ネットワーク

このセクションでは、ネットワークに関するポリシーを構成できます。

> Wi-Fi構成は、 **WiFi configurations**
> を介してシステムによってプロビジョニングおよび管理されます。 **Configure Wi-Fi**
> に設定された値によっては、ユーザーによるネットワークの追加や変更の操作が制限されるか、ある
> いは一切できなくなる場合があります。

デバイスの無線状態

1. Wi-Fi状態

Wi-Fiの現在の状態、およびユーザーがその状態を変更できるかどうかを制御します。

ユーザーによる選択（デフォルト） ：ユーザーが Wi-Fiの有効 /無効を切り替えることができます。

Enabled: Wi-Fiがオンになり、ユーザーはオフにすることはできません（ Android 13以降）。

Disabled: Wi-Fiがオフになり、ユーザーはオンにすることはできません（ Android 13以降）。

2. 最小 Wi-Fiセキュリティレベル

デバイスが接続可能な Wi-Fi
ネットワークの最小要件セキュリティレベルです。フル管理デバイス、および会社所有の Android 15
以降の仕事用プロファイルにおいて、 Android 13以降でサポートされています。

Open network (default): デバイスはあらゆる種類の Wi-Fiネットワークに接続できます。

Personal network: オープンな Wi-Fi
ネットワークを禁止します。少なくとも個人用セキュリティ（例: WPA2-PSK）が必要になります。

Enterprise network: エンタープライズ EAP
ネットワークを要求します。このセキュリティレベルに満たない Wi-Fi
ネットワークへの接続は禁止されます。

- **192-bit enterprise network**: 192 [illegible]

3. Ultra wideband (UWB) [illegible]

Ultra wideband[illegible] UWB[illegible] / [illegible]

- [illegible]: [illegible] UWB[illegible] /[illegible]

- **Disabled**: UWB[illegible] UWB[illegible] / [illegible] Android 14[illegible]

[illegible]

4. Bluetooth[illegible]

Bluetooth[illegible]

- **Allowed**: Bluetooth[illegible] Android 8[illegible]

- **Disallowed**: Bluetooth[illegible] Android 8 [illegible]

5. Wi-Fi[illegible]

Wi-Fi[illegible] Wi-Fi [illegible]

- **Allow configuring Wi-Fi (default)**: [illegible] Wi-Fi[illegible]

- **Disallow add Wi-Fi config**: [illegible] Wi-Fi [illegible] Android 13[illegible] Android 15[illegible]

- **Disallow configuring Wi-Fi**: Wi-Fi [illegible]

[illegible] **WiFi configurations**

[illegible]

[illegible] Wi-Fi[illegible] /[illegible] /

[illegible]

> Wi-Fi[illegible]
>
> [illegible]
>
> [illegible]

6. Wi-Fi Direct[illegible]

Wi-Fi Direct[illegible] Android 13

[illegible]

- **Allow (default)**: [illegible] Wi-Fi Direct[illegible]

- **Disallow**: [illegible] Wi-Fi Direct[illegible]

7. [illegible]

[illegible]

[illegible]

- [illegible] :
  [illegible]

- **Wi-Fi**[illegible] : [illegible] Wi-Fi[illegible] Android 13[illegible]

- [illegible] : [illegible] +
  [illegible]

8. Wi-Fi SSID[illegible]

[illegible] Wi-Fi SSID

[illegible] Android 13

[illegible]

- **SSID**[illegible] : [illegible] SSID[illegible] Wi-Fi
  [illegible]

SSID : SSID SSID

SSID

SSID SSID

UI SSID **Wi-Fi SSID** **Wi-Fi SSID**

9. Wi-Fi

SSID Wi-Fi **Wi-Fi**

SSID: SSID

Wi-Fi : / / Android 15

10. Bluetooth

Bluetooth Bluetooth

11. Bluetooth

Bluetooth

12. Bluetooth

Bluetoothの設定変更を無効にするかどうか。

13. ネットワークリセットの無効化

ネットワーク設定のリセットを無効にするかどうか。

14. アウトゴーイングビームの無効化

NFCを使用してアプリからデータをビーム送信することを無効にするかどうか。

VPN

15. Always On VPNアプリ

指定されたマネージドアプリからのデータが常に構成済みの VPNを経由するように、 Always On VPN のパッケージ名を指定します。

> 注意 ：この機能を使用するには、 Always Onとアプリごとの VPN機能の両方をサポートする VPN クライアントをデプロイする必要があります。

16. VPNロックダウン

VPNが接続されていないときに、ネットワーク通信を禁止します。

17. VPN構成の無効化

VPNの設定変更を無効にするかどうか。

プロキシおよびネットワークサービス

18. 推奨ネットワークサービス

ワークプロファイルで推奨ネットワークサービスを有効にするかどうかを制御します。例えば、組織が通信事業者と、業務データは企業専用のネットワークサービス（例: 5G ネットワークのエキスパートスライスなど）を介して送信するという契約を結んでいる場合があります。これはフルマネージドデバイスには影響しません。

