and the work profile, on devices running Android 9 and above with a work profile. This has no effect on other devices.

> **Allow unified lock**: A common lock for the device and the work profile is allowed.
>
> **Require separate work lock**: A separate lock for the work profile is required.

5. Factory reset disabled

Whether factory resetting from settings is disabled. Only apply to fully managed devices.

6. Factory reset protection

Email addresses of device administrators for factory reset protection. When the device experiences an unauthorized factory reset, it will require one of these admins to log in with the Google account email and password to unlock the device. If no admins are specified, the device won't provide factory reset protection. Only apply to fully managed devices.

Administrator emails: use **Enable Factory Reset Protection** to start configuring administrators. Then use **Add administrator email** to add addresses and remove them with the delete action.

7. Keyguard features

Keyguard (lock screen) features that can be disabled.

7.1. Disable all

Disable all current and future keyguard customizations.

7.2. Disable camera

Disable the camera on secure keyguard screens (e.g. PIN).

7.3. Disable notifications

Disable showing all notifications on secure keyguard screens.

7.4. Disable unredacted notifications

Disable unredacted notifications on secure keyguard screens.

7.5. Ignore trust agent state

Ignore trust agent state on secure keyguard screens.

7.6. Disable fingerprint

Disable fingerprint sensor on secure keyguard screens.

7.7. Disable text entry into notifications

Disable text entry into notifications on secure keyguard screens.

7.8. Disable face authentication

Disable face authentication on secure keyguard screens.

7.9. Disable iris authentication

Disable iris authentication on secure keyguard screens.

7.10. Disable all biometric authentication

Disable all biometric authentication on secure keyguard screens.

7.11. Disable all shortcuts

Disable all shortcuts on secure keyguard screen on Android 14 and above.

Revision #55
Created 2022-03-28 09:17:42 UTC by Admin
Updated 2026-06-23 17:10:56 UTC by Admin