Azure MFA Requirements for Microsoft CSPs

https://campus.barracuda.com/doc/88539275/

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 (MFA) impacts all Barracuda Networks partners who are Microsoft Cloud Solution Providers (CSPs) and who configure Azure AD in Barracuda Cloud Control. Barracuda Cloud Control does not yet support the use of Azure MFA, which causes login failures if Azure MFA is enabled or required. As a workaround to bypass MFA, you can configure a conditional access policy in Azure AD for users signing in from trusted IPs or create an app password to allow apps access to your Office 365 account.

Conditional Access Policy

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

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

- 35.170.131.81
- 54.156.244.63
- 54.209.169.44

If you are using Exchange Integration, you must also open the following outbound ports referred to in Data Transfer IP Ranges.

App Password

You can set up Exchange Integration jobs with Exchange Online using EWS instead of a service account with an app password. See How to Configure Microsoft Exchange Online Email Import Using EWS.

To enable EWS support for the Barracuda Cloud Archiving Service, contact Barracuda Networks

To generate an app password to connect apps to Office 365, refer to the Microsoft article [Create an app password for Office 365](#). Using an app password allows Barracuda to run Exchange Integration jobs without the need to authenticate with MFA.