Netzwerk

Der Abschnitt **Netzwerk** des Apple-Richtlinieneditors konfiguriert Wi-Fi-Netzwerke und VPNs auf den Geräten, installiert Zertifikate und schränkt Konnektivitätsfunktionen wie AirDrop und Bluetooth ein. Jedes Wi-Fi-Netzwerk, VPN und Zertifikat wird als eigenes Konfigurationsprofil installiert, das Sie auf dem Gerät unter **Einstellungen > Allgemein > VPN & Geräteverwaltung** (Mac: **Systemeinstellungen > Allgemein > Geräteverwaltung** oder **Datenschutz & Sicherheit > Profile** unter macOS 13 und 14) und im Bereich **Profile, Zertifikate und Sicherheit** der Geräteseite sehen können.

> Zertifikate stammen von der Seite **Zertifikate**: Importieren Sie sie zuerst dort. Die Richtlinie verweist nur auf sie, daher wird ein Zertifikat nie in die Richtlinie kopiert.

Einschränkungen

- **AirDrop erlauben**
- **Eingehende AirPlay-Anfragen erlauben**
- **Bluetooth-Änderung erlauben**
- **Änderung der Bluetooth-Freigabe erlauben**
- **Zugriff von Dateien auf Netzwerklaufwerke erlauben**
- **Änderung der Internetfreigabe erlauben**
- **Inhalts-Caching erlauben**
- **iTunes-Dateifreigabe erlauben**

Wi-Fi-Netzwerke

Klicken Sie auf **Wi-Fi-Netzwerk hinzufügen** und füllen Sie aus:

- **Netzwerkname (SSID)**: der Name des Netzwerks, bis zu 32 Zeichen.
- **Sicherheit**: keine (offenes Netzwerk), WEP, WPA oder WPA2, WPA2 oder WPA3, nur WPA3 oder beliebig.
- **Passwort**: das Passwort eines persönlichen Netzwerks.
- **Automatisch beitreten** und **Verborgenes Netzwerk** (für Netzwerke, die ihren Namen nicht senden).
- **Proxy**: keiner, manuell (Server und Port) oder automatisch (eine PAC-Datei-URL oder leer, um die Einstellungen mit WPAD im Netzwerk zu finden).

- **Profilname** (optional) und **Gilt für**, um das Netzwerk auf bestimmte Gerätetypen zu beschränken.

Unternehmensnetzwerke (802.1X)

Aktivieren Sie **Unternehmen (802.1X)**, wenn Benutzer sich mit ihren eigenen Zugangsdaten oder einem Zertifikat anstelle eines gemeinsam genutzten Passworts authentifizieren.

- **Authentifizierung**: PEAP, TTLS (mit ihrer inneren Authentifizierung, zum Beispiel MSCHAPv2) oder TLS (nur Zertifikat).
- **Zugangsdaten des Gerätebenutzers**: Jedes Gerät verwendet die EAP-Identität, die anonyme Identität und das Passwort seines Benutzers, die auf der Seite „Benutzer“ festgelegt sind. Geräte ohne Benutzer erhalten das Netzwerk nicht.
- **Identität**, **Anonyme Identität** und **Passwort**: für jedes Gerät gleich. Die Identität kann die Variablen $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ und $UDID$ enthalten. Lassen Sie das Passwort leer, damit der Benutzer es auf dem Gerät eingeben kann.
- **Identitätszertifikat**: das Client-Zertifikat, das das Gerät vorlegt (für TLS erforderlich). Siehe die Zertifikatoptionen unten.
- **Vertrauenswürdige Zertifikate**: die CA-Zertifikate, die das Zertifikat Ihres RADIUS-Servers ausgestellt haben. Sie werden mit dem Netzwerk installiert.
- **Vertrauenswürdige Servernamen**: die Namen der RADIUS-Serverzertifikate, die die Geräte akzeptieren, zum Beispiel radius.example.com oder *.example.com.

VPN

Klicken Sie auf **VPN hinzufügen**, um ein IKEv2- oder Cisco-IPSec-VPN zu konfigurieren, das in iOS, iPadOS und macOS integriert ist (keine VPN-App erforderlich).

- **Typ** und **Server**. Für IKEv2 außerdem die **Remote-Identität** (die Serveridentität, leer bedeutet die Serveradresse) und die **Lokale Identität**, die die Variablen $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ und $UDID$ enthalten kann.
- **Authentifizierung** des Geräts: ein Zertifikat (von der Seite „Zertifikate“, das Zertifikat des Gerätebenutzers oder von einem SCEP-Server angefordert), ein gemeinsames Geheimnis (mit dem optionalen Gruppennamen für IPSec) oder keine für IKEv2-Server, die nur Benutzername und Passwort prüfen.
- **Vertrauenswürdige Zertifikate**: die CA-Zertifikate Ihres VPN-Servers, die mit dem VPN installiert werden. Für IKEv2 können Sie auch den erwarteten Aussteller und Namen des Serverzertifikats festlegen.
- **Benutzername und Passwort**: Der Benutzer authentifiziert sich zusätzlich mit einem Benutzernamen (Variablen erlaubt) und einem Passwort (EAP für IKEv2, XAuth für IPSec). Lassen Sie das Passwort leer, damit der Benutzer es auf dem Gerät eingeben kann.
- **VPN-Name** (in den Einstellungen angezeigt) und **Gilt für**.

