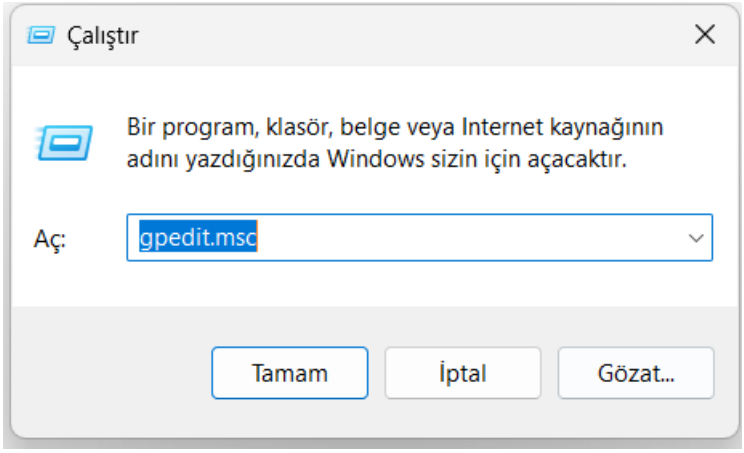
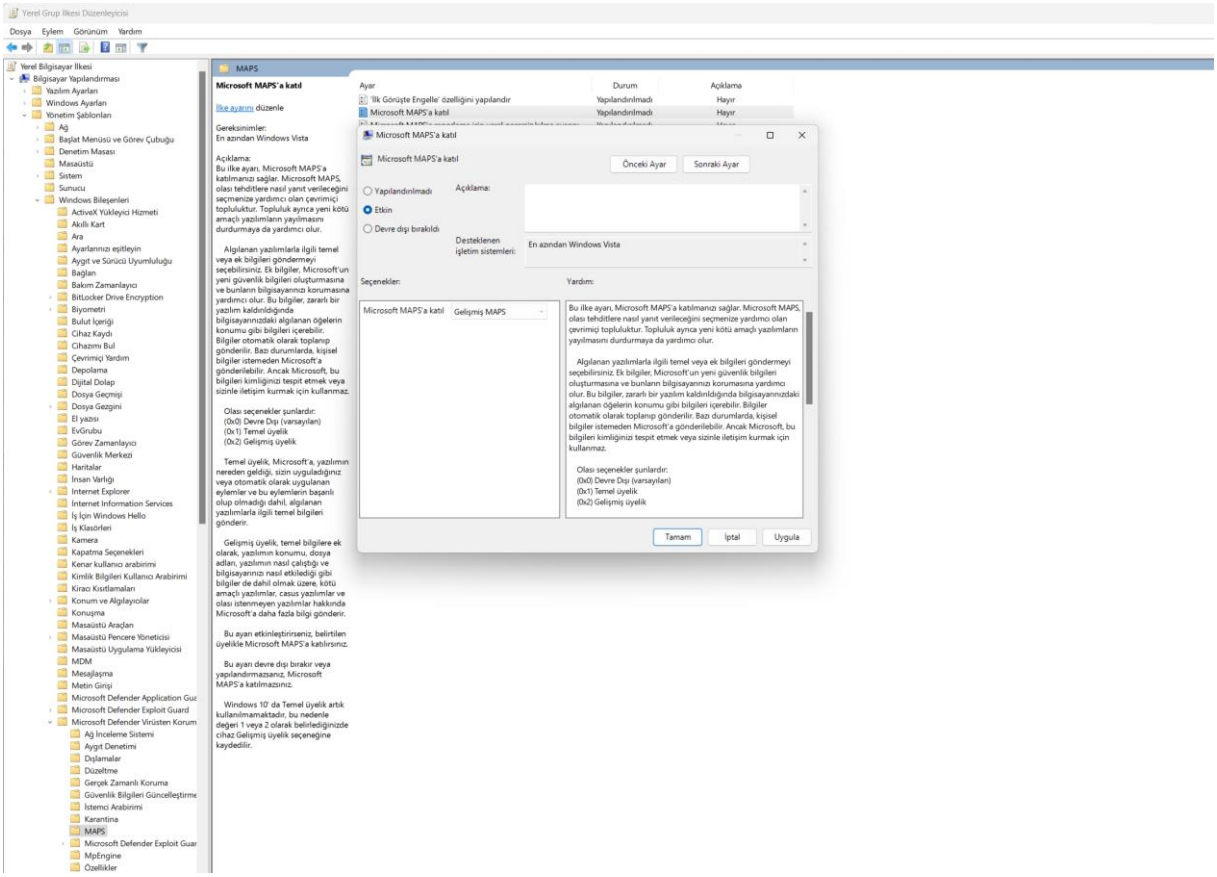
Öncelikle yerel grup ilkesine gidiyorum.



