1. MDM uygulaması tarafından kullanılan bağlantı noktaları nelerdir?

Proxy/güvenlik duvarında aşağıdaki bağlantı noktalarının açık olduğundan emin olun.

Port numarası	Tip	Amaç	Bağlantı Yönü	Trafik
9020	HTTP	ME MDM uygulaması ve sunucu iletişimi.	Sunucuya Gelen	↑↓
9383	HTTPS	ME MDM Uygulaması ve sunucu iletişimi.	Sunucuya Gelen	↑↓
443	HTTPS	APN, FCM, WNS sunucusuna ulaşmak için Mobile Device Manager Plus sunucusunda açık olmalıdır. **Android cihazlar için:** android.googleapis.com; www.google.com; android.clients.google.com; *.googleapis.com; play.google.com; google-analytics.com; googleusercontent.com; gstatic.com; *.gvt1.com; *ggpht.com; dl.google.com; hesaplar.google.com; gcm-http.googleapis.com; fcm.googleapis.com; fcm-xmpp.googleapis.com; pki.google.com; client1.google.com; müşteriler[2…6].google.com Sunucunun bulunduğu ülkeye bağlı olarak aşağıdaki alan adları açık olmalıdır: **ABD** : gslb.secb2b.com; us-elm.secb2b.com; us-knox.secb2b.com; **Çin** : c hina-gslb.secb2b.com.cn ; çin-elm.secb2b.com.cn; china-knox.secb2b.com.cn **Asya, Afrika, Avrupa veya diğer bölgeler** : gslb.secb2b.com; eu-elm.secb2b.com; eu-knox.secb2b.com; **Apple cihazları için:** albert.apple.com; captive.apple.com; gs.apple.com; humb.apple.com; static.ips.apple.com; tbsc.apple.com; *.push.apple.com; gdmf.apple.com; deviceenrollment.apple.com; deviceservices-external.apple.com; kimlik.apple.com; iprofiles.apple.com; mdmenrollment.apple.com; setup.icloud.com; vpp.itunes.apple.com; gg.apple.com; gnf-mdn.apple.com; gnf-mr.apple.com; gs.apple.com; ig.apple.com; mesu.apple.com; ns.itunes.apple.com; oscdn.apple.com; osrecovery.apple.com; skl.apple.com; swdist.apple.com; swdownload.apple.com; swscan.apple.com; update.cdn-apple.com; xp.apple.com; *.itunes.apple.com; *.apps.apple.com; *.mzstatic.com; ppq.apple.com **Windows cihazları için:** https://login.live.com; https://*.notify.windows.co	Sunucuya Giden	↑
2195	HTTPS	APN'lere ulaşmak için Mobile Device Manager Plus sunucusunda açık olmalıdır. Ana bilgisayar adresi: gateway.push.apple.com	Sunucuya Giden	↑
5223	HTTPS	Açık olmalı, mobil cihaz kurumsal Wi-Fi üzerinden internete bağlanıyorsa, IP'yi 17.0.0.0/8 aralığında yapılandırmanız önerilir.	Kurumsal Ağ Güvenlik Duvarından Giden	↑↓
5228, 5229, 5230	HTTPS	FCM'nin yönetilen mobil cihaza ulaşması için. Ana bilgisayar adresi: https://android.com; play.google.com; android.clients.google.com; www.google.com; googleapis.com; android.googleapis.com; gstatic.com; google-analytics.com; googleusercontent.com; *.gvt1.com; *ggpht.com; dl.google.com; fcm.googleapis.com; fcm-xmpp.googleapis.com; gcm-http.googleapis.com; gcm-xmpp.googleapis.com	Kurumsal Ağ Güvenlik Duvarından Giden	↑↓
5235,5236	HTTPS	Firebase Bulut Mesajlaşma için (örn. EMM-DPC iletişimi). Ana bilgisayar adresi: https://gcm-xmpp.googleapis.com; gcm-http.googleapis.com; android.googleapis.com	Kurumsal Ağ Güvenlik Duvarından Giden	↑↓

Cihazları MDM'ye kaydetmek için TLS ve **TCP** protokolleri kullanılır **.**

Hem MDM sunucusu hem de MDM'ye kaydedilecek cihaz, güvenlik duvarında ve/veya herhangi bir üçüncü taraf filtresinde hariç tutulacak/izin verilecek olan aşağıdaki etki alanlarına erişime sahip olmalıdır.