Verbindung

- **Der Benutzer verbindet sich in den Einstellungen**: Das VPN wird installiert und der Benutzer aktiviert es bei Bedarf.
- **Bei Bedarf**: Das Gerät verbindet das VPN automatisch. Mit **außer in vertrauenswürdigem Wi-Fi** wird das VPN nicht in den von Ihnen aufgeführten Wi-Fi-Netzwerken verwendet, zum Beispiel im Büronetzwerk.
- **Immer an** (nur IKEv2, überwachte iPhones und iPads): Der gesamte Datenverkehr läuft über Mobilfunk und Wi-Fi durch das VPN, und der Benutzer kann es nicht deaktivieren. Andere Geräte erhalten dieses VPN nicht. Wenn das VPN einen Benutzernamen verwendet, muss das Passwort in der Richtlinie festgelegt werden.
- **VPN pro App**: Nur einige Apps verwenden das VPN. Wählen Sie das VPN für jede App im Abschnitt **App-Verwaltung** (Feld **VPN** der App, auf dem Mac nicht verfügbar), und führen Sie optional Safari-Domains auf, die es verwenden.

> Testen Sie ein Immer-an- oder Bei-Bedarf-VPN zuerst auf einem Testgerät: Wenn der Server nicht erreichbar ist, hat das Gerät möglicherweise keine Verbindung.

Globaler Proxy, verschlüsseltes DNS und Webinhaltsfilter

Diese Einstellungen gelten für den gesamten Datenverkehr des Geräts. Aktivieren Sie sie mit ihrem Schalter.

- **Globaler HTTP-Proxy** (überwachte iPhones und iPads, Mac): Der gesamte HTTP-Datenverkehr läuft in jedem Netzwerk über den Proxy. Legen Sie Server und Port (mit optionalem Benutzernamen und Passwort) oder eine automatische Konfiguration fest (PAC-Datei-URL oder leer, um sie im Netzwerk zu finden). **Wi-Fi-Anmeldeseiten erlauben** ermöglicht dem Benutzer, sich ohne den Proxy bei öffentlichen Wi-Fi-Netzwerken anzumelden.
- **Verschlüsseltes DNS**: Das Gerät löst Namen mit Ihrem DNS-Server über DNS over HTTPS (Server-URL) oder DNS over TLS (Servername) auf, optional nur für bestimmte Domains. Auf überwachten Geräten können Sie verhindern, dass der Benutzer es deaktiviert.
- **Webinhaltsfilter** (überwachte iPhones und iPads): Der in iOS integrierte Filter beschränkt Websites für Erwachsene, mit Listen von Websites, die immer erlaubt oder immer blockiert sind, oder erlaubt nur eine Liste von Websites, die in Safari als Lesezeichen angezeigt werden.

>

> Ein falscher Proxy- oder DNS-Server kann die Geräte ohne Verbindung zurücklassen: Testen Sie die Einstellungen zuerst auf einem Testgerät.

Zertifikate

Klicken Sie auf **Zertifikat hinzufügen**, um ein Zertifikat separat zu installieren: eine Zertifizierungsstelle, der Safari und die Apps vertrauen müssen, oder eine von Apps verwendete Identität. Die Zertifikate eines Wi-Fi-Netzwerks oder eines VPNs müssen hier nicht hinzugefügt werden.

Zertifikatoptionen

- **Ein Zertifikat der Seite „Zertifikate“**: dasselbe Zertifikat auf jedem Gerät. Klicken Sie auf **Zertifikat auswählen**, um es auszuwählen.
- **Das Zertifikat des Gerätebenutzers**: Jedes Gerät erhält das mit seinem Benutzer verknüpfte Client-Zertifikat. Geräte, deren Benutzer kein Zertifikat hat, erhalten es nicht. Wenn Sie dem Benutzer ein anderes Zertifikat zuordnen, werden die Geräte aktualisiert.
- **Von einem SCEP-Server angefordert**: Jedes Gerät fordert sein eigenes Zertifikat von Ihrem SCEP-Server an (zum Beispiel Microsoft NDES), sodass der private Schlüssel das Gerät nie verlässt. Legen Sie die Server-URL, die Challenge, falls der Server eine verlangt, den Betreff (zum Beispiel CN=$EMAIL$), die alternativen Namen, die Schlüsselgröße und die Schlüsselverwendung fest.

> Client-Zertifikate (.p12), die mit der alten RC2-Verschlüsselung geschützt sind, können nicht auf Apple-Geräten installiert werden. Exportieren Sie sie vor dem Importieren erneut mit 3DES- oder AES-Verschlüsselung.

Sicherheit

Profile, die Passwörter oder private Schlüssel enthalten, werden nur an das Gerät gesendet, für das sie erstellt wurden: Das Gerät muss seine Anforderung mit seinem Verwaltungszertifikat signieren. Passwörter und Zertifikate werden nicht in den Protokollen geschrieben.

Revision #7
Created 2026-11-10 15:14:09 UTC by Admin
Updated 2026-11-12 09:53:52 UTC by Admin