Troubleshooting Client VPN

This article outlines troubleshooting methods for Client VPN connectivity issues, primarily for Windows-based clients, including a list of common errors. This article also outlines some common issues and solutions for accessing resources over Client VPN.

Configuration Requirements

Client Device

Please reference our documentation for instructions on Configuring Client VPN on the Client Device.

Encryption Method

Client VPN uses the L2TP/IP protocol, with 3DES and SHA1 respectively as the encryption and hashing algorithms. As a best practice, the shared secret should not contain any special characters at the beginning or end.

MX-Z Security Appliance

Please see the following link to configure the MX-Z for Client VPN. If the MX-Z sits behind another NAT device or firewall, please make sure that the following UDP ports are forwarded/allowed to the MX-Z:

- UDP 500 (IKE)
- UDP 4500 (IPSec NAT-T)

Note: Since the MX is the device communicating from UDP 500/4500, those ports need to be forwarded on any devices upstream of the MX, not on the MX itself.

Verifying a Successful Connection

There are three primary ways to determine if the Client VPN connection is successfully connected to an MX:

- Check the device for connection status using common network utilities (this will vary depending on the operating system being used). The Event Log contains entries each time a client connects or disconnects from Client VPN. These logs can be viewed from Monitor > Event log. Deselect all event categories except VPN followed by clicking on the Search button. Client VPN logs will have one of two Event types: VPN client connected or VPN client disconnected. Here is an example set of log messages that shows a client connecting and then disconnecting from Client VPN:
The client list can also be used to see if a client is currently connected to Client VPN. Browse to Monitor > Clients in the Dashboard. Add an additional column by clicking on the + button and select MAC address. Clients can then be filtered by 'N/A (Client VPN)' as the MAC address.

Common Connection Issues

This section of the article will outline common configuration errors and the resulting Event log message/client error message.

Note: If your Windows device is failing to connect to the VPN, it is recommended that you verify the VPN configuration on your device to ensure it matches the Client VPN OS Configuration requirements.

Finding Error Codes in Windows

If a Client VPN connection is failing to establish from a Windows device but no error message appeared on the screen, the Event Viewer can be used to find an error code associated with the failed connection:

1. Press the Windows key and type in "Event Viewer," then click on Event Viewer in the search results.
2. In Event Viewer, navigate to Windows Logs > Application.
3. A Client VPN connection failure should show up as an Error event type. Clicking on the event will show the associated error code:

This Microsoft knowledge base article lists error codes and their meanings.
Windows Error 789

Example event log entries:


This issue may also result in no event log messages, if the client's traffic doesn't successfully reach the MX's WAN interface.

Possible causes and solutions:

- **Incorrect secret key (pre-shared key in Windows)**
  
  *Solution:* Ensure that the shared secret is configured correctly on the client machine. It must match between the MX and the client. More information about setting the shared secret can be found in the links at the top of the page.

- **Firewall blocking VPN traffic to MX**
  
  *Solution:* Ensure UDP ports 500 (IKE) and 4500 (IPsec NAT-T) are being forwarded to the MX and not blocked. If traffic cannot reach the MX on these ports, the connection will timeout and fail.

- **IKE and AuthIP IPsec Keying Modules disabled (Windows only)**
  
  *Solution:* This occurs most often when 3rd party VPN software has been installed and disables the IKEEXT service. This can be re-enabled by navigating in Windows to **Control Panel > Administrative Tools > Services**. Find the service named "IKE and AuthIP IPsec Keying Modules" and open it. Change the **Startup type** to "Automatic". If this automatically reverts to "Disabled" or fails to start, it may be necessary to remove the 3rd party VPN software:
Windows Error 691

Example event log entries:

- Jul 2 14:00:40 VPN msg: not matched
- Jul 2 14:00:40 VPN msg: ISAKMP-SA established 82.35.46.78[4500]-174.45.35.220[4500]
  spi:b74e92b3b5360c16:ce602504804696a9

Possible causes and solutions:

- **Invalid user credentials**
  *Solution:* Confirm user credentials are correct. When using Meraki authentication, usernames should be in e-mail format (ex. user@example.com). When using AD or RADIUS authentication, be sure to enter the username in a format that will be recognized by the server, including the domain if needed (ex. DOMAIN\user).

- **User not authorized**
  *Solution:* If using Meraki Authentication, ensure that the user has been authorized to connect to the VPN.

- **No certificate on AD server**
  *Solution:* If using Active Directory authentication with Client VPN, make sure the AD server has a valid certificate for TLS.

- **Incorrect DNS name resolution from the MX’s upstream DNS server**
  *Solution:* If the MX is configured with an ISP DNS server, change this to a Non-ISP public DNS server such as Google 8.8.8.8

  Alternatively, this message can be caused when a mismatch of pre-shared secrets between a RADIUS server and MX results in bad encryption of the password. Test this by changing the pre-shared secret in Dashboard and for the RADIUS client on the server to something simple, such as "Meraki". If the error disappears, verify the secret used is correct on both devices, and simplify the password if needed.

Windows Error 809

If this error appears, the Event Log won't have any relevant logs, as the traffic doesn't reach the MX’s WAN interface.

