Partner MFA Setup
& Security Score Compliance Guide

Enable, register, and maintain MFA across your Partner Center tenant, and the customer tenants you access

Microsoft enforced MFA on the Microsoft 365 admin centre from 9 February 2026. Admins without MFA are now blocked from **admin.microsoft.com**, **admin.cloud.microsoft**, and **portal.office.com/adminportal/home**. Separately, **entra.microsoft.com** and **intune.microsoft.com** have required MFA since late 2024 for any create, update, or delete action, that enforcement wave is already complete. A second phase now covers Azure CLI, PowerShell, the Azure mobile app, Infrastructure-as-Code tools, and REST API calls to management.azure.com. Tenants that requested more time had until 1 July 2026 to prepare, that grace period has now closed. For AppXite's Microsoft partners, MFA coverage is no longer just good practice, it is a mandatory input to your Partner Center Secure Score and a condition of keeping CSP authorisation.

This applies at three levels: MFA for everyone in your own Partner Center tenant, MFA enforcement carrying through to any customer tenant you access via GDAP, and MFA for administrative users inside those customer tenants themselves. Microsoft increasingly evaluates security controls across partner and customer environments, making MFA adoption important across all three areas.

This guide has five parts: your Partner Center Secure Score and what it requires, your responsibility for customer tenant MFA as a reseller, how to enable MFA across your own organisation, how users register their account, and a monthly checklist to stay compliant.

Part 1: Your Partner Center Secure Score

Microsoft scores CSP partners on a dedicated Secure Score inside Partner Center. This is separate from Microsoft Secure Score for M365, and it feeds directly into CSP authorisation, this is the section with the most riding on it.

How it's scored

- Scale of 0 to 100, calculated from a set of security requirements and recommendations
- Mandatory requirements must be completed to maintain CSP authorisation eligibility
- Recommended requirements improve your overall security posture and increase your Security Score but are not required for CSP authorisation, worth treating as effectively mandatory given how often Microsoft tightens these criteria

The three mandatory requirements

- MFA enabled for all administrative users in the CSP tenant (non-Microsoft MFA solutions such as Okta, Ping, or Duo are not recognised and will not count towards the score)
- A designated security contact named within Partner Center
- Security alerts responded to within 24 hours or less (this specific requirement does not apply to indirect reseller partners)

The two recommended requirements

- Administrative users in customer tenants have MFA enabled, worth 20 of the 30 recommended points, and covered in Part 2 below
- All Azure subscriptions have a spending budget configured, worth the remaining 10 points

View your current score at: Partner Center > Security > Security requirements dashboard.

IMPORTANT
The Security Requirements dashboard is available to CSP partners and should be reviewed regularly to monitor compliance with Microsoft's security requirements and recommendations.

Part 2: Customer Tenant MFA — Reseller Responsibility

Customer tenant MFA is one of the most significant recommended security requirements within the Partner Center Security Requirements dashboard and can have a substantial impact on your overall Security Score. As Indirect Resellers, you hold the GDAP access into your customers' tenants, which puts you in the best position to identify and resolve gaps there.

This is not yet a mandatory Microsoft requirement, but it is worth treating as one. Microsoft has a track record of moving recommended requirements to mandatory over time, and being ahead of that shift is safer than reacting to it after the fact.

What this covers

- Review MFA status for every administrative role in each customer tenant you manage via GDAP, not just your own Partner Center tenant
- Enable Security Defaults in customer tenants that don't already manage MFA themselves (free, no licence required), or Conditional Access where the customer holds Entra ID P1 or higher
- Flag and remove stale or unused admin accounts in customer tenants during the same review, these are rarely monitored and are an easy target
- Keep a record of what you've reviewed and actioned per customer, in case Microsoft or AppXite asks for evidence

WHY IT MATTERS
An admin account without MFA is one compromised password away from full tenant control. That can mean data breaches, service disruption, or fraudulent Azure usage such as cryptomining running up the customer's bill. Stale, unmonitored admin accounts are the easiest way in, and the first thing worth checking.

If a customer pushes back on enabling MFA, or you hit a licensing or technical blocker you can't resolve, come to your AppXite account team. We'll help build an action plan, or raise it with Microsoft directly where needed. Don't leave a gap unresolved without flagging it to us.

Part 3: For Admins — Enabling MFA

1 Check who needs MFA

In the Microsoft Entra admin centre (**entra.microsoft.com**), go to:

- **Protection > Authentication methods > User registration details**

Filter by MFA Capable = No to identify users who cannot currently satisfy Microsoft Entra MFA requirements. Prioritise administrative accounts first, then work through remaining users to ensure MFA readiness across the organisation.

NOTE
The legacy MFA management experience was retired on 30 September 2025. Use the Authentication Methods reporting experience and Microsoft Entra security reports to monitor MFA registration and compliance.

2 Enable Security Defaults

Security Defaults is Microsoft's free baseline policy. It requires all users to register for MFA, enforces MFA for admins on every sign-in, prompts users for MFA when Microsoft determines it is necessary, and blocks legacy authentication protocols.

