Gerenciamento de apps

Nesta seção, você pode definir políticas relacionadas à disponibilidade de aplicativos, instalação, atualizações e gerenciamento de permissões.

> As Contas do Google Play Gerenciado são criadas automaticamente quando os dispositivos são provisionados.

1. Modo da Play Store

Este modo controla quais aplicativos estão disponíveis para o usuário na Play Store e o comportamento no dispositivo quando os aplicativos são removidos da política.

Lista de permissões (padrão): Apenas os aplicativos que estão na política estarão disponíveis, e qualquer aplicativo que não esteja na política será desinstalado automaticamente do dispositivo. A Play Store mostrará apenas os aplicativos disponíveis.

Lista de bloqueio: Todos os aplicativos estão disponíveis, e qualquer aplicativo que não deva estar no dispositivo deve ser explicitamente marcado como **bloqueado** na política de aplicativos. A Play Store mostrará todos os aplicativos, exceto os bloqueados.

2. Política de aplicativos não confiáveis

A política para aplicativos não confiáveis (aplicativos de fontes desconhecidas) aplicada ao dispositivo. Esta opção controla a configuração do sistema Android que determina se um usuário pode instalar aplicativos de fora da Play Store (sideloading).

Não permitir (padrão): Não permitir a instalação de aplicativos não confiáveis em todo o dispositivo.

Apenas no perfil pessoal: Para dispositivos com perfis de trabalho, permite a instalação de aplicativos não confiáveis apenas no perfil pessoal do dispositivo.

Permitir: Permitir a instalação de aplicativos não confiáveis em todo o dispositivo.

3. Google Play Protect

Se a verificação de aplicativos do Google Play Protect é aplicada.

Aplicada (padrão): Força a verificação de aplicativos.

Escolha do usuário: Permite que o usuário escolha se deseja ativar a verificação de aplicativos.

4. Política de permissão padrão

A política para conceder solicitações de permissão em tempo de execução aos aplicativos.

Solicitar (padrão): Solicita que o usuário conceda uma permissão.

Conceder: Concede uma permissão automaticamente.

Negar: Nega uma permissão automaticamente.

5. Funções de aplicativos

Controla se os aplicativos em dispositivos totalmente gerenciados ou em perfis de trabalho têm permissão para expor funções do aplicativo. Requer Android 16 ou superior.

Permitido (padrão): Aplicativos em dispositivos totalmente gerenciados ou em perfis de trabalho podem expor funções do aplicativo.

Não permitido: Aplicativos em dispositivos totalmente gerenciados ou em perfis de trabalho não podem expor funções do aplicativo.

6. Instalação de aplicativos desativada

Se a instalação de aplicativos pelo usuário está desativada.

7. Desinstalação de aplicativos desativada

Se a desinstalação de aplicativos pelo usuário está desativada.

8. Políticas de permissão

Concessões ou negações explícitas de permissão individual ou em grupo para todos os aplicativos. Esses valores substituem a configuração de **Política de permissão padrão**.

Use **Adicionar política de permissão** para criar entradas e remova-as com a ação de excluir.

Cada entrada inclui:

> **Permissão/grupo Android**: A permissão ou grupo Android (obrigatório), por exemplo **android.permission.READ_CALENDAR** ou **android.permission_group.CALENDAR**.
>
> **Política**: Conceder / Negar / Solicitar (usa as mesmas opções de política da **Política de permissão padrão**).

9. Aplicativos

Lista de aplicativos que devem ser incluídos na política. O comportamento do conteúdo da lista depende do valor definido em **Modo da Play Store**.

Se o **Modo da Play Store** estiver definido como **lista de permissões**, apenas os aplicativos que estão na política estarão disponíveis e qualquer aplicativo que não esteja na política será desinstalado automaticamente do dispositivo.

Se o **Modo da Play Store** estiver definido como **lista de bloqueio**, todos os aplicativos estarão disponíveis e qualquer aplicativo que não deva estar no dispositivo deve ser explicitamente marcado como **bloqueado** na política de aplicativos.

Para adicionar um novo aplicativo, clique no botão **Adicionar aplicativos** (ou no ícone **Adicionar aplicativos**), escolha o aplicativo na Play Store e clique no botão **Selecionar** no card do aplicativo.