Tüm platformlar için
Yalnızca sunucuda izin verilir
https://creator.zoho.com
https://mdm.manageengine.com:443
iOS için
Hem sunucuda hem de cihazda izin verilir
https://gateway.push.apple.com
https://api.push.apple.com
https://itunes.apple.com:443
http://itunes.apple.com:80
https://deploy.apple.com
https://vpp.itunes.apple.com
albert.apple.com
iprofiles.apple.com
crl3.digicert.com
crl4.digicert.com
ocsp.digicert.com
setup.icloud.com
gateway.icloud.com
Yalnızca cihazda izin verilir
https://ax.init.itunes.apple.com
https://ppq.apple.com
http://is2.mzstatic.com
ocsp.apple.com
https://buy.itunes.apple.com/
Yalnızca sunucuda izin verilir
https://uclient-api.itunes.apple.com
*.zohoassist.com:443
Windows için
Yalnızca sunucuda izin verilir
https://login.live.com
https://*.notify.windows.com
https://*.wns.windows.com
https://*notify.live.net
Android için
Samsung olmayan cihazlar
Yalnızca cihazda izin verilir
https://www.google.com
mtalk.google.com:5228
mtalk.google.com:5229
mtalk.google.com:5230

Kurumsal Ağ Güvenlik Duvarında İzin Verilir

*.googleapis.com
play.google.com
android.com
google-analytics.com
googleusercontent.com
gstatic.com

*.gvt1.com
*.gvt2.com
*.gvt3.com

*.ggpht.com
dl.google.com
dl-ssl.google.com
androidclients.google.com gcm-http.googleapis.com gcm-xmpp.googleapis.com
android.googleapis.com
fcm.googleapis.com fcm-xmpp.googleapis.com
pki.google.com
client1.google.com
clinets[2...6].google.com
*.zoho.com:443
*.zohoassist.com:443
googleapis.com:443
accounts.google.com:443
notification.google.com:443
https://mdmdatabase.manageengine.com

Samsung cihazları Yalnızca cihazda izin verilir

sadece Çin

https://china-gslb.secb2b.com.cn:443
https://china-elm.secb2b.com.cn:443
https://china-knox.secb2b.com.cn:443
https://china-b2c-klm.secb2b.com.cn:443
https://china-prod-klm.secb2b.com.cn:443

Yalnızca Amerika Birleşik Devletleri
https://gslb.secb2b.com:443
https://us-elm.secb2b.com:443
https://us-knox.secb2b.com:443
https://us-b2c-klm.secb2b.com:443
https://us-prod-klm.secb2b.com:443
diğer tüm ülkeler
https://gslb.secb2b.com:443
https://eu-elm.secb2b.com:443
https://eu-knox.secb2b.com:443
https://eu-prod-klm-b2c.secb2b.com:443
https://eu-prod-klm.secb2b.com:443
Samsung Knox Kaydı İçin Güvenlik duvarında izin verilmesi gerekenler
*.samsungknox.com:443
*.samsungknox.com:80
*.secb2b.com:443
*.secb2b.com:80
https://eula.secb2b.com:80
https://eula.secb2b.com:443
https://umc-cdn.secb2b.com:80
https://umc-cdn.secb2b.com:443
https://dir-apis.samsungdm.com:443
https://account.samsung.com:443
https://us-kme.samsungknox.com
https://us-kme.api.samsungknox.com
https://us-kme.api.mssl.samsungknox.com
https://us-kme-reseller.samsungknox.com
https://mdmdatabase.manageengine.com