無効 ：ワークプロファイルで推奨ネットワークサービスが無効になります。

有効 ：ワークプロファイルで推奨ネットワークサービスが有効になります。

エンタープライズネットワークスライシングを使用する場合は、**Cellular**ポリシーパネル内の **5G** ネットワークスライシング設定 も構成し、 推奨ネットワーク 設定を使用してアプリをスライスに割り当ててください。

19. 推奨グローバルプロキシ

ネットワークに依存しないグローバル HTTPプロキシです。通常、プロキシは Wi-Fi 設定においてネットワークごとに構成されるべきものです。グローバルプロキシは、一般的な内部フィルタリングのような特殊な構成において有用な場合があります。なお、グローバルプロキシはあくまで推奨事項であり、一部のアプリでは無視される場合があります。

無効

ダイレクトプロキシ

プロキシ自動設定 **(PAC)**

19.1. ホスト

ダイレクトプロキシのホスト。

19.2. ポート

ダイレクトプロキシのポート。

19.3. PAC URI

プロキシを構成するために使用される PACスクリプトの URI。

19.4. [illegible]

[illegible] ***.example.com** [illegible]

Add excluded host [illegible]

Wi-Fi[illegible]

[illegible] Wi-Fi[illegible] **Wi-Fi**[illegible]

20. Wi-Fi[illegible]

[illegible]

- [illegible]: [illegible]
- **SSID**: [illegible]
- [illegible]: [illegible]
- [illegible] **(Fast Transition)**: [illegible] (IEEE 802.11r-2008) [illegible]
- [illegible] **SSID**: SSID[illegible]
- **MAC**[illegible]: [illegible] Android 13[illegible]

20.1. [illegible]

Wi-Fi[illegible]

- **WEP-PSK**: WEP ([illegible])[illegible]
- **WPA-PSK**: WPA/WPA2/WPA3-Personal ([illegible])[illegible]
- **WPA-EAP**: WPA/WPA2/WPA3-Enterprise ([illegible])[illegible]
- **WPA3 192**[illegible]: WPA-EAP[illegible] WPA3 192[illegible]

20.2. パスフレーズ（事前共有鍵）

セキュリティが **WEP-PSK** または **WPA-PSK** のときに表示されます。パスフレーズは必須です。

20.3. EAPメソッド（エンタープライズ）

セキュリティが **WPA-EAP** または **WPA3 192**ビットモード のときに表示されます。いずれか 1つの EAP アウターメソッドを選択してください:

- **EAP-TLS**
- **EAP-TTLS**
- **PEAP**
- **EAP-SIM**
- **EAP-AKA**

20.4. フェーズ 2認証

トンネリングアウターメソッド（ **EAP-TTLS** および **PEAP**）の場合に表示されます。

- **MSCHAPv2**
- **PAP**

20.5. ユーザーによる EAP認証情報

有効にすると、システムはデバイス上でユーザーごとに EAP 認証情報を自動的に適用します。ユーザーの認証情報は ユーザー セクションで構成できます。

20.6. クライアント証明書

EAP-TLSでは、 Wi-Fi認証に使用するクライアント証明書を割り当てることができます。詳細については、証明書管理 ページをご参照ください。

すでに証明書が割り当てられている場合は、 証明書を開く で表示するか、 証明書を変更 で別の証明書を選択できます。

または、 Androidのキーチェーンに保存され、 Wi-Fi認証が許可されているクライアント証明書を参照する クライアント証明書キーペアエイリアス を指定することもできます。

> **Client certificate と Client certificate key pair alias**
> の両方が設定されている場合、キーペアエイリアスは無視されます。

20.7. ID (Identity)

ユーザーの　　IDです。トンネリングアウタープロトコル（　　PEAP、EAP-TTLS
）の場合、これはトンネル内での認証に使用され、　匿名　**ID**がトンネル外の　　EAP ID
として使用されます。非トンネリングアウタープロトコルの場合は、これが　　EAP IDとして使用されます。

20.8. 匿名　ID

トンネリングプロトコルのみにおいて、これはアウタープロトコルに提示されるユーザーの　　IDを示します。

20.9. パスワード

ユーザーのパスワード。指定しない場合は、デフォルトでユーザーへのプロンプト表示となります。

20.10. サーバー　　CA証明書

ホストの証明書チェーンを検証するために使用される　CA証明書のリストです。少なくとも　1つの　CA
証明書が一致する必要があります。詳細については、　証明書管理_____ページをご覧ください。

Add Server CA certificate を使用してエントリを追加し、削除アクションでそれらを削除します。

20.11. ドメインサフィックスの一致

サーバーのドメイン名に対する制約リストです。これらのエントリは、認証サーバー証明書の代替サブジェ
クト名（　　SAN）の　DNS名に対するサフィックス一致要件として使用されます。

Revision #6
Created 2026-06-24 08:08:36 UTC by Admin
Updated 2026-06-24 09:43:06 UTC by Admin