# 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.

---

Revision #57
Created 2025-12-17 09:34:36 UTC by Admin
Updated 2026-11-12 09:57:00 UTC by Admin