Políticas - Android

Resumo

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

Você pode visualizar suas políticas e criar novas a partir da seção **Políticas** no painel. Para abrir uma política para Android, clique na linha da política na tabela: o sistema abrirá a página **Editor de Políticas**.

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

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

> Muitas opções de política se aplicam apenas a tipos específicos de dispositivos (gerenciados, dedicados, perfil de trabalho) e versões do Android. Configurações não suportadas podem ser ignoradas pelo dispositivo ou reportadas como não compatíveis.

Layout do editor de políticas

O editor de políticas é organizado em seções expansíveis. No topo da página, você sempre pode editar:

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

As seções abaixo correspondem aos painéis do Editor de Políticas (por exemplo: Gerenciamento de aplicativos, Segurança, Rede, Sistema, Uso pessoal, Políticas entre perfis e muito mais). Use as páginas de cada capítulo deste manual para entender cada painel em detalhes.

Salvar, excluir e dispositivos associados

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

Se você abriu uma política existente (que possui um ID), a página exibirá uma ação "**Excluir política** e uma lista de "**Dispositivos associados** na parte inferior, para que você possa ver quantos dispositivos estão atualmente usando a política.

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.

Modo quiosque

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

Em **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, tornando-o um dispositivo dedicado para esse aplicativo específico. Para habilitar este modo, especifique um aplicativo na seção **Gerenciamento de aplicativos** com o **tipo de instalação** definido como **Quiosque**.

Em **modo quiosque com múltiplos aplicativos**, os dispositivos têm acesso a vários aplicativos. Os usuários finais podem navegar entre vários aplicativos por meio de um lançador personalizado. Para habilitar este modo, ative a opção de **lançador quiosque personalizado**.

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

Lançador personalizado para modo quiosque

Indica se o lançador personalizado para modo quiosque está habilitado. Isso substitui a tela inicial por um lançador que restringe o dispositivo aos aplicativos instalados através da configuração de **Gerenciamento de aplicativos**. Os aplicativos aparecem em uma única página em ordem alfabética.

Ações do botão de energia

Define o comportamento do dispositivo no modo kiosk quando o usuário pressiona e mantém pressionado (pressionamento longo) o botão de energia.

> **Disponível (padrão)**: O menu de energia (por exemplo, Desligar, Reiniciar) é exibido quando um usuário pressiona e mantém pressionado (pressionamento longo) o botão de energia de um dispositivo no modo kiosk.
>
> **Bloqueado**: O menu de energia (por exemplo, Desligar, Reiniciar) não é exibido quando um usuário pressiona e mantém pressionado o botão de energia de um dispositivo no modo kiosk. Observe: isso pode impedir que os usuários desliguem o dispositivo.

Alertas de erro do sistema

Especifica se as caixas de diálogo de erro do sistema para aplicativos que travam ou não respondem são bloqueadas no modo kiosk. Quando bloqueadas, o sistema forçará o encerramento 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 travamentos e aplicativos que não respondem (ANR), são bloqueadas. Quando bloqueadas, o sistema força o encerramento do aplicativo, como se o usuário o fechasse pela interface do usuário.

Ativado: Todas as caixas de diálogo de erro do sistema, como travamentos e aplicativos que não respondem (ANR), são exibidas.

Navegação do sistema

Define quais recursos de navegação estão habilitados (por exemplo, botões Início, Visão geral) no modo kiosk.

Desabilitado (padrão): Os botões Início e Visão Geral não estão acessíveis.

Apenas a tela inicial: Apenas o botão "Início" está habilitado.

Ativado: Os botões "Início" e "Visão geral" estão habilitados.

Barra de status

Especifica se as informações do sistema e as notificações são desativadas no modo kiosk.

Desativado (padrão): As informações do sistema e as notificações são desativadas no modo kiosk.

Apenas sistema: Apenas informações do sistema são exibidas na barra de status.

Ativado: Informações do sistema e notificações são exibidas na barra de status no modo kiosk. Observação: Para que esta política entre em vigor, o botão "home" do dispositivo deve estar habilitado usando kioskCustomization.systemNavigation.

Configurações do dispositivo

Especifica se o aplicativo de configurações é permitido no modo kiosk.

Permitido (padrão): Permite o acesso ao aplicativo de configurações no modo kiosk.

Bloqueado: O acesso ao aplicativo de configurações não é permitido no modo kiosk.

Segurança

Nesta seção, você pode configurar políticas relacionadas à segurança.

Ações de risco de segurança

Escolha o que fazer quando um dispositivo relata um Risco de Segurança nos relatórios de status.

Tipos de Risco de Segurança suportados:

Sistema operacional desconhecido: A API Play Integrity detecta que o dispositivo está executando um sistema operacional desconhecido (o teste básicoIntegrity é bem-sucedido, mas ctsProfileMatch falha).

Sistema operacional comprometido: A API Play Integrity detectou que o dispositivo está executando um sistema operacional comprometido (o teste básicoIntegrity falhou).

Avaliação baseada em hardware falhou: A API Play Integrity detectou que o dispositivo não possui uma garantia forte de integridade do sistema, caso o rótulo MEETS_STRONG_INTEGRITY não seja exibido no campo de integridade do dispositivo.

Ações disponíveis:

Limpar dados corporativos (padrão): Desinscrever e limpar os dados de trabalho (apaga todo o dispositivo, se totalmente gerenciado, ou apenas o perfil de trabalho, se gerenciado apenas pelo perfil).

Nenhuma ação: Mantenha o dispositivo inscrito e não execute nenhuma ação automaticamente.

Quando você seleciona "**Apagar dados corporativos**", você também pode configurar opções de limpeza:

Manter a proteção de restauração de fábrica: Mantenha os dados de Proteção de Restauração de Fábrica (FRP) ao limpar o dispositivo.

Limpar o armazenamento externo: Além disso, limpe o armazenamento externo do dispositivo (como cartões SD) ao realizar a limpeza.

Limpar eSIMs: Para dispositivos pertencentes à empresa, isso remove todos os eSIMs do dispositivo durante a limpeza. Em dispositivos de propriedade pessoal, isso removerá os eSIMs gerenciados (eSIMs adicionados via o comando ADD_ESIM) nos dispositivos, e nenhum eSIM de propriedade pessoal será removido.

