Gerenciamento de aplicativos

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

> Contas do Google Play gerenciadas são criadas automaticamente quando os dispositivos são configurados.

1. Modo da Play Store

Este modo controla quais aplicativos estão disponíveis para o usuário na Play Store e o comportamento do dispositivo quando os aplicativos são removidos da política.

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

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

2. Política de aplicativos não confiáveis

Política para aplicativos não confiáveis (aplicativos de fontes desconhecidas) aplicada no dispositivo. Esta opção controla a configuração do sistema Android que determina se um usuário pode instalar aplicativos fora da Play Store (instalação por outros meios).

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

Apenas perfil pessoal: Para dispositivos com perfis de trabalho, permitir 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

Verificação de aplicativos pelo Google Play Protect: habilitado ou desabilitado.

Obrigatório (padrão): Habilita a verificação de aplicativos de forma forçada.

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

4. Política de permissões padrão

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

Solicitação (padrão): Solicite ao usuário que conceda uma permissão.

Conceder: Conceder automaticamente uma permissão.

Negar: Negar automaticamente uma permissão.

5. Funções do aplicativo

Controla se aplicativos em dispositivos totalmente gerenciados ou em perfis de trabalho podem expor suas funções. Requer Android 16 ou superior.

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

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

6. Instalação de aplicativos desativada

Se a instalação de aplicativos por usuários está desativada.

7. Desinstalação de aplicativos desativada

Se a desinstalação de aplicativos pelo usuário estiver desativada.

8. Políticas de permissões

Permissões explícitas ou concessões/negações de grupos para todos os aplicativos. Esses valores substituem a configuração da **política de permissão padrão**.

Use **Política de permissões** para criar entradas e removê-las usando a ação de exclusão.

Cada entrada inclui:

> **Permissão/grupo do Android**: A permissão ou grupo do Android (obrigatório), por exemplo **android.permission.READ_CALENDAR** ou **android.permission_group.CALENDAR**.
>
> **Política**: Permitir / Negar / Solicitar (utiliza 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 **Play Store** estiver definido como **lista de permissões**, apenas os aplicativos que estão na política estarão disponíveis, e qualquer aplicativo que não estiver na política será desinstalado automaticamente do dispositivo.

Se o modo **Play Store** estiver definido como **lista de bloqueios**, todos os aplicativos estarão disponíveis, e qualquer aplicativo que não deve 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**), e, em seguida, selecione o aplicativo na Play Store e clique no botão **Selecionar** no cartão do aplicativo.

> Todos os aplicativos disponíveis na Play Store do seu país estão selecionados por padrão. Para selecionar seus próprios aplicativos privados ou web, você deve primeiro carregá-los para o sistema. Para mais informações, leia a página **Aplicativos privados**.

Cada aplicativo pode ser configurado com suas próprias configurações, que são exibidas visualmente em um cartão:

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 anteriormente por meio de uma política, ele será desinstalado.

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

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

9.2. Instalar restrições

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

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

Rede sem limites de dados: Instale o aplicativo somente quando o dispositivo estiver conectado a uma rede sem limites de dados (por exemplo, Wi-Fi).

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

Ocioso: Instale o aplicativo somente 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 condições são atendidas: (1) o dispositivo não está em uso ativo, (2) o dispositivo está conectado a uma rede sem custos adicionais, (3) o dispositivo está carregando. O dispositivo é notificado sobre uma nova atualização dentro de 24 horas após sua publicação pelo desenvolvedor, após o que o aplicativo é atualizado na próxima vez que as condições acima forem atendidas.

Adiado: O aplicativo não é atualizado automaticamente por um período máximo de 90 dias após a data em que ele se torna desatualizado. Após 90 dias da data em que o aplicativo se torna 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 é atualizado automaticamente novamente até 90 dias após se tornar

desatualizado novamente. O usuário ainda pode atualizar o aplicativo manualmente na 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. Versão mínima (código)

A versão mínima do aplicativo que pode ser executada no dispositivo. Se definido, o dispositivo tentará atualizar o aplicativo para pelo menos esta 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 deve já 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 mínima por política.

9.5. Escopos delegados

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

Instalação de certificado: Permite acesso à instalação e gerenciamento de certificados.

Configurações gerenciadas: Permite acesso ao gerenciamento de configurações gerenciadas.

Bloquear desinstalação: Permite o acesso à funcionalidade de bloqueio de desinstalação.

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

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

Aplicativo do sistema: Permite o acesso para habilitar aplicativos do sistema.

9.6. Rede preferencial

O serviço de rede preferencial a ser utilizado por este aplicativo. Se configurado, o aplicativo utilizará a fatia de rede corporativa especificada para suas conexões, quando disponível. Isso deve corresponder a uma fatia de rede configurada na seção **Configuração de Fatias de Rede 5G** do painel **Celular**.

9.7. Política de permissões padrão

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

Solicitação (padrão): Solicite ao usuário que conceda uma permissão.

Conceder: Conceder automaticamente uma permissão.

Negar: Negar automaticamente uma permissão.

