Rete

La sezione **Rete** dell'Apple Policy Editor configura reti Wi-Fi e VPN sui dispositivi, installa certificati e limita funzionalità di connettività come AirDrop e Bluetooth. Ogni rete Wi-Fi, VPN e certificato viene installato come profilo di configurazione separato, che puoi vedere sul dispositivo in **Impostazioni > Generali > VPN e gestione dispositivo** (Mac: **Impostazioni di Sistema > Generali > Gestione dispositivo**, oppure **Privacy e sicurezza > Profili** su macOS 13 e 14) e nel pannello **Profili, certificati e sicurezza** della pagina del dispositivo.

> I certificati vengono presi dalla pagina **Certificati**: importali prima lì. La policy vi fa solo riferimento, quindi un certificato non viene mai copiato nella policy.

Restrizioni

- **Consenti AirDrop**
- **Consenti richieste AirPlay in entrata**
- **Consenti modifica Bluetooth**
- **Consenti modifica condivisione Bluetooth**
- **Consenti accesso alle unità di rete in File**
- **Consenti modifica condivisione Internet**
- **Consenti cache dei contenuti**
- **Consenti condivisione file di iTunes**

Reti Wi-Fi

Fai clic su **Aggiungi rete Wi-Fi** e compila:

- **Nome della rete (SSID)**: il nome della rete, fino a 32 caratteri.
- **Sicurezza**: nessuna (rete aperta), WEP, WPA o WPA2, WPA2 o WPA3, solo WPA3 oppure qualsiasi.
- **Password**: la password di una rete personale.
- **Unisciti automaticamente** e **Rete nascosta** (per le reti che non trasmettono il proprio nome).
- **Proxy**: nessuno, manuale (server e porta) o automatico (l’URL di un file PAC, oppure vuoto per trovare le impostazioni sulla rete con WPAD).

- **Nome del profilo** (facoltativo) e **Si applica a**, per limitare la rete ad alcuni tipi di dispositivi.

Reti aziendali (802.1X)

Attiva **Aziendale (802.1X)** quando gli utenti si autenticano con le proprie credenziali o un certificato invece di una password condivisa.

- **Autenticazione**: PEAP, TTLS (con la sua autenticazione interna, ad esempio MSCHAPv2) o TLS (solo certificato).
- **Credenziali dell'utente del dispositivo**: ogni dispositivo usa l'identità EAP, l'identità anonima e la password del suo utente, impostate nella pagina Utenti. I dispositivi senza utente non ricevono la rete.
- **Identità**, **Identità anonima** e **Password**: le stesse per ogni dispositivo. L'identità può contenere le variabili $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ e $UDID$. Lascia vuota la password per consentire all'utente di digitarla sul dispositivo.
- **Certificato di identità**: il certificato client che il dispositivo presenta (obbligatorio per TLS). Vedi le opzioni dei certificati di seguito.
- **Certificati attendibili**: i certificati CA che hanno emesso il certificato del tuo server RADIUS. Vengono installati con la rete.
- **Nomi dei server attendibili**: i nomi dei certificati del server RADIUS che i dispositivi accettano, ad esempio radius.example.com o *.example.com.

VPN

Fai clic su **Aggiungi VPN** per configurare una VPN IKEv2 o Cisco IPSec, integrata in iOS, iPadOS e macOS (non serve un'app VPN).

- **Tipo** e **Server**. Per IKEv2 anche l'**Identificatore remoto** (l'identità del server, vuoto significa l'indirizzo del server) e l'**Identificatore locale**, che può contenere le variabili $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ e $UDID$.
- **Autenticazione** del dispositivo: un certificato (dalla pagina Certificati, il certificato dell'utente del dispositivo o richiesto a un server SCEP), un segreto condiviso (con il nome del gruppo facoltativo per IPSec) oppure nessuna per i server IKEv2 che controllano solo nome utente e password.
- **Certificati attendibili**: i certificati CA del tuo server VPN, installati con la VPN. Per IKEv2 puoi anche impostare l'emittente e il nome attesi del certificato del server.
- **Nome utente e password**: l'utente si autentica anche con un nome utente (variabili consentite) e una password (EAP per IKEv2, XAuth per IPSec). Lascia vuota la password per consentire all'utente di digitarla sul dispositivo.
- **Nome VPN** (mostrato in Impostazioni) e **Si applica a**.

