Seguridad

En esta sección, puedes configurar políticas relacionadas con la seguridad.

Acciones ante riesgos de seguridad

Elige qué hacer cuando un dispositivo informa de un SecurityRisk en los informes de estado.

Tipos de SecurityRisk compatibles:

SO desconocido: La API de Play Integrity detecta que el dispositivo ejecuta un SO desconocido (la comprobación basicIntegrity se supera, pero ctsProfileMatch falla).

SO comprometido: La API de Play Integrity detecta que el dispositivo ejecuta un SO comprometido (la comprobación basicIntegrity falla).

Error en la evaluación respaldada por hardware: La API de Play Integrity detecta que el dispositivo no tiene una garantía sólida de integridad del sistema, si la etiqueta MEETS_STRONG_INTEGRITY no aparece en el campo de integridad del dispositivo.

Acciones disponibles:

Borrar datos corporativos (predeterminado): Anula la inscripción y borra los datos de trabajo (todo el dispositivo si está totalmente gestionado o solo el perfil de trabajo en dispositivos con perfil de trabajo).

Ninguna acción: Deja el dispositivo inscrito y no hagas nada automáticamente.

Cuando seleccionas **Borrar datos corporativos**, también puedes configurar opciones de borrado:

Conservar la protección contra el restablecimiento de fábrica: Conserva los datos de la Protección contra restablecimiento de fábrica (FRP) al borrar el dispositivo.

Borrar almacenamiento externo: Borra además el almacenamiento externo del dispositivo (como las tarjetas SD) al realizar el borrado.

Borrar eSIM: En dispositivos propiedad de la empresa, esto elimina todas las eSIM del dispositivo cuando se borra. En dispositivos de propiedad personal, se eliminan las eSIM gestionadas (eSIM añadidas mediante el comando ADD_ESIM) y no se elimina ninguna eSIM de propiedad personal.

1. Tiempo máximo para bloquear

Tiempo máximo (en segundos) de actividad del usuario antes de que se bloquee el dispositivo. Un valor de 0 significa que no hay restricción.

2. Mantener encendido durante la carga

Los modos de conexión de la batería en los que el dispositivo permanece encendido. Cuando uses esta configuración, se recomienda borrar **Tiempo máximo para bloquear** para que el dispositivo no se bloquee mientras permanece encendido.

Cargador de CA: La fuente de alimentación es un cargador de CA.

Puerto USB: La fuente de alimentación es un puerto USB.

Cargador inalámbrico: La fuente de alimentación es inalámbrica.

3. Bloqueo de pantalla deshabilitado

Si es verdadero, deshabilita la pantalla de bloqueo de las pantallas principal o secundaria. Esta política solo es compatible con el modo de gestión de dispositivos dedicados.

4. Requisitos de contraseña

Políticas de requisitos de contraseña.

Usa **Configurar requisitos de contraseña** para agregar uno o varios bloques de requisitos de contraseña. Usa **Borrar todo** para eliminar todos los requisitos de contraseña configurados.

Los requisitos de contraseña pueden usar el ámbito **Automático** (un solo requisito) o ámbitos separados de **Dispositivo**/**Perfil de trabajo**. Los requisitos basados en la complejidad deben combinarse con requisitos basados en la calidad para el mismo ámbito.

4.1. Ámbito

El ámbito al que se aplica el requisito de contraseña.

Automático: El ámbito no está especificado. Los requisitos de contraseña se aplican al perfil de trabajo en dispositivos con perfil de trabajo y a todo el dispositivo en dispositivos totalmente gestionados o dedicados.

Dispositivo: Los requisitos de contraseña solo se aplican al dispositivo.

Perfil de trabajo: Los requisitos de contraseña solo se aplican al perfil de trabajo.

4.2. Longitud del historial de contraseñas

La longitud del historial de contraseñas. Después de establecer este campo, el usuario no podrá introducir una contraseña nueva que sea igual a cualquiera del historial. Un valor de 0 significa que no hay restricción.

4.3. Máximo de contraseñas fallidas antes de borrar

Número de contraseñas de desbloqueo incorrectas que se pueden introducir antes de que se borre el dispositivo. Un valor de 0 significa que no hay restricción.

4.4. Tiempo de caducidad de la contraseña (días)

Esta configuración obliga al usuario a actualizar periódicamente su contraseña, tras el número de días especificado.

4.5. Requerir desbloqueo con contraseña

El tiempo tras desbloquear un dispositivo o perfil de trabajo con una forma de autenticación segura (contraseña, PIN, patrón) durante el que se puede desbloquear con cualquier otro método de autenticación (por ejemplo, huella digital, agentes de confianza, rostro). Una vez transcurrido el periodo especificado, solo se pueden usar formas de autenticación seguras para desbloquear el dispositivo o el perfil de trabajo.

Predeterminado del dispositivo: El periodo de tiempo de espera se establece en el valor predeterminado del dispositivo.

Cada día: El periodo de tiempo de espera se establece en 24 horas.

4.6. Calidad de la contraseña

La calidad de contraseña requerida.

Complejidad alta: Define la banda de complejidad de contraseña alta como: En Android 12 y versiones posteriores: PIN sin secuencias repetidas (4444) ni ordenadas (1234, 4321, 2468), con una longitud mínima de 8; alfabética, con una longitud mínima de 6; alfanumérica, con una longitud mínima de 6.

