

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

<https://campus.barracuda.com/doc/96026120/>

Install a Network Policy Server (NPS) extension for Azure Multi-Factor Authentication (MFA), configure an Azure Multi-Factor Authentication (MFA) server, and set up RADIUS authentication with the CloudGen Firewall as RADIUS client. The Azure MFA server supports only PAP and MSCHAPv2 when acting as a RADIUS server. Multi-Factor Authentication using Time-Based One-Time Passwords (TOTP) requires an Advanced Remote Access subscription. For more information, see [Subscriptions](#).

IMPORTANT:

As of July 2019, Microsoft no longer offers the MFA server for new deployments. New customers should use cloud-based Microsoft Entra ID (former Azure AD) multi-factor authentication (MFA) when requiring multi-factor authentication during sign-in events.

Configure the Network Policy Server (NPS) Extension for Azure MFA

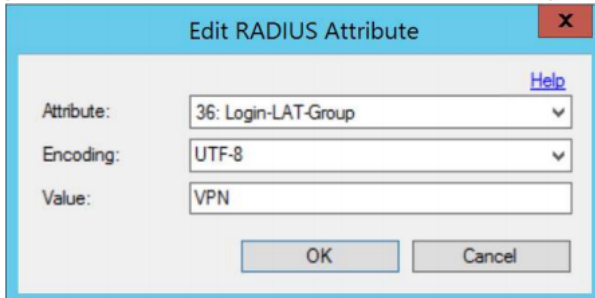
1. Install your NPS extension for Azure MFA. For detailed instructions, see: <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-nps-extension>.
2. Configure the NPS server:
 1. Add a new RADIUS client with the IP address of the Barracuda CloudGen Firewall.
 2. Create a suitable **Shared Secret**.
 3. In the **Advanced** settings, set **Vendor** to **RADIUS Standard**.
3. Configure connection and network policies as required.
 - For Barracuda VPN Client support, you must enable **Unencrypted authentication** between the Firewall and the NPS.
 - For Microsoft IPSECv2 clients, you can use a suitable Microsoft method such as MS-CHAP-v2 or EAP-MSCHAP-v2.
4. (Optional) Lock the **Connection Request Policy** to the Barracuda IP address using the **NAS IPv4 Address** condition.
5. (Optional) Use **Settings / Attributes** to translate an external and internal domain if necessary, or follow the advanced instructions for the NPS extension.

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-g>

[et-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. Click **Lock**.
4. From the **Configuration Mode** menu on the left, select **Advanced View**.
5. 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. Enter the **NAS IP Address** if you wish to use that attribute to lock this to a connection profile.
 2. Increase the **Timeout** to 60 seconds or more to handle MFA delays.
 3. Click **OK**.
 4. Set **User Info Helper Scheme** to **MSAD**.
 5. Set **OTP Preserves State** to **Yes**.
6. In the left navigation pane, select **Timeouts and Logging**.
7. 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.)
8. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > VPN Settings**.
9. In the left navigation bar, click **General**.

10. In the section **TINA**, 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).

TINA	
Handshake Timeout (sec)	<input type="text" value="30"/>
Tunnel HA Sync	<input type="checkbox"/>
Pending session limit	<input checked="" type="checkbox"/>
Prebuild cookies on startup	<input type="checkbox"/>
Global TOS copy	<input type="checkbox"/>
Global replay window size [packets]	<input type="text" value="256"/>
Allow Dynamic Mesh	<input checked="" type="checkbox"/>

11. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > Client to Site**.
12. Go to **External CA** and click the **Rules** tab.
13. Select **Click here for options** and select **radius** as the **Default 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.

Server	
Primary Authentication Scheme	<input type="text" value="Default Authentication Sch"/>
Default Authentication Scheme	<input type="text" value="radius"/>
Secondary Authentication Scheme	<input type="text" value="-NONE-"/>
	<input type="checkbox"/> Ras Login permission required
Server	<input type="text" value="-Use-Default-"/>
Server Protocol Key	<input type="text" value="-From-Server-Cert-"/>
Used Root Certificates	<input type="text" value="-Use-All-Known-"/>
X509 Login Extraction Field	<input type="text" value="-NONE-"/>

14. Click **Send Changes** and **Activate**.
15. 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.
16. 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 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. Make sure that **OTP Preserves State** is set to **Yes**.

User Info Helper Scheme	MSAD	▼	📋
OTP Preserves State	Yes	▼	📋

Figures

1. mfa01.png
2. vpn_settings_set_handshake_timeout.png
3. mfa04.png
4. mfa02.png

© Barracuda Networks Inc., 2024 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.