Políticas - Android

- Resumo
- Gerenciamento de apps
- Modo quiosque
- Segurança
- Multimídia
- Celular
- Rede
- Sistema
- Localização e geocercas
- Gerenciamento de usuários
- Uso pessoal
- Políticas entre perfis
- Relatórios de status
- Diversos
- Regras de conformidade

Resumo

As políticas do Android são as entidades centrais do sistema: elas definem as regras que são aplicadas e impostas nos dispositivos gerenciados.

Você pode navegar pelas suas políticas e criar novas na seção **Políticas** do painel. Para abrir uma política do Android, clique na linha da política na tabela: o sistema abre a página **Editor de políticas**.

Uma política pode ser associada a um token de registro, para que seja aplicada automaticamente aos dispositivos durante o processo de provisionamento. Você também pode alterar a política atribuída a um dispositivo após o provisionamento.

> Cada dispositivo pode ser associado a apenas uma política por vez.

> Muitas opções de política se aplicam apenas a tipos específicos de dispositivo (totalmente gerenciado, dedicado, perfil de trabalho) e versões do Android. Configurações sem suporte podem ser ignoradas pelo dispositivo ou relatadas como fora de conformidade.

Layout do Editor de políticas

O Editor de políticas é organizado como um conjunto de seções expansíveis. No topo da página, você sempre pode editar:

- **Nome** (obrigatório)
- **Id** (somente leitura)
- **Descrição** (opcional)

As seções abaixo correspondem aos painéis do Editor de Política (por exemplo: Gerenciamento de apps, Segurança, Rede, Sistema, Uso pessoal, Políticas entre perfis e muito mais). Quando você abre uma política salva, as seções com configurações alteradas já estão abertas e as demais permanecem fechadas. Use as páginas de capítulo deste manual para entender cada painel em detalhes.

Salvar, excluir e dispositivos associados

Use **Salvar política** para aplicar suas alterações. O botão fica desativado quando não há edições pendentes ou quando a licença está expirada.

Se você abriu uma política existente (ela tem um Id), a página mostra uma ação **Excluir política** e uma lista **Dispositivos associados** na parte inferior, para que você possa ver quantos dispositivos estão usando a política no momento.

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.

Modo quiosque

Com o modo quiosque, você pode restringir a funcionalidade de um dispositivo a um único aplicativo ou a vários aplicativos. A escolha entre o modo quiosque de aplicativo único e o de vários aplicativos depende dos objetivos do seu negócio.

No **modo quiosque de aplicativo único**, um dispositivo é configurado para um único aplicativo e não permite que os usuários finais acessem outros aplicativos no dispositivo. Eles também não podem sair do aplicativo, o que o torna um dispositivo dedicado a esse aplicativo específico. Para ativar esse modo, especifique um aplicativo na seção **Gerenciamento de aplicativos** com **Tipo de instalação** definido como **Quiosque**.

No **modo quiosque de vários aplicativos**, os dispositivos podem acessar vários aplicativos. Os usuários finais podem navegar entre vários aplicativos por meio de um launcher personalizado. Para ativar esse modo, ative a opção **Launcher personalizado de quiosque**.

Quando o modo quiosque está ativado, você também pode configurar se os usuários finais podem acessar determinados recursos do sistema, como configurações do sistema e a barra de status.

Launcher personalizado de quiosque

Se o launcher personalizado de quiosque está ativado. Isso substitui a tela inicial por um launcher que restringe o dispositivo aos aplicativos instalados pela configuração **Gerenciamento de aplicativos**. Os aplicativos aparecem em uma única página em ordem alfabética.

Ações do botão liga/desliga

Define o comportamento de um dispositivo no modo quiosque quando um usuário pressiona e mantém pressionado o botão liga/desliga.

> **Disponível (padrão)**: O menu de energia (por exemplo, Desligar, Reiniciar) é exibido quando um usuário mantém pressionado o botão liga/desliga de um dispositivo no modo quiosque.
>
> **Bloqueado**: O menu de energia (por exemplo, Desligar, Reiniciar) não é exibido quando um usuário mantém pressionado o botão liga/desliga de um dispositivo no modo quiosque. Observação: isso pode impedir que os usuários desliguem o dispositivo.

Avisos de erro do sistema

Especifica se as caixas de diálogo de erro do sistema para aplicativos que travaram ou não respondem são bloqueadas no modo quiosque. Quando bloqueadas, o sistema forçará a parada do aplicativo como se o usuário escolhesse a opção "fechar aplicativo" na interface.

> **Bloqueado (padrão)**: Todas as caixas de diálogo de erro do sistema, como falhas e aplicativo sem resposta (ANR), são bloqueadas. Quando bloqueadas, o sistema força a parada do aplicativo como se o usuário fechasse o aplicativo pela interface.
>
> **Ativado**: Todas as caixas de diálogo de erro do sistema, como falhas e aplicativo sem resposta (ANR), são exibidas.

Navegação do sistema

Especifica quais recursos de navegação estão ativados (por exemplo, botões Início e Visão geral) no modo quiosque.

> **Desativado (padrão)**: Os botões Início e Visão geral não estão acessíveis.
>
> **Somente Início**: Apenas o botão Início está ativado.
>
> **Ativado**: Os botões Início e Visão geral estão ativados.

Barra de status

Especifica se as informações do sistema e as notificações estão desativadas no modo quiosque.

> **Desativado (padrão)**: As informações do sistema e as notificações estão desativadas no modo quiosque.
>
> **Somente sistema**: Apenas as informações do sistema são exibidas na barra de status.
>
> **Ativado**: As informações do sistema e as notificações são exibidas na barra de status no modo quiosque. Observação: Para que esta política tenha efeito, o botão Início do dispositivo deve estar ativado usando kioskCustomization.systemNavigation.

Configurações do dispositivo

Especifica se o aplicativo Configurações é permitido no modo quiosque.

Permitido (padrão): O acesso ao aplicativo Configurações é permitido no modo quiosque.

Bloqueado: O acesso ao aplicativo Configurações não é permitido no modo quiosque.

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.

Multimídia

Nesta seção, você pode configurar o comportamento da câmera/microfone, o acesso a dados via USB, a impressão e as restrições relacionadas à tela.

1. Acesso à câmera

Controla o uso da câmera e se o usuário pode acessar a chave de acesso à câmera (Android 12+). Em geral, desativar a câmera se aplica a todo o dispositivo em dispositivos totalmente gerenciados e apenas dentro do perfil de trabalho em dispositivos com perfil de trabalho.

