1. **AMAÇ VE KAPSAM**

Bu dokümantasyonda Windows 11 işletim sisteminin hardening ayarları ele alınmıştır. Windows her sürümüne özel varsayılan konfigürasyonlara sahip olup güvenlik açısından belirli bir seviyede olsa da bu konfigürasyonlar ayarlanarak güvenlik açısından daha iyi hale getirilebilir. Güvenliğin en temel seviyede, sistem seviyesinde ele alınmasını sağlayan bu çalışmalara hardening denir. Hardening, özelleştirilmiş güvenlik ayarlarından daha çok sistem üzerinde yapılan ayarlarla şirketlerin sistem üzerinde güvenliğini geliştirmesine olanak sağlar.

1. **TANIMLAR**

**Profil Tanımları**

**Level 1(L1) Kurumsal Ortam** (Genel Kullanımlar)

* çoğu kurumun temel kurallarıdır
* pratik ve tedbirlidir
* karışık olmayan güvenlik yararları vardır
* kullanımı kabul edilebilir teknolojilerin kullanımını engellemez

**Level 2 ( L2) - Yüksek Güvenlik ve Hassas Data Ortamları İçin** ( kısıtlı kullanım)

* Güvenliğin daha kritik olduğu ancak yönetim ve kullanım açısından daha kısıtlı alanlarda kullanılır
* Kullanımı kabul edilebilir teknolojileri kısıtlayabilir
* Remote kullanımı kısıtlar

Level 2 kullanımı için Level 1 ayarları geçerli olmalıdır.

**BitLocker (BL) - İsteğe Bağlı Eklenti**

**Next Generation Windows Security (NG) - En son teknolojilere yönelik isteğe bağlı eklenti**

Windows güvenliğine yönelik spesifik konfigurasyonlar içeren ancak her sisteme entegresi olmayan bir profildir. Bu yüzden kullanılmadan önce test edilmesi tavsiye edilir.

**Kelime Tanımlar**

**Remote:** Remote yani uzaktan çalışma, bir çalışanın ofisten uzak bir konumda çalışmasına imkân sağlayan bir tür esnek çalışma modelidir.

**BitLocker :** Windows'un önceki sürümlerinde mevcut olmayan sürücü şifreleme özelliği sayesinde bütün diskin belirli bir algoritma ile şifrelenmesini sağlayan bir sistemdir.

**Next Generation Windows Security:** En son Windows teknolojilerine entegre edilmiş güvenlik hizmetleridir.

**Parola:** Bilgisayar sistemlerinde bazı kaynaklara erişimi kontrol etmek için gizli bilgileri kullanan bir kimlik doğrulama biçimidir.

**Kimlik Bilgileri Yöneticisi:** Web siteleri, bağlı uygulamalar ve ağlar için kaydedilmiş oturum açma bilgilerini görüntülemenize ve silmenize olanak tanır.

**Yerel Sistem:** Makine üzerindeki en yetkili hesaptır. Hatta Administrator hesabından daha yetkilidir diyebiliriz. Hem yerel hem de network kaynaklarına erişebilir.

**Ağ Servisi:** Local System / Administrator kullanıcısına göre daha az yetkili olup network kaynaklarına erişecek servis kullanıcısıdır.

**Yerel Servis:** Network Service kullanıcısıyla aynı sınırlı yetkilere sahip olup tek farkı network kaynaklarına erişemez. Bu kullanıcı genellikle makinenin dışındaki kaynaklara erişmeyecek servisler tarafında tercih edilir.

**Uzak Masaüstü Kullanıcısı:** Yerel makineye ağ üzerinden uzaktan bağlanarak servisleri yönetebilen kullanıcıdır.

**Yönetici:** Bir bilgisayarda, söz konusu bilgisayardaki diğer kullanıcıları etkileyecek değişiklikler yapabilen kişidir.

**Toplu iş:** Bilgisayarda belirli bir sırayla yapılması istenen işlemlerin müdahaleye gerek duyulmadan yapılmasını sağlayan işlemlere denir

**Aygıt Sürücüsü:** İstenilen donanımın çalışmasını ve kontrol edilmesini sağlayan yazılımlardır. Program ve donanımlar arasında bağlantı görevi görür.