1. Tempo máximo para bloqueio

Tempo máximo (em segundos) de atividade do usuário antes do bloqueio do dispositivo. Um valor de 0 significa que não há restrição.

2. Permanece ligado durante o carregamento

Os modos de carregamento em que o dispositivo permanece ligado. Ao usar essa configuração, recomenda-se limpar **Tempo máximo de bloqueio** para que o dispositivo não se bloqueie enquanto estiver ligado.

Carregador de tomada: A fonte de energia é um carregador de tomada.

Porta USB: A fonte de energia é uma porta USB.

Carregador sem fio: A fonte de energia é sem fio.

3. Tela de bloqueio desativada

Se verdadeiro, isso desativa a tela de bloqueio para as telas primárias e/ou secundárias. Essa política é suportada 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** (um único requisito) ou escopos separados de **Dispositivo**/**Perfil de trabalho**. Os requisitos baseados em complexidade devem ser combinados com requisitos baseados em qualidade para o mesmo escopo.

4.1. Escopo

O escopo a que se aplica a exigência de senha.

> **Dispositivo** O escopo não está especificado. As exigências de senha são aplicadas ao perfil de trabalho para dispositivos com perfil de trabalho e a todo o dispositivo para dispositivos totalmente gerenciados ou dedicados.
>
> **Dispositivo**: As exigências de senha são aplicadas apenas ao dispositivo.
>
> **Perfil de trabalho**: Os requisitos de senha são aplicados apenas ao perfil de trabalho.

4.2. Comprimento do histórico de senhas

Comprimento do histórico de senhas. Após definir este campo, o usuário não poderá usar uma nova senha que seja igual a qualquer senha no histórico. Um valor de 0 significa que não há restrição.

4.3. Número máximo de tentativas de senha inválidas antes de apagar o dispositivo

Número máximo de senhas incorretas para desbloquear o dispositivo antes que ele seja apagado. Um valor de 0 significa que não há restrição.

4.4. Tempo limite de expiração da senha (em dias)

Esta configuração obriga o usuário a alterar a senha periodicamente, após o número de dias especificado.

4.5. Requer desbloqueio por senha

O tempo decorrido após o desbloqueio do dispositivo ou perfil de trabalho usando uma forma de autenticação forte (senha, PIN, padrão) durante o qual ele pode ser desbloqueado usando qualquer outro método de autenticação (por exemplo, impressão digital, agentes de confiança, reconhecimento facial). Após o período de tempo especificado, apenas formas de autenticação fortes podem ser usadas para desbloquear o dispositivo ou perfil de trabalho.

> **Configuração padrão do dispositivo**: O período de inatividade está definido para a configuração padrão do dispositivo.
>
> **Todos os dias**: O período de inatividade está definido como 24 horas.

4.6. Qualidade da senha

A qualidade de senha exigida.

> **Complexidade alta**: Defina a faixa de complexidade alta para senhas como: No Android 12 e versões superiores: PIN sem sequências repetidas (4444) ou ordenadas (1234, 4321, 2468),

comprimento mínimo de 8; alfabético, comprimento mínimo de 6; alfanumérico, comprimento mínimo de 6.

Complexidade média: Defina a faixa de complexidade média para senhas como: PIN sem sequências repetidas (4444) ou ordenadas (1234, 4321, 2468), comprimento mínimo de 4; alfabético, comprimento mínimo de 4; alfanumérico, comprimento mínimo de 4.

Complexidade baixa: Defina a faixa de complexidade baixa para senhas como: padrão; PIN com sequências repetidas (4444) ou ordenadas (1234, 4321, 2468).

Nenhum: Não há requisitos para senhas.

Fraco: O dispositivo deve ser protegido com uma tecnologia de reconhecimento biométrico de baixa segurança, no mínimo. Isso inclui tecnologias que podem reconhecer a identidade de um indivíduo que são aproximadamente equivalentes a um PIN de 3 dígitos (a taxa de falsos positivos é inferior a 1 em 1.000).

Qualquer: É necessário definir uma senha, mas não há restrições quanto ao conteúdo da senha.

Numérico: A senha deve conter caracteres numéricos.

Numérico complexo: A senha deve conter caracteres numéricos, sem repetições (4444) ou sequências ordenadas (1234, 4321, 2468).

Alfanumérico: A senha deve conter caracteres alfabéticos (ou símbolos).

Alfanumérico: A senha deve conter tanto números quanto caracteres 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

Comprimento mínimo da senha permitido. Um valor de 0 significa que não há restrição.

4.8. Número mínimo de letras

Número mínimo de letras exigido na senha.

4.9. Número mínimo de letras minúsculas

Número mínimo de letras minúsculas exigidas na senha.

4.10. Número mínimo de letras maiúsculas

Número mínimo de letras maiúsculas exigidas na senha.

4.11. Número mínimo de caracteres não alfabéticos

Número mínimo de caracteres não alfabéticos (dígitos numéricos ou símbolos) exigidos na senha.

4.12. Número mínimo de dígitos numéricos

Número mínimo de dígitos numéricos exigidos na senha.

4.13. Número mínimo de símbolos

Número mínimo de símbolos exigidos na senha.

4.14. Bloqueio unificado

Controla se o bloqueio unificado é permitido para o dispositivo e o perfil de trabalho, em dispositivos com Android 9 ou superior e que possuem um perfil de trabalho. Isso não tem efeito em outros dispositivos.

> **Permitir bloqueio unificado**: Um bloqueio comum é permitido para o dispositivo e o perfil de trabalho.
>
> **Exigir bloqueio de trabalho separado**: É necessário um bloqueio separado para o perfil de trabalho.

5. Restauração de fábrica desativada

A opção de restaurar as configurações de fábrica nas 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 proteção contra restauração de fábrica. Quando o dispositivo sofre uma restauração de fábrica não autorizada, um desses administradores precisará fazer login com o e-mail e a senha da conta Google para desbloquear o dispositivo. Se nenhum administrador for especificado, o dispositivo não terá proteção contra restauração de fábrica. Aplica-se apenas a dispositivos totalmente gerenciados.

Endereços de e-mail dos administradores: utilize **Ativar Proteção contra Restauração de Fábrica** para começar a configurar os administradores. Em seguida, utilize **Adicionar endereço de e-mail do administrador** para adicionar os endereços e remova-os com a ação de exclusão.

