Segurança

Nesta seção, você pode configurar políticas relacionadas à segurança.

Ações de risco de segurança

Escolha o que fazer quando um dispositivo relata um Risco de Segurança nos relatórios de status.

Tipos de Risco de Segurança suportados:

Sistema operacional desconhecido: A API Play Integrity detecta que o dispositivo está executando um sistema operacional desconhecido (o teste básicoIntegrity é bem-sucedido, mas ctsProfileMatch falha).

Sistema operacional comprometido: A API Play Integrity detectou que o dispositivo está executando um sistema operacional comprometido (o teste básicoIntegrity falhou).

Avaliação baseada em hardware falhou: A API Play Integrity detectou que o dispositivo não possui uma garantia forte de integridade do sistema, caso o rótulo MEETS_STRONG_INTEGRITY não seja exibido no campo de integridade do dispositivo.

Ações disponíveis:

Limpar dados corporativos (padrão): Desinscrever e limpar os dados de trabalho (apaga todo o dispositivo, se totalmente gerenciado, ou apenas o perfil de trabalho, se gerenciado apenas pelo perfil).

Nenhuma ação: Mantenha o dispositivo inscrito e não execute nenhuma ação automaticamente.

Quando você seleciona "**Apagar dados corporativos**", você também pode configurar opções de limpeza:

Manter a proteção de restauração de fábrica: Mantenha os dados de Proteção de Restauração de Fábrica (FRP) ao limpar o dispositivo.

Limpar o armazenamento externo: Além disso, limpe o armazenamento externo do dispositivo (como cartões SD) ao realizar a limpeza.

Limpar eSIMs: Para dispositivos pertencentes à empresa, isso remove todos os eSIMs do dispositivo durante a limpeza. Em dispositivos de propriedade pessoal, isso removerá os eSIMs gerenciados (eSIMs adicionados via o comando ADD_ESIM) nos dispositivos, e nenhum eSIM de propriedade pessoal será removido.

1. Tempo máximo para bloqueio

Tempo máximo (em segundos) de atividade do usuário antes do bloqueio do dispositivo. Um valor de 0 significa que não há restrição.

2. Permanece ligado durante o carregamento

Os modos de carregamento em que o dispositivo permanece ligado. Ao usar essa configuração, recomenda-se limpar **Tempo máximo de bloqueio** para que o dispositivo não se bloqueie enquanto estiver ligado.

Carregador de tomada: A fonte de energia é um carregador de tomada.

Porta USB: A fonte de energia é uma porta USB.

Carregador sem fio: A fonte de energia é sem fio.

3. Tela de bloqueio desativada

Se verdadeiro, isso desativa a tela de bloqueio para as telas primárias e/ou secundárias. Essa política é suportada apenas no modo de gerenciamento de dispositivo dedicado.

4. Requisitos de senha

Políticas de requisitos de senha.

Use **Configurar Requisitos de Senha** para adicionar um ou mais blocos de requisitos de senha. Use **Limpar Tudo** para remover todos os requisitos de senha configurados.

Os requisitos de senha podem usar o escopo **Automático** (um único requisito) ou escopos separados de **Dispositivo**/**Perfil de trabalho**. Os requisitos baseados em complexidade devem ser combinados com requisitos baseados em qualidade para o mesmo escopo.

4.1. Escopo

O escopo a que se aplica a exigência de senha.

> **Dispositivo** O escopo não está especificado. As exigências de senha são aplicadas ao perfil de trabalho para dispositivos com perfil de trabalho e a todo o dispositivo para dispositivos totalmente gerenciados ou dedicados.
>
> **Dispositivo**: As exigências de senha são aplicadas apenas ao dispositivo.
>
> **Perfil de trabalho**: Os requisitos de senha são aplicados apenas ao perfil de trabalho.

4.2. Comprimento do histórico de senhas

Comprimento do histórico de senhas. Após definir este campo, o usuário não poderá usar uma nova senha que seja igual a qualquer senha no histórico. Um valor de 0 significa que não há restrição.

4.3. Número máximo de tentativas de senha inválidas antes de apagar o dispositivo

Número máximo de senhas incorretas para desbloquear o dispositivo antes que ele seja apagado. Um valor de 0 significa que não há restrição.

4.4. Tempo limite de expiração da senha (em dias)

Esta configuração obriga o usuário a alterar a senha periodicamente, após o número de dias especificado.

4.5. Requer desbloqueio por senha

O tempo decorrido após o desbloqueio do dispositivo ou perfil de trabalho usando uma forma de autenticação forte (senha, PIN, padrão) durante o qual ele pode ser desbloqueado usando qualquer outro método de autenticação (por exemplo, impressão digital, agentes de confiança, reconhecimento facial). Após o período de tempo especificado, apenas formas de autenticação fortes podem ser usadas para desbloquear o dispositivo ou perfil de trabalho.

> **Configuração padrão do dispositivo**: O período de inatividade está definido para a configuração padrão do dispositivo.
>
> **Todos os dias**: O período de inatividade está definido como 24 horas.

4.6. Qualidade da senha

A qualidade de senha exigida.

> **Complexidade alta**: Defina a faixa de complexidade alta para senhas como: No Android 12 e versões superiores: PIN sem sequências repetidas (4444) ou ordenadas (1234, 4321, 2468),

comprimento mínimo de 8; alfabético, comprimento mínimo de 6; alfanumérico, comprimento mínimo de 6.

