Client VPN OS Configuration

Client VPN OS Configuration

This article outlines instructions to configure a client VPN connection on commonly used operating systems.

Learn more with these free online training courses on the Meraki Learning Hub:

- Implementing Remote Access with IPsec Client VPN

Sign in with your Cisco SSO or create a free account to start training.

Android

> **Note**: Android devices running Android 12 and above do not support Layer 2 Tunneling Protocol/Internet Protocol Security (L2TP/IPsec) VPNs. Devices with existing configurations will continue to work. Client VPN connection cannot be configured on new devices.
>
> To check the Android version of a device, see Check & update your Android version in Google Support.

To configure an Android device to connect to the client VPN, see Connect to a virtual private network (VPN) on Android in Google Support.

The following VPN information is needed to complete the setup:

- **Name**: This can be anything you want to name the connection, for example, "*Work VPN*"
- **Type**: Select **L2TP/IPSEC PSK**
- **Server address**: Enter the hostname (for example: abcd.com) or the active WAN IP (for example: a.b.c.d)
  - Hostname is preferred to improve reliability during WAN failover
  - This information is located in the Meraki dashboard under **Security & SD-WAN** > **Monitor** > **Appliance status**
- **IPSec pre-shared key**: Enter the pre-shared key that admin created in **Security & SD-WAN > Configure > Client VPN**

Chrome OS

To configure a Chrome OS device to connect to client VPN, see Set up virtual private networks (VPNs) in Google Support.

The following VPN information is needed to complete the setup:

- **Service name**: This can be anything you want to name this connection, for example, "*Work VPN*"
- **Provider type**: Select **L2TP/IPsec**
- **Server hostname**: Enter the hostname (for example: abcd.com) or the active WAN IP (for example: a.b.c.d)
  - Hostname is preferred to improve reliability during WAN failover
  - This information is located in the Meraki dashboard under **Security & SD-WAN** > **Monitor** > **Appliance status**
- **Authentication type**: Select **Pre-shared key**
- **Username**: Credentials for connecting to VPN—if using Meraki authentication, this will be an email address
- **Password**: Credentials for connecting to VPN
- **Pre-shared key**: Enter the shared secret that admin created in **Security & SD-WAN** > **Configure** > **Client VPN**

iOS

To configure an iOS device to connect to the client VPN, follow these steps:

1. Navigate to **Settings** > **General** > **VPN & Device Management** > **VPN** > **Add VPN Configuration**
2. **Type**: Set to L2TP
3. **Description**: This can be anything you want to name this connection, for example, "*Work VPN*"
4. **Server**: Enter the hostname (for example: abcd.com) or the active WAN IP (for example: a.b.c.d)
   - Hostname is preferred to improve reliability during WAN failover
   - This information is located in the Meraki dashboard under **Security & SD-WAN** > **Monitor** > **Appliance status**
5. **Account**: Enter the username
6. **Password**: Enter if desired
   - If the password is left blank, it will need to be entered each time the device attempts to connect to the client VPN

7. **Secret**: Enter the shared secret that admin created in **Security & SD-WAN** > **Configure** > **Client VPN**
8. Ensure that **Send All Traffic** is set to on
9. Save the configuration

macOS

> The following authentication methods are supported:
>
> **User authentication:** Active Directory (AD), RADIUS, or Meraki-hosted authentication
> **Machine authentication:** Preshared keys (for example: shared secret)
>
> When using Meraki-hosted authentication, the VPN account and username setting is the user email address entered in the Meraki dashboard.

To configure a macOS device to connect to client VPN, see Set up a VPN connection on Mac in Apple Support.

The following VPN information is needed:

- **Display Name**: This can be anything you want to name this connection, for example, "*Work VPN*"
- **Server Address:** Enter the hostname (for example: abcd.com) or the active WAN IP (for example: a.b.c.d)
  - Hostname is preferred to improve reliability during WAN failover
  - This information is located in the Meraki dashboard under **Security & SD-WAN** > **Monitor** > **Appliance status**
- **Account Name:** Enter the account name of the user (based on AD, RADIUS, or Meraki cloud authentication)
- **Password:** User password (based on AD, RADIUS or Meraki cloud authentication)
- **Machine Authentication > Shared Secret:** Enter the shared secret that admin created in **Security & SD-WAN** > **Configure** > **Client VPN**

> Ensure that the MACs network adapter service order includes the VPN interface as the first item (in the list) otherwise all the traffic will not leave on the Client VPN tunnel. For more reference, see Change the order of the network services your Mac uses in Apple support.

Windows

> The following authentication methods are supported:
> User authentication: Active Directory (AD), RADIUS, or Meraki-hosted authentication
> Machine authentication: Pre-shared keys
>
> When using Meraki-hosted authentication, the VPN account and username setting is the user email address entered in the Meraki dashboard.

To configure a **Windows 10 or Windows 11** device to connect to client VPN, see Connect to a VPN in Windows in Microsoft Support page.

The following VPN information is needed to complete the setup:

- In the **Settings app** on your Windows device, select **Network & internet > VPN > Add VPN**.
  - **VPN provider**: Set to Windows (built-in)
  - **Connection name**: This can be anything you want to name this connection, for example, "Work VPN"
  - **Server name or address**: Enter the hostname (for example: abcd.com) or the active WAN IP (for example: a.b.c.d)
    - Hostname is preferred to improve reliability during WAN failover
    - This information is located in the Meraki dashboard under **Security & SD-WAN** > **Monitor** > **Appliance status**
  - **VPN type**: Select **L2TP/IPsec with pre-shared key**
  - **User name** and **Password**: optional

Windows-build-in-Client-VPN-config.jpg

After the VPN connection has been created, set the Authentication protocols:

1. Choose the VPN connection and then select **Advanced options** > **More VPN properties > Edit > Security Tab**.
   - **Note:** Alternatively, run **ncpa.cpl** directly from Search or Command prompt to quickly access your VPN adapters.
2. In the **Security** tab, under **Data encryption >** Select **Require encryption (disconnect if sever declines)**
3. Under **Authentication >** Select **Allow these protocols** > Tick the box **Unencrypted password (PAP)**
4. Verify that no other protocols are selected

Windows-build-in-Client-VPN-Security-Tab-Propoerties-config.jpg

>

> Passwords sent over an IPsec tunnel between the client device and the MX are always encrypted, even when using PAP authentication protocols. The password is fully secure and never sent in clear text over the WAN or the LAN.

Linux

To configure a Red Hat Linux device to connect to client VPN, see Configuring a VPN connection in Red Hat Documentation.

To configure an Ubuntu Linux device to connect to client VPN, see Connect to a VPN in Ubuntu Documentation.

The following packages, and their dependencies, are minimum requirements for Linux:

- xl2tpd to implement L2TP
- strongswan or libreswan to implement IPSec

GUI management of the connection requires the network-manager-l2tp-gnome VPN plugin.