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:

  Jun 27 12:24:38 05:00:08:ab:cd:ef VPN client connected remote_ip: 174.X.X.X, user_id: administrator, local_ip: 192.168.100.239
• 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:

   ![Event Viewer screenshot](image)

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

Windows Error 789

Connection to [redacted] using 'WAN Miniport (L2TP)'

Error 789: The L2TP connection attempt failed because the security layer encountered a processing error during initial negotiations with the remote computer.

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:

![IKE and AuthIP IPsec Keying Modules service](image)

**Windows Error 691**

![Error 691](image)

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 MXs 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

  Value data: 2

  Base: Decimal

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

  HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\PolicyAgent
RegValue: AssumeUDPEncapsulationContextOnSendRule
Type: DWORD
Value data: 2
Base: Decimal

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

Note: Some third party network programs can also Windows Error 809 to occur. SmartByte is one such program known to cause this issue. Disabling the program should resolve the issue and allow the VPN to connect.

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.

Connections to Clients with Dual NICs

Sometimes a user's endpoint utilizing the Client VPN connection may have connection issues to LAN endpoints that have dual NICs. Oftentimes LAN endpoints have both a WAN and a LAN NIC. If these devices are unpingable from an endpoint connected via Client VPN, check the routes on the LAN endpoints. In Windows, open the command prompt and type the command "route print". In macOS, open up the terminal and type the command "netstat -nr". Check that there are gateways set for the LAN routes and not just the WAN.

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.

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:

![VLANs and Routes table]

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

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

C:\Users\Administrator>
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:
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:

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:

**Resolving NetBIOS names over Client VPN**

Windows hosts utilize NetBIOS-based name resolution to locate Windows file and print shares located on other Windows hosts. A NetBIOS name syntax appears as "MYCOMPUTER" and is normally seen in UNC paths such as `\MYCOMPUTER\myfileshare`.

NetBIOS name resolution is a layer 2 broadcast based name discovery protocol. Layer 2 broadcasts do not traverse layer 3 boundaries such as the Client VPN interface on an MX.
WINS is a service that provides centralized name resolution of NetBIOS hostnames. NetBIOS clients register their hostnames on the WINS server and other NetBIOS clients query the WINS server to resolve NetBIOS names.

To allow hosts that utilize NetBIOS names to find network resources over Client VPN, specify the IP address of a WINS server in the Client VPN configuration. This is done using the WINS setting on the Security & SD-WAN > Configure > Client VPN page.

In the screenshot below the specified WINS server is 192.168.1.100:

![Client VPN Configuration](image)

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

<table>
<thead>
<tr>
<th>#</th>
<th>Policy</th>
<th>Application</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Deny</td>
<td>File sharing</td>
<td>All File sharing</td>
</tr>
</tbody>
</table>

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.
Troubleshooting Client VPN with Packet Captures

Client VPN connection issues can be effectively troubleshooting by using packet captures. In this section, best practices and expected behavior in terms of what can be seen in a packet capture will be discussed, and common troubleshooting steps are explained.

Negotiation Process

For any client VPN connection, expect to follow the above process. If the process breaks down at any point, there are some specific things to look for at each step. To start, take a WAN packet capture (on the primary WAN) and follow the guide below.

Understanding the WAN Packet Capture

Filter the WAN pcap for the client's public IP (and ISAKMP/ESP if necessary). Look for the ISAKMP "Next payload" field, which identifies the negotiation step. Start at the first "Security Association" from the client.
Troubleshooting Tips

If no ISAKMP traffic from the client is seen:

- Verify client is connecting to the primary MX WAN IP (VIP for warm spare)
- Verify inbound UDP 500 traffic is not being blocked/dropped upstream
- If the MX is behind a NAT, port forwarding may need to be configured on the upstream device for UDP ports 500 and 4500
- Some OS-specific behaviors may prevent the client machine from generating any traffic. Try to rule out by testing another device type (e.g. a different OS or smart phone)

ISAKMP Phase 1

1. Security Association

   Internet Security Association and Key Management Protocol
   
   Initiator SPI: af22861f0446c5ef
   Responder SPI: 0000000000000000
   Next payload: Security Association (1)

   The initiator sends a Security Association, and the responder sends a Security Association response.

2. Key Exchange

   Internet Security Association and Key Management Protocol
   
   Initiator SPI: af22861f0446c5ef
   Responder SPI: 9808fedf7e9f446a
   Next payload: Key Exchange (4)

   The initiator sends a Key Exchange, and the responder sends a Key Exchange response.

Troubleshooting Tips

- Phase 1 uses UDP 500, Phase 2 uses UDP 500 or UDP 4500 (NAT-T)
- If the MX doesn’t respond to the client, verify:
  - The destination IP and MAC addresses (or VIP for warm spare) are correct
  - Port forwarding isn’t configured on the MX for Port 500
  - Client isn’t trying to connect from behind the same MX
  - Client public IP doesn’t match any non-Meraki VPN peer IPs or another currently connected VPN client
  - Any extra configuration options manually applied to the MX that would override default client VPN settings
- If both sides are continually sending Security Association, this may indicate Port 500 traffic isn’t being received at the client
- If one side is continually sending Key Exchange, this may indicate one of the following problems:
ISAKMP Phase 2

3. Identification

\[\text{Internet Security Association and Key Management Protocol}\]

Initiator SPI: af22861f0446c5ef
Responder SPI: 9808fedf7e9f446a
Next payload: Identification (5)

The initiator sends an Identification, and the responder sends an Identification response.

4. Hash

\[\text{Internet Security Association and Key Management Protocol}\]

Initiator SPI: af22861f0446c5ef
Responder SPI: 9808fedf7e9f446a
Next payload: Hash (8)

The initiator sends a Hash, and the responder sends a Hash response.

Troubleshooting Tips

- Phase 2 uses UDP 4500 (NAT-T) or sometimes UDP 500
- If both sides are continually sending Phase 2 packets, this may indicate one of the following problems:
  - Incorrect encryption/authentication settings
  - Incorrect subnet definition (site-to-site only)
- The client may need to verify their VPN settings. For additional information on specific OS configuration, please follow this article on Client VPN OS Configuration.
  - Windows clients may need to install the registry fix as mentioned above.

ESP

If bi-directional ESP traffic is seen, the tunnel is up.

- User authentication happens at this step.
- The WAN packet capture will no longer be helpful, since everything is encrypted past this point.
- Verify if the authentication is successful between the MX and the authentication server

Troubleshooting Tips

- For Meraki Cloud authentication, verify:
The MX WAN port can resolve meraki.com via DNS, and all required cloud connections are allowed on upstream equipment. For additional explanation of what Meraki requires for cloud communication, please reference the documentation on upstream rules for cloud connectivity.

The account is "Authorized for client VPN" in dashboard, and password is correct.

- For RADIUS authentication, verify:
  - RADIUS authentication packets sent between MX and server must result in ACCESS-ACCEPT for successful connection
  - RADIUS server event log, which is explained in the RADIUS issue resolution guide.

- For Active Directory authentication, verify:
  - Active Directory packets sent between MX and server must show a successful TLS connection
  - Active Directory server event log

- For all authentication types:
  - If no authentication logs or packets are seen, the client may not be sending credentials.
    - The client may need to verify their VPN settings.
    - If the problem exists for only one client, troubleshooting may be required at the client machine (e.g. reboot, check for conflicting software)
  - If authentication is successful, but client still fails to connect, ensure the IP pool for the client VPN subnet is not exhausted.