Seguridad

En esta sección, puede configurar las políticas relacionadas con la seguridad.

Acciones de riesgo de seguridad

Elija qué hacer cuando un dispositivo informa un riesgo de seguridad en los informes de estado.

Tipos de riesgos de seguridad admitidos:

> **Sistema operativo desconocido**: La API de Play Integrity detecta que el dispositivo está ejecutando un sistema operativo desconocido (la comprobación básica de integridad se completa, pero ctsProfileMatch falla).
>
> **Sistema operativo comprometido**: La API de Play Integrity detecta que el dispositivo está ejecutando un sistema operativo comprometido (la comprobación básica de integridad falla).
>
> **La evaluación basada en hardware falló**: 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 se muestra en el campo de integridad del dispositivo.

Acciones disponibles:

> **Borrar datos corporativos (por defecto)**: Desregistrar y borrar los datos de trabajo (todo el dispositivo si está gestionado completamente, o solo el perfil de trabajo si es propiedad del perfil).
>
> **Ninguna acción**: No se realiza ninguna acción y el dispositivo permanece inscrito.

Cuando selecciona **Borrar datos corporativos**, también puede configurar opciones de borrado:

> **Mantener la protección de restablecimiento de fábrica**: Conserva los datos de la protección contra restablecimiento de fábrica (FRP) al borrar el dispositivo.
>
> **Borrar almacenamiento externo**: Además, se borrará el almacenamiento externo del dispositivo (como las tarjetas SD) al realizar el borrado.

Borrar eSIMs: Para dispositivos propiedad de la empresa, esto elimina todos los eSIM del dispositivo al realizar el borrado. En dispositivos de uso personal, esto eliminará los eSIM administrados (eSIM que se agregan mediante el comando ADD_ESIM) en los dispositivos, y no se eliminarán los eSIM de propiedad personal.

1. Tiempo máximo de bloqueo

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

2. Permanecer activo durante la carga

Los modos de carga en los que el dispositivo permanece encendido. Al usar esta configuración, se recomienda borrar **Tiempo máximo de bloqueo** para evitar que el dispositivo se bloquee mientras permanece encendido.

Cargador de corriente alterna: La fuente de alimentación es un cargador de corriente alterna.

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

Cargador inalámbrico: La fuente de alimentación es inalámbrica.

3. Clave de seguridad desactivada

Si es verdadero, esto deshabilita la pantalla de bloqueo para las pantallas principal(es) y/o secundaria(s). Esta política solo se admite en el modo de gestión de dispositivos dedicado.

4. Requisitos de contraseña

Políticas de requisitos de contraseña.

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

Los requisitos de contraseña pueden usar **el ámbito "Automático"** (un único requisito) o ámbitos separados de **dispositivo** y/o **perfil de trabajo**. Los requisitos basados en la complejidad deben combinarse con requisitos basados en la calidad para el mismo ámbito.

4.1. Ámbito de aplicación

El ámbito al que se aplica el requisito de contraseña.

Auto: El ámbito no está especificado. Los requisitos de contraseña se aplican al perfil de trabajo para los dispositivos con perfil de trabajo y a todo el dispositivo para los dispositivos 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

Longitud del historial de contraseñas. Después de establecer este valor, el usuario no podrá usar una contraseña nueva que sea idéntica a alguna de las contraseñas anteriores. Un valor de 0 indica que no hay restricciones.

4.3. Número máximo de intentos fallidos de contraseña antes de que se borre el dispositivo

Número de contraseñas incorrectas para desbloquear el dispositivo antes de que se borre. Un valor de 0 significa que no hay restricciones.

4.4. Tiempo de expiración de la contraseña (días)

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

4.5. Requiere desbloqueo con contraseña

El tiempo transcurrido después de que un dispositivo o perfil de trabajo se desbloquee mediante un método de autenticación seguro (contraseña, PIN, patrón), durante el cual se puede desbloquear con cualquier otro método (por ejemplo, huella digital, agentes de confianza, reconocimiento facial). Una vez transcurrido el período de tiempo especificado, solo se pueden usar métodos de autenticación seguros para desbloquear el dispositivo o el perfil de trabajo.

Configuración predeterminada del dispositivo: El período de tiempo se establece con la configuración predeterminada del dispositivo.

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

4.6. Calidad de la contraseña

La calidad de contraseña requerida.