Connessione

- **L’utente si connette in Impostazioni**: la VPN viene installata e l’utente la attiva quando serve.
- **Su richiesta**: il dispositivo connette automaticamente la VPN. Con **tranne che su Wi-Fi attendibili** la VPN non viene usata sulle reti Wi-Fi che elenchi, ad esempio la rete dell’ufficio.
- **Sempre attiva** (IKEv2, solo iPhone e iPad supervisionati): tutto il traffico passa attraverso la VPN su rete cellulare e Wi-Fi e l’utente non può disattivarla. Gli altri dispositivi non ricevono questa VPN. Se la VPN usa un nome utente, la password deve essere impostata nella policy.
- **VPN per app**: solo alcune app usano la VPN. Scegli la VPN per ogni app nella sezione **Gestione app** (campo **VPN** dell’app, non disponibile su Mac) e, facoltativamente, elenca i domini Safari che la usano.

> Prova prima una VPN Sempre attiva o su richiesta su un dispositivo di test: se il server non è raggiungibile, il dispositivo potrebbe non avere alcuna connessione.

Proxy globale, DNS cifrato e filtro dei contenuti web

Queste impostazioni si applicano a tutto il traffico del dispositivo. Attivale con il rispettivo interruttore.

- **Proxy HTTP globale** (iPhone e iPad supervisionati, Mac): tutto il traffico HTTP passa attraverso il proxy, su ogni rete. Imposta il server e la porta (con nome utente e password facoltativi) oppure una configurazione automatica (URL del file PAC, oppure vuoto per trovarlo sulla rete). **Consenti le pagine di accesso Wi-Fi** permette all’utente di accedere alle reti Wi-Fi pubbliche senza il proxy.
- **DNS cifrato**: il dispositivo risolve i nomi con il tuo server DNS tramite DNS over HTTPS (URL del server) o DNS over TLS (nome del server), facoltativamente solo per alcuni domini. Sui dispositivi supervisionati puoi impedire all’utente di disattivarlo.
- **Filtro dei contenuti web** (iPhone e iPad supervisionati): il filtro integrato in iOS limita i siti web per adulti, con elenchi di siti web sempre consentiti o sempre bloccati, oppure consente solo un elenco di siti web, mostrati come segnalibri in Safari.

> Un proxy o un server DNS errato può lasciare i dispositivi senza connessione: prova prima le impostazioni su un dispositivo di test.

Certificati

Fai clic su **Aggiungi certificato** per installare un certificato da solo: un’autorità di certificazione a cui Safari e le app devono fidarsi, oppure un’identità usata dalle app. I certificati di una rete Wi-Fi o di una VPN non devono essere aggiunti qui.

Opzioni dei certificati

- **Un certificato della pagina Certificati**: lo stesso certificato su ogni dispositivo. Fai clic su **Scegli un certificato** per selezionarlo.
- **Il certificato dell’utente del dispositivo**: ogni dispositivo riceve il certificato client collegato al suo utente. I dispositivi il cui utente non ha un certificato non lo ricevono. Quando colleghi un altro certificato all’utente, i dispositivi vengono aggiornati.
- **Richiesto a un server SCEP**: ogni dispositivo richiede il proprio certificato al tuo server SCEP (ad esempio Microsoft NDES), così la chiave privata non lascia mai il dispositivo. Imposta l’URL del server, la challenge se il server la richiede, il soggetto (ad esempio CN=$EMAIL$), i nomi alternativi, la dimensione della chiave e l’utilizzo della chiave.

> I certificati client (.p12) protetti con la vecchia crittografia RC2 non possono essere installati sui dispositivi Apple. Esportali di nuovo con crittografia 3DES o AES prima di importarli.

Sicurezza

I profili che contengono password o chiavi private vengono inviati solo al dispositivo per cui sono stati creati: il dispositivo deve firmare la sua richiesta con il suo certificato di gestione. Le password e i certificati non vengono scritti nei log.

Revision #7
Created 2026-11-10 15:12:52 UTC by Admin
Updated 2026-11-12 09:52:35 UTC by Admin