Complejidad media: Define la banda de complejidad de contraseña media como: PIN sin secuencias repetidas (4444) ni ordenadas (1234, 4321, 2468), con una longitud mínima de 4; alfabética, con una longitud mínima de 4; alfanumérica, con una longitud mínima de 4.

Complejidad baja: Define la banda de complejidad de contraseña baja como: patrón; PIN con secuencias repetidas (4444) u ordenadas (1234, 4321, 2468).

Ninguna: No hay requisitos de contraseña.

Débil: El dispositivo debe protegerse, como mínimo, con una tecnología de reconocimiento biométrico de baja seguridad. Esto incluye tecnologías que pueden reconocer la identidad de una persona y que equivalen aproximadamente a un PIN de 3 dígitos (la detección falsa es inferior a 1 entre 1000).

Cualquiera: Se requiere una contraseña, pero no hay restricciones sobre lo que debe contener.

Numérica: La contraseña debe contener caracteres numéricos.

Numérica compleja: La contraseña debe contener caracteres numéricos sin secuencias repetidas (4444) ni ordenadas (1234, 4321, 2468).

Alfabética: La contraseña debe contener caracteres alfabéticos (o símbolos).

Alfanumérica: La contraseña debe contener caracteres tanto numéricos como alfabéticos (o símbolos).

Compleja: La contraseña debe cumplir los requisitos mínimos especificados en passwordMinimumLength, passwordMinimumLetters, passwordMinimumSymbols, etc. Por ejemplo, si passwordMinimumSymbols es 2, la contraseña debe contener al menos dos símbolos.

4.7. Longitud mínima

La longitud mínima permitida de la contraseña. Un valor de 0 significa que no hay restricción.

4.8. Mínimo de letras

Número mínimo de letras requeridas en la contraseña.

4.9. Mínimo de letras minúsculas

Número mínimo de letras minúsculas requeridas en la contraseña.

4.10. Mínimo de letras mayúsculas

Número mínimo de letras mayúsculas requeridas en la contraseña.

4.11. Mínimo de caracteres no alfabéticos

Número mínimo de caracteres no alfabéticos (dígitos numéricos o símbolos) requeridos en la contraseña.

4.12. Mínimo de dígitos numéricos

Número mínimo de dígitos numéricos requeridos en la contraseña.

4.13. Mínimo de símbolos

Número mínimo de símbolos requeridos en la contraseña.

4.14. Bloqueo unificado

Controla si se permite un bloqueo unificado para el dispositivo y el perfil de trabajo, en dispositivos con Android 9 o posterior y con perfil de trabajo. No tiene efecto en otros dispositivos.

> **Permitir bloqueo unificado**: Se permite un bloqueo común para el dispositivo y el perfil de trabajo.
>
> **Requerir bloqueo de trabajo independiente**: Se requiere un bloqueo independiente para el perfil de trabajo.

5. Restablecimiento de fábrica deshabilitado

Indica si se deshabilita el restablecimiento de fábrica desde la configuración. Solo se aplica a dispositivos totalmente gestionados.

6. Protección contra restablecimiento de fábrica

Direcciones de correo electrónico de los administradores del dispositivo para la Protección contra restablecimiento de fábrica. Cuando el dispositivo sufra un restablecimiento de fábrica no autorizado, se requerirá que uno de estos administradores inicie sesión con el correo electrónico y la contraseña de la cuenta de Google para desbloquear el dispositivo. Si no se especifica ningún administrador, el dispositivo no ofrecerá protección contra restablecimiento de fábrica. Solo se aplica a dispositivos totalmente gestionados.

Correos electrónicos de administradores: usa **Habilitar la Protección contra restablecimiento de fábrica** para empezar a configurar administradores. Después, usa **Agregar correo electrónico de administrador** para añadir direcciones y eliminarlas con la acción de eliminar.

7. Funciones de bloqueo de pantalla

Funciones de bloqueo de pantalla (pantalla de bloqueo) que se pueden deshabilitar.

7.1. Deshabilitar todo

Deshabilita todas las personalizaciones actuales y futuras del bloqueo de pantalla.

7.2. Deshabilitar cámara

Deshabilita la cámara en las pantallas de bloqueo seguras (por ejemplo, con PIN).

7.3. Deshabilitar notificaciones

Deshabilita la visualización de todas las notificaciones en las pantallas de bloqueo seguras.

7.4. Deshabilitar notificaciones no censuradas

Deshabilita las notificaciones no censuradas en las pantallas de bloqueo seguras.

7.5. Ignorar el estado del agente de confianza

Ignora el estado del agente de confianza en las pantallas de bloqueo seguras.

7.6. Deshabilitar huella digital

Deshabilita el sensor de huella digital en las pantallas de bloqueo seguras.

7.7. Deshabilitar la introducción de texto en las notificaciones

Deshabilita la introducción de texto en las notificaciones en las pantallas de bloqueo seguras.

7.8. Deshabilitar autenticación facial

Deshabilita la autenticación facial en las pantallas de bloqueo seguras.

7.9. Deshabilitar autenticación por iris

Deshabilita la autenticación por iris en las pantallas de bloqueo seguras.

7.10. Deshabilitar toda la autenticación biométrica

Deshabilita toda la autenticación biométrica en las pantallas de bloqueo seguras.

7.11. Deshabilitar todos los accesos directos

Deshabilita todos los accesos directos en la pantalla de bloqueo segura en Android 14 y versiones posteriores.

Revision #59
Created 2025-12-17 09:33:17 UTC by Admin
Updated 2026-11-12 09:54:31 UTC by Admin