> **Escolha do usuário (padrão)**: Comportamento padrão do dispositivo. As câmeras estão disponíveis e (Android 12+) o usuário pode alternar o acesso à câmera.
>
> **Desativado**: Todas as câmeras são desativadas (totalmente gerenciado: todo o dispositivo; perfil de trabalho: somente para aplicativos do perfil de trabalho). A chave de acesso à câmera não tem efeito no escopo gerenciado.
>
> **Aplicado**: As câmeras estão disponíveis. Em dispositivos totalmente gerenciados com Android 12+, o usuário não pode alternar o acesso à câmera. Em outros dispositivos/versões, isso se comporta como Escolha do usuário.

2. Acesso ao microfone

Em dispositivos totalmente gerenciados, controla o uso do microfone e se o usuário pode acessar a chave de acesso ao microfone (Android 12+). Esta configuração não tem efeito em dispositivos que não são totalmente gerenciados.

> **Escolha do usuário (padrão)**: Comportamento padrão. O microfone está disponível e (Android 12+) o usuário pode alternar o acesso ao microfone.
>
> **Desativado**: O microfone está desativado (em todo o dispositivo). A chave de acesso ao microfone não tem efeito.
>
> **Aplicado**: O microfone está disponível. No Android 12+, o usuário não pode alternar o acesso ao microfone. No Android 11 ou anterior, isso se comporta como Escolha do usuário.

3. Acesso a dados via USB

Controla quais arquivos e/ou dados podem ser transferidos via USB. Compatível apenas com dispositivos corporativos.

Não permitir transferência de arquivos (padrão): As transferências de arquivos são proibidas, mas outras conexões de dados USB (por exemplo, mouse/teclado) são permitidas.

Não permitir transferência de dados: Todos os tipos de transferência de dados USB são proibidos (Android 12+ com USB HAL 1.3+). Se não houver suporte, o dispositivo usará Não permitir transferência de arquivos como alternativa.

Permitir transferência de dados: Todos os tipos de transferência de dados USB são permitidos.

4. Impressão

Controla se a impressão é permitida (Android 9+).

Permitido (padrão): A impressão é permitida.

Não permitido: A impressão não é permitida (Android 9+).

5. Configurações de brilho da tela

Controla o modo de brilho da tela e (opcionalmente) o valor de brilho.

Modo de brilho da tela:

Escolha do usuário (padrão): O usuário pode configurar o brilho da tela.

Automático: O brilho é automático e o usuário não pode alterá-lo. Você ainda pode definir um valor de brilho, que é usado como parte do ajuste automático (totalmente gerenciado no Android 9+; perfis de trabalho em dispositivos corporativos com Android 15+).

Fixo: O brilho é definido com o valor configurado e o usuário não pode alterá-lo. O valor de brilho é obrigatório (totalmente gerenciado no Android 9+; perfis de trabalho em dispositivos corporativos com Android 15+).

Brilho da tela:

Valor de 1 a 255 (1 = mais baixo, 255 = mais alto). Um valor 0 significa que nenhum valor de brilho está definido.

6. Configurações de tempo limite da tela

Controla se o usuário pode configurar o tempo limite da tela e, quando aplicado, o valor do tempo limite.

O campo **Modo de tempo limite da tela** seleciona entre o comportamento controlado pelo usuário e o comportamento aplicado.

> **Escolha do usuário (padrão)**: O usuário pode configurar o tempo limite da tela.
>
> **Aplicado**: O tempo limite da tela é definido com o valor configurado e o usuário não pode alterá-lo (totalmente gerenciado no Android 9+; perfis de trabalho em dispositivos corporativos com Android 15+).

Tempo limite da tela:

> Duração do tempo limite em segundos. O valor deve ser maior que 0. Se for maior que **Tempo máximo para bloquear**, o sistema poderá limitá-lo e relatar não conformidade.

7. Captura de tela desativada

Se a captura de tela está desativada.

8. Ajuste de volume desativado

Se o ajuste do volume principal está desativado.

9. Montagem de mídia física desativada

Se a montagem de mídia física externa está desativada.

Celular

Nesta seção, você pode configurar políticas relacionadas à rede celular.

1. Modo avião

Controla se o usuário pode ativar ou desativar o modo avião.

> **Escolha do usuário (padrão)**: o usuário pode ativar ou desativar o modo avião.
>
> **Desativado**: o modo avião fica desativado. O usuário não pode ativar o modo avião. Compatível com Android 9 e superior.

2. 2G celular

Controla se o usuário pode ativar ou desativar a configuração de 2G celular.

> **Escolha do usuário (padrão)**: o usuário pode ativar ou desativar o 2G celular.
>
> **Desativado**: o 2G celular fica desativado. O usuário não pode ativar o 2G celular pelas configurações. Compatível com Android 14 e superior.

3. Substituir APNs

Controla se os APNs de substituição estão ativados ou desativados. Quando ativados, somente os APNs de substituição configurados são usados, e todos os outros APNs no dispositivo são ignorados.

> **Desativado (padrão)**: Todas as configurações de APN definidas são salvas no dispositivo, mas ficam desativadas e não têm efeito. Todos os outros APNs no dispositivo continuam em uso.
>
> **Ativado**: Somente os APNs de substituição são usados; todos os outros APNs são ignorados. Esta configuração só pode ser definida em dispositivos totalmente gerenciados com Android 10 ou superior.

4. Configurações de APN

Configure uma ou mais entradas de APN. Use **Adicionar APN** para criar uma entrada e **Remover APN** para excluí-la.

Cada APN tem campos obrigatórios:

Tipos de APN: Selecione um ou mais tipos de tráfego para este APN (a disponibilidade depende do modo de gerenciamento e da versão do Android).

Nome do APN: O identificador do APN fornecido pela sua operadora.

Nome de exibição: Nome amigável mostrado na interface.

Campos opcionais de APN:

Tipo de autenticação, **Nome de usuário**, **Senha**: Configure a autenticação da operadora (se necessário).

Protocolo e **Protocolo de roaming**: Configuração do protocolo IP.

Tipos de rede: Restrinja as tecnologias celulares que o APN pode usar (por exemplo, LTE/5G NR).

Endereço do proxy e **Porta do proxy**: Proxy HTTP para tráfego de dados (se aplicável).

