Regras de conformidade

Se um dispositivo ou perfil de trabalho não estiver em conformidade com qualquer uma das configurações de política listadas abaixo, o Android Device Policy bloqueará imediatamente o uso do dispositivo ou perfil de trabalho por padrão:

- **Requisitos de senha**
- **Política de criptografia**
- **Bloqueio de tela desativado**
- **Métodos de entrada permitidos**
- **Serviços de acessibilidade permitidos**

Se o dispositivo ou o perfil de trabalho continuar não conforme após 10 dias, o Android Device Policy fará a redefinição de fábrica do dispositivo ou excluirá o perfil de trabalho.

Nesta seção, você pode substituir as regras padrão de aplicação de conformidade ou adicionar novas regras.

Regras

Lista de regras que definem o comportamento quando uma política específica não pode ser aplicada a um dispositivo.

Use **Adicionar regra** para criar uma nova regra. Cada cartão de regra pode ser removido usando a ação de excluir.

Nome da configuração

A política de nível superior a ser aplicada. Por exemplo, **Aplicativos** ou **Requisitos de senha**.

Obrigatório. O valor deve corresponder a um nome de política de nível superior com suporte; caso contrário, o campo será marcado como inválido.

Bloquear após dias

Número de dias em que a política fica fora de conformidade antes de o dispositivo ou perfil de trabalho ser bloqueado. Para bloquear o acesso imediatamente, defina como 0. **Bloquear após dias** deve ser menor que **Apagar após dias**. Aplicável apenas a dispositivos corporativos.

Intervalo permitido: 0–300.

Escopo do bloqueio

Especifica o escopo da ação de bloqueio. Aplicável apenas a dispositivos corporativos.

Padrão (nova regra): **Perfil de trabalho**.

> **Perfil de trabalho**: A ação de bloqueio é aplicada apenas aos apps do perfil de trabalho. Os apps do perfil pessoal não são afetados.
>
> **Dispositivo inteiro**: A ação de bloqueio é aplicada ao dispositivo inteiro, incluindo os apps do perfil pessoal.

Apagar após dias

Número de dias em que a política fica fora de conformidade antes de o dispositivo ou perfil de trabalho ser apagado.
Apagar após dias deve ser maior que **Bloquear após dias**. Aplicável apenas a dispositivos corporativos.

Obrigatório. Padrão (nova regra): **1**.

Intervalo permitido: 1–300.

Preservar a proteção contra restauração de fábrica

Se os dados de proteção contra restauração de fábrica são preservados no dispositivo. Esta configuração não se aplica a perfis de trabalho.

Padrão (nova regra): ativado.

Revision #6
Created 2026-11-10 15:17:24 UTC by Admin
Updated 2026-11-12 09:57:03 UTC by Admin