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).

Revision #36
Created 2025-12-17 09:34:36 UTC by Admin
Updated 2026-04-22 15:52:42 UTC by Admin