Endereço do proxy MMS, **Porta do proxy MMS**, **MMSC (URI do centro de MMS)**: Configurações relacionadas a MMS.

ID numérico da operadora (MCC+MNC) e **ID da operadora**: Campos de identificação da operadora.

Configuração sempre ativa: Se a sessão PDU ativada por este APN deve permanecer sempre ativa. Compatível com Android 15 ou superior.

Tipo de MVNO: Tipo de identificador da operadora de rede virtual móvel.

MTU IPv4 e **MTU IPv6**: Unidade máxima de transmissão para rotas IPv4/IPv6. Compatível com Android 13 ou superior.

5. Configuração de transmissão celular desativada

Se a configuração de transmissão celular está desativada.

6. Configuração de redes móveis desativada

Se a configuração de redes móveis está desativada.

7. Dados em roaming desativados

Se os serviços de dados em roaming estão desativados.

8. Chamadas de saída desativadas

Se as chamadas de saída estão desativadas.

9. SMS desativados

Se o envio e o recebimento de mensagens SMS estão desativados.

10. Configuração de fatiamento de rede 5G

Configure os serviços de rede preferencial para ativar o fatiamento de rede 5G corporativo. Você pode configurar até 5 fatias corporativas e atribuir aplicativos a redes específicas para otimizar o roteamento de tráfego.

10.1. Rede preferencial padrão

ID da rede preferencial padrão para aplicativos que não estão na lista de aplicativos, ou se a **Rede preferencial** de um aplicativo não estiver definida. É preciso ter uma configuração para o ID de rede especificado (a menos que esteja definido como **Nenhuma rede preferencial**).

Observação: aplicativos críticos como **com.google.android.apps.work.clouddpc** e **com.google.android.gms** são excluídos desta configuração padrão.

10.2. Configurações de serviço de rede

Use **Adicionar configuração de rede** para criar uma configuração de fatia. Você pode adicionar até 5 configurações. Cada configuração tem:

ID da rede preferencial (atribuído automaticamente): O ID da rede é atribuído automaticamente e não pode ser alterado.

Recorrer à conexão padrão: Se o fallback para a rede padrão de todo o dispositivo é permitido. Se não for permitido, os aplicativos não poderão acessar a internet caso a fatia 5G não esteja disponível.

Redes não correspondentes: Se os aplicativos sujeitos a esta configuração podem usar redes diferentes do serviço preferencial. Se definido como **Não permitido**, **Recorrer à conexão padrão** também deve ser **Não permitido**. Requer Android 14 ou superior.

Rede

Nesta seção, você pode configurar políticas relacionadas a rede.

> As configurações de Wi-Fi podem ser provisionadas e gerenciadas pelo sistema por meio de **Configurações de WiFi**. Dependendo do valor definido em **Configurar Wi-Fi**, os usuários podem ter controle limitado ou nenhum controle sobre adicionar/modificar redes.

Estado do rádio do dispositivo

1. Estado do Wi-Fi

Controla o estado atual do Wi-Fi e se o usuário pode alterar esse estado.

Escolha do usuário (padrão): O usuário pode ativar/desativar o Wi-Fi.

Ativado: O Wi-Fi está ligado e o usuário não pode desativá-lo (Android 13+).

Desativado: O Wi-Fi está desligado e o usuário não pode ativá-lo (Android 13+).

2. Nível mínimo de segurança do Wi-Fi

O nível mínimo de segurança exigido das redes Wi-Fi às quais o dispositivo pode se conectar. Compatível com Android 13 ou superior, para dispositivos totalmente gerenciados e perfis de trabalho em dispositivos corporativos.

Rede aberta (padrão): O dispositivo pode se conectar a todos os tipos de redes Wi-Fi.

Rede pessoal: Não permite redes Wi-Fi abertas; exige pelo menos segurança pessoal (por exemplo, WPA2-PSK).

Rede corporativa: Exige redes EAP corporativas; não permite redes Wi-Fi abaixo deste nível de segurança.

Rede corporativa de 192 bits: Exige redes corporativas de 192 bits; opção mais restritiva.

3. Estado da banda ultralarga (UWB)

Controla o estado da configuração de banda ultralarga e se o usuário pode ativá-la ou desativá-la.

Escolha do usuário (padrão): O usuário pode ativar ou desativar o UWB.

Desativado: O UWB está desativado e o usuário não pode ativá-lo pelas configurações (Android 14+).

Gerenciamento de conectividade do dispositivo

4. Compartilhamento por Bluetooth

Controla se o compartilhamento por Bluetooth é permitido.

Permitido: O compartilhamento por Bluetooth é permitido (padrão em dispositivos totalmente gerenciados, Android 8+).

Não permitido: O compartilhamento por Bluetooth não é permitido (padrão em perfis de trabalho, Android 8+).

5. Configurar Wi-Fi

Controla os privilégios de configuração do Wi-Fi. Dependendo da opção selecionada, o usuário tem controle total, limitado ou nenhum controle na configuração de redes Wi-Fi.

Permitir configurar o Wi-Fi (padrão): O usuário pode configurar o Wi-Fi.

Não permitir adicionar configuração de Wi-Fi: Não é permitido adicionar novas configurações de Wi-Fi. O usuário pode alternar entre redes já configuradas (Android 13+; totalmente gerenciado e perfis de trabalho corporativos).

Não permitir configurar o Wi-Fi: Não permite configurar redes Wi-Fi. Em dispositivos totalmente gerenciados, isso remove as redes configuradas pelo usuário e mantém apenas as redes configuradas via **Configurações de WiFi**. Em perfis de trabalho corporativos, as

redes existentes não são afetadas, mas os usuários não podem adicionar/remover/modificar redes Wi-Fi.

> Quando a configuração do Wi-Fi está desativada e o dispositivo não consegue se conectar na inicialização, o sistema pode mostrar o **mecanismo de escape de rede** para permitir que o usuário se conecte temporariamente e atualize a política.

6. Configurações de Wi-Fi Direct

Controla a configuração e o uso das configurações de Wi-Fi Direct. Compatível com dispositivos corporativos com Android 13 ou superior.

Permitir (padrão): O usuário pode usar o Wi-Fi Direct.

Não permitir: O usuário não pode usar o Wi-Fi Direct.

7. Configurações de ancoragem

Controla as configurações de ancoragem. Com base no valor definido, o usuário fica parcial ou totalmente impedido de usar diferentes formas de ancoragem.

