Rede

A seção **Rede** do Editor de Política da Apple configura redes Wi-Fi e VPNs nos dispositivos, instala certificados e restringe recursos de conectividade como AirDrop e Bluetooth. Cada rede Wi-Fi, VPN e certificado é instalado como seu próprio perfil de configuração, que você pode ver no dispositivo em **Configurações > Geral > VPN & Gerenciamento de Dispositivos** (Mac: **Ajustes do Sistema > Geral > Gerenciamento de Dispositivos**, ou **Privacidade e Segurança > Perfis** no macOS 13 e 14) e no painel **Perfis, certificados e segurança** da página do dispositivo.

> Os certificados são obtidos na página **Certificados**: importe-os lá primeiro. A política apenas se refere a eles, então um certificado nunca é copiado na política.

Restrições

- **Permitir AirDrop**
- **Permitir solicitações recebidas do AirPlay**
- **Permitir modificação do Bluetooth**
- **Permitir modificação do Compartilhamento Bluetooth**
- **Permitir acesso a unidades de rede no app Arquivos**
- **Permitir modificação do Compartilhamento de Internet**
- **Permitir cache de conteúdo**
- **Permitir compartilhamento de arquivos do iTunes**

Redes Wi-Fi

Clique em **Adicionar rede Wi-Fi** e preencha:

- **Nome da rede (SSID)**: o nome da rede, com até 32 caracteres.
- **Segurança**: nenhuma (rede aberta), WEP, WPA ou WPA2, WPA2 ou WPA3, somente WPA3, ou qualquer uma.
- **Senha**: a senha de uma rede pessoal.
- **Entrar automaticamente** e **Rede oculta** (para redes que não transmitem o nome).
- **Proxy**: nenhum, manual (servidor e porta) ou automático (uma URL de arquivo PAC, ou vazio para encontrar as configurações na rede com WPAD).
- **Nome do perfil** (opcional) e **Aplica-se a**, para limitar a rede a alguns tipos de dispositivo.

Redes corporativas (802.1X)

Ative **Corporativa (802.1X)** quando os usuários se autenticam com as próprias credenciais ou um certificado em vez de uma senha compartilhada.

- **Autenticação**: PEAP, TTLS (com a autenticação interna dele, por exemplo MSCHAPv2) ou TLS (somente certificado).
- **Credenciais do usuário do dispositivo**: cada dispositivo usa a identidade EAP, a identidade anônima e a senha do usuário dele, definidas na página Usuários. Dispositivos sem um usuário não recebem a rede.
- **Identidade**, **Identidade anônima** e **Senha**: iguais para todos os dispositivos. A identidade pode conter as variáveis $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ e $UDID$. Deixe a senha vazia para permitir que o usuário a digite no dispositivo.
- **Certificado de identidade**: o certificado de cliente que o dispositivo apresenta (obrigatório para TLS). Consulte as opções de certificado abaixo.
- **Certificados confiáveis**: os certificados da CA que emitiram o certificado do seu servidor RADIUS. Eles são instalados com a rede.
- **Nomes de servidor confiáveis**: os nomes dos certificados do servidor RADIUS que os dispositivos aceitam, por exemplo radius.example.com ou *.example.com.

VPN

Clique em **Adicionar VPN** para configurar uma VPN IKEv2 ou Cisco IPSec, integrada ao iOS, iPadOS e macOS (não é necessário um app de VPN).

- **Tipo** e **Servidor**. Para IKEv2, também o **Identificador remoto** (a identidade do servidor, vazio significa o endereço do servidor) e o **Identificador local**, que pode conter as variáveis $EMAIL$, $USERNAME$, $FULLNAME$, $SERIAL$ e $UDID$.
- **Autenticação** do dispositivo: um certificado (da página Certificados, o certificado do usuário do dispositivo, ou solicitado a um servidor SCEP), um segredo compartilhado (com o nome do grupo opcional para IPSec), ou nenhuma para servidores IKEv2 que verificam apenas o nome de usuário e a senha.
- **Certificados confiáveis**: os certificados da CA do seu servidor VPN, instalados com a VPN. Para IKEv2, você também pode definir o emissor e o nome esperados do certificado do servidor.
- **Nome de usuário e senha**: o usuário também se autentica com um nome de usuário (variáveis permitidas) e uma senha (EAP para IKEv2, XAuth para IPSec). Deixe a senha vazia para permitir que o usuário a digite no dispositivo.
- **Nome da VPN** (mostrado em Ajustes) e **Aplica-se a**.

