Redes

En esta sección, puedes configurar políticas relacionadas con las redes.

> El sistema puede aprovisionar y gestionar las configuraciones de Wi-Fi mediante **Configuraciones de WiFi**. Según el valor establecido en **Configurar Wi-Fi**, los usuarios pueden tener un control limitado o nulo sobre la adición y modificación de redes.

Estado de radio del dispositivo

1. Estado de Wi-Fi

Controla el estado actual de Wi-Fi y si el usuario puede cambiarlo.

> **Elección del usuario (predeterminado)**: El usuario puede habilitar o deshabilitar Wi-Fi.
>
> **Habilitado**: Wi-Fi está activado y el usuario no puede desactivarlo (Android 13 o superior).
>
> **Deshabilitado**: Wi-Fi está desactivado y el usuario no puede activarlo (Android 13 o superior).

2. Nivel mínimo de seguridad de Wi-Fi

El nivel de seguridad mínimo requerido de las redes Wi-Fi a las que se puede conectar el dispositivo. Compatible con Android 13 o superior, para dispositivos totalmente gestionados y perfiles de trabajo en dispositivos propiedad de la empresa.

> **Red abierta (predeterminado)**: El dispositivo se puede conectar a todo tipo de redes Wi-Fi.
>
> **Red personal**: No permite redes Wi-Fi abiertas; requiere al menos seguridad personal (por ejemplo, WPA2-PSK).
>
> **Red empresarial**: Requiere redes EAP empresariales; no permite redes Wi-Fi por debajo de este nivel de seguridad.

Red empresarial de 192 bits: Requiere redes empresariales de 192 bits; la opción más estricta.

3. Estado de banda ultraancha (UWB)

Controla el estado del ajuste de banda ultraancha y si el usuario puede activarlo o desactivarlo.

Elección del usuario (predeterminado): El usuario puede activar o desactivar UWB.

Deshabilitado: UWB está deshabilitado y el usuario no puede activarlo ni desactivarlo desde los ajustes (Android 14 o superior).

Gestión de la conectividad del dispositivo

4. Uso compartido por Bluetooth

Controla si se permite el uso compartido por Bluetooth.

Permitido: Se permite el uso compartido por Bluetooth (predeterminado en dispositivos totalmente gestionados, Android 8 o superior).

No permitido: No se permite el uso compartido por Bluetooth (predeterminado en perfiles de trabajo, Android 8 o superior).

5. Configurar Wi-Fi

Controla los privilegios de configuración de Wi-Fi. Según la opción seleccionada, el usuario tiene control total, limitado o nulo para configurar redes Wi-Fi.

Permitir configurar Wi-Fi (predeterminado): El usuario puede configurar Wi-Fi.

No permitir añadir configuración de Wi-Fi: No se permite añadir nuevas configuraciones de Wi-Fi. El usuario puede cambiar entre las redes ya configuradas (Android 13 o superior; dispositivos totalmente gestionados y perfiles de trabajo de dispositivos propiedad de la empresa).

No permitir configurar Wi-Fi: No permite configurar redes Wi-Fi. En los dispositivos totalmente gestionados, esto elimina las redes configuradas por el usuario y conserva solo las redes configuradas mediante **Configuraciones de WiFi**. En los perfiles de trabajo de dispositivos propiedad de la empresa, las redes existentes no se ven afectadas, pero los usuarios no pueden añadir, quitar ni modificar redes Wi-Fi.

> Cuando la configuración de Wi-Fi está deshabilitada y el dispositivo no puede conectarse al arrancar, el sistema puede mostrar la **vía de escape de red** para que el usuario se conecte temporalmente y actualice la política.

6. Ajustes de Wi-Fi Direct

Controla la configuración y el uso de los ajustes de Wi-Fi Direct. Compatible con dispositivos propiedad de la empresa que ejecutan Android 13 o superior.

Permitir (predeterminado): El usuario puede usar Wi-Fi Direct.

No permitir: El usuario no puede usar Wi-Fi Direct.

7. Ajustes de anclaje a red

Controla los ajustes de anclaje a red. Según el valor establecido, se prohíbe al usuario parcial o totalmente el uso de distintas formas de anclaje a red.

Permitir todo el anclaje a red (predeterminado): Permite configurar y usar todas las formas de anclaje a red.

No permitir anclaje a red Wi-Fi: Impide que el usuario use el anclaje a red Wi-Fi (dispositivos propiedad de la empresa con Android 13 o superior).

No permitir ningún anclaje a red: No permite ninguna forma de anclaje a red (dispositivos totalmente gestionados y perfiles de trabajo de dispositivos propiedad de la empresa).

8. Política de SSID de Wi-Fi

Restricciones sobre los SSID de Wi-Fi a los que se puede conectar el dispositivo (esto no afecta a qué redes se pueden configurar en el dispositivo). Compatible con dispositivos propiedad de la empresa que ejecutan Android 13 o superior.

Lista de SSID denegados (predeterminado): El dispositivo no puede conectarse a ninguna red Wi-Fi cuyo SSID esté en la lista, pero puede conectarse a otras redes.

Lista de SSID permitidos: El dispositivo solo puede conectarse a los SSID de la lista. La lista de SSID no debe estar vacía.

Usa **Añadir SSID** para añadir entradas. Según el tipo de política seleccionado, la lista se interpreta como SSID permitidos o denegados.

En la interfaz del editor de políticas, la lista de SSID se denomina **SSID de Wi-Fi permitidos** para las listas de permitidos y **SSID de Wi-Fi denegados** para las listas de denegados.

9. Ajustes de itinerancia de Wi-Fi

Configura el modo de itinerancia de Wi-Fi por SSID. Usa **Añadir ajuste de itinerancia de Wi-Fi** para crear entradas.

Cada entrada incluye:

SSID: El SSID al que se aplica el ajuste de itinerancia (obligatorio).

Modo de itinerancia de Wi-Fi: Predeterminado / Deshabilitado / Agresivo. Deshabilitado y Agresivo requieren Android 15 o superior y solo son compatibles con dispositivos totalmente gestionados y perfiles de trabajo en dispositivos propiedad de la empresa.

Restricciones de red

10. Bluetooth deshabilitado

Indica si Bluetooth está deshabilitado. Es preferible este ajuste al de configuración de Bluetooth deshabilitada, ya que el usuario puede eludir este último.

11. Uso compartido de contactos por Bluetooth deshabilitado

Indica si el uso compartido de contactos por Bluetooth está deshabilitado.

12. Configuración de Bluetooth deshabilitada

Indica si la configuración de Bluetooth está deshabilitada.

13. Restablecimiento de red deshabilitado

Indica si el restablecimiento de los ajustes de red está deshabilitado.

14. Beam saliente deshabilitado

Indica si el uso de NFC para transmitir datos desde aplicaciones está deshabilitado.

VPN

15. Aplicación de VPN Always On

Especifica un nombre de paquete de VPN Always On para garantizar que los datos de las aplicaciones gestionadas especificadas pasen siempre por una VPN configurada.

> Nota: Esta función requiere implementar un cliente VPN compatible con las funciones Always On y de VPN por aplicación.

16. Bloqueo de VPN

No permite la conexión de red cuando la VPN no está conectada.

17. Configuración de VPN deshabilitada

Indica si la configuración de la VPN está deshabilitada.

Proxy y servicios de red

18. Servicio de red preferente

Controla si el servicio de red preferente está habilitado en el perfil de trabajo. Por ejemplo, una organización puede tener un acuerdo con un operador para que los datos de trabajo se envíen mediante un servicio de red del operador dedicado al uso empresarial (por ejemplo, un segmento empresarial en redes 5G). Esto no tiene efecto en los dispositivos totalmente gestionados.

Deshabilitado: El servicio de red preferente está deshabilitado en el perfil de trabajo.

Habilitado: El servicio de red preferente está habilitado en el perfil de trabajo.

> Si usas la segmentación de red empresarial, configura también **Configuración de segmentación de red 5G** en el panel de políticas **Celular** y asigna aplicaciones a un segmento mediante su ajuste **Red preferente**.

19. Proxy global recomendado

El proxy HTTP global independiente de la red. Normalmente, los proxies deben configurarse por red en las configuraciones de WiFi. Un proxy global puede ser útil para configuraciones poco habituales, como el filtrado interno general. El proxy global solo es una recomendación y algunas aplicaciones pueden ignorarlo.

Deshabilitado

Proxy directo

Configuración automática de proxy (PAC)

19.1. Host

El host del proxy directo.

19.2. Puerto

El puerto del proxy directo.

19.3. URI del PAC

El URI del script PAC que se usa para configurar el proxy.

19.4. Hosts excluidos

En un proxy directo, los hosts para los que se omite el proxy. Los nombres de host pueden contener comodines como ***.example.com**.

Usa **Añadir host excluido** para agregar entradas (disponible solo para el proxy directo).

Configuraciones de Wi-Fi

Define configuraciones de red Wi-Fi que el sistema aplicará en los dispositivos. Usa **Añadir configuración Wi-Fi** para crear una entrada y eliminarla con la acción de eliminar.

20. Campos de configuración de Wi-Fi

Cada configuración incluye:

Nombre de la configuración: Obligatorio.

SSID: Obligatorio.

Conexión automática: Indica si la red debe conectarse automáticamente cuando esté dentro del alcance.

Fast Transition: Indica si el cliente debe intentar usar Fast Transition (IEEE 802.11r-2008) con la red.

SSID oculto: Indica si el SSID se difundirá.

Modo de aleatorización de MAC: Hardware o Automático (Android 13+).

20.1. Seguridad

Opciones de seguridad de Wi-Fi:

WEP-PSK: WEP (clave precompartida).

WPA-PSK: WPA/WPA2/WPA3-Personal (clave precompartida).

WPA-EAP: WPA/WPA2/WPA3-Enterprise (Protocolo de autenticación extensible).

Modo WPA3 de 192 bits: Red WPA-EAP que solo permite el modo WPA3 de 192 bits.

20.2. Frase de contraseña (clave precompartida)

Se muestra cuando la seguridad es **WEP-PSK** o **WPA-PSK**. La frase de contraseña es obligatoria.

20.3. Método EAP (Enterprise)

Se muestra cuando la seguridad es **WPA-EAP** o **Modo WPA3 de 192 bits**. Selecciona un método EAP externo:

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

20.4. Autenticación de fase 2

Se muestra para los métodos externos de túnel (**EAP-TTLS** y **PEAP**).

MSCHAPv2

PAP

20.5. Credenciales EAP de los usuarios

Cuando está habilitado, el sistema aplica automáticamente las credenciales EAP en los dispositivos para cada usuario. Puedes configurar las credenciales de usuario en la sección **Usuarios**.

20.6. Certificado de cliente

Para **EAP-TLS**, puedes asignar un certificado de cliente que se use para la autenticación Wi-Fi.

Para obtener más información, consulta la página **Gestión de certificados**.

Si ya hay un certificado asignado, puedes usar **Abrir certificado** para verlo o **Cambiar certificado** para seleccionar otro.

También puedes especificar el **Alias del par de claves del certificado de cliente**, que hace referencia a un certificado de cliente almacenado en el llavero de Android y permitido para la autenticación Wi-Fi.

> Si se establecen tanto **Certificado de cliente** como **Alias del par de claves del certificado de cliente**, se omite el alias del par de claves.

20.7. Identidad

Identidad del usuario. En los protocolos externos de túnel (PEAP, EAP-TTLS), se usa para autenticarse dentro del túnel, y la **Identidad anónima** se usa para la identidad EAP fuera del túnel. En los protocolos externos sin túnel, se usa para la identidad EAP.

20.8. Identidad anónima

Solo para protocolos de túnel, indica la identidad del usuario presentada al protocolo externo.

20.9. Contraseña

Contraseña del usuario. Si no se especifica, se solicita al usuario de forma predeterminada.

20.10. Certificados de CA del servidor

Lista de certificados de CA que se usarán para verificar la cadena de certificados del host. Al menos un certificado de CA debe coincidir. Para obtener más información, consulta la página **Gestión de certificados**.

Usa **Añadir certificado de CA del servidor** para agregar entradas y eliminarlas con la acción de eliminar.

20.11. Coincidencias de sufijo de dominio

Una lista de restricciones para el nombre de dominio del servidor. Las entradas se usan como requisitos de coincidencia de sufijo con los nombres DNS del nombre alternativo del sujeto de un certificado del servidor de autenticación.

Revision #59
Created 2025-12-17 09:33:19 UTC by Admin
Updated 2026-11-12 09:54:34 UTC by Admin