Rede

Nesta seção, você pode configurar políticas relacionadas à rede.

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

Estado do rádio do dispositivo

1. Estado do Wi-Fi

Controla o estado atual do Wi-Fi e se o usuário pode alterar seu estado.

Escolha do usuário (padrão): O usuário tem permissão para ativar/desativar o Wi-Fi.

Ativado: O Wi-Fi está ligado e o usuário não tem permissão para desligá-lo (Android 13+).

Desativado: O Wi-Fi está desligado e o usuário não tem permissão para ligá-lo (Android 13+).

2. Nível mínimo de segurança do Wi-Fi

O nível mínimo de segurança exigido para redes Wi-Fi às quais o dispositivo pode se conectar. Suportado no Android 13 ou superior, para dispositivos totalmente gerenciados e perfis de trabalho em dispositivos de propriedade da empresa.

Rede aberta (padrão): O dispositivo pode se conectar a todos os tipos de redes Wi-Fi.

Rede pessoal: Não permite redes Wi-Fi abertas; exige pelo menos segurança pessoal (por exemplo, WPA2-PSK).

Rede corporativa: Exige redes EAP corporativas; não permite redes Wi-Fi abaixo deste nível de segurança.

Rede corporativa de 192 bits: Exige redes corporativas de 192 bits; opção mais rigorosa.

3. Estado de banda ultralarga (UWB)

Controla o estado da configuração de banda ultralarga e se o usuário pode ativá-la ou desativá-la.

Escolha do usuário (padrão): O usuário tem permissão para ativar ou desativar o UWB.

Desativado: O UWB está desativado e o usuário não tem permissão para ativá-lo via configurações (Android 14+).

Gerenciamento de conectividade do dispositivo

4. Compartilhamento via Bluetooth

Controla se o compartilhamento via Bluetooth é permitido.

Permitido: O compartilhamento via Bluetooth é permitido (padrão em dispositivos totalmente gerenciados, Android 8+).

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

5. Configurar Wi-Fi

Controla os privilégios de configuração do Wi-Fi. Dependendo da opção selecionada, o usuário terá controle total, limitado ou nenhum sobre a configuração de redes Wi-Fi.

Permitir configuração de Wi-Fi (padrão): O usuário tem permissão para configurar o Wi-Fi.

Não permitir adição de configuração de Wi-Fi: A adição de novas configurações de Wi-Fi não é permitida. O usuário pode alternar entre redes já configuradas (Android 13+; dispositivos totalmente gerenciados e perfis de trabalho em dispositivos de propriedade da empresa).

Não permitir configuração de Wi-Fi: Não permite a configuração de redes Wi-Fi. Para dispositivos totalmente gerenciados, isso remove as redes configuradas pelo usuário e mantém apenas as redes configuradas via **configurações de Wi-Fi**. Para perfis de trabalho em dispositivos de propriedade da empresa, as redes existentes não são afetadas, mas os usuários não podem adicionar/remover/modificar redes Wi-Fi.

> Quando a configuração de Wi-Fi está desativada e o dispositivo não consegue se conectar no momento da inicialização, o sistema pode exibir a **válvula de escape de rede** para permitir que o usuário se conecte temporariamente e atualize a política.

6. Configurações de Wi-Fi Direct

Controla a configuração e o uso das definições de Wi-Fi Direct. Suportado em dispositivos de propriedade da empresa com Android 13 ou superior.

Permitir (padrão): O usuário tem permissão para usar o Wi-Fi Direct.

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

7. Configurações de roteamento (tethering)

Controla as configurações de roteamento (tethering). Dependendo do valor definido, o usuário pode ter o uso de diferentes formas de roteamento parcialmente ou totalmente proibido.

Permitir todo o roteamento (padrão): Permite a configuração e o uso de todas as formas de roteamento.

Não permitir roteamento via Wi-Fi: Impede que o usuário utilize o roteamento via Wi-Fi (Android 13+ de propriedade da empresa).

Não permitir todo o roteamento: Impede todas as formas de roteamento (dispositivos totalmente gerenciados + perfis de trabalho em dispositivos de propriedade da empresa).

8. Política de SSID do Wi-Fi

Restrições sobre a quais SSIDs de 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 SSID (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 SSID: O dispositivo pode se conectar apenas aos SSIDs listados. A lista de SSID não deve estar vazia.

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

Na interface do Editor de Políticas, a lista de SSID é rotulada como **SSIDs de Wi-Fi permitidos** para listas de permissão e **SSIDs de Wi-Fi negados** para listas de bloqueio.

9. Configurações de roaming de Wi-Fi

Configure o modo de roaming de Wi-Fi por SSID. Use **Adicionar configuração de roaming de Wi-Fi** para criar entradas.

Cada entrada inclui:

SSID: O SSID ao qual a configuração de roaming se aplica (obrigatório).

Modo de roaming de Wi-Fi: Padrão / Desativado / Agressivo. As opções Desativado e Agressivo exigem Android 15+ e são suportadas apenas em dispositivos totalmente gerenciados e perfis de trabalho em dispositivos de propriedade da empresa.

Restrições de rede

10. Bluetooth desativado

Se o Bluetooth está desativado. Prefira esta configuração em vez de "Configuração de Bluetooth desativada", pois a configuração de Bluetooth desativada pode ser contornada pelo usuário.

11. Compartilhamento de contatos via Bluetooth desativado

Se o compartilhamento de contatos via Bluetooth está desativado.

12. Configuração de Bluetooth desativada

Se a configuração de Bluetooth está desativada.

13. Redefinição de rede desativada

Se a redefinição das configurações de rede está desativada.

14. Beam de saída desativado

Se o uso de NFC para transmitir dados de aplicativos está desativado.

VPN

15. Aplicativo de VPN sempre ativa (Always On VPN)

Especifique o nome do pacote de um aplicativo de VPN sempre ativa para garantir que os dados dos aplicativos gerenciados especificados passem sempre por uma VPN configurada.

> Nota: Este recurso exige a implantação de um cliente VPN que suporte os recursos de "Sempre Ativa" (Always On) e de VPN por aplicativo.

16. Bloqueio de rede via VPN (VPN lockdown)

Impede o uso de rede quando a VPN não estiver conectada.

17. Configuração de VPN desativada

Se a configuração de VPN está desativada.

Proxy e serviços de rede

18. Serviço de rede preferencial

Controla se o serviço de rede preferencial está ativado no perfil de trabalho. Por exemplo, uma organização pode ter um acordo com uma operadora para que os dados de trabalho sejam enviados por meio de um serviço de rede da operadora dedicado ao uso corporativo (por exemplo, um slice corporativo 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 ativado no perfil de trabalho.

> Se você usa o fatiamento de rede corporativa (network slicing), configure também a **Configuração de fatiamento de rede 5G** no painel de política **Celular** e atribua os aplicativos a um slice usando a configuração de **Rede preferencial**.

19. Proxy global recomendado

O proxy HTTP global independente de rede. Normalmente, os proxies devem ser configurados por 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 autoconfiguração (PAC)

19.1. Host

O host do proxy direto.

19.2. Porta

A porta do proxy direto.

19.3. URI do PAC

A URI do script PAC usado para configurar o proxy.

19.4. Hosts excluídos

Para um proxy direto, os hosts pelos quais o proxy é ignorado. Os nomes de host 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: Se a rede deve ser conectada automaticamente quando estiver ao alcance.

Transição Rápida: Se o cliente deve tentar usar a Transição Rápida (IEEE 802.11r-2008) com a rede.

SSID oculto: Se o SSID será transmitido.

Modo de randomização de MAC: Hardware ou Automático (Android 13+).

20.1. Segurança

Opções de segurança de Wi-Fi:

WEP-PSK: WEP (Chave Pré-Compartilhada).

WPA-PSK: WPA/WPA2/WPA3-Personal (Chave Pré-Compartilhada).

WPA-EAP: WPA/WPA2/WPA3-Enterprise (Extensible Authentication Protocol).

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

20.2. Passphrase (Chave Pré-Compartilhada)

Exibido quando a Segurança é **WEP-PSK** ou **WPA-PSK**. A frase de passagem é obrigatória.

20.3. Método EAP (Enterprise)

Exibido quando a Segurança é **WPA-EAP** ou **Modo WPA3 de 192 bits**. Selecione um método EAP externo:

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Autenticação de fase 2

Exibido para métodos externos de tunelamento (**EAP-TTLS** e **PEAP**).

MSCHAPv2

PAP

20.5. Credenciais EAP dos usuários

Quando ativado, o sistema aplica automaticamente as credenciais EAP nos dispositivos com base em cada usuário. Você pode configurar as credenciais do usuário na seção **Usuários**.

20.6. Certificado do cliente

Para **EAP-TLS**, você pode atribuir um certificado de cliente usado para a autenticação Wi-Fi. Para mais informações, leia a página **Gerenciamento de certificados**.

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

Como alternativa, você pode especificar o **Alias do par de chaves do certificado do cliente**, que faz referência a um certificado de cliente armazenado no chaveiro do Android e permitido para autenticação Wi-Fi.

> Se tanto o **Certificado do cliente** quanto o **Alias do par de chaves do certificado do cliente** estiverem configurados, o alias do par de chaves será ignorado.

20.7. Identidade

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

20.8. Identidade anônima

Apenas 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 padrão será solicitar ao usuário.

20.10. Certificados CA do servidor

Lista de certificados CA a serem usados para verificar a cadeia de certificados do host. 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 remova-as com a ação de excluir.

20.11. Correspondências de sufixo de domínio

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 assunto de um certificado de servidor de autenticação.

Revision #49
Created 2025-12-17 09:34:38 UTC by Admin
Updated 2026-07-07 10:57:03 UTC by Admin