Complexidade média: Defina a faixa de complexidade média para senhas como: PIN sem sequências repetidas (4444) ou ordenadas (1234, 4321, 2468), comprimento mínimo de 4; alfabético, comprimento mínimo de 4; alfanumérico, comprimento mínimo de 4.

Complexidade baixa: Defina a faixa de complexidade baixa para senhas como: padrão; PIN com sequências repetidas (4444) ou ordenadas (1234, 4321, 2468).

Nenhum: Não há requisitos para senhas.

Fraco: O dispositivo deve ser protegido com uma tecnologia de reconhecimento biométrico de baixa segurança, no mínimo. Isso inclui tecnologias que podem reconhecer a identidade de um indivíduo que são aproximadamente equivalentes a um PIN de 3 dígitos (a taxa de falsos positivos é inferior a 1 em 1.000).

Qualquer: É necessário definir uma senha, mas não há restrições quanto ao conteúdo da senha.

Numérico: A senha deve conter caracteres numéricos.

Numérico complexo: A senha deve conter caracteres numéricos, sem repetições (4444) ou sequências ordenadas (1234, 4321, 2468).

Alfanumérico: A senha deve conter caracteres alfabéticos (ou símbolos).

Alfanumérico: A senha deve conter tanto números quanto caracteres alfabéticos (ou símbolos).

Complexa: A senha deve atender aos requisitos mínimos especificados em passwordMinimumLength, passwordMinimumLetters, passwordMinimumSymbols, etc. Por exemplo, se passwordMinimumSymbols for 2, a senha deve conter pelo menos dois símbolos.

4.7. Comprimento mínimo

Comprimento mínimo da senha permitido. Um valor de 0 significa que não há restrição.

4.8. Número mínimo de letras

Número mínimo de letras exigido na senha.

4.9. Número mínimo de letras minúsculas

Número mínimo de letras minúsculas exigidas na senha.

4.10. Número mínimo de letras maiúsculas

Número mínimo de letras maiúsculas exigidas na senha.

4.11. Número mínimo de caracteres não alfabéticos

Número mínimo de caracteres não alfabéticos (dígitos numéricos ou símbolos) exigidos na senha.

4.12. Número mínimo de dígitos numéricos

Número mínimo de dígitos numéricos exigidos na senha.

4.13. Número mínimo de símbolos

Número mínimo de símbolos exigidos na senha.

4.14. Bloqueio unificado

Controla se o bloqueio unificado é permitido para o dispositivo e o perfil de trabalho, em dispositivos com Android 9 ou superior e que possuem um perfil de trabalho. Isso não tem efeito em outros dispositivos.

> **Permitir bloqueio unificado**: Um bloqueio comum é permitido para o dispositivo e o perfil de trabalho.
>
> **Exigir bloqueio de trabalho separado**: É necessário um bloqueio separado para o perfil de trabalho.

5. Restauração de fábrica desativada

A opção de restaurar as configurações de fábrica nas configurações está desativada. Aplica-se apenas a dispositivos totalmente gerenciados.

6. Proteção contra restauração de fábrica

Endereços de e-mail dos administradores do dispositivo para proteção contra restauração de fábrica. Quando o dispositivo sofre uma restauração de fábrica não autorizada, um desses administradores precisará fazer login com o e-mail e a senha da conta Google para desbloquear o dispositivo. Se nenhum administrador for especificado, o dispositivo não terá proteção contra restauração de fábrica. Aplica-se apenas a dispositivos totalmente gerenciados.

Endereços de e-mail dos administradores: utilize **Ativar Proteção contra Restauração de Fábrica** para começar a configurar os administradores. Em seguida, utilize **Adicionar endereço de e-mail do administrador** para adicionar os endereços e remova-os com a ação de exclusão.

7. Recursos do Keyguard

Recursos do Keyguard (tela de bloqueio) que podem ser desativados.

7.1. Desativar tudo

Desativar todas as personalizações atuais e futuras da tela de bloqueio.

7.2. Desativar câmera

Desativar a câmera em telas de bloqueio seguras (por exemplo, PIN).

7.3. Desativar notificações

Desativar a exibição de todas as notificações nas telas de bloqueio seguras.

7.4. Desativar notificações sem informações censuradas

Desativar notificações sem informações censuradas em telas de bloqueio seguras.

7.5. Ignorar o estado do agente de confiança

Ignorar o estado do agente de confiança em telas de bloqueio seguras.

7.6. Desativar impressão digital

Desativar o sensor de impressão digital nas telas de bloqueio seguras.

7.7. Desativar a entrada de texto nas notificações

Desativar a entrada de texto nas notificações em telas de bloqueio seguras.

7.8. Desativar autenticação por reconhecimento facial

Desativar a autenticação por reconhecimento facial em telas de bloqueio seguras.

7.9. Desativar a autenticação por íris

Desativar a autenticação por íris em telas de bloqueio seguras.

7.10. Desativar todas as autenticações biométricas

Desativar todas as autenticações biométricas nas telas de bloqueio seguras.

7.11. Desativar todos os atalhos

Desativar todos os atalhos na tela de bloqueio segura no Android 14 e versões superiores.

Revision #36
Created 2025-12-17 09:34:38 UTC by Admin
Updated 2026-04-22 15:52:45 UTC by Admin