> Todos os aplicativos publicados na Play Store em seu país estão disponíveis para seleção por padrão. Para selecionar seus próprios aplicativos privados ou da web, você deve primeiro carregá-los no sistema. Para mais informações, leia a página de **Aplicativos privados**).

Cada aplicativo pode ser configurado com suas próprias definições, que estão contidas visualmente em um card:

9.1. Tipo de instalação

O tipo de instalação a ser realizada para um aplicativo.

> **Disponível**: O aplicativo está disponível para instalação.
>
> **Pré-instalado**: O aplicativo é instalado automaticamente e pode ser removido pelo usuário.

Instalação forçada: O aplicativo é instalado automaticamente e não pode ser removido pelo usuário.

Bloqueado: O aplicativo está bloqueado e não pode ser instalado. Se o aplicativo foi instalado sob uma política anterior, ele será desinstalado.

Obrigatório para configuração: O aplicativo é instalado automaticamente, não pode ser removido pelo usuário e impedirá a conclusão da configuração até que a instalação seja concluída.

Quiosque: O aplicativo é instalado automaticamente no modo quiosque: ele é definido como a intenção de tela inicial preferencial e incluído na lista de permissões para o modo de tarefa bloqueada. A configuração do dispositivo não será concluída até que o aplicativo seja instalado. Após a instalação, os usuários não poderão remover o aplicativo. Você só pode definir este **tipo de instalação** para um aplicativo por política. Quando isso estiver presente na política, a barra de status será desativada automaticamente. Para mais informações, leia a página dedicada ao **Modo quiosque**.

9.2. Restrições de instalação

Define um conjunto de restrições para a instalação do aplicativo. Quando várias restrições são selecionadas, todas elas devem ser atendidas para que o aplicativo seja instalado.

> Esta opção é exibida apenas quando o **Tipo de instalação** for **Pré-instalado** ou **Instalação forçada**.

Rede sem limite de dados: Instale o aplicativo apenas quando o dispositivo estiver conectado a uma rede sem limite de dados (ex: Wi-Fi).

Carregando: Instale o aplicativo apenas quando o dispositivo estiver carregando.

Inativo: Instale o aplicativo apenas quando o dispositivo estiver inativo.

9.3. Modo de atualização automática

Controla o modo de atualização automática do aplicativo.

Padrão: O aplicativo é atualizado automaticamente com baixa prioridade para minimizar o impacto no usuário. O aplicativo é atualizado quando todas as seguintes restrições forem atendidas: (1) o dispositivo não estiver sendo usado ativamente, (2) o dispositivo estiver conectado a uma rede sem limite de dados, (3) o dispositivo estiver carregando. O dispositivo é notificado sobre uma nova atualização em até 24 horas após ser publicada pelo desenvolvedor, após o que o aplicativo será atualizado na próxima vez que as restrições acima forem atendidas.

Adiado: O aplicativo não é atualizado automaticamente por um período máximo de 90 dias após o aplicativo ficar desatualizado. Após 90 dias do aplicativo ficar desatualizado, a versão mais recente disponível é instalada automaticamente com baixa prioridade (veja o modo de **Atualização automática Padrão**). Após a atualização do aplicativo, ele não será atualizado automaticamente de novo até que se passem 90 dias após ficar desatualizado novamente. O usuário ainda pode atualizar o aplicativo manualmente pela Play Store a qualquer momento.

Prioridade alta: O aplicativo é atualizado o mais rápido possível. Nenhuma restrição é aplicada. O dispositivo é notificado imediatamente sobre uma nova atualização assim que ela estiver disponível.

9.4. Código de versão mínimo

A versão mínima do aplicativo que é executada no dispositivo. Se definida, o dispositivo tentará atualizar o aplicativo para pelo menos este código de versão. Se o aplicativo não estiver atualizado, o dispositivo exibirá um **detalhe de não conformidade** com o **motivo de não conformidade** definido como **APP_NOT_UPDATED**. O aplicativo já deve estar publicado no Google Play com um código de versão maior ou igual a este valor. No máximo 20 aplicativos podem especificar um código de versão mínimo por política.

9.5. Escopos delegados

Os escopos delegados ao aplicativo a partir do Android Device Policy. Você pode conceder a outros aplicativos uma seleção de permissões especiais do Android:

Instalação de certificados: Concede acesso à instalação e ao gerenciamento de certificados.

