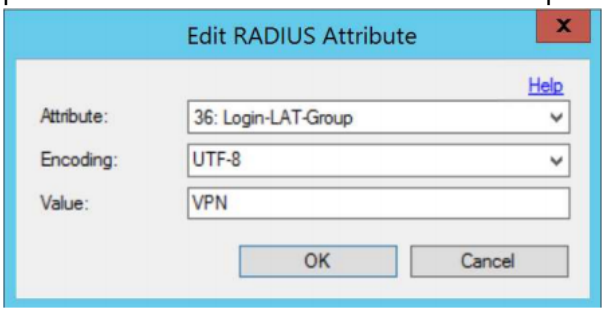
How to Configure the Azure Multi-Factor Authentication Server for VPN Client Authentication

https://campus.barracuda.com/doc/76284326/

Install an Azure Multi-Factor Authentication (MFA) server and configure RADIUS authentication with the CloudGen Firewall as RADIUS client. The Azure MFA server supports only PAP and MSCHAPv2 when acting as a RADIUS server.

Configure the MFA Server

1. Install your MFA server as described in https://docs.microsoft.com/en-gb/azure/multi-factor-authentication/multi-factor-authentication-get-started-server-radius.
2. On the MFA server, configure RADIUS authentication with the CloudGen Firewall as RADIUS client. Ideally, enable **Require Multi-Factor Authentication** user match, but you can also import/create the users manually.
3. In the MFA RADIUS authentication, you can assign a group in one of two ways:
   - To set one manually, go to **Attributes** on the MFA server, add **Login-LAT-Group**, and provide a value. Note that the firewall expects a group provided from the RADIUS server.

     Or:
   - The CloudGen Firewall can take the groups from Active Directory if LDAP servers are available. For more information, see How to Configure MSAD Authentication.

Configure RADIUS Authentication on the CloudGen Firewall

1. On the firewall, go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Authentication Service**.
2. In the left navigation pane, select **RADIUS Authentication**.
3. From the **Configuration Mode** menu on the left, select **Advanced View**.
4. Enable the RADIUS scheme and add a new RADIUS server. Configure the settings with the correct IP address and port to match your MFA server details. For more information, see How to Configure RADIUS Authentication.
   - In combination with manual group setup, leave **Group Attribute** values as default.
   - To allow the firewall to look up the users group via the MSAD scheme:

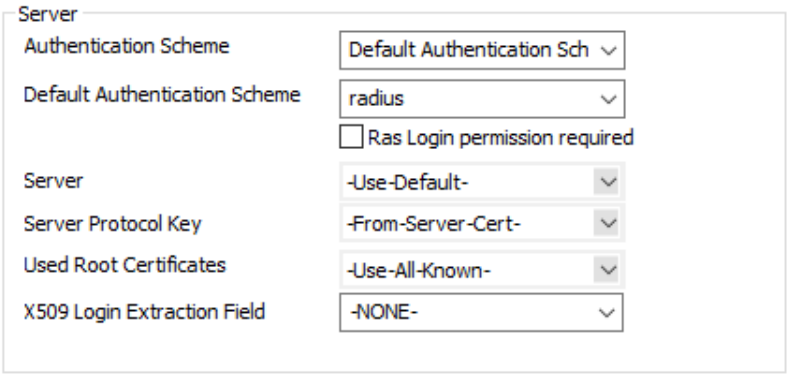
1. Set **User Info Helper Scheme** to **MSAD**.
2. Set **OTP Preserves State** to **Yes**.

5. Go to **Timeouts and Logging**.
6. Increase the **Request Timeout [s]** value from 10 to 130. (You may need to increase this value if your users are struggling to authenticate in time.)
7. Go to **VPN Settings** and **Click here for Server Settings**.
8. Increase the value for **Handshake Timeout (sec)** to 30. (You may need to increase this value if users are struggling to complete authentication in time.)

Server Configuration

Port 443 VPN Listener	Yes
CRL Poll Time (min)	0
Global TOS Copy	Off
Global Replay Window Size, Packets(0...Use Default)	
Use Site to Site Tunnels for Authentication	Yes
Pending Session Limitation	Yes
Prebuild Cookies on Startup	No
Tunnel HA Sync	Yes
Maximum Number of Tunnels	<auto>
Allow Fast Requests	Yes
Handshake Timeout (sec)	30
Allow Dynamic Mesh	Yes
Add VPN Routes to Main Routing Table (Single Routing Table)	No
Allow Concurrent User Sessions	<auto>
Use Perfect Forward Secrecy	Yes
Accounting Information Storage Time (Days)	14

9. Under **VPN > Client to Site**, go to **External CA** and click the **Rules** tab.
10. Select **Click here for options** and select **radius** as the **Authentication Scheme**. If you are not using MSAD as the Group Helper, configure the VPN group attribute value found to match the value you provided.



11. On the VPN clients, you may also need to go into the **Advanced Settings** of the profile and adjust the **Connect Timeout** from the default of 10 to 60 (or greater) to give users enough time to complete the process.
    The more complex the method, the more time users will need.
12. Configure the remaining settings as recommended at Client-to-Site VPN.

MFA Validation Methods

In the Microsoft MFA methods, you can configure the method either globally (**Company Settings**) or per user.

To enable the OTP via text message, you must make two changes:

1. As indicated in the **User-** or **Company Settings**, configure **Text message with One-Way OTP** or **OTP plus PIN**. If you use **OTP plus PIN**, the OTP and the PIN must be entered as one value. For example: 123459876
2. To support OTP via the firewall:
    1. Go to **CONFIGURATION > Configuration Tree > Box > Infrastructure Services > Authentication Service**.

2. In the left navigation pane, select **RADIUS Authentication**.
3. Set **OTP Preserves State** to **Yes**.

Figures

1. mfa01.png
2. mfa02.png
3. mfa03.png
4. mfa04.png
5. mfa_valid.png
6. mfa02.png