Client VPN OS Configuration

This article outlines instructions to configure a client VPN connection on commonly-used operating systems. For more information about client VPN, please refer to our documentation.

Android

To configure an Android device to connect to the Client VPN, follow these steps:

- Navigate to Settings -> Wireless & Networks -> VPN
- Click the Plus Icon to add an additional VPN profile

Enter a VPN Name for the connection.

For the Type drop-down select L2TP/IPSEC PSK VPN

Enter the public IP (found in Dashboard, under Security appliance > Monitor > Appliance status > Uplink) of the MX device under Server address.

Enter the pre-shared key under IPSec pre-shared key.
• Save the configuration.

You will be prompted for credentials when you connect.
Chrome OS

Chrome OS based devices can be configured to connect to the Client VPN feature on MX Security Appliances. This allows remote users to securely connect to the LAN. This article will cover how to configure the VPN connection on a Chrome OS device. For more information on how to setup the Client VPN feature of the MX or how to connect from other operating systems, please visit the [MX documentation](#).

1. If you haven't already, sign in to your Chromebook.
2. Click the status area at the bottom of your screen, where your account picture is located.
3. Select **Settings**.
4. In the "Internet connection" section, click **Add connection**.
5. Select **Add private network**.
6. In the box that appears, fill in the information below:
   a. **Server hostname**: The DNS name or IP address of the MX to which the client should be connecting.
   b. **Service name**: This can be anything you want to name this connection, for example, "Work VPN."
   c. **Provider type**: Select L2TP/IPsec + Pre-shared key.
   d. **Pre-shared key**: This will be the Secret created when configuring the Client VPN on the MX.
   e. **Username** credentials for connecting to VPN. If using Meraki authentication, this will be an e-mail address.
   f. **Password** credentials for connecting to VPN.
7. Click **Connect**.

For more information regarding the configuration of VPN connections in Chrome OS, visit the [Google Support page](#).
To configure an iOS device to connect to the Client VPN, follow these steps:

1. Navigate to **Settings** -> **General** -> **VPN** -> **Add VPN Configuration** ...
2. On the **Add Configuration** screen that appears, set the **Type** to L2TP.
3. Enter a **Description** for the VPN connection.
4. Enter the public IP of the MX device (found in Dashboard, under **Security appliance** > **Monitor** > **Appliance status** > **Uplink**) as the **Server**.
5. Under **Account**, enter the username to be used to connect to the Client VPN.
6. Enter the **Password** 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. Enter the VPN **Secret**.
8. Ensure that **Send All Traffic** is set to On.
9. Save the configuration.

**Note:** Apple has removed the native support and pass-through capabilities of PPTP VPN connections through iOS10+ devices. The Meraki Client VPN utilizes a more secure L2TP connection and can still successfully connect through a mobile hotspot broadcast from an iOS device.
Add Configuration

Type: L2TP

Description: Required
Server: Required
Account: Required
RSA SecurID: [off]
Password: Ask Every Time
Secret: Required
Send All Traffic: [on]

PROXY
- Off
- Manual
- Auto
The instructions below are tested on Mac OS 10.7.3 (Lion).

Open **System Preferences > Network** from Mac applications menu. Click the "+" button to create a new service, then select VPN as the interface type, and choose **L2TP over IPsec** from the pull-down menu.

- **Server Address**: Enter the public IP address (found in Dashboard, under **Security appliance > Monitor > Appliance status > Uplink**).
- **Account Name**: Enter the account name of the user (based on AD, RADIUS or Meraki Hosted authentication).

Click **Authentication Settings** and provide the following information:

Currently only the following authentication mechanisms are supported:

- User authentication: Active Directory (AD), RADIUS, or Meraki hosted authentication.
- Machine authentication: Preshared keys (a.k.a., shared secret).

When using Meraki hosted authentication, **VPN account/user name setting** on client devices (e.g., PC or Mac) **is the user email address** entered in the Dashboard.
- **User Authentication > Password**: User password (based on AD, RADIUS or Meraki Hosted authentication).
- **Machine Authentication > Shared Secret**: The preshared key that you’ve created in Configure > Client VPN settings for the MX.

![User Authentication and Machine Authentication configurations](image)

Click **OK** to go back to the main VPN settings page, then click **Advanced** and enable the **Send all traffic over VPN connection** option.
The VPN connectivity will not be established if you don't enable the **Send all traffic over VPN connection** option!

**Windows 7**

Currently only the following authentication mechanisms are supported:

- User authentication: Active Directory (AD), RADIUS, or Meraki hosted authentication.
- Machine authentication: Preshared keys (a.k.a., shared secret).

