M365 Kimlik Doğrulama Yapılandırması ve Sorun Giderme

Teknik Mimari Raporu

Hazırlayan: Harun Kürşat Bal • Sürüm: 1.0 • Haziran 2026

1. Giriş ve Raporun Amacı

Bu teknik rapor, Microsoft 365 (M365) ortamlarında sistem yöneticileri tarafından sıkça raporlanan sürekli MFA (Çok Faktörlü Kimlik Doğrulama) istekleri, Outlook üzerinde oluşan parola döngüleri ve kimlik doğrulama uç noktası (endpoint) engellemelerini sistematik bir metodolojiyle çözmek amacıyla hazırlanmıştır. Doküman, kimlik doğrulama mimarisindeki olası tıkanıklıkları gidermek için yapılandırma adımlarını ve ağ katmanı gereksinimlerini bir mimar bakış açısıyla ele almaktadır.

2. Kimlik Doğrulama Sorunları İçin 6 Adımlı Teknik Kontrol Listesi

M365 kimlik doğrulama akışındaki hataları ayıklarken aşağıdaki 6 adım sırasıyla takip edilmelidir. Her adım, bir sonrakine geçmeden önce elenmesi gereken birer kontrol noktasıdır.

1

Security Defaults (Güvenlik Varsayılanları)

Konum: Entra Portal → Identity → Overview → Properties → Manage Security Defaults

Mimari Mantık: Eğer kuruluşunuzda Koşullu Erişim (Conditional Access) politikaları aktifse, Security Defaults mimari gereği otomatik olarak Disabled kalmalıdır.

Durum	MFA Üzerindeki Etkisi
Enabled	Tenant üzerindeki TÜM kullanıcılar için MFA zorunlu hale gelir.
Disabled	Security Defaults MFA uygulamıyor. Sorun kaynağı olarak elenebilir.

2 Conditional Access (Koşullu Erişim) Politikaları

Konum: Entra Portal → Identity → Protection → Conditional Access → Policies

Denetim Prosedürü:
• Durumu On (Açık) olan tüm politikalar incelenmelidir.
• Grant bölümünde "Require multifactor authentication" seçeneği aktif mi?
• İlgili kullanıcı Include listesinde mi? Exclude'dakilere bu politika uygulanmaz.

Not: "Report-only" modundaki politikalar akışı kesmez, yalnızca log üretir.

3 Per-user MFA Durumu

Konum: Entra Portal → Users → [Kullanıcı] → Per-user MFA veya aka.ms/mfasetup

Durum	Outlook Davranışı
Disabled	Bu katmanda MFA zorlanmıyor.
Enabled	MFA zorunlu; kullanıcı kayıt sürecini tamamlamamışsa challenge başlar.
⚠ **Enforced**	MFA kesinlikle zorunlu. Yöntem kayıtsızsa Outlook sürekli parola sorarak döngüy

4 Identity Protection Risk Politikaları

Konum: Entra Portal → Identity → Protection → Identity Protection → User/Sign-in risk policy

Politikalar Enabled ise ve kapsamda All users veya ilgili kullanıcının grubu varsa, sistem yüksek risk algıladığında MFA tetikler.

Lisans Kısıtı: Bu özellik genellikle Microsoft Entra ID P2 lisansı gerektirir. P1 tenant'larda ayarlar görüntülense de etkin olmayabilir.

5 SSPR (Self-Service Password Reset) Kayıt Zorunluluğu

Konum: Entra Portal → Identity → Protection → Password reset → Registration / Properties

Registration: "Require users to register when signing in" ayarı Yes ise kullanıcı SSPR kayıt sayfasına yönlendirilir.

Ağ Etkileşimi: Outlook bu kayıt sayfasını dahili web-view ile açar. Firewall SSPR uç noktalarını engelliyorsa sayfa sessizce hata verir ve Outlook parola döngüsüne girer.

Properties: SSPR = None ise bu adım sorun kaynağı olarak elenebilir.

6 Firewall (Güvenlik Duvarı) Kontrolü

Yukarıdaki 5 adımda yapılandırma hatası saptanmadıysa, sorun kesinlikle ağ katmanındadır. Kimlik doğrulama uç noktalarının (authentication endpoints) trafiğe izin verilip verilmediğini kontrol edin.

3. Kritik Ağ ve Firewall Beyaz Liste (Whitelist) Gereksinimleri

Kimlik doğrulama akışının başarıyla tamamlanması için aşağıdaki FQDN'lerin 443/TCP (HTTPS) portu üzerinden erişime açık olması zorunludur.