Permitir toda ancoragem (padrão): Permite a configuração e o uso de todas as formas de ancoragem.

Não permitir ancoragem Wi-Fi: Impede o usuário de usar ancoragem Wi-Fi (dispositivos corporativos com Android 13+).

Não permitir toda ancoragem: Não permite nenhuma forma de ancoragem (totalmente gerenciado + perfis de trabalho corporativos).

8. Política de SSID do Wi-Fi

Restrições sobre a quais SSIDs de Wi-Fi o dispositivo pode se conectar (isso não afeta quais redes podem ser configuradas no dispositivo). Compatível com dispositivos corporativos com Android 13 ou superior.

Lista de bloqueio de SSID (padrão): O dispositivo não pode se conectar a nenhuma rede Wi-Fi cujo SSID esteja listado, mas pode se conectar a outras redes.

Lista de permissões de SSID: O dispositivo pode se conectar apenas aos SSIDs listados. A lista de SSIDs não pode estar vazia.

Use **Adicionar SSID** para adicionar entradas. Dependendo do tipo de política selecionado, a lista é interpretada como SSIDs permitidos ou negados.

Na interface do Editor de Políticas, a lista de SSIDs é rotulada como **SSIDs de Wi-Fi permitidos** para listas de permissões e **SSIDs de Wi-Fi negados** para listas de bloqueio.

9. Configurações de roaming do Wi-Fi

Configure o modo de roaming do Wi-Fi por SSID. Use **Adicionar configuração de roaming Wi-Fi** para criar entradas.

Cada entrada inclui:

SSID: O SSID ao qual a configuração de roaming se aplica (obrigatório).

Modo de roaming do Wi-Fi: Padrão / Desativado / Agressivo. Desativado e Agressivo exigem Android 15+ e são compatíveis apenas com dispositivos totalmente gerenciados e perfis de trabalho em dispositivos corporativos.

Restrições de rede

10. Bluetooth desativado

Se o Bluetooth está desativado. Prefira esta configuração em vez de Configuração de Bluetooth desativada, pois a configuração de Bluetooth desativada pode ser contornada pelo usuário.

11. Compartilhamento de contatos por Bluetooth desativado

Se o compartilhamento de contatos por Bluetooth está desativado.

12. Configuração de Bluetooth desativada

Se a configuração do Bluetooth está desativada.

13. Redefinição de rede desativada

Se a redefinição das configurações de rede está desativada.

14. Beam de saída desativado

Se o uso de NFC para transmitir dados de aplicativos está desativado.

VPN

15. Aplicativo de VPN Always On

Especifique um nome de pacote de VPN Always On para garantir que os dados dos aplicativos gerenciados especificados sempre passem por uma VPN configurada.

> Observação: este recurso exige a implantação de um cliente VPN compatível com os recursos Always On e VPN por aplicativo.

16. Bloqueio de VPN

Não permite o uso da rede quando a VPN não está conectada.

17. Configuração de VPN desativada

Se a configuração da VPN está desativada.

Proxy e serviços de rede

18. Serviço de rede preferencial

Controla se o serviço de rede preferencial está ativado no perfil de trabalho. Por exemplo, uma organização pode ter um acordo com uma operadora para que os dados de trabalho sejam enviados por um serviço de rede da operadora dedicado ao uso corporativo (por exemplo, uma fatia corporativa em redes 5G). Isso não tem efeito em dispositivos totalmente gerenciados.

Desativado: O serviço de rede preferencial está desativado no perfil de trabalho.

Ativado: O serviço de rede preferencial está ativado no perfil de trabalho.

> Se você usar fatiamento de rede corporativo, configure também **Configuração de fatiamento de rede 5G** no painel de política **Celular** e atribua aplicativos a uma fatia usando a configuração **Rede preferencial** deles.

19. Proxy global recomendado

O proxy HTTP global independente de rede. Normalmente, os proxies devem ser configurados por rede nas configurações de WiFi. Um proxy global pode ser útil para configurações incomuns, como filtragem interna geral. O proxy global é apenas uma recomendação e alguns aplicativos podem ignorá-lo.

Desativado

Proxy direto

Configuração automática de proxy (PAC)

19.1. Host

O host do proxy direto.

19.2. Porta

A porta do proxy direto.

19.3. URI do PAC

O URI do script PAC usado para configurar o proxy.

19.4. Hosts excluídos

Para um proxy direto, os hosts para os quais o proxy é ignorado. Os nomes de host podem conter curingas, como ***.example.com**.

Use **Adicionar host excluído** para adicionar entradas (disponível apenas para proxy direto).

Configurações de Wi-Fi

Defina configurações de rede Wi-Fi que o sistema aplicará nos dispositivos. Use **Adicionar configuração de Wi-Fi** para criar uma entrada e remova-a com a ação de excluir.

20. Campos de configuração de Wi-Fi

Cada configuração inclui:

Nome da configuração: Obrigatório.

SSID: Obrigatório.

Conexão automática: Se a rede deve ser conectada automaticamente quando estiver ao alcance.

Transição rápida: Se o cliente deve tentar usar a Transição rápida (IEEE 802.11r-2008) com a rede.

SSID oculto: Se o SSID será transmitido.

Modo de randomização de MAC: Hardware ou Automático (Android 13+).

20.1. Segurança

Opções de segurança de Wi-Fi:

WEP-PSK: WEP (Chave pré-compartilhada).

WPA-PSK: WPA/WPA2/WPA3-Personal (Chave pré-compartilhada).

WPA-EAP: WPA/WPA2/WPA3-Enterprise (Extensible Authentication Protocol).

Modo de 192 bits do WPA3: Rede WPA-EAP que permite apenas o modo de 192 bits do WPA3.

20.2. Frase secreta (Chave pré-compartilhada)

Exibido quando a Segurança é **WEP-PSK** ou **WPA-PSK**. A frase secreta é obrigatória.

20.3. Método EAP (Enterprise)

Exibido quando a Segurança é **WPA-EAP** ou **Modo de 192 bits do WPA3**. Selecione um método externo EAP:

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Autenticação da fase 2

Exibido para métodos externos de tunelamento (**EAP-TTLS** e **PEAP**).

MSCHAPv2

PAP

20.5. Credenciais EAP dos usuários

Quando ativado, o sistema aplica automaticamente as credenciais EAP nos dispositivos por usuário. Você pode configurar as credenciais do usuário na seção **Usuários**.

20.6. Certificado do cliente

Para **EAP-TLS**, você pode atribuir um certificado de cliente usado para autenticação Wi-Fi. Para mais informações, leia a página **Gerenciamento de certificados**.

Se um certificado já estiver atribuído, você pode usar **Abrir certificado** para visualizá-lo ou **Alterar certificado** para selecionar outro.

Como alternativa, você pode especificar o **Alias do par de chaves do certificado do cliente**, que faz referência a um certificado de cliente armazenado no chaveiro do Android e permitido para autenticação Wi-Fi.

> Se tanto**Certificado do cliente** quanto **Alias do par de chaves do certificado do cliente** estiverem definidos, o alias do par de chaves será ignorado.

20.7. Identidade

Identidade do usuário. Para protocolos externos de tunelamento (PEAP, EAP-TTLS), ela é usada para autenticar dentro do túnel, e a **Identidade anônima** é usada para a identidade EAP fora do túnel. Para protocolos externos sem tunelamento, ela é usada para a identidade EAP.

20.8. Identidade anônima

Apenas para protocolos de tunelamento, indica a identidade do usuário apresentada ao protocolo externo.

20.9. Senha

Senha do usuário. Se não especificada, o padrão é solicitar ao usuário.

20.10. Certificados de CA do servidor

Lista de certificados de CA a serem usados para verificar a cadeia de certificados do host. Pelo menos um certificado de CA deve corresponder. Para mais informações, leia a página **Gerenciamento de certificados**.

Use **Adicionar certificado de CA do servidor** para adicionar entradas e remova-as com a ação de excluir.

20.11. Correspondências de sufixo de domínio

Uma lista de restrições para o nome de domínio do servidor. As entradas são usadas como requisitos de correspondência de sufixo em relação ao(s) nome(s) DNS do nome alternativo da entidade de um certificado de servidor de autenticação.

Sistema

Nesta seção, você pode configurar políticas relacionadas ao sistema.

1. Nível mínimo de API

O nível mínimo de API do Android permitido.

2. Política de criptografia

Se a criptografia está ativada.

Padrão: Este valor é ignorado, ou seja, nenhuma criptografia é exigida.

Ativada sem senha: Criptografia exigida, mas nenhuma senha é necessária para inicializar.

Ativada com senha: Criptografia exigida com senha necessária para inicializar.

3. Data e hora automáticas

Se a data, a hora e o fuso horário automáticos estão ativados em um dispositivo corporativo.

Escolha do usuário (padrão): A data, a hora e o fuso horário automáticos ficam a critério do usuário.

Aplicado: Aplica data, hora e fuso horário automáticos no dispositivo.

4. Configurações do desenvolvedor

Controla o acesso às configurações do desenvolvedor: opções do desenvolvedor e inicialização segura.

Desativado (padrão): desativa todas as configurações do desenvolvedor e impede que o usuário acesse.

Permitido: permite todas as configurações do desenvolvedor. O usuário pode acessar e, opcionalmente, configurar as configurações.

5. Modo Common Criteria

Controla o Modo Common Criteria — padrões de segurança definidos no Common Criteria for Information Technology Security Evaluation (CC). Ativar o Modo Common Criteria aumenta determinados componentes de segurança em um dispositivo (por exemplo: criptografia AES-GCM de Bluetooth Long Term Keys, validação adicional de alguns certificados de rede e verificações de integridade da política criptográfica). O Modo Common Criteria é compatível apenas com dispositivos de propriedade da empresa que executam Android 11 ou superior. Aviso: o Modo Common Criteria impõe um modelo de segurança rígido, normalmente necessário apenas para organizações altamente sensíveis. O uso padrão do dispositivo pode ser afetado; ative-o somente se necessário.

Desativado (padrão): desativa o Modo Common Criteria.

Ativado: ativa o Modo Common Criteria.

6. Memory Tagging Extension (MTE)

Controla o Memory Tagging Extension (MTE) no dispositivo.

Escolha do usuário (padrão): o usuário pode escolher ativar ou desativar o MTE no dispositivo (se o dispositivo for compatível).

Imposto: o MTE está ativado e o usuário não tem permissão para alterá-lo (Android 14+; compatível com dispositivos totalmente gerenciados e perfis de trabalho em dispositivos de propriedade da empresa).

Desativado: o MTE está desativado e o usuário não tem permissão para alterá-lo (Android 14+; compatível apenas com dispositivos totalmente gerenciados).

7. Proteção de conteúdo

Controla se a proteção de conteúdo (que verifica apps enganosos) está ativada. Isso é compatível com Android 15 e superior.

Desativado (padrão): a proteção de conteúdo está desativada e o usuário não pode alterar isso.

Imposto: a proteção de conteúdo está ativada e o usuário não pode alterar isso (Android 15+).

Escolha do usuário: a proteção de conteúdo não é controlada pela política; o usuário pode escolher (Android 15+).

8. Conteúdo do Assist

Controla se o AssistContent pode ser enviado a um app privilegiado, como um app assistente (por exemplo, Circle to Search). O AssistContent inclui capturas de tela e informações sobre um app, como o nome do pacote. Isso é compatível com Android 15 e superior.

Permitido (padrão): o conteúdo do Assist pode ser enviado a um app privilegiado (Android 15+).

Não permitido: o conteúdo do Assist é bloqueado e não pode ser enviado a um app privilegiado (Android 15+).

9. Criação de janelas desativada

Se a criação de janelas além das janelas de apps está desativada. Esta opção impede a exibição das seguintes interfaces do sistema: toasts e snackbars, atividades do telefone (como chamadas recebidas) e atividades prioritárias do telefone (como chamadas em andamento), alertas do sistema, erros do sistema e sobreposições do sistema.

10. Válvula de escape de rede

Se a válvula de escape de rede está ativada. Se não for possível estabelecer uma conexão de rede na inicialização, a válvula de escape solicita que o usuário se conecte temporariamente a uma rede para atualizar a política do dispositivo. Após a aplicação da política, a rede temporária será esquecida e o dispositivo continuará a inicialização. Isso evita ficar sem conexão de rede quando não houver uma rede adequada na última política e o dispositivo iniciar em um app no modo de tarefa bloqueada, ou quando o usuário não conseguir acessar as configurações do dispositivo.

11. Atividades padrão

Uma lista de atividades padrão para processar intents que correspondem a um filtro de intent específico. Por exemplo, este recurso permite que os administradores de TI escolham qual app de

navegador abre automaticamente links da web ou qual app launcher é usado ao tocar no botão home.