**Dizin / Dosya:** Dosya sisteminde diğer bilgisayar dosyalarına referans kayıtları tutan bir kataloglama yapısıdır.

**Konuk Hesabı:** Bilgisayarınızı kullanmasına izin vermek istediğiniz diğer kişiler için oluşturulan hesaplardır

**Konsol:** Bir konsol geleneksel olarak kullanıcının komutları girebileceği ve girilen komutların sonuçları veya bilgisayardan durum mesajları gibi çıktıları görüntüleyebileceği bir bilgisayar terminalini ifade eder.

**Çıkarılabilir Medya:** Genellikle manyetik veya optik yollarla bilgisayar verilerini saklama yöntemidir.Örneğin USB, CD, DVD vb.

**Etki Alanı Denetleyicisi**: Etki alanı denetleyicisi, kimlik doğrulama işlemlerinin tek bir yerden yönetilmesini sağlayan ve bilgisayar ağlarındaki kullanıcıların bağlı bulunduğu sunucuya verilen isimdir.

**Etki Alanı:** Ortak bir bilgisayar ağındaki kullanıcıların bağlı bulunduğu sunucuya verilen isim

**Kanal:** Elektronik ortamlar arasında verilerin, birinden diğerine ulaşması için gerekli olan yapılar.

**Önbellek**: Genellikle güç kaybolduğunda verilerin kalıcı olmayacağı geçici bellektir.

**İş İstasyonu:** Teknik ve bilimsel uygulamalar için tasarlanmış bir bilgisayardır. Tek bir kullanıcının kullanması için tasarlanmışlardır.

**Ağ istemcisi:** Bir ağ üzerinde, sunucu bilgisayarlardan hizmet alan kullanıcı bilgisayarlarıdır. Bilgiye erişim yetkileri sunucu tarafından belirlenir.

**SMB (Sunucu İleti Bloğu):** Ağ dosya paylaşımı ve veri doku protokolüdür. İstemciler sunucularda verilere erişmek için SMB kullanır.

**Service Principal Name (SPN):** Objeler üzerinde bulunan öznitelik ismi olarak bilinmektedir. User ya da bir computer hesabı için kontrol etmek isterseniz, “serviceprincipalname” kısmından öz niteliğini görebilirsiniz

**SID:** Bilgisayar kullanıcılara ve Security gruplarına verilen evrensel bir kimliktir. Yani Her vatandaşın kendine has bir T.C. Numarasının olduğunu düşünürsek, Bilgisayarda yeni bir işletim sistemi kurulduğunda ve bilgisayardaki her bir kullanıcıya verilen bağımsız bir kimlik numarasına Windows SID denir.

**Yazılım Varlık Yönetimi (SAM):** Şirketlerde sahip olduğu donanımlarda kullanılan tüm Microsoft yazılımlarının sayımı ve tespiti için yapılan çalışmadır

**Adlandırılmış Kanallar:** Bir kanal sunucusu ve bir veya daha fazla kanal istemcisi arasındaki işlemler arası iletişimi sağlar.

**NTLM (New Technology LAN Manager)**: Sınama-yanıt (challenge-response) yapısını kullanarak şifrelenmemiş kullanıcı adı parola bilgisi yerine Windows kimlik bilgileri ile doğrulamayı gerçekleştirir.

**Null** : Herhangi bir değere sahip olmama durumu

**Kerberos :** Güvenli olmayan bir ağ üzerinde haberleşen kaynakların, bilet mantığını kullanarak kendi kimliklerini ispatlamak suretiyle iletişim kurmalarını sağlayan bir bilgisayar ağı kimlik doğrulama protokolüdür

**AES128:** AES algoritması ile 128 bit şifreleme kullanan algoritmadır.

**HMAC\_SHA1:** Karma tabanlı ileti kimlik doğrulama kodu olarak kullanılan anahtarlı karma algoritması türüdür.

**LAN Manager:** