Networking

IT admins can silently provision enterprise Wi-Fi configurations on managed devices. Wi-Fi configurations can also be lock down, to prevent users from creating configurations or modifying corporate configurations.

1. Bluetooth disabled

Whether bluetooth is disabled. Prefer this setting over bluetoothConfigDisabled because bluetoothConfigDisabled can be bypassed by the user.

2. Bluetooth contact sharing disabled

Whether bluetooth contact sharing is disabled.

3. Bluetooth config disabled

Whether configuring bluetooth is disabled.

4. Tethering config disabled

Whether configuring tethering and portable hotspots is disabled.

5. Wi-Fi config disabled

Whether configuring Wi-Fi access points is disabled.

6. Network reset disabled

Whether resetting network settings is disabled.

7. Outgoing beam disabled

Whether using NFC to beam data from apps is disabled.

8. Always On VPN app

Specify an Always On VPN to ensure that data from specified managed apps will always go through a configured VPN.

Note: this feature requires deploying a VPN client that supports both Always On and per-app VPN features.

9. VPN lockdown

Disallows networking when the VPN is not connected.

10. VPN config disabled

Whether configuring VPN is disabled.

11. Preferential network service

Controls whether preferential network service is enabled on the work profile. For example, an organization may have an agreement with a carrier that all of the work data from its employees' devices will be sent via a network service dedicated for enterprise use. An example of a supported preferential network service is the enterprise slice on 5G networks. This has no effect on fully managed devices.

> **Disabled**: Preferential network service is disabled on the work profile.
>
> **Enabled**: Preferential network service is enabled on the work profile.

12. Recommended global proxy

The network-independent global HTTP proxy. Typically proxies should be configured per-network in openNetworkConfiguration. However for unusual configurations like general internal filtering a global HTTP proxy may be useful. If the proxy is not accessible, network access may break. The global proxy is only a recommendation and some apps may ignore it.

Disabled

Direct proxy

Proxy auto-config (PAC)

12.1 Host

The host of the direct proxy.

12.2 Port

The port of the direct proxy.

12.3. PAC URI

The URI of the PAC script used to configure the proxy.

12.4. Excluded hosts

For a direct proxy, the hosts for which the proxy is bypassed. The host names may contain wildcards such as *.example.com.

13. WiFi configurations

Network configuration for the device.

13.1. Configuration name

13.2. SSID

13.3. Auto connect

Whether the network should be connected to automatically when in range.

13.4. Fast Transition

Indicating if the client should attempt to use Fast Transition (IEEE 802.11r-2008) with the network.

13.5. Hidden SSID

Indicating if the SSID will be broadcast.

13.6. Security

WEP (Pre-Shared Key)

WPA/WPA2/WPA3-Personal (Pre-Shared Key)

WPA/WPA2/WPA3-Enterprise (Extensible Authentication Protocol)

13.7. Passphrase

Password, for **Pre-Shared Key** security options.

13.8. EAP method

Extensible Authentication Protocol method

EAP-TLS

EAP-TTLS

PEAP

EAP-SIM

EAP-AKA

13.9. Phase 2 authentication

MSCHAPv2

PAP

13.10. EAP credentials from users

When enabled, the system will automatically apply EAP credentials on devices on a per-user basis. You can configure user's credentials in the **Users** section.

13.11. Client certificate

Certificate to use for authenticating devices with this WiFi network. For more information read the **Certificate management** section.

13.12. Identity

Identity of user. For tunneling outer protocols (PEAP, EAP-TTLS), this is used to authenticate inside the tunnel, and **Anonymous identity** is used for the EAP identity outside the tunnel. For non-tunneling outer protocols, this is used for the EAP identity. This value is subject to string expansions.

13.13. Anonymous identity

For tunnelling protocols only, this indicates the identity of the user presented to the outer protocol. This value is subject to string expansions. If not specified, use empty string.

13.14. Password

Password of user. If not specified, defaults to prompting the user.

13.15. Server CA certificates

List of CA certificates to be used for verifying the host‘s certificate chain. At least one of the CA certificates must match. If not set, the client does not check that the server certificate is signed by a specific CA. A verification using the system’s CA certificates may still apply. For more information read the **Certificate management** section.

Revision #4
Created 28 March 2022 10:17:35 by Admin
Updated 13 April 2022 14:50:55 by Admin