To enable:

- Sign in to entra.microsoft.com as a Conditional Access Administrator
- Go to: **Entra ID > Overview > Properties**
- Select **Manage security defaults**, set to **Enabled**, and **Save**

> **IMPORTANT**
> Security Defaults and Conditional Access cannot run at the same time. If your tenant has Microsoft Entra ID P1 or higher (Microsoft 365 Business Premium, E3, E5), Conditional Access is the alternative, contact your AppXite account team for help configuring it.

Before enabling, check that no users rely on legacy authentication clients (Office 2010, IMAP, SMTP, POP3), as these will be blocked immediately.

Microsoft-managed Conditional Access policies may already be active in your tenant. Review existing policies before enabling Security Defaults.

> **PHASE 2 UPDATE**
> If anyone on your team runs scripts, Terraform, or other automation against Azure using a regular user account rather than a managed identity or service principal, that account now needs MFA too. This has applied since 1 July 2026 with no further extensions available.

3 Tell your users and verify compliance

Once enabled, all users will be prompted to register at next sign-in. Microsoft provides communication templates at aka.ms/mfatemplates, use these to inform users in advance.

Ask users to register proactively at: aka.ms/MFASetup

After a few days, return to the User registration details report and review users showing MFA Capable = No. Investigate any remaining accounts and ensure users complete MFA registration where required.

> **TIP**
> If you see users showing MFA capable: No, check whether they have ever signed in. New accounts created with a temporary password appear as not MFA capable until the user completes their first sign-in. With Security Defaults enabled, those users will be forced through MFA registration on first login, there is no way to bypass it. These are not a gap in enforcement, just accounts pending first use.

Disabled and soft-deleted accounts do not appear in the User registration details report. Delete unused accounts (Entra > Identity > Users > All Users, filter: Account status = Disabled) to keep reporting accurate.

Part 4: For All Users — Registering for MFA

Once your admin has enabled MFA, you will be prompted to register at next sign-in. You can also register in advance, it takes about 5 minutes.

1 Install Microsoft Authenticator on your phone

Download Microsoft Authenticator from the App Store (iOS) or Google Play (Android). Open the app and allow notifications when prompted.

2 Register your account

On your computer, go to: aka.ms/MFASetup

Sign in with your work email and password, then select Add sign-in method > Authenticator app, and follow the on-screen instructions.

In the Authenticator app, tap Add account > Work or school account > Scan QR code, then scan the code shown in your browser. Approve the test notification when prompted.

> **NOTE**
> Microsoft Authenticator is the recommended MFA method and provides stronger protection against account compromise. SMS and voice-based authentication methods remain supported but are considered less secure. Where possible, use Microsoft Authenticator, passkeys, or FIDO2 security keys.

After registration, Microsoft determines when to prompt for MFA based on factors like location, device, and risk, you may not be prompted on every login.

Part 5: Monthly Monitoring Checklist (Admins)

Run these checks once a month, about 15-20 minutes, to keep your tenant compliant.

#	Check	Where	Done?
1	Confirm Security Defaults is still enabled (or your Conditional Access MFA policy is set to On)	*Entra > Entra ID > Overview > Properties*	☐
2	Review User registration details, filter by MFA capable: No and address any remaining users	*Entra > Protection > Authentication methods > User registration details*	☐
3	Check Registration and reset events, investigate any failed registration attempts	*Entra > Protection > Authentication methods > Registration and reset events*	☐
4	Review new users added in the last 30 days, confirm they have completed MFA registration	*M365 admin centre > Users > Active users (sort by Created)*	☐
5	Clean up disabled accounts, delete those no longer in use	*Entra > Identity > Users > All Users (filter: Disabled)*	☐
6	Check admin role assignments, confirm no unexpected users in privileged roles	*Entra > Identity > Roles & admins > All roles*	☐
7	Review sign-in logs for MFA failures or suspicious sign-in attempts	*Entra > Identity > Monitoring & health > Sign-in logs*	☐
8	Confirm no user accounts (rather than managed identities or service principals) are running scripts or automation against Azure without MFA	*Entra > Identity > Applications, cross-check with Azure activity logs*	☐
9	Check your Partner Center Secure Score and confirm mandatory requirements are still met	*Partner Center > Security > Security requirements dashboard*	☐
10	Review MFA status for admin users across your GDAP-managed customer tenants, remediate or flag blockers to AppXite	*Entra > Protection > Authentication methods > User registration details (per customer tenant, via GDAP)*	☐

Need help?

Contact your AppXite account team for help with setup, reviewing tenant settings, or configuring Conditional Access.

Maintained by **AppXite Partner Programs**.

Microsoft references

- aka.ms/MFASetup — user registration
- aka.ms/mfatemplates — communication templates
- learn.microsoft.com/entra/fundamentals/security-defaults — Security Defaults documentation
- learn.microsoft.com/partner-center/security/security-requirements — Partner Center Secure Score documentation