# Sistema

Nesta seção, você pode configurar políticas relacionadas ao sistema.

## 1. Nível de API mínimo

O nível de API do Android mínimo permitido.

## 2. Política de criptografia

Se a criptografia está ativada.

> **Padrão**: Este valor é ignorado, ou seja, nenhuma criptografia é exigida.
>
> **Ativado sem senha**: A criptografia é exigida, mas não é necessária uma senha para a inicialização.
>
> **Ativado com senha**: A criptografia é exigida, com senha necessária para a inicialização.

## 3. Data e hora automáticas

Se a data, hora e fuso horário automáticos estão ativados em um dispositivo de propriedade da empresa.

> **Escolha do usuário (padrão)**: A data, hora e fuso horário automáticos ficam a critério do usuário.
>
> **Imposto**: Força a configuração de 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 essas opções.

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

## 5. Modo Common Criteria

Controla o Modo Common Criteria — padrões de segurança definidos no Common Criteria for Information Technology Security Evaluation (CC). A ativação do Modo Common Criteria aumenta certos componentes de segurança no dispositivo (por exemplo: criptografia AES-GCM de chaves de longo prazo do Bluetooth, validação adicional para alguns certificados de rede e verificações de integridade da política criptográfica). O Modo Common Criteria é suportado apenas em dispositivos de propriedade da empresa com Android 11 ou superior. Aviso: O Modo Common Criteria impõe um modelo de segurança rigoroso, normalmente exigido apenas para organizações altamente sensíveis. O uso padrão do dispositivo pode ser afetado; ative-o apenas se for necessário.

**Desativado (padrão)**: Desativa o Modo Common Criteria.

**Ativado**: Ativa o Modo Common Criteria.

## 6. Memory Tagging Extension (MTE)

Controla a Memory Tagging Extension (MTE) no dispositivo.

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

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

**Desativado**: O MTE é desativado e o usuário não tem permissão para alterá-lo (Android 14+; suportado apenas em dispositivos totalmente gerenciados).

## 7. Proteção de conteúdo

Controla se a proteção de conteúdo (que verifica aplicativos enganosos) está ativada. Isso é suportado no Android 15 ou 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 de assistência

Controla se o AssistContent pode ser enviado para um aplicativo privilegiado, como um aplicativo de assistência (por exemplo, o 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 ou superior.

**Permitido (padrão)**: O conteúdo de assistência pode ser enviado para um aplicativo privilegiado (Android 15+).

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

## 9. Desativação de janelas de criação

Se a criação de janelas além das janelas de aplicativos está desativada. Esta opção impede a exibição das seguintes interfaces do sistema: toasts e snackbars, atividades de 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 de rede

Se a saída de emergência de rede está ativada. Se uma conexão de rede não puder ser estabelecida no momento da inicialização, a saída de emergência solicitará 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 que o usuário fique impossibilitado de se conectar a uma rede caso não haja uma rede adequada na última política aplicada e o dispositivo inicie diretamente em um aplicativo no modo de tarefa bloqueada (lock task mode), ou se o usuário estiver impossibilitado de acessar as configurações do dispositivo por outros motivos.

# 11. Atividades padrão

Uma lista de atividades padrão para lidar com intents que correspondam a um filtro de intent específico. Por exemplo, este recurso permitiria aos administradores de TI escolher qual aplicativo de navegador abre links da web automaticamente ou qual aplicativo de inicialização (launcher) 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 intent.

## 11.1. Atividade de receptor

A atividade que deve ser o manipulador de intent padrão. Deve ser um nome de 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 a Política de Dispositivo Android escolha uma atividade apropriada do aplicativo para lidar com a intent.

## 11.2. Ação

As ações de intent para correspondência no filtro. Se houver ações incluídas no filtro, a ação da intent deve ser um desses valores para que ocorra a correspondência. Se nenhuma ação for incluída, a ação da intent será ignorada.

## 11.3. Categoria

As categorias de intent para correspondência no filtro. Uma intent inclui as categorias que ela exige, e todas elas devem estar incluídas no filtro para que ocorra a correspondência. Em outras palavras, adicionar uma categoria ao filtro não tem impacto na correspondência, a menos que essa categoria seja especificada na 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 pacotes de métodos de entrada que são permitidos. Aplica-se apenas quando **Métodos de entrada permitidos** estiver definido como **Apenas do sistema e fornecidos**.

Use **Adicionar método de entrada** para adicionar entradas e remova-as 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** estiver definido como **Apenas do sistema e fornecidos**.

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

# 14. Política de atualização do sistema

Configuração para o gerenciamento de atualizações do sistema.

> **Padrão**: Segue o comportamento de atualização padrão do dispositivo, que normalmente exige que o usuário aceite as atualizações do sistema.
>
> **Automático**: Instala automaticamente assim que uma atualização estiver disponível.
>
> **Janela de manutenção**: Instala automaticamente dentro de uma janela de manutenção diária. Isso também configura os aplicativos do Play para serem atualizados dentro da janela. Isso é altamente recomendado para dispositivos de quiosque, pois é a única maneira de atualizar aplicativos fixados permanentemente em primeiro plano pelo Play.
>
> **Adiar**: Adia a instalação automática por até um máximo de 30 dias.

## 14.1. Janela de manutenção (Apenas para o modo Janela)

Quando a **Política de atualização do sistema** estiver definida como **Janela de manutenção**, você poderá definir a janela de manutenção diária usando os campos **de** e **até**.

## 14.2. Períodos de congelamento de atualização do sistema

Um período de tempo que se repete anualmente, no qual as atualizações do sistema via rede (OTA) são adiadas para congelar a versão do SO em execução no 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 deve exceder 90 dias.

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

# 15. Provedores de credenciais padrão

Controla quais aplicativos têm permissão para atuar como provedores de credenciais no Android 14 ou superior.

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

---

Revision #49
Created 2025-12-17 09:34:36 UTC by Admin
Updated 2026-07-07 10:56:59 UTC by Admin