Configurações gerenciadas: Concede acesso ao gerenciamento de configurações gerenciadas.

Bloquear desinstalação: Concede acesso ao bloqueio de desinstalação.

Permissões: Concede acesso à política de permissões e ao estado de concessão de permissões.

Acesso a pacotes: Concede acesso ao estado de acesso a pacotes.

App do sistema: Concede acesso para habilitar aplicativos do sistema.

9.6. Rede preferencial

O serviço de rede preferencial a ser usado para este aplicativo. Se definido, o aplicativo usará o fatiamento de rede empresarial especificado para suas conexões quando disponível. Isso deve corresponder a um fatiamento de rede configurado na seção **Configuração de Fatiamento de Rede 5G** do painel **Celular**.

9.7. Política de permissão padrão

A política padrão para todas as permissões solicitadas pelo aplicativo. Se especificada, esta substitui a **Política de permissão padrão** de nível de política, que se aplica a todos os aplicativos. Ela não substitui as **Políticas de permissão** que se aplicam a todos os aplicativos.

Solicitar (padrão): Solicita que o usuário conceda uma permissão.

Conceder: Concede uma permissão automaticamente.

Negar: Nega uma permissão automaticamente.

9.8. App de trabalho e pessoal conectados

Controla se o aplicativo pode se comunicar entre os perfis de trabalho e pessoal do dispositivo, sujeito ao consentimento do usuário (Android 11+).

Não permitido (padrão): Impede que o aplicativo se comunique entre perfis.

Permitido: Permite que o aplicativo se comunique entre perfis após receber o consentimento do usuário.

9.9. Isenção de bloqueio do Always On VPN

Especifica se o aplicativo tem permissão para usar a rede quando a VPN não estiver conectada e o **bloqueio ativado** estiver ativo. Suportado apenas em dispositivos com Android 10 ou superior.

Aplicada (padrão): O aplicativo respeita a configuração de bloqueio do Always On VPN.

Isento: O aplicativo está isento da configuração de bloqueio do Always On VPN.

9.10. Widgets do perfil de trabalho

Especifica se o aplicativo instalado no perfil de trabalho tem permissão para adicionar widgets à tela inicial.

Permitido: O aplicativo pode adicionar widgets à tela inicial.

Não permitido: O aplicativo não pode adicionar widgets à tela inicial.

9.11. Configurações de controle do usuário

Especifica se o controle do usuário é permitido para um determinado aplicativo. O controle do usuário inclui ações como forçar a parada e limpar os dados do aplicativo (Android 11+). Se o **extensionConfig** estiver ativado para um aplicativo, o controle do usuário será desativado, independentemente desta configuração. Para aplicativos de quiosque, você pode usar **Permitido** para permitir o controle do usuário.

Não especificado: Usa o comportamento padrão do aplicativo para determinar se o controle do usuário é permitido ou não.

Permitido: O controle do usuário é permitido para o aplicativo.

Não permitido: O controle do usuário não é permitido para o aplicativo.

9.12. Desativado

Se o aplicativo está desativado. Quando desativado, os dados do aplicativo ainda são preservados.

9.13. Permitir Provedor de Credenciais

Se o aplicativo tem permissão para atuar como um provedor de credenciais no Android 14 ou superior.

9.14. Configuração gerenciada

Para configurar as definições gerenciadas do aplicativo, clique no botão **Ativar configuração gerenciada**. Se uma configuração gerenciada já estiver definida para o aplicativo, você pode modificá-la com o botão **Configuração gerenciada** ou excluí-la com o botão **Remover configuração**.

> A opção de **Configuração gerenciada** está disponível apenas para aplicativos que suportam essa funcionalidade.

9.15. Políticas de permissão

Concessões ou negações explícitas de permissão para o aplicativo. Esses valores substituem a **Política de permissão padrão** e as **Políticas de permissão** que se aplicam a todos os aplicativos.

Use **Adicionar política de permissão** para adicionar uma ou mais regras de permissão ao card do aplicativo e remova-as com a ação de excluir.

9.16. IDs de trilha

Lista dos IDs de trilha de teste fechado do aplicativo que um dispositivo pode acessar. Se vários IDs de trilha forem selecionados, os dispositivos receberão a versão mais recente entre todas as trilhas acessíveis. Se nenhum ID de trilha for selecionado, os dispositivos terão acesso apenas à trilha de produção do aplicativo.

