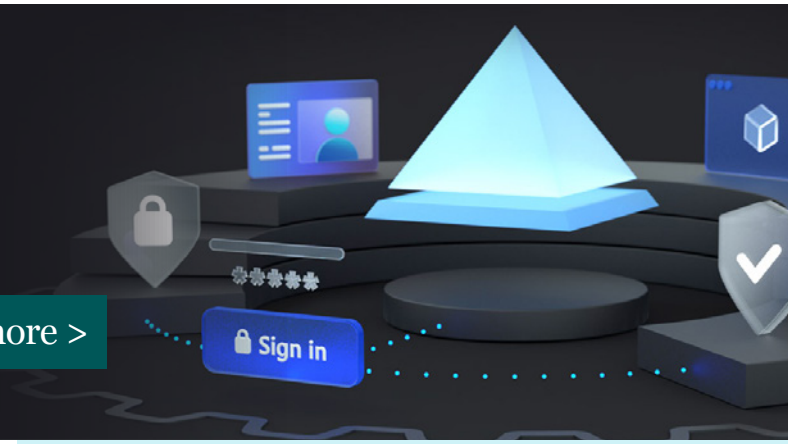
TD SYNNEX | Microsoft

Enable MFA for all user accounts in your partner tenant

Find out more >



You must enforce MFA on all user accounts in your partner tenants. Users must be challenged by MFA when they sign in to Microsoft commercial cloud services or when they transact in the Cloud Solution Provider program through Partner Center or via APIs.

MFA enforcement follows these guidelines:

- Partners who use Microsoft-supported Azure AD Multi-Factor Authentication. For more information, see Multiple ways to enable Azure AD MFA **(MFA supported).**
- Partner who implemented any third-party MFA and part of the exception list can still access Partner Center portal and APIs with exceptions but can't manage customer using DAP/GDAP (no exception allowed).
- If the partner's organization was previously granted an exception for MFA, users who manage customer tenants as part of the CSP program must have enabled Microsoft MFA requirements before March 1, 2022. Failure to comply with MFA requirements may result in the loss of customer tenant access.
- Learn more about mandating multi-factor authentication (MFA) for your partner tenant.

Note: Partners are now provided with free 24 months Azure AD Premium P2 license for each CSP tenant, and each tenant has up to 25 seats to redeem. Review Azure AD conditional access along with risk-based conditional access to quickly gain access to the promotion and set up Azure AD support MFA for strong authentication. Learn more about securing user sign-in events with Azure AD MFA.

Mandating multi-factor authentication (MFA) for your partner tenant

This article gives detailed examples and guidance for mandating multi-factor authentication (MFA) in Partner Center. The intent of this feature is to help partners secure their access to customer resources against credentials compromize. Partners are required to enforce MFA for all user accounts in their partner tenant, including guest users. Users will be mandated to complete MFA verification for the following areas:

Partner Center Dashboard >

Partner Center API >

Partner Delegated Administration >

Greater and ongoing security and privacy safeguards are among our top priorities and we continue to help partners protect their customers and tenants. All partners participating in the Cloud Solution Provider (CSP) program, Control Panel Vendors (CPVs), and Advisors should implement the Partner Security Requirements to stay compliant.

To help partners protect their businesses and customers from identity-theft and unauthorized access, we activated additional security safeguards for partner tenants which mandate and verify MFA.

Partner Center dashboard

Certain pages in the Partner Center dashboard will be MFA-protected, including the following.

- All pages under the **Customers** tab (all pages that can be accessed through the following URLs: https://partner.microsoft.com/commerce/*)
- All pages under the **Support > Customer** requests tab, e.g the page accessed under https://partner.microsoft.com/dashboard/support/cspcustomers/*
- Billing page

TD SYNNEX | Microsoft

The following table shows which user types are authorized to access these MFA-protected pages (and are therefore affected by this feature).

MFA-protected page	Admin agents	Sales agents	Helpdesk agents	Global administrator	Billing administrator
All pages under Customers tab	✖	✖	✖		
All pages under Support > Customer requests tab	✖		✖		
Billing page	✖			✖	✖

If you try to access any of these pages and you haven't completed MFA verification earlier, you will be required to do so. Other pages on Partner Center such as the Overview page, Service Health Status check page do not require MFA.

The table below shows what scenarios are impacted when the MFA exception is removed.

Important: Partners must use the Azure MFA to manage the customer tenants with DAP or GDAP. No exceptions are supported.

MFA exception are only allowed when using a compatible third-party MFA within the Partner Center Portal and APIs. They are not allowed when managing the customer tenant using DAP or GDAP.

Partner Center portal and APIs

For Partner Center APIs in the following table, App+User access is required.

Scenario	Azure AD Support MFA	Any 3rd-party MFA	No MFA
Discover (price/catalog/promotion)	MFA supported	Exception supported	No access
Transact and manage	MFA supported	Exception supported	No access
Billing and reconciliation	MFA supported	Exception supported	No access
Manage customers using delegated access/AOBO	MFA supported	No exception supported	No access
User and license assignment (with DAP only)	MFA supported	Exception supported	No access
User and license assignment (with GDAP)	MFA supported	No exception supported	No access
Granular Admin Relationships Request and access assignment	MFA supported	No exception supported	No access

Additional workloads

Potential additional workloads for this category include Azure AD and Microsoft Exchange.

Scenario	Azure AD Supported MFA	Any 3rd-party MFA
Discover (Price/Catalog/Promotion)	N/A	N/A
Transact and manage	N/A	N/A
Billing and Recon	N/A	N/A
Manage customers using delegated access/AOBO	MFA supported	No exceptions supported
User and License Assignment	MFA supported	No exceptions supported