7. Recursos do Keyguard

Recursos do Keyguard (tela de bloqueio) que podem ser desativados.

7.1. Desativar tudo

Desativar todas as personalizações atuais e futuras da tela de bloqueio.

7.2. Desativar câmera

Desativar a câmera em telas de bloqueio seguras (por exemplo, PIN).

7.3. Desativar notificações

Desativar a exibição de todas as notificações nas telas de bloqueio seguras.

7.4. Desativar notificações sem informações censuradas

Desativar notificações sem informações censuradas em telas de bloqueio seguras.

7.5. Ignorar o estado do agente de confiança

Ignorar o estado do agente de confiança em telas de bloqueio seguras.

7.6. Desativar impressão digital

Desativar o sensor de impressão digital nas telas de bloqueio seguras.

7.7. Desativar a entrada de texto nas notificações

Desativar a entrada de texto nas notificações em telas de bloqueio seguras.

7.8. Desativar autenticação por reconhecimento facial

Desativar a autenticação por reconhecimento facial em telas de bloqueio seguras.

7.9. Desativar a autenticação por íris

Desativar a autenticação por íris em telas de bloqueio seguras.

7.10. Desativar todas as autenticações biométricas

Desativar todas as autenticações biométricas nas telas de bloqueio seguras.

7.11. Desativar todos os atalhos

Desativar todos os atalhos na tela de bloqueio segura no Android 14 e versões superiores.

Mídia

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

1. Acesso à câmera

Controla o uso da câmera e se o usuário pode ativar/desativar o acesso à câmera (Android 12+). Em geral, desativar a câmera afeta todo o dispositivo em dispositivos 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 ativar/desativar o acesso à câmera.
>
> **Desativado**: Todas as câmeras estão desativadas (gerenciamento total: em todo o dispositivo; perfil de trabalho: apenas para aplicativos do perfil de trabalho). O botão de alternância de acesso à câmera não tem efeito no ambiente gerenciado.
>
> **Ativado**: As câmeras estão disponíveis. Em dispositivos totalmente gerenciados com Android 12 ou superior, o usuário não pode ativar ou desativar o acesso à câmera. Em outros dispositivos/versões, o comportamento é semelhante à 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 alternância de permissão do microfone (Android 12+). Essa 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 ativar ou desativar o acesso ao microfone.
>
> **Desativado**: O microfone está desativado (em todo o dispositivo). O botão de alternância de acesso ao microfone não terá efeito.
>
> **Imposto**: O microfone está disponível. No Android 12 ou superior, o usuário não pode alternar o acesso ao microfone. No Android 11 ou versões anteriores, o comportamento é semelhante à seleção do usuário.

Acesso a dados via USB

Controla quais arquivos e/ou dados podem ser transferidos via USB. Suportado apenas em dispositivos pertencentes à empresa.

Não permitir transferência de arquivos (padrão): A transferência de arquivos é desabilitada, mas outras conexões de dados USB (por exemplo, mouse/teclado) são permitidas.

Desabilitar transferência de dados: Todos os tipos de transferências de dados via USB são bloqueados (Android 12+ com USB HAL 1.3+). Caso não seja suportado, o dispositivo retorna à opção "Desabilitar transferência de arquivos".

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

4. Impressão

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

Permitido (padrão): A impressão está habilitada.

Não permitido: A impressão não é permitida (Android 9 e versões mais recentes).

5. Configurações de brilho da tela

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

Modo de brilho da tela:

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

Automático: O brilho é ajustado automaticamente e o usuário não pode alterá-lo. Você ainda pode definir um valor de brilho, que é usado como parte do ajuste automático (Android 9+ com gerenciamento total; perfis de trabalho em dispositivos Android 15+ de propriedade da empresa).

Fixa: O brilho é definido para o valor configurado e o usuário não pode alterá-lo. O valor de brilho é obrigatório (Android totalmente gerenciado, versão 9 ou superior; perfis de trabalho em dispositivos Android 15 ou superior de propriedade da empresa).

Brilho da tela: o valor é definido pela configuração e o usuário não pode alterá-lo. O valor do brilho é obrigatório (Android totalmente gerenciado, versão 9 ou superior; perfis de trabalho em dispositivos Android 15 ou superior de propriedade da empresa)

Valor de 1 a 255 (1 = mínimo, 255 = máximo). Um valor de 0 indica que nenhum valor de brilho foi definido.

6. Configurações de tempo limite da tela

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

O campo **Modo de tempo limite da tela** permite escolher entre o comportamento controlado pelo usuário e o comportamento imposto.

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

Obrigatório: O tempo limite da tela é definido com o valor configurado e o usuário não pode alterá-lo (Android 9+ com gerenciamento total; perfis de trabalho em dispositivos Android 15+ de propriedade da empresa).

Tempo de inatividade da tela: Obrigatório: O tempo limite da tela é definido com o valor configurado e o usuário não pode alterá-lo (Android 9+ com gerenciamento total; perfis de trabalho em dispositivos Android 15+ de propriedade da empresa)

Duração do tempo limite em segundos. O valor deve ser maior que 0. Se for maior que **Tempo máximo de bloqueio**, o sistema pode limitar esse valor e reportar não conformidade.

7. Captura de tela desabilitada

Se a captura de tela está desabilitada.

Ajuste de volume desativado

Se o ajuste do volume principal está desativado.

9. Montar mídia física desabilitado

A montagem de mídia física externa está desabilitada.

Celular

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

1. Modo avião

Controla se o modo avião pode ser ativado ou desativado pelo usuário ou não.

Opção do usuário (padrão): O usuário pode ativar ou desativar o modo avião.

Desativado: O modo avião está desativado. O usuário não tem permissão para ativar ou desativar o modo avião. Compatível com Android 9 e versões mais recentes.

2. Celular 2G

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

Escolha do usuário (padrão): O usuário pode ativar ou desativar a rede celular 2G.

Desativado: A rede celular 2G está desativada. O usuário não pode ativar a rede celular 2G nas configurações. Compatível com Android 14 e versões superiores.

3. Substituir APNs

Controla se as configurações de APN personalizadas estão habilitadas ou desabilitadas. Quando habilitadas, apenas as configurações de APN personalizadas configuradas são usadas e todas as outras configurações de APN no dispositivo são ignoradas.