Alta complejidad: Defina el rango de alta complejidad de la contraseña como: En Android 12 y versiones posteriores: PIN sin secuencias repetidas (4444) ni ordenadas (1234, 4321, 2468), longitud mínima de 8; alfabético, longitud mínima de 6; alfanumérico, longitud mínima de 6.

Complejidad media: Defina el rango de complejidad media de la contraseña como: PIN sin secuencias repetidas (4444) ni ordenadas (1234, 4321, 2468), longitud mínima de 4; alfabético, longitud mínima de 4; alfanumérico, longitud mínima de 4.

Baja complejidad: Defina el nivel de complejidad baja de la contraseña como: patrón; PIN con secuencias repetidas (4444) o ordenadas (1234, 4321, 2468).

Ninguno: No se aplican requisitos de contraseña.

Débil: El dispositivo debe estar protegido con una tecnología de reconocimiento biométrico de baja seguridad, como mínimo. Esto incluye tecnologías que pueden reconocer la identidad de una persona y que son aproximadamente equivalentes a un PIN de 3 dígitos (la tasa de falsos positivos es inferior a 1 en 1000).

Cualquier: Se requiere una contraseña, pero no hay restricciones sobre su contenido.

Numérico: La contraseña debe contener caracteres numéricos.

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

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

Alfanumérico: La contraseña debe contener tanto números como caracteres alfabéticos (o símbolos).

Compleja: La contraseña debe cumplir con 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

Longitud mínima de contraseña permitida. Un valor de 0 indica que no hay restricción.

4.8. Mínimo de letras

Número mínimo de letras requeridas en la contraseña.

4.9. Número mínimo de letras minúsculas

Número mínimo de letras minúsculas requeridas en la contraseña.

4.10. Número mínimo de letras mayúsculas

Número mínimo de letras mayúsculas requeridas en la contraseña.

4.11. Número mínimo de caracteres no alfabéticos

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

4.12. Mínimo de dígitos numéricos

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 que ejecutan Android 9 y versiones posteriores con un perfil de trabajo. Esto no tiene efecto en otros dispositivos.

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

5. Restablecimiento de fábrica deshabilitado

¿Está desactivada la opción de restablecimiento de fábrica desde la configuración? Solo se aplica a dispositivos completamente gestionados.

6. Protección contra el restablecimiento de fábrica

Direcciones de correo electrónico de los administradores del dispositivo para la protección contra el restablecimiento de fábrica. Cuando el dispositivo experimenta un restablecimiento de fábrica no autorizado, requerirá que uno de estos administradores inicie sesión con la dirección de correo electrónico y la contraseña de la cuenta de Google para desbloquear el dispositivo. Si no se especifican administradores, el dispositivo no proporcionará protección contra el restablecimiento de fábrica. Solo se aplica a dispositivos completamente administrados.

Direcciones de correo electrónico de los administradores: utilice **Activar protección contra restablecimiento de fábrica** para comenzar a configurar los administradores. Luego, utilice **Añadir dirección de correo electrónico del administrador** para agregar direcciones y eliminarlas con la acción de eliminar.

7. Funciones de bloqueo de pantalla

Funciones de la pantalla de bloqueo que se pueden desactivar.

7.1. Desactivar todo

Desactivar todas las personalizaciones actuales y futuras de la pantalla de bloqueo.

7.2. Desactivar cámara

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

7.3. Desactivar las notificaciones

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

7.4. Desactivar notificaciones sin censura

Desactivar notificaciones sin censura en las pantallas de bloqueo seguras.

7.5. Ignorar el estado del agente de confianza

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

7.6. Desactivar huella digital

Desactivar el sensor de huellas dactilares en las pantallas de bloqueo seguras.

7.7. Desactivar la entrada de texto en las notificaciones

Desactivar la entrada de texto en las notificaciones en las pantallas de bloqueo seguras.

7.8. Desactivar la autenticación facial

Desactivar la autenticación facial en las pantallas de bloqueo seguras.

7.9. Desactivar la autenticación mediante el iris

Desactivar la autenticación mediante el iris en las pantallas de bloqueo seguras.

7.10. Desactivar toda la autenticación biométrica

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

7.11. Desactivar todos los atajos

Desactivar todos los atajos en la pantalla de bloqueo segura en Android 14 y versiones posteriores.

Revision #37
Created 2025-12-17 09:33:17 UTC by Admin
Updated 2026-04-22 15:49:34 UTC by Admin