Segurança

Nesta seção, você pode configurar políticas relacionadas à segurança.

Ações para riscos de segurança

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

Tipos de SecurityRisk com suporte:

Sistema operacional desconhecido: A Play Integrity API detecta que o dispositivo está executando um sistema operacional desconhecido (a verificação basicIntegrity é bem-sucedida, mas ctsProfileMatch falha).

Sistema operacional comprometido: A Play Integrity API detecta que o dispositivo está executando um sistema operacional comprometido (a verificação basicIntegrity falha).

Falha na avaliação com suporte de hardware: A Play Integrity API detecta que o dispositivo não tem uma garantia forte de integridade do sistema, se o rótulo MEETS_STRONG_INTEGRITY não aparecer no campo de integridade do dispositivo.

Ações disponíveis:

Apagar dados corporativos (padrão): Cancela o registro e apaga os dados de trabalho (dispositivo inteiro, se totalmente gerenciado, ou apenas o perfil de trabalho, quando o dispositivo tiver um perfil de trabalho).

Nenhuma ação: Mantenha o dispositivo registrado e não faça nada automaticamente.

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

Preservar a proteção contra restauração de fábrica: Preserva os dados da Proteção contra restauração de fábrica (FRP) ao apagar o dispositivo.

Apagar o armazenamento externo: Apaga também o armazenamento externo do dispositivo (como cartões SD) ao realizar a exclusão.

Apagar eSIMs: Para dispositivos corporativos, isso remove todas as eSIMs do dispositivo quando ele é apagado. Em dispositivos de propriedade pessoal, isso removerá as eSIMs gerenciadas (eSIMs adicionadas pelo comando ADD_ESIM) dos dispositivos, e nenhuma eSIM de propriedade pessoal será removida.

1. Tempo máximo para bloquear

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

2. Permanecer ligado durante o carregamento

Os modos de bateria conectada nos quais o dispositivo permanece ligado. Ao usar esta configuração, recomenda-se limpar o **Tempo máximo para bloquear** para que o dispositivo não se bloqueie enquanto permanecer ligado.

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

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

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

3. Bloqueio de tela desativado

Se verdadeiro, desativa a tela de bloqueio para as telas principal e/ou secundárias. Esta política tem suporte 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** (requisito único) ou escopos separados de **Dispositivo**/**Perfil de trabalho**. Requisitos baseados em complexidade devem estar

associados a requisitos baseados em qualidade para o mesmo escopo.

4.1. Escopo

O escopo ao qual o requisito de senha se aplica.

Automático: O escopo não é especificado. Os requisitos de senha são aplicados ao perfil de trabalho para dispositivos com perfil de trabalho e ao dispositivo inteiro para dispositivos totalmente gerenciados ou dedicados.

Dispositivo: Os requisitos de senha são aplicados apenas ao dispositivo.

Perfil de trabalho: Os requisitos de senha são aplicados apenas ao perfil de trabalho.

4.2. Comprimento do histórico de senhas

O comprimento do histórico de senhas. Após definir este campo, o usuário não poderá inserir uma nova senha igual a qualquer senha do histórico. Um valor de 0 significa que não há restrição.

4.3. Máximo de senhas incorretas para apagar

Número de senhas incorretas de desbloqueio do dispositivo que podem ser inseridas antes de o dispositivo ser apagado. Um valor de 0 significa que não há restrição.

4.4. Tempo limite de expiração da senha (dias)

Esta configuração força o usuário a atualizar periodicamente a senha após o número de dias especificado.

4.5. Exigir desbloqueio por senha

O período após o dispositivo ou perfil de trabalho ser desbloqueado usando uma forma forte de autenticação (senha, PIN, padrão) em que ele pode ser desbloqueado usando qualquer outro método de autenticação (por exemplo, impressão digital, agentes de confiança, rosto). Após o período especificado, apenas formas fortes de autenticação poderão ser usadas para desbloquear o dispositivo ou o perfil de trabalho.

Padrão do dispositivo: O período de tempo limite é definido como o padrão do dispositivo.