Possible causes and solutions:

- **Client behind NAT devices**
  *Solution:* Modern Windows devices do not support L2TP/IPsec connections when the Windows computer or VPN server are located behind a NAT. If the Windows VPN client fails with Error 809 when trying to establish a VPN connection to an MX located behind a NAT, add the "AssumeUDPEncapsulationContextOnSendRule" DWORD value to the Windows registry. This DWORD value allows Windows to establish security associations when both the
VPN server and the Windows based VPN client computer are behind NAT devices.

For Windows XP:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\IPSec

RegValue: AssumeUDPEncapsulationContextOnSendRule

Type: DWORD

Data Value: 2

For Windows Vista, 7, 8, 10, and 2008 Server:

HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent

RegValue: AssumeUDPEncapsulationContextOnSendRule

Type: DWORD

Data Value: 2

Note that after creating this key you will need to reboot the machine. For more information, reference the Microsoft Support Knowledge Base.

IPv6 and Mobile Devices

Sometimes the event log will log the message, "msg: unsupported ID type 5." If the identification field value is 5 in the identification payload, this means the payload is carrying the ID type 'ID_IPV6_ADDR.' Meraki does not currently support ID type 5, so an error will appear for these ISAKMP messages. This message will appear for devices that do not have an IPv4 address assigned to them directly, and, as such, are reliant upon an IPv6 transition mechanism like NAT64 to reach the Internet. Such devices will not be able to connect to our Client VPN solution at this time.

Other Problems

Client VPN on Cisco Meraki devices uses the L2TP over IPsec standard, which is supported out-of-the-box by the majority of client devices. If a client is unable to establish a VPN connection, resulting in an error code not discussed in this article, it is recommended to first check for OS-specific documentation about that error. From there, ensure that the
client has been configured correctly, and has a network connection to the MX that is not filtering UDP ports 500 or 4500. It may also be helpful to confirm with a packet capture that the client’s traffic is reaching the MX.

If the MX is in a Warm Spare configuration, the virtual IP for the uplink will have to be used on the client device for the destination server address.

Problems Accessing Network Resources

Occasionally, end users will report that their Client VPN connection is not working, but this does not necessarily mean there is a problem with the Client VPN tunnel; the client may simply be unable to access the network resource(s) they want.

The following sections outline steps to diagnose and fix problems with Client VPN users accessing network resources.

Verify VPN Connectivity

The first troubleshooting step should be verifying that the Client VPN connection is established, and passing traffic to the MX. Active Client VPN users can be seen on the Monitor > Clients page, and can be found by IP address or MAC address (will appear as "N/A (Client VPN)). The event log also records each time a user connects and disconnects to the MX using Client VPN.

Open a command prompt or terminal on the Client VPN device, and ping the LAN IP address of the MX. The LAN IP address can be found on the Configure > Addressing & VLANs page in Dashboard. Choose an MX IP address from a VLAN that is configured to participate in VPN. In this example the MX has a LAN IP address of 192.168.10.1:
Test Connectivity to Resources

At this point it has been verified that the Client VPN session is established and working. From a command prompt or terminal, ping the IP address of the resource the client are trying to use. Keep in mind that the device the client is trying to reach may not respond to ICMP, so it is useful to test pinging other devices over the VPN that do respond to ICMP. Here, connectivity is tested to a file server that has a LAN IP address of 192.168.10.3:

```
C:\Users\Administrator>ping 192.168.10.1
Pinging 192.168.10.1 with 32 bytes of data:
Reply from 192.168.10.1: bytes=32 time<1ms TTL=64
Reply from 192.168.10.1: bytes=32 time<1ms TTL=64
Reply from 192.168.10.1: bytes=32 time<1ms TTL=64
Reply from 192.168.10.1: bytes=32 time<1ms TTL=64
Ping statistics for 192.168.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
```
If the network resource does not respond to ping but the Client VPN tunnel is established, make sure the resource’s firewall allows it to respond to requests from the Client VPN subnet configured under Security appliance > Configure > Client VPN. Note that Microsoft’s Windows firewall typically blocks communication from unknown private subnets by default.

Testing DNS Resolution

Since client VPN users will not be provided with DHCP option 15, make sure any DNS lookups over client VPN specify the FQDN instead of the Short Name.

Most end users will access resources using hostnames, so also test DNS resolution from a command prompt or terminal. In this example, fileserver01 should resolve to 192.168.10.3:

```
C:\Users\Administrator>ping fileserver01
Ping request could not find host fileserver01. Please check the name and try again.
```

Verify the configured DNS servers on the Security Appliance > Configure > Client VPN page. The default configuration sets the clients DNS server to Google public DNS.
Custom DNS nameservers can also be defined for Client VPN users. From the DNS nameservers drop down menu, select 'Specify nameservers...' and enter the IP addresses of the desired internal DNS servers. In this example the IP address of the internal DNS server is 192.168.10.2:

After configuring a custom nameserver, DNS resolution should be functioning properly, so users should be able to reach resources over the Client VPN connection by name:
Additional Checks

End users may report that they are unable to map network shares over the Client VPN tunnel. This could be potentially caused by a layer 7 firewall rule configured to block file sharing. Check the layer 7 firewall rules under Security appliance > Configure > Firewall > Layer 7.

Layer 7

![Firewall rules](image)

Add a layer 7 firewall rule

Also, check any group policies that are applied to the target resource to ensure file sharing is not blocked in the group policy.

Max Sessions per User Account

For security purposes, we limit each user's account to five (5) simultaneous VPN connections to an MX. If you need to change this number, please contact Cisco Meraki Support.