> A opção de **IDs de trilha** está disponível apenas para aplicativos que possuem pelo menos um ID de trilha disponível para sua organização. Para mais detalhes sobre como adicionar sua organização a uma trilha de teste fechado para um aplicativo específico, leia

aqui.

10. Configurações de aplicativos padrão

Defina aplicativos padrão para os tipos suportados. Quando um aplicativo padrão é definido para pelo menos um tipo, os usuários são impedidos de alterar os aplicativos padrão naquele perfil.

> Apenas uma configuração de aplicativo padrão é permitida por **Tipo de aplicativo padrão**. A lista de aplicativos padrão não deve conter duplicatas.

10.1. Tipo de aplicativo padrão

Selecione a categoria de aplicativo para configurar (por exemplo, Navegador, Discador, SMS, Carteira ou Assistente). A disponibilidade depende da versão do Android e do modo de gerenciamento.

10.2. Escopos de aplicativo padrão

Selecione onde o aplicativo padrão deve ser aplicado (Totalmente gerenciado, Perfil de trabalho ou Perfil pessoal). Apenas os escopos suportados pelo tipo selecionado podem ser escolhidos.

> Se nenhum dos escopos selecionados for aplicável ao modo de gerenciamento do dispositivo, o dispositivo reportará um detalhe de não conformidade.

10.3. Aplicativos padrão

Lista de aplicativos que podem ser definidos como padrão para o tipo selecionado. O primeiro aplicativo instalado e elegível é definido como o padrão.

> Se os escopos incluírem **Totalmente gerenciado** ou **Perfil de trabalho**, cada aplicativo também deve existir na lista de **Aplicativos** com o **Tipo de instalação** não definido como **Bloqueado**.

11. Seleção de chave privada

Permite a exibição da interface no dispositivo para que o usuário escolha um alias de chave privada caso não haja regras correspondentes em **Escolher regras de chave privada**.

>

Para dispositivos com versão inferior ao Android P, a definição desta opção pode deixar as chaves empresariais vulneráveis.

12. Escolher regras de chave privada

Controla o acesso dos aplicativos às chaves privadas. A regra determina qual chave privada, se houver, o Android Device Policy concede ao aplicativo especificado. O acesso é concedido quando o aplicativo chama `KeyChain.choosePrivateKeyAlias` (ou qualquer sobrecarga) para solicitar um alias de chave privada para uma determinada URL, ou para regras que não são específicas de URL (ou seja, se `urlPattern` não estiver definido, ou estiver definido como string vazia ou `.*`) no Android 11 e superior, diretamente para que o aplicativo possa chamar `KeyChain.getPrivateKey`, sem ter que chamar primeiro `KeyChain.choosePrivateKeyAlias`. Quando um aplicativo chama `KeyChain.choosePrivateKeyAlias` e mais de uma regra de `choosePrivateKeyRules` coincide, a última regra correspondente define qual alias de chave será retornado.

Use **Adicionar regra de chave privada** para criar entradas e remova-as com a ação de excluir.

12.1. Alias de chave privada

O alias da chave privada a ser utilizada.

12.2. Padrão de URL

O padrão de URL para correspondência com a URL da solicitação. Se não for definido ou estiver vazio, corresponderá a todas as URLs. Isso utiliza a sintaxe de expressão regular de java.util.regex.Pattern.

12.3. Nomes de pacotes

Os nomes de pacotes aos quais esta regra se aplica. O hash do certificado de assinatura de cada aplicativo é verificado em relação ao hash fornecido pelo Play. Se nenhum nome de pacote for especificado, o alias será fornecido a todos os aplicativos que chamarem `KeyChain.choosePrivateKeyAlias` ou qualquer sobrecarga (mas não sem chamar `KeyChain.choosePrivateKeyAlias`, mesmo no Android 11 ou superior). Qualquer aplicativo com o mesmo UID do Android de um pacote especificado aqui terá acesso ao chamar `KeyChain.choosePrivateKeyAlias`.

Use **Adicionar nome de pacote** para adicionar entradas e remova-as com a ação de excluir.

Para excluir um aplicativo, clique no ícone de **lixeira** na parte inferior do card do aplicativo.

Revision #10
Created 2026-06-24 08:10:10 UTC by Admin
Updated 2026-07-07 10:57:06 UTC by Admin