Gerenciamento de apps

Nesta seção, você pode definir políticas relacionadas à disponibilidade, instalação e atualização de apps, além do gerenciamento de permissões.

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

1. Modo da Play Store

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

Lista de permissões (padrão): somente os apps que estão na política ficam disponíveis, e qualquer app que não esteja na política será desinstalado automaticamente do dispositivo. A Play Store mostrará somente os apps disponíveis.

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

2. Política de apps não confiáveis

A política para apps não confiáveis (apps de fontes desconhecidas) aplicada no dispositivo. Esta opção controla a configuração do sistema Android que determina se o usuário pode instalar apps de fora da Play Store (sideloading).

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

Somente perfil pessoal: para dispositivos com perfis de trabalho, permitir a instalação de apps não confiáveis somente no perfil pessoal do dispositivo.

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

3. Google Play Protect

Indica se a verificação de apps do Google Play Protect é aplicada.

Aplicado (padrão): força a ativação da verificação de apps.

Escolha do usuário: permite que o usuário escolha se deseja ativar a verificação de apps.

4. Política de permissões padrão

A política para conceder solicitações de permissões de tempo de execução aos apps.

Perguntar (padrão): solicitar ao usuário que conceda uma permissão.

Conceder: conceder uma permissão automaticamente.

Negar: negar uma permissão automaticamente.

5. Funções de app

Controla se os apps em dispositivos totalmente gerenciados ou em perfis de trabalho podem expor funções de app. Requer Android 16 ou superior.

Permitido (padrão): apps em dispositivos totalmente gerenciados ou em perfis de trabalho podem expor funções de app.

Não permitido: apps em dispositivos totalmente gerenciados ou em perfis de trabalho não podem expor funções de app.

6. Instalação de apps desativada

Indica se a instalação de apps pelo usuário está desativada.

7. Desinstalação de apps desativada

Indica se a desinstalação de aplicativos pelo usuário está desativada.

8. Políticas de permissão

Concessões ou negações explícitas de permissões ou grupos para todos os apps. Esses valores substituem a configuração **Política de permissões padrão**.

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

Cada entrada inclui:

> **Permissão/grupo do Android**: a permissão ou o grupo do Android (obrigatório), por exemplo **android.permission.READ_CALENDAR** ou **android.permission_group.CALENDAR**.
>
> **Política**: Conceder / Negar / Perguntar (usa as mesmas opções de política de **Política de permissões 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**, somente os apps que estão na política ficam disponíveis, e qualquer app que não esteja na política será desinstalado automaticamente do dispositivo.

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

Para adicionar um novo app, clique no botão **Adicionar aplicativos** (ou no ícone **Adicionar aplicativos**), selecione **Do Managed Google Play**, escolha o app na Play Store e clique no botão **Selecionar** no cartão do app.

Para adicionar um app que não está publicado no Google Play mas já está presente no dispositivo (por exemplo, um app de sistema ou do fabricante), clique em **Adicionar aplicativos**, selecione **Por nome do pacote (apps pré-instalados)**, digite o nome do pacote do app (por exemplo, **com.example.app**) e clique em **Adicionar**.O app é adicionado com o tipo de instalação **Instalação forçada**. Para mostrar o app no launcher personalizado de quiosque, seu **Tipo de instalação** deve ser **Pré-instalado** ou **Instalação forçada**: com **Disponível** o app não é mostrado.

> Os apps que não estão disponíveis no Managed Google Play são marcados com um ícone do Android na lista de aplicativos. Eles não podem ser instalados pelo Google Play, então já devem estar presentes no dispositivo: dispositivos que não têm o app não podem instalá-lo.

>

> Todos os apps publicados na Play Store no seu país ficam disponíveis para seleção por padrão. Para selecionar seus próprios apps privados ou web, você precisa primeiro enviá-los ao sistema. Para mais informações, leia a página **Apps privados**.

Cada app pode ser configurado com suas próprias definições, que ficam visualmente contidas em um cartão:

9.1. Tipo de instalação

O tipo de instalação a realizar para um app.

Disponível: o app está disponível para instalação.

Pré-instalado: o app é instalado automaticamente e pode ser removido pelo usuário.

Instalação forçada: o app é instalado automaticamente e não pode ser removido pelo usuário.

Bloqueado: o app é bloqueado e não pode ser instalado. Se o app foi instalado segundo uma política anterior, ele será desinstalado.

Obrigatório para a configuração: o app é instalado automaticamente e não pode ser removido pelo usuário; ele impedirá a conclusão da configuração até que a instalação seja concluída.

Quiosque: o app é instalado automaticamente no modo quiosque: ele é definido como a intent inicial preferida e incluído na lista de permissões do modo de tarefa de bloqueio. A configuração do dispositivo não será concluída até que o app seja instalado. Após a instalação, os usuários não poderão remover o app. Você só pode definir este **tipo de instalação** para um app por política. Quando ele 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 app. Quando várias restrições são selecionadas, todas devem ser atendidas para que o app seja instalado.

> Esta opção é mostrada somente quando o **Tipo de instalação** é **Pré-instalado** ou **Instalação forçada**.

Rede sem limite de dados: instalar o app somente quando o dispositivo estiver conectado a uma rede sem limite de dados (por exemplo, Wi-Fi).

Carregando: instalar o app somente quando o dispositivo estiver carregando.

Ocioso: instalar o app somente quando o dispositivo estiver ocioso.

9.3. Modo de atualização automática

Controla o modo de atualização automática do app.