When using Meraki hosted authentication, **VPN account/user name setting** on client devices (e.g., PC or Mac).
is the user email address entered in the Dashboard.

Open Start Menu > Control Panel, click on Network and Internet, click on View network status and tasks.

In the Set up a connection or network pop-up window, choose Connect to a workplace (Set up a dial-up or VPN connection to your workplace).
Choose **Use my Internet connection (VPN)**, in the **Connect to a workspace** dialog window.
In the **Connect to a Workplace** dialog box, enter:

- **Internet address**: Enter the public IP address (found in Dashboard, under **Security appliance > Monitor > Appliance status > Uplink**) for the MX appliance.
- **Destination name**: Optionally enter a name for the VPN connection.
Click Next. In the next dialog window, enter the user credentials, and click Create.
Close the VPN connection wizard.
Go to Networking and Sharing Center and click **Change Adapter Settings**

![Network and Sharing Center](image)

- Control Panel Home
- Change adapter settings
- Change advanced sharing settings

**View your basic network information and set up**

- WIN7-DAGHAN (This computer)
- Network

View your active networks

**Network 13**

Work network

Change your networking settings

- Set up a new connection or network
- Set up a wireless, broadband, dial-up, ad hoc...
In Network Connections window, right click on the new VPN connection settings and choose **Properties**

In the **General** tab, verify that the public IP address or the URL of the MX appliance.
In the **Options** tab, make sure "**Include Windows logon domain**" is unchecked.
In the "Security" tab, choose "Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)". Then, check "Unencrypted password (PAP)" and uncheck all other options.

Despite the name "Unencrypted PAP", the client's password is sent **encrypted** over an IPsec tunnel between the client device and the MX. The password is fully secure and never sent in clear text over either the WAN or the LAN.
Click on "Advanced settings".
In **Advanced Properties** dialog box, choose "Use preshared key for authentication" and enter the same key you used for the client VPN settings in the Dashboard. Note: if you are enabling client VPN for your employees, you will need to distribute this key.

Click **OK**.
Back at the **Network Connections** window, right-click on the **VPN connection** and click **Connect**.

Verify your user name and click **Connect**.
Currently only the following authentication mechanisms are supported:

- User authentication: Active Directory (AD), RADIUS, or Meraki hosted authentication.
- Machine authentication: Preshared keys (a.k.a., shared secret).

When using Meraki hosted authentication, **VPN account/user name setting** on client devices (e.g., PC or Mac) **is the user email address** entered in the Dashboard.

Open **Start Menu > Network and Sharing Center** and click **Settings**.
In the **Network and Sharing Center**, click **Set up a new connection or network**.
In the **Set Up a Connection or Network** pop-up window, choose **Connect to a workplace**.
(Set up a dial-up or VPN connection to your workplace).
Choose **Use my Internet connection (VPN)**, in the **Connect to a Workspace** dialog window.
In the **Connect to a Workplace** dialog box, enter:

- **Internet address**: Enter the public IP address (found in Dashboard, under Security appliance > Monitor > Appliance status > Uplink) for the MX appliance.
- **Destination name**: Optionally enter a name for the VPN connection.

Click **Create**.
Go back to **Network and Sharing Center** and click **Change Adapter Settings**.

- **Control Panel Home**
- **Change adapter settings**
- **Change advanced sharing settings**

**View your basic network information**

- **View your active networks**
- **Meraki-Corp**
  - Public network

**Change your networking settings**

- **Set up a new connection or network**
  - Set up a broadband, dial-up, or VPN
In the **Networks Connections** window, right click on the **VPN connection** icon and choose **Properties**.

In the **General** tab, verify that the public IP address or the URL of the MX appliance.
In the "Security" tab, choose "Layer 2 Tunneling Protocol with IPsec (L2TP/IPSec)". Then, check "Unencrypted password (PAP)", and uncheck all other options.

Despite the name "Unencrypted PAP", the client's password is sent encrypted over an IPsec tunnel between the client device and the MX. The password is fully secure and never sent in clear text over either the WAN or the LAN.
Click on "Advanced settings".
In Advanced Properties dialog box, choose "Use preshared key for authentication" and enter the same key you used for the client VPN settings in the Dashboard. Note: if you are enabling client VPN for your employees, you will need to distribute this key.
Click OK.
Back at the Network Connections window, right-click on the VPN connection and click Connect / Disconnect.
Find your VPN profile and click **Connect**.
Enter your user name and password. 
Click OK.
Currently only the following authentication mechanisms are supported:

- User authentication: Active Directory (AD), RADIUS, or Meraki hosted authentication.
- Machine authentication: Preshared keys (a.k.a., shared secret).