Conexão

- **O usuário se conecta em Ajustes**: a VPN é instalada e o usuário a ativa quando precisar.
- **Sob demanda**: o dispositivo conecta a VPN automaticamente. Com **exceto em Wi-Fi confiável**, a VPN não é usada nas redes Wi-Fi que você listar, por exemplo a rede do escritório.
- **Sempre ativa** (IKEv2, somente iPhone e iPad supervisionados): todo o tráfego passa pela VPN em celular e Wi-Fi e o usuário não pode desativá-la. Outros dispositivos não recebem esta VPN. Se a VPN usar um nome de usuário, a senha deve ser definida na política.
- **VPN por app**: somente alguns apps usam a VPN. Escolha a VPN de cada app na seção **Gerenciamento de apps** (campo **VPN** do app, não disponível no Mac), e opcionalmente liste domínios do Safari que a usam.

> Teste uma VPN sempre ativa ou sob demanda em um dispositivo de teste primeiro: se o servidor não puder ser alcançado, o dispositivo pode ficar sem conexão.

Proxy global, DNS criptografado e filtro de conteúdo da web

Essas configurações se aplicam a todo o tráfego do dispositivo. Ative-as com o alternador correspondente.

- **Proxy HTTP global** (iPhone e iPad supervisionados, Mac): todo o tráfego HTTP passa pelo proxy, em todas as redes. Defina o servidor e a porta (com um nome de usuário e senha opcionais) ou uma configuração automática (URL de arquivo PAC, ou vazio para encontrá-la na rede). **Permitir páginas de login de Wi-Fi** permite que o usuário entre em redes Wi-Fi públicas sem o proxy.
- **DNS criptografado**: o dispositivo resolve nomes com o seu servidor DNS por DNS over HTTPS (URL do servidor) ou DNS over TLS (nome do servidor), opcionalmente somente para alguns domínios. Em dispositivos supervisionados, você pode impedir que o usuário o desative.
- **Filtro de conteúdo da web** (iPhone e iPad supervisionados): o filtro integrado ao iOS limita sites adultos, com listas de sites sempre permitidos ou sempre bloqueados, ou permite somente uma lista de sites, mostrada como favoritos no Safari.

> Um proxy ou servidor DNS errado pode deixar os dispositivos sem conexão: teste as configurações em um dispositivo de teste primeiro.

Certificados

Clique em **Adicionar certificado** para instalar um certificado de forma independente: uma autoridade de certificação em que o Safari e os apps devem confiar, ou uma identidade usada por apps. Os certificados de uma rede Wi-Fi ou de uma VPN não precisam ser adicionados aqui.

Opções de certificado

- **Um certificado da página Certificados**: o mesmo certificado em todos os dispositivos. Clique em **Escolher um certificado** para escolhê-lo.
- **O certificado do usuário do dispositivo**: cada dispositivo recebe o certificado de cliente vinculado ao usuário dele. Dispositivos cujo usuário não tem um certificado não o recebem. Quando você vincula outro certificado ao usuário, os dispositivos são atualizados.
- **Solicitado a um servidor SCEP**: cada dispositivo solicita o próprio certificado ao seu servidor SCEP (por exemplo Microsoft NDES), então a chave privada nunca sai do dispositivo. Defina a URL do servidor, o desafio se o servidor exigir, o assunto (por exemplo CN=$EMAIL$), os nomes alternativos, o tamanho da chave e o uso da chave.

> Certificados de cliente (.p12) protegidos com a antiga criptografia RC2 não podem ser instalados em dispositivos Apple. Exporte-os novamente com criptografia 3DES ou AES antes de importá-los.

Segurança

Perfis que contêm senhas ou chaves privadas são enviados somente ao dispositivo para o qual foram criados: o dispositivo deve assinar a solicitação com o certificado de gerenciamento dele. Senhas e certificados não são gravados nos registros.

Revision #6
Created 2026-11-10 15:17:43 UTC by Admin
Updated 2026-11-12 09:57:21 UTC by Admin