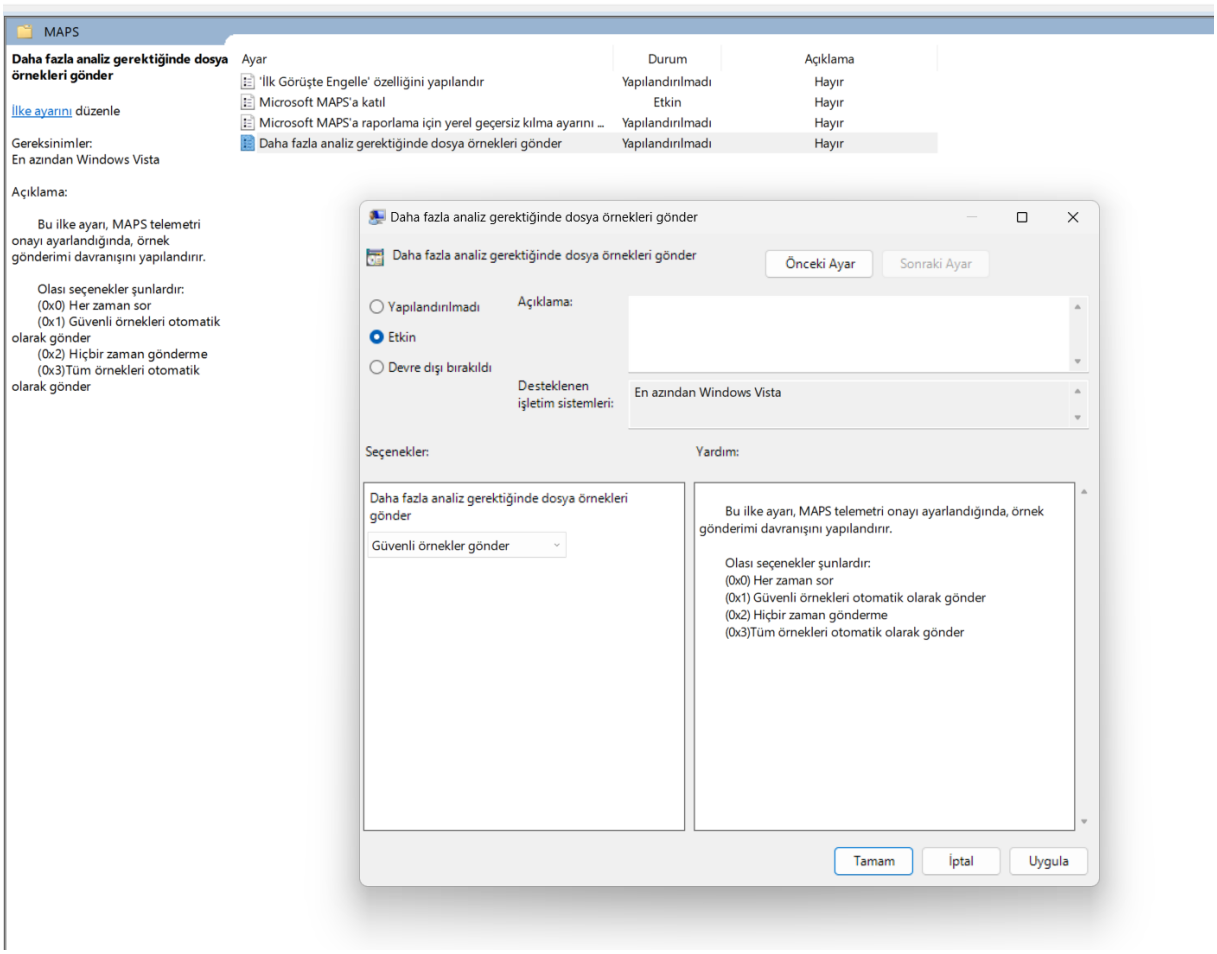
Karşıma gelen ekrandan

Bilgisayar yapılandırması / Yönetim Şablonları / Windows Bileşenleri / Microsoft Defender Virüstün Koruma / MAPS sekmesine geliyorum ve ilk olarak **“Microsoft MAPS’a katıl”** ı aktif ediyorum.



Böylelikle Microsoft’un aktif gelişmiş Bulut koruma hizmeti devreye almış oluyorum.

İkinci adımda ise yina aynı arayüzden “Daha Fazla Analiz Gerektiğinde Dosya Örnekleri Gönder” seçeneği etkin yapıyorum.



Maps Etkinleştirme ile sisteminize şunları kazandırmış olacaksınız.

MAPS, kurumsal yazılım güvenliğiniz için ne yapabilir?

Sisteminizde MAPS'ı etkinleştirmek size şunları sağlar:

- Bulut üzerinden sağlanan kötü amaçlı yazılım engelleme kararları sayesinde kötü amaçlı yazılımlara karşı daha fazla koruma

Şüpheli olaylara karşı bulut çağrılarını tetiklemek için MAPS'ı etkinleştirin. Bunu yapmak, makinenin Microsoft Kötü Amaçlı Yazılımdan Koruma Merkezi (MMPC) araştırma ekibinden, arka uç büyük verisinden ve makine öğrenimi mantığından elde edilen en son kötü amaçlı yazılım bilgilerini kullanmasına yardımcı olur.

- Toplu koruma telemetrisi Bulut aracılığıyla sunulan ekosistem çapındaki en yeni algılama tekniklerinden yararlanın. Microsoft, bir milyardan fazla

istemciden gelen koruma telemetrisini toplar ve bunlara çok sayıda sinyalle çapraz referans verir.