Desativado (padrão): Todas as configurações de APN configuradas são armazenadas no dispositivo, mas estão desativadas e não têm efeito. Todas as outras configurações de APN no dispositivo permanecem em uso.

Ativado: Apenas as configurações de APN de substituição são utilizadas, todas as outras configurações de APN são ignoradas. Essa configuração só pode ser configurada 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 possui 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 exibido na interface do usuário.

Campos APN opcionais:

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 utilizar (por exemplo, LTE/5G NR).

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

Endereço do Proxy MMS, **Porta do Proxy MMS**, **MMSC (URI do Centro MMS)**: Configurações relacionadas ao MMS.

ID do Operador Numérico (MCC+MNC) e **ID da Operadora**: Campos de identificação da operadora.

Configuração Sempre Ativa: Define se a sessão PDU ativada por esta APN deve permanecer sempre ativa. Suportado no Android 15 e versões superiores.

Tipo de Operadora Virtual de Telefonia Móvel: Identificador do tipo de operadora virtual de rede móvel.

MTU IPv4 e **MTU IPv6**: Unidade Máxima de Transmissão para rotas IPv4/IPv6. Suportado no Android 13 e versões superiores.

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 de roaming desativados

Serviços de roaming de dados desativados.

8. Chamadas de saída desativadas

Se as chamadas de saída estão desativadas.

9. SMS desativado

Se o envio e recebimento de mensagens SMS está desativado.

10. Configuração de Fatiamento de Rede 5G

Configure as configurações de serviço de rede prioritário para habilitar o fatiamento de rede 5G corporativo. Você pode configurar até 5 fatias corporativas e atribuir aplicativos a redes específicas para roteamento de tráfego otimizado.

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. Deve haver 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 dessa configuração padrão.

10.2. Configurações dos serviços de rede

Use **Adicionar Configuração de Rede** para criar uma configuração de slice. Você pode adicionar até 5 configurações. Cada configuração possui:

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

Utilizar conexão padrão: Define se a conexão padrão do dispositivo deve ser utilizada. Se desativado, os aplicativos não poderão acessar a internet caso a rede 5G não esteja disponível.

Redes Incompatíveis: Define se os aplicativos sujeitos a esta configuração podem usar redes diferentes da rede preferencial. Se definido como **Não Permitido**, a opção **Alternar para Conexão Padrão** também deve estar **Não Permitido**. Requer Android 14 ou superior.

Rede

Nesta seção, você pode configurar políticas relacionadas à rede.

> As configurações de Wi-Fi podem ser provisionadas e gerenciadas pelo sistema através de **Configurações de Wi-Fi**. Dependendo do valor definido em **Configurar Wi-Fi**, os usuários podem ter controle limitado ou nenhum controle sobre a adição/modificação de redes.

Estado da rede sem fio 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 ou desativar o Wi-Fi.

Ativado: O Wi-Fi está ligado e o usuário não tem permissão para desativá-lo (Android 13 e versões mais recentes).

Desativado: O Wi-Fi está desligado e o usuário não tem permissão para ativá-lo (Android 13 e versões mais recentes).

2. Nível mínimo de segurança do Wi-Fi

O nível mínimo de segurança de redes Wi-Fi que o dispositivo pode se conectar. Suportado no Android 13 e versões superiores, 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: Desativa redes Wi-Fi abertas; requer, no mínimo, segurança pessoal (por exemplo, WPA2-PSK).

Rede corporativa: Requer redes EAP corporativas; desabilita redes Wi-Fi com níveis de segurança inferiores a este.

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

3. Estado do Ultra Banda Larga (UWB)

Controla o estado da configuração de Ultra Banda Larga e se o usuário pode ativá-la ou desativá-la.

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

Desativado: UWB está desativado e o usuário não pode ativá-lo ou desativá-lo através das configurações (Android 14 ou superior).

Gerenciamento da conectividade do dispositivo

4. Compartilhamento via Bluetooth

Controla se o compartilhamento via Bluetooth está permitido.

Permitido: Compartilhamento via Bluetooth está permitido (padrão em dispositivos totalmente gerenciados, Android 8+).

Não permitido: Compartilhamento via Bluetooth não é permitido (padrão em perfis de trabalho, Android 8+).

5. Configurar Wi?Fi

Controle as permissões 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 a configuração do Wi-Fi (padrão): O usuário pode configurar o Wi-Fi.

Não permitir a adição de configurações de Wi-Fi: A adição de novas configurações de Wi-Fi não é permitida. O usuário pode alternar entre as redes já configuradas (Android 13 ou superior; perfis de trabalho gerenciados e de propriedade da empresa).

Não permitir a configuração de Wi-Fi: Impede a configuração de redes Wi-Fi. Em dispositivos totalmente gerenciados, essa opção remove as redes configuradas pelo usuário e mantém apenas as redes configuradas por meio das **configurações de Wi-Fi**. Em perfis de trabalho de dispositivos da empresa, as redes existentes não são afetadas, mas os usuários não podem adicionar, remover ou modificar redes Wi-Fi.

> Quando a configuração de Wi-Fi está desabilitada e o dispositivo não consegue se conectar durante a inicialização, o sistema pode exibir a **opção de conexão emergencial** para permitir que o usuário se conecte temporariamente e atualize as configurações.

6. Configurações de Wi?Fi Direct

Controles para configurar e usar as configurações de Wi-Fi Direct. Compatível com dispositivos corporativos que executam o Android 13 ou superior.

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

Não permitir: O usuário não tem permissão para usar o Wi-Fi Direct.

7. Configurações de compartilhamento de conexão

Controla as configurações de compartilhamento de conexão. Com base no valor definido, o usuário pode ser impedido, parcialmente ou totalmente, de usar diferentes métodos de compartilhamento de conexão.

Permitir todos os tipos de compartilhamento de conexão (padrão): Permite a configuração e o uso de todas as formas de compartilhamento de conexão.

Desativar compartilhamento de conexão Wi-Fi: Impede que o usuário utilize o compartilhamento de conexão Wi-Fi (dispositivos Android 13 ou superior pertencentes à empresa).

Desabilitar todos os tipos de compartilhamento de conexão: Impede todos os tipos de compartilhamento de conexão (dispositivos totalmente gerenciados e perfis de trabalho corporativos pertencentes à empresa).