FQDN	Açıklama
login.microsoftonline.com	Entra ID / Azure AD ana kimlik doğrulama uç noktası
login.windows.net	Modern Authentication token alım noktası
*.outlook.office.com	Birincil Outlook servis erişimi
*.outlook.office365.com	Alternatif Outlook servis erişimi
autodiscover-s.outlook.com	Outlook Autodiscover servisleri
device.login.microsoftonline.com	Cihaz kaydı ve token yenileme işlemleri
enterpriseregistration.windows.net	Hibrit Azure AD Join / Cihaz kayıt süreçleri

⚠ ÖNEMLİ MİMARİ UYARI: Güvenlik duvarı kurallarında IP tabanlı kısıtlamalar yerine kesinlikle FQDN tabanlı kurallar kullanılmalıdır. Microsoft, kimlik doğrulama servislerinin IP adreslerini önceden bildirmeksizin dinamik olarak değiştirebilir. IP tabanlı kurallar erişim kesintilerine ve operasyonel hatalara yol açacaktır.

4. Dış (Guest) Kullanıcı MFA ve Erişim Sorunları

Dış kullanıcıların SharePoint veya OneDrive paylaşımlarında yaşadığı MFA tıkanıklıkları, genellikle Email One-Time Passcode (OTP) yapılandırmasının kapalı olmasından kaynaklanır.

Email One-Time Passcode (OTP) Yapılandırması

1. Entra Portal'da External Identities sekmesine gidin (Görünmüyorsa "Show More" kullanın).
2. All identity providers altındaki Built-in sekmesine tıklayın.
3. Email One-Time Passcode seçeneğini bulun.
4. Açılan panelde durumu Enabled olarak işaretleyin ve kaydedin.

Dış İş Birliği Ayarları

External collaboration settings altındaki konuk kullanıcı erişim düzeylerini teyit edin:

✔ İdeal: "Guest users have limited access to properties and memberships of directory objects" seçili olmalıdır.

✖ Kritik Engel: "Deny access" seçeneği tüm dış iş birliğini keser; seçili olmadığından emin olun.

5. Gelişmiş Sorun Giderme: AADSTS90072 Hatası ve Çözümü

Bu hata, bir dış kullanıcının sisteme daha önce hatalı (örneğin kişisel Microsoft hesabı olarak) kaydedilmesi ve yeni yapılandırmaların bu "bozuk" kayıt nedeniyle tanınmaması durumunda ortaya çıkar.

Kullanıcı Kaydını Sıfırlama Prosedürü

1. Mevcut Kaydı Silin: Entra ID > Users altından ilgili dış kullanıcıyı silin.

   Not: Silinen Konuk kullanıcı 30 gün boyunca kurtarılabilir. Yeniden davet sonrası mevcut paylaşımları kontrol edin.

2. Ayar Doğrulaması: Email One-Time Passcode ayarının halen Enabled olduğunu teyit edin.
3. Yeniden Davet: Kullanıcıya SharePoint/OneDrive üzerinden yeni bir davet gönderin. Sistem kullanıcıyı "Sıfır Konuk" olarak tanıyacak ve OTP akışını tetikleyecektir.
4. Kritik İpucu: Kullanıcının yeni davet linkini mutlaka Gizli Sekme (InPrivate/Incognito) üzerinden açmasını sağlayın.

✔ Başarılı Erişim Akışı: (1) Dahili kullanıcı paylaşım linkini gönderir → (2) Dış kullanıcı linke tıklar → (3) Entra ID kullanıcıyı Guest olarak tanımlar → (4) 6 haneli OTP kodu e-postaya iletilir → (5) Kullanıcı kodu girerek paylaşıma erişir.

6. Yapılandırma Hızlı Kontrol Özeti

Sistem yöneticileri için bu tablo, bir sorun anında ilk bakılması gereken check-off listesidir:

#	Kontrol Noktası	Elenme Kriteri
1	Security Defaults	Disabled ise elenebilir
2	Conditional Access Policies	MFA Grant'ı yok veya kullanıcı Exclude'da ise elenebilir
3	Per-user MFA	Status = Disabled ise elenebilir
4	Identity Protection	Disabled veya kullanıcı kapsam dışı ise elenebilir
5	SSPR Kayıt Zorunluluğu	SSPR = None ise elenebilir
6	Firewall FQDN Whitelist	Tüm kritik endpoint'ler (443/TCP) açık mı?