Use **Adicionar atividade padrão** para criar entradas. Dentro de uma entrada, use **Adicionar ação** e **Adicionar categoria** para montar o filtro de intent.

11.1. Atividade receptora

A atividade que deve ser o manipulador de intent padrão. Deve ser um nome de componente Android, por exemplo, com.android.enterprise.app/.MainActivity. Como alternativa, o valor pode ser o nome do pacote de um app, o que faz o Android Device Policy escolher uma atividade apropriada do app para processar o intent.

11.2. Ação

As ações de intent a serem correspondidas no filtro. Se alguma ação estiver incluída no filtro, a ação de um intent deverá ser um desses valores para haver correspondência. Se nenhuma ação estiver incluída, a ação do intent será ignorada.

11.3. Categoria

As categorias de intent a serem correspondidas no filtro. Um intent inclui as categorias de que precisa, e todas elas devem estar incluídas no filtro para haver correspondência. Em outras palavras, adicionar uma categoria ao filtro não afeta a correspondência, a menos que essa categoria seja especificada no intent.

12. Métodos de entrada permitidos

Especifica os métodos de entrada permitidos.

> **Todos permitidos**: nenhuma restrição aplicada. Todos os métodos de entrada são permitidos.
>
> **Apenas do sistema**: apenas os métodos de entrada integrados do sistema são permitidos.
>
> **Apenas do sistema e fornecidos**: apenas os métodos de entrada fornecidos e os integrados do sistema são permitidos.

12.1. Métodos de entrada permitidos

Nomes de pacote de métodos de entrada permitidos. Aplica-se apenas quando **Métodos de entrada permitidos** está definido como **Apenas do sistema e fornecidos**.

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

13. Serviços de acessibilidade permitidos

Especifica os serviços de acessibilidade permitidos.

> **Todos permitidos**: qualquer serviço de acessibilidade pode ser usado.
>
> **Apenas do sistema**: apenas os serviços de acessibilidade integrados do sistema podem ser usados.
>
> **Apenas do sistema e fornecidos**: apenas os serviços de acessibilidade fornecidos e os integrados do sistema podem ser usados.

13.1. Serviços de acessibilidade permitidos

Serviços de acessibilidade permitidos. Aplica-se apenas quando **Serviços de acessibilidade permitidos** está definido como **Apenas do sistema e fornecidos**.

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

14. Política de atualização do sistema

Configuração para gerenciar atualizações do sistema.

> **Padrão**: segue o comportamento padrão de atualização do dispositivo, que normalmente exige que o usuário aceite as atualizações do sistema.
>
> **Automático**: instala automaticamente assim que uma atualização estiver disponível.
>
> **Em janela**: instala automaticamente dentro de uma janela de manutenção diária. Isso também configura os apps do Play para serem atualizados dentro da janela. Essa opção é altamente recomendada para dispositivos do tipo quiosque, pois é a única forma de o Play atualizar apps fixados permanentemente em primeiro plano.
>
> **Adiar**: adia a instalação automática por até no máximo 30 dias.

14.1. Janela de manutenção (somente Em janela)

Quando **Política de atualização do sistema** está definida como **Em janela**, você pode definir a janela de manutenção diária usando os campos **de** e **até**.

14.2. Períodos de congelamento de atualizações do sistema

Um período repetido anualmente em que as atualizações do sistema via over-the-air (OTA) são adiadas para congelar a versão do sistema operacional em execução em um dispositivo. Para evitar o congelamento indefinido do dispositivo, cada período de congelamento deve ser separado por pelo menos 60 dias. Cada período de congelamento não pode exceder 90 dias.

Use **Adicionar período de congelamento de atualizações do sistema** para criar entradas.

15. Provedores de credenciais padrão

Controla quais apps podem atuar como provedores de credenciais no Android 14 e superior.

> **Não permitido (padrão)**: apps com credentialProviderPolicy não especificado não podem atuar como provedor de credenciais.
>
> **Não permitido, exceto sistema**: apps com credentialProviderPolicy não especificado não podem atuar como provedor de credenciais, exceto os provedores de credenciais padrão do OEM.

Localização e geocercas

Este painel agrupa as configurações de política do Android que controlam o relatório de localização do dispositivo, a aplicação de localização e as definições de cerca geográfica. Use-o quando quiser que o Cerberus Enterprise colete as localizações dos dispositivos ou detecte quando eles entram ou saem de áreas configuradas.

Relatório de localização

Relatar localização

Ativa o relatório de geolocalização do dispositivo. Os dados de localização coletados por esta configuração são usados pelo **mapa de localização do painel**, pelo histórico de localização na visão geral do dispositivo e pelo processamento de cercas geográficas.

> O histórico de localização e os eventos de geocerca são mantidos por **90 dias** e os dados mais antigos são excluídos automaticamente todas as noites. A última localização de cada dispositivo registrado é sempre mantida, então ele continua nos mapas.

> Em dispositivos que não são totalmente gerenciados, os dados de localização ainda podem depender de o app Cerberus Enterprise ter as permissões de localização necessárias e de os serviços de localização estarem habilitados no dispositivo.

> Em dispositivos Apple pessoais (Registro de Usuário), a localização e as cercas geográficas ficam desativadas por padrão: só estão disponíveis quando a política da Apple tem **Localização e cercas geográficas em dispositivos pessoais** ativado e apenas se o usuário permitir a localização para o aplicativo Cerberus Enterprise.

Modo de localização

Controla a configuração de localização do dispositivo em dispositivos corporativos.

- **Escolha do usuário**: os serviços de localização não são restritos pela política.
- **Aplicado**: os serviços de localização são ativados no dispositivo.

- **Desativado**: os serviços de localização são desativados no dispositivo.

Compartilhamento de localização desativado

Desativa o compartilhamento de localização para aplicativos de trabalho. Em dispositivos com proprietário de perfil, isso afeta o perfil de trabalho. Em dispositivos totalmente gerenciados, desativa a localização de todo o dispositivo e substitui o modo de localização do dispositivo.

Comportamento automático com cercas geográficas ativas

As cercas geográficas ativas exigem que o relatório de localização funcione. Quando pelo menos uma cerca geográfica está ativa, o Cerberus Enterprise mantém automaticamente a consistência das configurações de localização relacionadas.

- **Relatar localização** fica forçado como ativado enquanto existirem cercas geográficas ativas.
- **Modo de localização** é forçado para **Aplicado**.
- **Compartilhamento de localização desativado** fica forçado como desativado.