8. Política de SSID de Wi-Fi

Restrições sobre quais SSIDs Wi-Fi o dispositivo pode se conectar (isso não afeta quais redes podem ser configuradas no dispositivo). Suportado em dispositivos de propriedade da empresa com Android 13 ou superior.

Lista de bloqueio de SSIDs (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 permissão de SSIDs: O dispositivo só pode se conectar aos SSIDs listados. A lista de SSIDs não pode estar vazia.

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

Na interface de edição de políticas, a lista de SSIDs é identificada como **SSIDs Wi-Fi permitidos** para listas de permissão e **SSIDs Wi-Fi bloqueados** para listas de bloqueio.

9. Configurações de roaming Wi?Fi

Configure o modo de roaming Wi-Fi para cada 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 Wi-Fi**: Padrão / Desativado / Agressivo. As opções Desativado e Agressivo requerem Android 15 ou superior e são suportadas apenas em dispositivos totalmente gerenciados e perfis de trabalho em dispositivos pertencentes à empresa.

Restrições de rede

10. Bluetooth desativado

Bluetooth está desativado.

Compartilhamento de contatos via Bluetooth desativado

Compartilhamento de contatos via Bluetooth está desativado.

12. Configuração do Bluetooth desativada

A configuração do Bluetooth está desativada.

13. Redefinição de rede desativada

Se a redefinição das configurações de rede está desativada.

14. Transmissão de dados desativada

Se o uso de NFC para transferir dados entre aplicativos está desativado.

VPN

15. Aplicativo VPN de conexão sempre ativa

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

> Observação: Este recurso requer a instalação de um cliente VPN que suporte tanto o recurso "Always On" quanto o recurso de VPN por aplicativo.

16. Bloqueio por VPN

Impede o acesso à rede quando a VPN não estiver conectada.

17. Configuração de VPN desativada

A configuração de VPN está desativada.

Serviços de proxy e de rede

18. Serviço de rede preferencial

Controla se o serviço de rede preferencial está habilitado no perfil de trabalho. Por exemplo, uma organização pode ter um acordo com uma operadora que os dados de trabalho sejam enviados através de um serviço de rede dedicado para uso empresarial (por exemplo, uma fatia empresarial 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 habilitado no perfil de trabalho.

> Se você utiliza fatiamento de rede corporativo, também configure **Configuração de Fatiamento de Rede 5G** no painel de política **Celular** e atribua aplicativos a um slice usando sua configuração de **Rede Preferencial**.

19. Proxy global recomendado

Proxy HTTP global independente da rede. Normalmente, os proxies devem ser configurados para cada rede nas configurações de Wi-Fi. 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

Proxy de configuração automática (PAC)

19.1. Host

O servidor que hospeda o 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, especifique os hosts para os quais o proxy será ignorado. Os nomes dos hosts podem conter caracteres curinga, como ***.example.com**.

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

Configurações de Wi-Fi

Defina as 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.

Conectar automaticamente: Define se a rede deve ser conectada automaticamente quando estiver ao alcance.

Transição Rápida: Define se o dispositivo deve tentar usar a Transição Rápida (IEEE 802.11r-2008) com a rede.

SSID Oculto: Indica se o SSID será transmitido.

Modo de aleatorização do MAC: Hardware ou Automático (Android 13 ou superior).

20.1. Segurança

Opções de segurança Wi-Fi:

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

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

WPA-EAP: WPA/WPA2/WPA3-Enterprise (Protocolo de Autenticação Extensível).

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

20.2. Frase secreta (chave pré-compartilhada)

Aparece quando a segurança é **WEP-PSK** ou **WPA-PSK**. A frase secreta é necessária.

20.3. Método EAP (Enterprise)

Aparece quando a segurança é **WPA-EAP** ou **WPA3 em modo de 192 bits**. Selecione um método EAP externo:

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Etapa 2 de autenticação

Mostrado para túneis de métodos externos (**EAP-TTLS** e **PEAP**).

MSCHAPv2

PAP

20.5. Credenciais EAP dos usuários

Quando ativado, o sistema aplica automaticamente as credenciais EAP nos dispositivos, individualmente para cada usuário. Você pode configurar as credenciais dos usuários 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 de **Gerenciamento de certificados**.

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

Alternativamente, você pode especificar **o alias do par de chaves do certificado do cliente**, que faz referência a um certificado de cliente armazenado no armazenamento de chaves do Android e permite a autenticação Wi-Fi.

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

20.7. Identidade

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

20.8. Identidade anônima

Para protocolos de tunelamento, isso indica a identidade do usuário apresentada ao protocolo externo.

20.9. Senha

Senha do usuário. Se não for especificada, o sistema solicitará a senha ao usuário.

20/10. Certificados CA do servidor

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

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

20.11. O sufixo do domínio corresponde

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 do certificado do servidor de autenticação.

Sistema

Nesta seção, você pode configurar políticas relacionadas ao sistema.

1. Versão mínima da API

A versão mínima permitida da API do Android.

2. Política de criptografia

Se a criptografia está habilitada.

> **Padrão**: Este valor é ignorado, ou seja, nenhuma criptografia é necessária.
>
> **Ativado sem senha**: Criptografia habilitada, mas não é necessária uma senha para inicializar o dispositivo.
>
> **Ativado com senha**: Criptografia exigida, com senha necessária para inicializar o dispositivo.

3. Data e hora automáticos

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

> **Escolha do usuário (padrão)**: A configuração de data, hora e fuso horário automático é definida pela escolha do usuário.
>
> **Obrigatório:** Forçar a configuração automática de data, hora e fuso horário no dispositivo.

4. Configurações para desenvolvedores

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

> **Desativado (padrão)**: Desativa todas as configurações de desenvolvedor e impede que o usuário acesse-as.

Permitido: Permite todas as configurações de desenvolvedor. O usuário pode acessar e, opcionalmente, configurar as configurações.

5. Modo de Conformidade com os Critérios Comuns

Modo de Critérios Comuns — padrões de segurança definidos nos Critérios Comuns para Avaliação de Segurança de Tecnologia da Informação (CC). Ativar o Modo de Critérios Comuns aumenta certos componentes de segurança em um dispositivo (por exemplo: criptografia AES-GCM de chaves de longo prazo Bluetooth, validação adicional para alguns certificados de rede e verificações de integridade de políticas criptográficas). O Modo de Critérios Comuns é suportado apenas em dispositivos de propriedade da empresa com Android 11 ou superior. Aviso: o Modo de Critérios Comuns impõe um modelo de segurança rigoroso, normalmente necessário apenas para organizações altamente sensíveis. O uso normal do dispositivo pode ser afetado; ative-o apenas se necessário.

