

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.

Revision #36

Created 2025-12-17 09:34:38 UTC by Admin

Updated 2026-04-22 15:52:47 UTC by Admin