Se você tentar desativar **Relatar localização** enquanto uma ou mais cercas geográficas estiverem ativas, o Cerberus Enterprise exibirá uma caixa de diálogo de confirmação. Se você continuar, todas as cercas geográficas ativas na política serão desativadas.

Lista de cercas geográficas

Uma política pode conter até **10 cercas geográficas**. Os nomes das cercas geográficas devem ser exclusivos dentro da política.

Use **Adicionar cerca geográfica** para criar uma nova entrada. Cada cerca geográfica contém estes campos principais:

- **Nome**: obrigatório e exclusivo.
- **Latitude** e **Longitude**: o centro da área.
- **Raio (m)**: obrigatório, de **200** a **10000** metros.
- **Descrição**: observações opcionais para administradores.

- **Relatar entrada** e **Relatar saída**: escolha quais eventos de transição devem ser gerados.
- **Ativa**: ativa ou desativa a cerca geográfica sem excluí-la.

> Pelo menos uma das opções **Relatar entrada** ou **Relatar saída** deve permanecer ativada para cada cerca geográfica.

> O raio mínimo era de 100 metros anteriormente. As cercas geográficas existentes menores que 200 metros continuam funcionando e são mantidas como estão quando você salva a política, mesmo se você as mover ou renomear. Se você alterar o raio delas, ele deve ser de pelo menos 200 metros.

Ferramentas de edição do mapa

Cada cartão de cerca geográfica inclui uma prévia do mapa da área. Você pode editar a geometria pelo mapa ou pelos campos numéricos.

- Clique no mapa para mover o centro da cerca geográfica quando a edição da área estiver desbloqueada.
- Use o botão **Localização atual** para centralizar o mapa na posição atual do seu navegador.
- Use o botão **Recentralizar mapa** para restaurar a visualização preferida dessa cerca geográfica.
- Use o botão de bloqueio para evitar alterações acidentais na geometria da cerca geográfica.

Onde os dados de cerca geográfica aparecem

As transições de cerca geográfica podem ser revisadas na página **Visão geral do dispositivo** do Android, na aba **Cerca geográfica** do painel de localização. Essa aba mostra as transições em um mapa dedicado, junto com ferramentas de filtragem e a lista de transições.

Gerenciamento de usuários

Adição de usuário desativada

Se a adição de novos usuários e perfis está desativada. Para dispositivos em que managementMode é **DEVICE_OWNER**, este campo é ignorado e o usuário nunca tem permissão para adicionar ou remover usuários.

Modificação de contas desativada

Se a adição ou remoção de contas está desativada.

Configuração de credenciais do usuário desativada

Se a configuração de credenciais do usuário está desativada.

Remoção de usuário desativada

Se a remoção de outros usuários está desativada.

Definição do ícone do usuário desativada

Se a alteração do ícone do usuário está desativada.

Definição do papel de parede desativada

Se a alteração do papel de parede está desativada.

Autenticação na configuração da conta de trabalho

Controla como os usuários se autenticam durante a configuração da conta de trabalho. Esta opção está disponível apenas para empresas Android com um domínio gerenciado do Google (Google Workspace).

Durante a configuração/registro do dispositivo, esta política influencia se é necessário entrar com uma conta de trabalho, mas a configuração **Autenticar usando o Google** do Google Admin Console e o tipo de token de registro ainda podem exigir autenticação.

Para dispositivos já registrados, esta política só se aplica se o dispositivo for gerenciado por uma conta do Managed Google Play (ou seja, registrado sem **Autenticar usando o registro do Google**).

Para mais detalhes e solução de problemas, consulte **Autenticar usando o registro do Google**.

Tipos de conta bloqueados

Tipos de conta que não podem ser gerenciados pelo usuário. Esta opção impede que os usuários do dispositivo adicionem contas não aprovadas.

Use **Adicionar tipo de conta bloqueado** para adicionar um ou mais tipos de conta.

Cada entrada tem um campo **Tipo de conta** (obrigatório). Insira uma string como **com.google**. Remova uma entrada usando a ação de excluir.

Uso pessoal

Ao provisionar um dispositivo corporativo para uso profissional e pessoal, você pode especificar algumas regras para limitar como o usuário pode operar o dispositivo para uso pessoal, fora do perfil de trabalho.

> Esta seção se aplica apenas a dispositivos corporativos com perfil de trabalho. Ela não terá efeito em dispositivos totalmente gerenciados ou de propriedade pessoal.

1. Câmera desativada

Se a câmera está desativada.

2. Captura de tela desativada

Se a captura de tela está desativada.

3. Máximo de dias com o trabalho desligado

Controla por quanto tempo o perfil de trabalho pode permanecer desligado.

4. Compartilhamento via Bluetooth

Controla se o compartilhamento via Bluetooth é permitido no perfil pessoal de um dispositivo corporativo com perfil de trabalho.

5. Espaço privado

Controla se um espaço privado é permitido no dispositivo.

6. Modo da Play Store

Este modo controla quais apps são permitidos ou bloqueados para o usuário na Play Store do perfil pessoal.

> **Lista de bloqueio (padrão)**: Todos os apps estão disponíveis e qualquer app que não deva estar no dispositivo deve ser marcado explicitamente como **Bloqueado** na seção **Aplicativos**.
>
> **Lista de permissões**: Apenas apps especificados explicitamente na seção **Aplicativos** com **Tipo de instalação** definido como **Disponível** podem ser instalados no perfil pessoal.

7. Aplicativos

Lista de aplicativos que devem ser permitidos ou bloqueados no perfil pessoal. O comportamento do conteúdo da lista depende do valor definido em **Modo da Play Store**.

Para adicionar um novo app da Play Store, clique no ícone **+**.

7.1. Tipo de instalação

Tipos de comportamentos de instalação que um aplicativo do perfil pessoal pode ter.

> **Bloqueado**: O app está bloqueado e não pode ser instalado no perfil pessoal.
>
> **Disponível**: O app está disponível para instalação no perfil pessoal.

8. Tipos de conta bloqueados

Tipos de conta que não podem ser gerenciados pelo usuário. Esta opção impede que os usuários do dispositivo adicionem contas não aprovadas no perfil pessoal.

Políticas entre perfis

Aplica-se apenas a dispositivos com perfis pessoal e de trabalho.