9.8. Trabalho conectado e aplicativos pessoais

Controla se o aplicativo pode se comunicar com ele mesmo entre os perfis de trabalho e pessoal do dispositivo, sujeito à permissão do usuário (Android 11+).

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

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

9.9. Exceção para o bloqueio VPN Always On

Especifica se o aplicativo tem permissão para usar a rede quando a VPN não está conectada e a função de bloqueio **está ativa**. Suportado apenas em dispositivos com Android 10 ou versões mais recentes.

Aplicativo bloqueado (padrão): O aplicativo respeita a configuração de bloqueio VPN sempre ativa.

Exceção: O aplicativo está isento da configuração de bloqueio VPN sempre ativa.

9.10. Widgets do perfil de trabalho

Especifica se o aplicativo 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 pelo usuário é permitido para um determinado aplicativo. O controle pelo usuário inclui ações como forçar a interrupção e limpar os dados do aplicativo (Android 11+). Se a **configuração de extensão** estiver habilitada para um aplicativo, o controle pelo usuário é desabilitado, independentemente dessa configuração. Para aplicativos de quiosque, você pode usar **Permitido** para permitir o controle pelo usuário.

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

Permitido: O controle pelo usuário está habilitado para o aplicativo.

Não permitido: O controle pelo usuário não está habilitado 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 pode atuar como um provedor de credenciais no Android 14 e versões superiores.

9.14. Configuração gerenciada

Para configurar as configurações gerenciadas do aplicativo, clique no botão **Habilitar configuração gerenciada**. Se uma configuração gerenciada já estiver definida para o aplicativo, você pode modificar a configuração 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 permissões

Concessão ou negação explícita de permissões para o aplicativo. Esses valores substituem a **política de permissões padrão** e as **políticas de permissão** que se aplicam a todos os aplicativos.

Use **Política de permissão** para adicionar uma ou mais regras de permissão para o cartão do aplicativo e removê-las com a ação de exclusão.

9.16. Rastreie os IDs

Lista dos IDs de teste fechado do aplicativo que um dispositivo pode acessar. Se vários IDs de teste forem selecionados, os dispositivos recebem a versão mais recente entre todos os testes disponíveis. Se nenhum ID de teste for selecionado, os dispositivos têm acesso apenas à versão de produção do aplicativo.

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

10. Configurações padrão do aplicativo

Definir aplicativos padrão para os tipos suportados. Quando um aplicativo padrão é definido para pelo menos um tipo, os usuários não podem alterar os aplicativos padrão nesse perfil.

>

É permitido apenas um aplicativo padrão por **tipo de aplicativo padrão**. A lista de aplicativos padrão não pode conter duplicatas.

10.1. Tipo de aplicativo padrão

Selecione a categoria do 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 aplicativos padrão

Selecione onde o aplicativo padrão deve ser aplicado (Gerenciamento total, 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 relatará 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 padrão.

Se os escopos incluem **Gerenciamento total** ou **Perfil de trabalho**, cada aplicativo também deve existir na lista de **Aplicativos** com o tipo de **Instalação** não definido como **Bloqueado**.

11. Seleção da chave privada

Permite exibir uma interface para que o usuário selecione um alias de chave privada, caso não haja regras correspondentes em **Regras de seleção de chave privada**.

Para dispositivos com versões do Android anteriores à P, definir esta opção pode deixar as chaves corporativas vulneráveis.

12. Escolha as regras para a chave privada

Controla o acesso dos aplicativos às chaves privadas. A regra determina qual chave privada, se houver, a política de dispositivo Android concede ao aplicativo especificado. O acesso é concedido quando o aplicativo chama KeyChain.choosePrivateKeyAlias (ou qualquer variação) 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 uma string vazia ou "."), no Android 11 e versões superiores, diretamente, para que o aplicativo possa chamar KeyChain.getPrivateKey, sem precisar primeiro chamar KeyChain.choosePrivateKeyAlias. Quando um aplicativo chama KeyChain.choosePrivateKeyAlias e mais de uma choosePrivateKeyRules corresponde, a última regra correspondente define qual alias de chave será retornado.

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

12.1. Alias da chave privada

O alias da chave privada a ser utilizada.

12.2. Padrão da URL

O padrão de URL a ser comparado com a URL da requisição. Se não for definido ou estiver vazio, corresponderá a todas as URLs. Utiliza a sintaxe de expressão regular do java.util.regex.Pattern.

12.3. Nomes dos pacotes

Os nomes dos 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 é fornecido a todos os aplicativos que chamam KeyChain.choosePrivateKeyAlias ou qualquer função equivalente (mas não sem chamar KeyChain.choosePrivateKeyAlias, mesmo no Android 11 e versões superiores). Qualquer aplicativo com o mesmo UID do Android de um pacote especificado aqui terá acesso ao chamar KeyChain.choosePrivateKeyAlias.

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

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

Revision #39
Created 2025-12-17 09:34:42 UTC by Admin
Updated 2026-06-23 17:17:04 UTC by Admin