When using Meraki hosted authentication, **VPN account/user name setting** on client devices (e.g., PC or Mac) is the user email address entered in the Dashboard.

Open **Start Menu > Search “VPN” > Click Change virtual private networks (VPN)**
From the VPN settings page, click **Add a VPN connection**.
In the Add a VPN connection dialog:

- Set the **VPN provider** to Windows (built-in)
- Provide a **Connection name** for the VPN connection
- Specify a public IP address (found in Dashboard, under Security appliance > Monitor > Appliance status > Uplink) or hostname for the **Server name or address**
- Select L2TP/IPsec with pre-shared key for the **VPN type**
- Provide a **User name** and **Password** (optional)
After the VPN connection has been created, click Change adapter options under Related settings.
Right click on the **VPN Connection** from the list of adapters and click **Properties**.
In the **Security** tab, select "**Require encryption (disconnect if sever declines)**" under **Data encryption**. Then, select **Allow these protocols** under **Authentication**. From the list of protocols, check "**Unencrypted password (PAP)**", and uncheck all other options.

Despite the name "Unencrypted PAP", the client's password is sent **encrypted** over an IPsec tunnel between the client device and the MX. The password is fully secure and never sent in clear text over either the WAN or the LAN.
Click on "Advanced settings"

In Advanced Properties dialog box, choose "Use preshared key for authentication" and enter the same key you used for the client VPN settings in the Dashboard. Note: if you are enabling client VPN for your employees, you will need to distribute this key.
Back at the **Network Connections** window, right-click on the **VPN connection** and click **Connect / Disconnect**.

Find your VPN profile and click **Connect**.
Enter your user name and password.
Click OK.
Open **Start Menu > Control Panel**, click on **Network Connections**.

Windows XP

Currently only the following authentication mechanisms are supported:

- User authentication: Active Directory (AD), RADIUS, or Meraki hosted authentication.
- Machine authentication: Preshared keys (a.k.a., shared secret).

When using Meraki hosted authentication, **use the email address** for VPN account / user name.
In the **Network Tasks section**, click on **Create a new connection**.
Choose **Connect to the network at my workplace**, in the **New Connection Wizard** window.

Choose **Virtual Private Network connection** in the next section.
Create the following connection:

- **Dial-up connection**
  Connect using a modem and a regular phone line or an Integrated Services Digital Network (ISDN) phone line.

- **Virtual Private Network connection**
  Connect to the network using a virtual private network (VPN) connection over the Internet.

Then, give a name for this connection:
Enter the public IP address for the MX appliance (found in Dashboard, under Security appliance > Monitor > Appliance status > Uplink):

Company Name

Ilkarem VPN

For example, you could type the name of your workplace or the name of a server you will connect to.
In the Connect <Connection Name> box, click on Properties.
In the **General** tab, verify that the public IP address or the URL of the MX appliance.

![Ikarem VPN Properties](image)

In the **Options** tab, make sure "**Include Windows logon domain**" is unchecked.
In the **Security** tab, choose **Advanced (custom settings)**. Click **Settings**
In **Advanced Security Settings** page, select **Optional encryption** from the **Data encryption** pull-down menu. Choose **Unencrypted password (PAP)** from the **Allow these protocols** options and uncheck everything else.

Despite the name "Unencrypted PAP", the client's password is sent **encrypted** over an IPsec tunnel between the client device and the MX. The password is fully secure and never sent in clear text over either the WAN or the LAN.
Back on the Security tab, click IPSec Settings...
Check "Use pre-shared key for authentication" and enter the same key you used for the client VPN settings in the Dashboard. Note: if you are enabling client VPN for your employees, you will need to distribute this key. Click OK.

In Networking tab, choose L2TP IPSec VPN from the Type of VPN options.
Back at the Network Connections window, right-click on the VPN connection and click Connect.
Verify your user name and click Connect
Linux

Since Client VPN uses the L2TP over IPsec standard, any Linux client that properly supports this standard should suffice. Please note that newer versions of Ubuntu do not ship with a VPN client that supports L2TP/IP, and will therefore require a 3rd party VPN client that supports the protocol.

Note: The xl2tp package does not send user credentials properly to the MX when using Meraki Cloud Controller authentication, and this causes the authentication request to fail. Active Directory or RADIUS authentication can be used instead for successful authentication.