Desativado (padrão): Desativa o Modo de Critérios Comuns.

Ativado: Habilita o Modo de Critérios Comuns.

6. Extensão de Marcação de Memória (MTE)

Controla a Extensão de Marcação de Memória (MTE) no dispositivo.

Escolha do usuário (padrão): O usuário pode optar por ativar ou desativar o MTE no dispositivo (se suportado pelo dispositivo).

Obrigatório: O MTE está ativado e o usuário não pode alterá-lo (Android 14 ou superior; disponível em dispositivos totalmente gerenciados e perfis de trabalho em dispositivos corporativos).

Desativado: O MTE está desativado e o usuário não pode alterá-lo (Android 14 ou superior; disponível apenas em dispositivos totalmente gerenciados).

7. Proteção de conteúdo

Controla se a proteção de conteúdo (que verifica a presença de aplicativos maliciosos) está ativada. Compatível com Android 15 e versões superiores.

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

Aplicada (padrão): A proteção de conteúdo está ativada e o usuário não pode alterar isso (Android 15 ou superior).

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

8. Assistir conteúdo

Controla se o AssistContent pode ser enviado para um aplicativo privilegiado, como um aplicativo assistente (por exemplo, Circle to Search). O AssistContent inclui capturas de tela e informações sobre um aplicativo, como o nome do pacote. Isso é suportado no Android 15 e versões superiores.

Permitido (padrão): O envio de conteúdo de assistência para um aplicativo privilegiado é permitido (Android 15 ou superior).

Não permitido: O envio de conteúdo de assistência para um aplicativo privilegiado é bloqueado (Android 15 ou superior).

9. Criar janelas desabilitadas

Se a criação de janelas além das janelas do aplicativo está desabilitada. Esta opção impede a exibição das seguintes interfaces do sistema: notificações e barras de aviso, atividades do telefone (como chamadas recebidas) e atividades de telefone prioritárias (como chamadas em andamento), alertas do sistema, erros do sistema e sobreposições do sistema.

10. Saída de emergência da rede

Se a opção de "saída de emergência da rede" está habilitada. Se uma conexão de rede não puder ser estabelecida durante a inicialização, a saída de emergência solicita que o usuário se conecte temporariamente a uma rede para atualizar as configurações do dispositivo. Após a aplicação das configurações, a conexão temporária será removida e o dispositivo continuará a inicialização. Isso evita que o usuário fique sem conexão se não houver uma rede adequada nas configurações e o dispositivo iniciar em um aplicativo no modo de tarefa bloqueada, ou se o usuário não conseguir acessar as configurações do dispositivo.

11. Atividades padrão

Uma lista de atividades padrão para lidar com intenções que correspondem a um filtro de intenção específico. Por exemplo, esse recurso permitiria que os administradores de TI escolhessem qual aplicativo de navegador abre automaticamente links da web ou qual aplicativo de inicializador é

usado ao tocar no botão de início.

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

11.1. Atividade do receptor

A atividade que deve ser o manipulador de intenção padrão. Este deve ser o nome de um componente Android, por exemplo, com.android.enterprise.app/.MainActivity. Alternativamente, o valor pode ser o nome do pacote de um aplicativo, o que faz com que o Android Device Policy escolha uma atividade apropriada do aplicativo para manipular a intenção.

11.2. Ação

As ações de intenção a serem consideradas no filtro. Se alguma ação estiver incluída no filtro, a ação da intenção deve ser um desses valores para que corresponda. Se nenhuma ação estiver incluída, a ação da intenção é ignorada.

11.3. Categoria

As categorias de intenção a serem utilizadas no filtro. Uma intenção inclui as categorias que ela exige, e todas devem estar incluídas no filtro para que haja correspondência. Em outras palavras, adicionar uma categoria ao filtro não tem efeito na correspondência, a menos que essa categoria seja especificada na intenção.

12. Métodos de entrada permitidos

Especifica os métodos de entrada permitidos.

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

12.1. Métodos de entrada permitidos

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

Use **Adicionar método de entrada** para adicionar itens e removê-los com a ação de exclusão.

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 nativos do sistema podem ser utilizados.
>
> **Apenas os serviços**: Apenas os serviços de acessibilidade fornecidos e os serviços nativos do sistema podem ser utilizados.

13.1. Serviços de acessibilidade permitidos

Serviços de acessibilidade permitidos. Aplica-se apenas quando **Serviços de acessibilidade permitidos** está definido como **Apenas os serviços do sistema e os 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**: Utilize o comportamento padrão de atualização do dispositivo, que geralmente exige que o usuário aceite as atualizações do sistema.
>
> **Automático**: Instale automaticamente assim que uma atualização estiver disponível.
>
> **Modo Janela**: Instale automaticamente dentro de uma janela de manutenção diária. Isso também configura os aplicativos do Play para serem atualizados dentro dessa janela. É altamente recomendado para dispositivos em modo kiosk, pois esta é a única maneira de atualizar aplicativos que estão fixados permanentemente em primeiro plano através do Play.
>
> **Adiar**: Adie a instalação automática por um período máximo de 30 dias.

14.1. Janela de manutenção (Apenas janela)

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

14.2. Períodos de suspensão de atualização do sistema

Um período anual em que as atualizações do sistema via OTA (Over-The-Air) são suspensas para fixar a versão do sistema operacional executada em um dispositivo. Para evitar que o dispositivo fique bloqueado indefinidamente, cada período de bloqueio deve ser separado por pelo menos 60 dias. Cada período de bloqueio não deve exceder 90 dias.

Use **Definir período de bloqueio de atualização do sistema** para criar entradas.

15. Provedores de credenciais padrão

Controla quais aplicativos podem atuar como provedores de credenciais no Android 14 e versões superiores.