Padrão: o app é atualizado automaticamente com baixa prioridade para minimizar o impacto sobre o usuário. O app é atualizado quando todas as seguintes restrições são atendidas: (1) o dispositivo não está em uso ativo, (2) o dispositivo está conectado a uma rede sem limite de dados, (3) o dispositivo está carregando. O dispositivo é notificado sobre uma nova atualização em até 24 horas após ela ser publicada pelo desenvolvedor, e depois o app é atualizado na próxima vez em que as restrições acima forem atendidas.

Adiado: o app não é atualizado automaticamente por no máximo 90 dias após ficar desatualizado. Após 90 dias desde que ficou desatualizado, a versão mais recente disponível é instalada automaticamente com baixa prioridade (consulte o modo de atualização automática **Padrão**). Depois que o app é atualizado, ele não é atualizado automaticamente de novo até 90 dias após ficar desatualizado novamente. O usuário ainda pode atualizar o app manualmente pela Play Store a qualquer momento.

Alta prioridade: o app é atualizado o quanto antes. Nenhuma restrição é aplicada. O dispositivo é notificado imediatamente sobre uma nova atualização assim que ela fica disponível.

9.4. Código de versão mínimo

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

9.5. Escopos delegados

Os escopos delegados ao app pelo Android Device Policy. Você pode conceder a outros apps 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 ativar apps do sistema.

9.6. Rede preferencial

O serviço de rede preferencial a usar para este app. Se definido, o app usará a fatia de rede empresarial especificada para suas conexões quando disponível. Isso deve corresponder a uma fatia de rede configurada na seção **Configuração de fatiamento de rede 5G** do painel **Celular**.

9.7. Política de permissões padrão

A política padrão para todas as permissões solicitadas pelo app. Se especificada, ela substitui a **Política de permissões padrão** no nível da política, que se aplica a todos os apps. Ela não substitui as **Políticas de permissão** que se aplicam a todos os apps.

Perguntar (padrão): solicitar ao usuário que conceda uma permissão.

Conceder: conceder uma permissão automaticamente.

Negar: negar uma permissão automaticamente.

9.8. App conectado de trabalho e pessoal

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

Não permitido (padrão): impede que o app se comunique entre perfis.

Permitido: permite que o app se comunique entre perfis após receber o consentimento do usuário.

9.9. Isenção do bloqueio do Always On VPN

Especifica se o app pode usar a rede quando a VPN não está conectada e o **bloqueio ativado** está em vigor. Compatível somente com dispositivos que executam Android 10 ou superior.

Aplicado (padrão): o app respeita a configuração de bloqueio do Always On VPN.

Isento: o app está isento da configuração de bloqueio do Always On VPN.

9.10. Widgets do perfil de trabalho

Especifica se o app instalado no perfil de trabalho pode 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 app. O controle do usuário inclui ações como forçar a parada e limpar os dados do app (Android 11+). Se **extensionConfig** estiver ativado para um app, o controle do usuário será desativado independentemente desta configuração. Para apps de quiosque, você pode usar **Permitido** para permitir o controle do usuário.

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

Permitido: o controle do usuário é permitido para o app.

Não permitido: o controle do usuário não é permitido para o app.

9.12. Desativado

Indica se o app está desativado. Quando desativado, os dados do app ainda são preservados.

9.13. Permitir provedor de credenciais

Indica se o app pode atuar como provedor de credenciais no Android 14 e superior.

9.14. Configuração gerenciada

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

> **Configuração gerenciada** só está disponível para apps que oferecem suporte a essa funcionalidade.

9.15. Políticas de permissão

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

Use **Adicionar política de permissão** para adicionar uma ou mais regras de permissão ao cartão do app e removê-las com a ação de excluir.

9.16. IDs de faixa

Lista dos IDs das faixas de teste fechado do app às quais um dispositivo pode acessar. Se vários IDs de faixa forem selecionados, os dispositivos recebem a versão mais recente entre todas as faixas acessíveis. Se nenhum ID de faixa for selecionado, os dispositivos só têm acesso à faixa de produção do app.

> **IDs de faixa** só está disponível para apps que têm pelo menos um ID de faixa disponível para sua organização. Para mais detalhes sobre como adicionar sua organização a uma faixa de teste fechado de um app específico, leia aqui.

10. Configurações de aplicativo padrão

Defina apps padrão para os tipos compatíveis. Quando um app padrão é definido para pelo menos um tipo, os usuários ficam impedidos de alterar os apps padrão nesse perfil.

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

10.1. Tipo de aplicativo padrão

Selecione a categoria de app a 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 app padrão deve ser aplicado (Totalmente gerenciado, Perfil de trabalho ou Perfil pessoal). Só podem ser escolhidos escopos compatíveis com o tipo selecionado.

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

10.3. Aplicativos padrão

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

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

11. Seleção de chave privada

Permite mostrar uma interface no dispositivo para o usuário escolher um alias de chave privada se não houver regras correspondentes em **Escolher regras de chave privada**.

> Para dispositivos anteriores ao Android P, definir isso pode deixar as chaves corporativas vulneráveis.

12. Escolher regras de chave privada

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

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

12.1. Alias de chave privada

O alias da chave privada a ser usada.

12.2. Padrão de URL

O padrão de URL a corresponder ao URL da solicitação. Se não definido ou vazio, corresponde a todos os URLs. Isso usa a sintaxe de expressão regular de java.util.regex.Pattern.

12.3. Nomes de pacote

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

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

> Para excluir um app, clique no ícone de **lixeira** na parte inferior do cartão do app.

Revision #18
Created 2026-06-24 08:10:10 UTC by Admin
Updated 2026-11-12 09:57:08 UTC by Admin