Microsoft Entra MFA Requirements for Microsoft CSPs

https://campus.barracuda.com/doc/88114215/

Starting August 1, 2019, all Microsoft Cloud Solution Providers must use multi-factor authentication for all users, including service accounts, in their partner tenant.

For more information, see Partner Security Requirements.

Required use of multi-factor authentication impacts all Barracuda Networks partners who are also Microsoft CSPs and who configure Microsoft Entra ID in Barracuda Cloud Control. Barracuda Cloud Control does not yet support the use of Microsoft Entra MFA, which causes login failures if Microsoft Entra MFA is enabled or required. As a workaround, configure a conditional access policy in Microsoft Entra to bypass the multi-factor authentication for users signing in from trusted IPs.

To configure a conditional access policy and enable trusted IPs, refer to the section on Trusted IPs in the Microsoft support article Configure Microsoft Entra Multi-Factor Authentication settings.

The following Barracuda Networks IP addresses must be used to create the conditional access policy:

- 35.170.131.81
- 54.156.244.63
- 54.209.169.44