Copiar/colar entre perfis

Se o texto copiado de um perfil (pessoal ou de trabalho) pode ser colado no outro perfil.

> **Não permitido (padrão)**: Impede que os usuários colem no perfil pessoal textos copiados do perfil de trabalho. Textos copiados do perfil pessoal podem ser colados no perfil de trabalho.
>
> **Permitido**: O texto copiado em qualquer um dos perfis pode ser colado no outro perfil.

Compartilhamento de dados entre perfis

Se os dados de um perfil (pessoal ou de trabalho) podem ser compartilhados com aplicativos no outro perfil. Controla especificamente o compartilhamento simples de dados via intents. O gerenciamento de outros canais de comunicação entre perfis, como busca de contatos, copiar/colar,
ou aplicativos de trabalho e pessoais conectados, é configurado separadamente.

> **Não permitido**: Impede o compartilhamento de dados tanto do perfil pessoal para o perfil de trabalho quanto do perfil de trabalho para o perfil pessoal.
>
> **Trabalho para pessoal não permitido (padrão)**: Impede que os usuários compartilhem dados do perfil de trabalho com aplicativos no perfil pessoal. Dados pessoais podem ser compartilhados com aplicativos de trabalho.
>
> **Permitido**: Os dados de qualquer um dos perfis podem ser compartilhados com o outro perfil.

Padrão de widgets do perfil de trabalho

Comportamento padrão dos widgets do perfil de trabalho. Se um aplicativo específico não definir uma política de widgets, ele seguirá o padrão definido aqui.

Funções de aplicativos entre perfis

Controla se os aplicativos do perfil pessoal podem invocar funções de aplicativos do perfil de trabalho. Isso requer Android 16 ou superior.

> Esta configuração depende da opção **Funções de aplicativos** no nível da política (na seção Gerenciamento de aplicativos). Se Funções de aplicativos estiver definida como **Não permitido**, a API rejeitará Funções de aplicativos entre perfis definidas como **Permitido**.

Contatos de trabalho no perfil pessoal

Se os contatos armazenados no perfil de trabalho podem ser exibidos nas pesquisas de contatos e nas chamadas recebidas do perfil pessoal.

Permitido (padrão): Permite que os contatos do perfil de trabalho apareçam no perfil pessoal.

Não permitido: Impede que os aplicativos pessoais acessem os contatos do perfil de trabalho e pesquisem contatos de trabalho.

Não permitido, exceto sistema: Impede a maioria dos aplicativos pessoais de acessar os contatos do perfil de trabalho, exceto os aplicativos Discador, Mensagens e Contatos padrão do OEM (Android 14+).

Quando Contatos de trabalho no perfil pessoal está configurado, você pode definir opcionalmente uma lista de entradas de **Nome de pacote isento**. Dependendo do modo selecionado, essas isenções funcionam como lista de permissões ou lista de bloqueio para aplicativos pessoais.

Relatórios de status

Nesta seção, você pode configurar quais dados devem ser recuperados do dispositivo. Os dados de status podem ser visualizados na página do painel **Status do dispositivo**.

Relatórios de aplicativos

Se os relatórios de apps estão ativados. (Informações relatadas sobre um app instalado.)

> Esta opção é exigida pelo sistema (para integração com o app complementar) e está sempre ativada; não pode ser desativada.

Incluir apps removidos

Se os apps removidos são incluídos nos relatórios de aplicativos.

Configurações do dispositivo

Se o relatório de configurações do dispositivo está ativado. (Informações sobre configurações do dispositivo relacionadas à segurança.)

Informações de software

Se o relatório de informações de software está ativado. (Informações sobre o software do dispositivo.)

Informações de memória

Se o relatório de memória está ativado. (Um evento relacionado a medições de memória e armazenamento.)

Informações de rede

Se o relatório de informações de rede está ativado. (Informações de rede do dispositivo.)

Informações de tela

Se o relatório de telas está ativado. Os dados do relatório não estão disponíveis para dispositivos de propriedade pessoal com perfis de trabalho. (Informações de tela do dispositivo.)

Eventos de gerenciamento de energia

Se o relatório de eventos de gerenciamento de energia está ativado. Os dados do relatório não estão disponíveis para dispositivos de propriedade pessoal com perfis de trabalho.

Status de hardware

Se o relatório de status de hardware está ativado. Os dados do relatório não estão disponíveis para dispositivos de propriedade pessoal com perfis de trabalho.

Propriedades do sistema

Se o relatório de propriedades do sistema está ativado.

Modo Common Criteria

Se o relatório do Modo Common Criteria está ativado.

Diversos

1. Jogo easter egg desativado

Se o jogo easter egg nas Configurações está desativado.

2. Ignorar dicas de primeiro uso

Sinalizador para ignorar dicas no primeiro uso. O administrador corporativo pode ativar a recomendação do sistema para que os aplicativos ignorem o tutorial do usuário e outras dicas introdutórias na primeira inicialização.

3. Mensagem de suporte curta

Uma mensagem exibida ao usuário na tela de configurações sempre que uma funcionalidade tiver sido desativada pelo administrador. Se a mensagem tiver mais de 200 caracteres, ela poderá ser truncada.

4. Mensagem de suporte longa

Uma mensagem exibida ao usuário na tela de configurações dos administradores do dispositivo.

5. Informações do proprietário na tela de bloqueio

As informações do proprietário do dispositivo a serem exibidas na tela de bloqueio.

6. Ações de configuração

Ações a executar durante o processo de configuração. Durante o registro, você pode exigir que o usuário abra um ou mais aplicativos necessários para a configuração do dispositivo.

Use **Adicionar ação de configuração** para criar entradas e remova-as com a ação de exclusão.

6.1. Iniciar aplicativo

Nome do pacote do aplicativo a ser iniciado

6.2. Título

Fornece uma mensagem para o usuário, a fim de explicar por que o aplicativo precisa ser iniciado.

6.3. Descrição

Fornece uma mensagem para o usuário, a fim de explicar por que o aplicativo precisa ser iniciado.

7. Visibilidade do nome de exibição da empresa

Controla se o nome de exibição da empresa é visível no dispositivo (por exemplo, como mensagem na tela de bloqueio em dispositivos corporativos).

Visível (padrão): O nome de exibição da empresa é visível no dispositivo (compatível com perfis de trabalho no Android 7+ e dispositivos totalmente gerenciados no Android 8+).

Oculto: O nome de exibição da empresa fica oculto no dispositivo.

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.