MMPC tehdit istihbaratı, ekosistemdeki tehditlerin görünümünü oluşturmak ve yönetmek için algoritmalardan yararlanır. Uç nokta ürünü şüpheli etkinliklerle karşılaştığında, harekete geçmeden önce gerçek zamanlı analiz için buluta başvurabilir.

Bulutta bulunan geniş veri ve bilgi işlem kaynakları, polimorfik ve yeni ortaya çıkan tehditlerin hızla tespit edilmesine ve gelişmiş koruma tekniklerinin uygulanmasına olanak tanır.

İstemci makineleri, aşağıdakileri içeren Microsoft Kötü Amaçlı Yazılımdan Koruma Merkezi'nin (MMPC) bulut hizmetine seçici olarak gerçek zamanlı (algılama için) veya periyodik olarak (sağlık kontrolleri için) telemetri gönderir:

- Tehdit telemetrisi – tehditleri, tehditle ilgili kaynakları ve iyileştirme sonuçlarını belirlemek için
- Şüpheli davranış – numune toplamak, neyin izleneceğini ve düzeltileceğini belirlemek için
- Kalp atışı – antivirüs uygulamasının hala çalışıp çalışmadığını ve güncellenmiş sürüme sahip olup olmadığını öğrenmek için sistemin nabzını kontrol etmek için

MMPC bulut hizmeti istemci telemetrisine şu şekilde yanıt verir:

- Bulut eylemleri – potansiyel bir tehdidin nasıl ele alınacağına (örneğin, onu engellemeye) ilişkin bağlamı ve buluttan gelen bir dizi talimatı içerir.
- Yanlış pozitif kötü amaçlı yazılım tespitlerini bastırmak için bulut yanlış pozitif azaltma yanıtı