Todos os dias: O período de tempo limite é definido como 24 horas.

4.6. Qualidade da senha

A qualidade de senha exigida.

Complexidade alta: Define a faixa de alta complexidade de senha como: No Android 12 e superior: PIN sem sequências repetidas (4444) ou ordenadas (1234, 4321, 2468),

comprimento mínimo de 8; alfabética, comprimento mínimo de 6; alfanumérica, comprimento mínimo de 6.

Complexidade média: Define a faixa de média complexidade de senha como: PIN sem sequências repetidas (4444) ou ordenadas (1234, 4321, 2468), comprimento mínimo de 4; alfabética, comprimento mínimo de 4; alfanumérica, comprimento mínimo de 4.

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

Nenhum: Não há requisitos de senha.

Fraca: O dispositivo deve estar protegido no mínimo com uma tecnologia de reconhecimento biométrico de baixa segurança. Isso inclui tecnologias capazes de reconhecer a identidade de um indivíduo que sejam aproximadamente equivalentes a um PIN de 3 dígitos (detecção falsa inferior a 1 em 1.000).

Qualquer: Uma senha é obrigatória, mas não há restrições sobre o que ela deve conter.

Numérica: A senha deve conter caracteres numéricos.

Numérica complexa: A senha deve conter caracteres numéricos sem sequências repetidas (4444) ou ordenadas (1234, 4321, 2468).

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

Alfanumérica: A senha deve conter caracteres numéricos e 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

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

4.8. Mínimo de letras

Número mínimo de letras exigido na senha.

4.9. Mínimo de letras minúsculas

Número mínimo de letras minúsculas exigido na senha.

4.10. Mínimo de letras maiúsculas

Número mínimo de letras maiúsculas exigido na senha.

4.11. Mínimo de caracteres não alfabéticos

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

4.12. Mínimo de dígitos numéricos

Número mínimo de dígitos numéricos exigido na senha.

4.13. Mínimo de símbolos

Número mínimo de símbolos exigido na senha.

4.14. Bloqueio unificado

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

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

5. Restauração de fábrica desativada

Se a restauração de fábrica pelas 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 a proteção contra restauração de fábrica. Quando o dispositivo passar por uma restauração de fábrica não autorizada, será necessário que um desses administradores entre com o e-mail e a senha da conta do Google para desbloquear o dispositivo. Se nenhum administrador for especificado, o dispositivo não oferecerá proteção contra restauração de fábrica. Aplica-se apenas a dispositivos totalmente gerenciados.

E-mails dos administradores: use **Ativar a Proteção contra restauração de fábrica** para começar a configurar os administradores. Depois, use **Adicionar e-mail do administrador** para adicionar endereços e remova-os com a ação de excluir.

7. Recursos do bloqueio de tela

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

7.1. Desativar tudo

Desativa todas as personalizações atuais e futuras do bloqueio de tela.

7.2. Desativar câmera

Desativa a câmera nas telas de bloqueio seguras (por exemplo, PIN).

7.3. Desativar notificações

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

7.4. Desativar notificações não ocultadas

Desativa as notificações não ocultadas nas telas de bloqueio seguras.

7.5. Ignorar o estado do agente de confiança

Ignora o estado do agente de confiança nas telas de bloqueio seguras.

7.6. Desativar impressão digital

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

7.7. Desativar entrada de texto nas notificações

Desativa a entrada de texto nas notificações das telas de bloqueio seguras.

7.8. Desativar autenticação facial

Desativa a autenticação facial nas telas de bloqueio seguras.

7.9. Desativar autenticação por íris

Desativa a autenticação por íris nas telas de bloqueio seguras.

7.10. Desativar toda a autenticação biométrica

Desativa toda a autenticação biométrica nas telas de bloqueio seguras.

7.11. Desativar todos os atalhos

Desativa todos os atalhos na tela de bloqueio segura no Android 14 e superior.

Revision #57
Created 2025-12-17 09:34:38 UTC by Admin
Updated 2026-11-12 09:57:03 UTC by Admin