> **Não permitidos (padrão)**: Aplicativos com a política credentialProviderPolicy não especificada não são permitidos a atuar como um provedor de credenciais.
>
> **Não permitidos (exceto para o sistema)**: Aplicativos com a política credentialProviderPolicy não especificada não são permitidos a atuar como um provedor de credenciais, exceto para os provedores de credenciais padrão do fabricante (OEM).

Localização e cerca geográfica

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

Relatório de localização

Reportar localização

Habilita o relatório de geolocalização do dispositivo. Os dados de localização coletados por meio desta configuração são usados pelo **mapa de localização do painel**, o histórico de localização da visão geral do dispositivo e o processamento de cercas virtuais.

> Em dispositivos não totalmente gerenciados, os dados de localização podem depender da permissão de localização necessária para o app Cerberus Enterprise e da ativação dos serviços de localização no dispositivo.

Modo de localização

Controla a configuração de localização do dispositivo em dispositivos de propriedade da empresa.

- **Escolha do usuário**: os serviços de localização não são restritos pela política.
- **Aplicada**: os serviços de localização estão habilitados no dispositivo.
- **Desativado**: os serviços de localização estão desabilitados 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 para todo o dispositivo e sobrescreve o modo de localização do dispositivo.

Comportamento automático com cercas geográficas ativas

Cercas geográficas ativas exigem o envio de localização para funcionar. Quando pelo menos uma cerca geográfica estiver ativa, o Cerberus Enterprise mantém automaticamente as configurações de localização relacionadas consistentes.

- **O envio de localização** é forçado ao estar ativo quando cercas geográficas existirem.
- **Modo de localização** é forçado para **Ativado**.
- **Compartilhamento de localização desativado** está forçado a desligado.

Se você tentar desativar **Relatar localização** enquanto um ou mais cercas geográficas estiverem ativas, o Cerberus Enterprise exibe 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**. Nomes de cercas geográficas devem ser únicos dentro da política.

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

- **Nome**: obrigatório e único.
- **Latitude** e **Longitude**: o centro da área.
- **Raio (m)**: obrigatório, de **100** a **10000** metros.
- **Descrição**: notas opcionais para administradores.
- **Relatório de entrada** e **Relatório de saída**: escolha quais eventos de transição devem ser gerados.
- **Ativo**: habilita ou desabilita a cerca geográfica sem excluí-la.

> Pelo menos um de **Report entrar** ou **Report sair** deve permanecer ativado para cada cerca geográfica.

Ferramentas de edição de mapa

Cada cartão de cerca geográfica inclui uma visualização do mapa da área. Você pode editar a geometria a partir do mapa ou dos campos numéricos.

- Clique no mapa para mover o centro da cerca geográfica quando a edição de área estiver desbloqueada.
- Use the **Localização atual** button to center the map on your current browser position.
- Use the **Recentrar mapa** button to restore the preferred viewport for that geofence.

- Use o botão de bloqueio para evitar alterações acidentais na geometria da cerca geográfica.

Onde os dados da cerca geográfica aparecem

As transições de cercas virtuais podem ser revisadas na página **Visão geral do dispositivo**, dentro da aba **Cercas virtuais** do painel de localização. Essa aba exibe as transições em um mapa dedicado, juntamente com ferramentas de filtragem e a lista de transições.

Gerenciamento de usuários

Adicionar usuário desativado

A opção de adicionar novos usuários e perfis está desativada. Para dispositivos onde o modo de gerenciamento é **DEVICE_OWNER**, este campo é ignorado e o usuário nunca poderá adicionar ou remover usuários.

Modificar contas desativadas

Se a adição ou remoção de contas está desativada.

Configurações de credenciais do usuário desativadas

Se a configuração de credenciais do usuário está desativada.

Remover usuário desativado

Se a remoção de outros usuários está desativada.

Definir ícone de usuário como desativado

Se a opção de alterar o ícone do usuário está desativada.

Definir papel de parede desabilitado

Se a alteração do papel de parede está desabilitada.

Configuração de autenticação da conta de trabalho

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

Durante a configuração/inscrição do dispositivo, esta política influencia se é necessário fazer login na conta de trabalho, mas a configuração do Console de administração do Google **"Autenticar com o Google"** e o tipo de token de inscrição ainda podem exigir autenticação.

Para dispositivos já inscritos, esta política se aplica somente se o dispositivo for gerenciado por uma conta do Google Play corporativa (ou seja, inscrito sem **autenticação via Google**).

Para mais detalhes e solução de problemas, consulte **Autenticação via Google**.

Tipos de conta bloqueados

Tipos de conta que o usuário não pode gerenciar. 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 possui um campo de **Tipo de conta** (obrigatório). Insira uma string como, por exemplo, **com.google**. Remova uma entrada usando a ação de excluir.

Uso pessoal

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

> Esta seção se aplica apenas a dispositivos de propriedade da empresa que possuem um perfil de trabalho. Ela não terá efeito em dispositivos totalmente gerenciados ou em dispositivos de propriedade pessoal.

1. Câmera desativada

Câmera está desativada.

2. Captura de tela desativada

Se a captura de tela está desabilitada.

3. Máximo de dias de folga

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

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 aplicativos são permitidos ou bloqueados para o usuário na Play Store do perfil pessoal.

Lista de bloqueio (padrão): Todos os aplicativos estão disponíveis e qualquer aplicativo que não deve estar no dispositivo deve ser explicitamente marcado como **Bloqueado** na seção **Aplicativos**.

Lista de permissões: Apenas aplicativos explicitamente especificados na seção **Aplicativos** com o 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 Google Play Store**.

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

7.1. Tipo de instalação

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

Bloqueado: O aplicativo está bloqueado e não pode ser instalado no perfil pessoal.

Disponível: O aplicativo está disponível para instalação no perfil pessoal.

8. Tipos de conta bloqueados

Tipos de conta que o usuário não pode gerenciar. Essa opção impede que os usuários do dispositivo adicionem contas não aprovadas em seu perfil pessoal.

Políticas entre perfis

Aplica-se apenas a dispositivos com perfis pessoais e corporativos.

Cópia e colagem entre perfis

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

> **Não permitido (padrão)**: Impede que os usuários colem texto no perfil pessoal, que foi copiado do perfil profissional. O texto copiado do perfil pessoal pode ser colado no perfil profissional.
>
> **Permitido**: O texto copiado em qualquer um dos perfis pode ser colado no outro perfil.

