Configuring RADIUS Authentication with Client VPN

Cisco Meraki can be configured to use a RADIUS server to authenticate remote users against an existing userbase.

This article outlines the configuration requirements for RADIUS-authenticated Client VPN, as well as example RADIUS configuration steps using Microsoft NPS on Windows Server 2008.

RADIUS Configuration

While any RADIUS server can be used, the following configuration requirements are necessary for Client VPN integration:

• RADIUS must be configured to allow PAP (unencrypted authentication)

Note: Communication between the client and the MX will be encapsulated within IPsec, so this does not mean that client communication is unencrypted.

• The MX/Z1’s IP address must be configured on the server as a RADIUS client/authenticator, with a shared secret.

Please refer to your RADIUS server vendor’s documentation for configuration specifics.

Example RADIUS Server Configuration (Windows NPS + AD)

The following example configuration outlines how to configure an existing Windows 2008 server, running Network Policy Server (NPS) alongside Active Directory:

1. Add the MX Security Appliance as a RADIUS client on the NPS server.
2. Configure a RADIUS Connection Request in NPS.
3. Configure a RADIUS Network policy in NPS.

Note: This configuration assumes that NPS is already running on the Windows server. Please refer to Microsoft documentation for assistance in running NPS.

Add MX Security Appliance as RADIUS clients on the NPS server

In order for the MX to act as an authenticator for RADIUS, it must be added as a client on NPS.

1. Open the NPS Server Console by going to Start > Programs > Administrative Tools > Network Policy Server.
2. In the Left pane, expand the RADIUS Clients and Servers option.
3. Right-click the RADIUS Clients option and select New.
4. Enter a Friendly Name for the MX Security Appliance or Z1 Teleworker Gateway RADIUS Client.
5. Enter the IP Address of your MX Security Appliance or Z1 Teleworker Gateway. This IP will differ depending on
where the RADIUS server is located:

- **On a local subnet** - Use the IP address of the MX/Z1 on the subnet shared with the RADIUS server.
- **Over a static route** - Use the IP address of the MX/Z1 on the subnet shared with the next hop.
- **Over VPN** - Use the IP address of the MX/Z1 on the highest-numbered VLAN in VPN.

6. Create and enter a RADIUS **Shared Secret** (make note of this secret - we will need to add this to the Dashboard).

   ![MX Properties](image)

   **Note:** Currently only ASCII characters are supported for RADIUS shared secrets - Unicode characters will not work correctly.

7. Press **OK** when finished.

For additional information or troubleshooting assistance, please refer to [Microsoft documentation](#).

**Configure a RADIUS Connection Request**

1. In the **NPS Server Console**, navigate to **Policies > Connection Request Policies**. Right-click the **Connection Request Policies** folder and select **New**.
2. In the **Connection Request Policy Wizard**, enter a **Policy Name** and select the **Network Access Server Type unspecified** then press **Next**.

3. Click **Add** to add conditions to your policy. Access Request messages will need to meet these conditions to be allowed access.

4. From the list of conditions select the option for **Framed-Protocol**. Press **Add** and place a check next to the **PPP** option then press **Ok**.

5. Click **Add** to add another condition and select the option for **CallingStationID**. Enter **CLIENTVPN** into the text box and press Next.

6. On the next three pages of the wizard we will leave the default settings. Press **Next** on these pages to continue.

7. Review the settings then press **Finish**.

---

**Configure a RADIUS Network Policy**

1. In the Left pane of the **NPS Server Console**, right-click the **Network Policies** option and select New.

2. In the **Network Policy Wizard** enter a **Policy Name** and select the **Network Access Server**
type **unspecified** then press **Next**.

3. Click **Add** to add conditions to your policy.

4. From the list of conditions, select the option for **Windows Groups**. Click **Add Groups** and enter the name of **Windows Group** you would like to give Client VPN permission.

5. Click **Add** to add an additional condition. Select the option for **Framed Protocol**, press add and check the **PPP** option then press **Ok**

6. Click **Add** to add a final condition. Select the option for **CallingStationID**. Enter **CLIENTVPN** into the text box and press **Next**.

7. Leave the default settings on the **Specify Access Permission** page and press **Next**.

8. Deselect all checkboxes and select **Unencrypted authentication (PAP, SPAP)**. An informational box will be displayed press **No** to continue and press **Next**. For security information about using PAP click here.

9. The next 2 pages of the wizard we will leave the default settings. Press **Next** on these pages to continue.

10. Review the settings then press **Finish**.

**Note:** Some versions of Windows Server require that the CallingStationID is omitted. If you are unable to establish connectivity, remove the CallingStationID and leave the field blank.
**Dashboard Configuration**

Once a RADIUS server has been configured appropriately, the following steps outline how to configure Client VPN to use RADIUS:

1. Log onto the **Cisco Meraki Dashboard** and navigate to Configure > Client VPN.
2. Select the option to enable the **Client VPN Server**.
3. Set the **Client VPN Subnet**. This will be a unique IP subnet offered to clients connecting to the MX Security Appliance via a Client VPN connection.
4. Specify the **DNS servers**.
5. Enter a shared **secret** that will be used by the client devices to establish the VPN connection.

**Note:** This is a different value from the RADIUS shared secret.
6. Select RADIUS as the Authentication method.
7. Click the Add a RADIUS Server link.
   a. Enter your RADIUS Host IP Address.
   b. Enter the RADIUS Port that the MX Security Appliance will use to communicate to the NPS server. The default port is 1812.
   c. Enter the RADIUS Shared Secret (established when the MX was added as an authenticator).
8. Click Save changes.

Client Configuration

Installation of additional software is not required on client devices. The Cisco Meraki Client VPN solution uses L2TP over IPsec, which is supported by almost all device’s built-in native clients.

Please refer to our Client VPN documentation for client configuration instructions.

Additional Resources

For additional information about Client VPN, please refer to the following articles:

- Troubleshooting Client VPN
- Integrating Client VPN with Active Directory
- Configuring Split-tunnel Client VPN
- Two-factor Authentication with Client VPN