Microsoft Entra MFA Requirements for Microsoft CSPs

https://campus.barracuda.com/doc/88539268/

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 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 to bypass MFA, you can configure a conditional access policy in Microsoft Entra ID for users signing in from trusted IPs or create an app password to allow apps access to your Microsoft 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 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

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

Technical Support .

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

© 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.