Compartilhamento de dados entre perfis

Define se os dados de um perfil (pessoal ou profissional) podem ser compartilhados com aplicativos no outro perfil. Isso controla especificamente o compartilhamento simples de dados via intents. O gerenciamento de outros canais de comunicação entre perfis, como pesquisa de contatos, copiar/colar,
ou aplicativos de trabalho e pessoais conectados, são configurados separadamente.

> **Não permitido**: Impede o compartilhamento de dados entre o perfil pessoal e o perfil profissional, e vice-versa.
>
> **Compartilhamento de dados do perfil de trabalho para o perfil 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**: Dados de qualquer perfil podem ser compartilhados com o outro perfil.

Widgets do perfil de trabalho padrão

Comportamento padrão para 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 diferentes perfis

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

> Esta configuração depende da opção de nível de política "**Funções do aplicativo**") (na seção de gerenciamento de aplicativos). Se "Funções do aplicativo" estiver definido como "**Não permitido**", a API rejeitará as 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 do perfil pessoal e em chamadas recebidas.

> **Permitido (padrão)**: Permite que os contatos do perfil de trabalho apareçam no perfil pessoal.
>
> **Não Permitido**: Impede que aplicativos pessoais acessem contatos do perfil de trabalho e procurem contatos corporativos.
>
> **Não Permitido, exceto para aplicativos do sistema**: Impede que a maioria dos aplicativos pessoais acesse os contatos do perfil de trabalho, exceto para os aplicativos padrão do fabricante (OEM) como Discador, Mensagens e Contatos (Android 14 e versões mais recentes).

Quando os contatos do trabalho no perfil pessoal estão configurados, você pode definir opcionalmente uma lista de entradas de **nomes de pacotes isentos**. Dependendo do modo selecionado, essas isenções funcionam como uma lista de permissões ou uma lista de bloqueio para aplicativos pessoais.

Relatórios de status

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

Relatórios de aplicativos

Se os relatórios de aplicativos estão habilitados. (Informações reportadas sobre um aplicativo instalado.)

> Esta opção é obrigatória pelo sistema (para integração com aplicativos complementares) e está sempre habilitada; não é possível desabilitá-la.

Incluir aplicativos removidos

Se os aplicativos removidos são incluídos nos relatórios de aplicativos.

Configurações do dispositivo

Se o relatório de configurações do dispositivo está habilitado. (Informações sobre as configurações de segurança do dispositivo.)

Informações do software

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

Informações de memória

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

Informações da rede

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

Exibir informações

Exibição de informações do dispositivo. Os dados de relatório não estão disponíveis para dispositivos pessoais com perfis de trabalho

Eventos de gerenciamento de energia

Se o relatório de eventos de gerenciamento de energia está habilitado. Os dados de relatório não estão disponíveis para dispositivos pessoais com perfis de trabalho.

Status do hardware

Se o relatório de status do hardware está habilitado. Os dados de relatório não estão disponíveis para dispositivos pessoais com perfis de trabalho.

Propriedades do sistema

Se o relatório de propriedades do sistema está habilitado.

Modo de Conformidade com os Critérios Comuns

Se a geração de relatórios no modo de Conformidade com os Critérios Comuns está habilitada.

Diversos

1. Jogo de "Easter egg" desativado

Se o jogo de "Easter egg" nas configurações está desativado.

2. Pular dicas de primeira utilização

Marcar para ignorar as dicas na primeira utilização. Administradores de empresas podem ativar a recomendação do sistema para que os aplicativos ignorem seus tutoriais e outras dicas introdutórias na primeira inicialização.

3. Mensagem de suporte resumida

Mensagem exibida para o usuário na tela de configurações, indicando que uma funcionalidade foi desativada pelo administrador. Se a mensagem tiver mais de 200 caracteres, ela poderá ser truncada.

4. Mensagem de suporte detalhada

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

5. Informações da tela de bloqueio do proprietário

Informações do proprietário do dispositivo a serem exibidas na tela de bloqueio.

6. Ações de configuração

Ações a serem realizadas durante a configuração. Durante a inscrição, você pode exigir que o usuário abra um ou mais aplicativos necessários para a configuração do dispositivo.

Utilize a ação "**Adicionar 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

Exibe uma mensagem para o usuário, explicando por que o aplicativo precisa ser iniciado.

6.3. Descrição

Exibe uma mensagem para o usuário, explicando por que o aplicativo precisa ser iniciado.

7. Visibilidade do nome de exibição para empresas

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

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

Oculto: O nome de exibição da empresa não é visível no dispositivo.

Regras de aplicação de políticas

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

- **Requisitos de senha**
- **Política de criptografia**
- **Tela de bloqueio desativada**
- **Métodos de entrada permitidos**
- **Serviços de acessibilidade permitidos**

Se o dispositivo ou perfil de trabalho permanecerem não conformes após 10 dias, a Política de Dispositivo Android redefinirá o dispositivo para as configurações de fábrica ou excluirá o perfil de trabalho.

Nesta seção, você pode substituir as regras de aplicação de conformidade padrão 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 bloco de regra pode ser removido usando a ação de exclusão.

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 suportado; caso contrário, o campo será marcado como inválido.

Bloquear após X dias

Número de dias em que a política não está em conformidade antes que o dispositivo ou perfil de trabalho seja bloqueado. Para bloquear o acesso imediatamente, defina como 0. **Bloquear após X dias** deve ser menor que **Apagar após X dias**. Aplicável apenas a dispositivos de propriedade da empresa.

Intervalo permitido: 0–300.

Escopo de bloco

Define o escopo da ação do bloco. Aplicável apenas a dispositivos de propriedade da empresa.

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

> **Perfil de trabalho**: A ação de bloqueio é aplicada apenas aos aplicativos no perfil de trabalho. Os aplicativos no perfil pessoal não são afetados.
>
> **Dispositivo inteiro**: A ação de bloqueio é aplicada a todo o dispositivo, incluindo os aplicativos no perfil pessoal.

Apagar após dias

Número de dias em que a política está em não conformidade antes que o dispositivo ou o perfil de trabalho sejam apagados.
Apagar após dias deve ser maior que **Bloquear após dias**. Aplicável apenas a dispositivos de propriedade da empresa.

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

Intervalo permitido: 1–300.

Mantenha a proteção de fábrica

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

Padrão (nova regra): ativado.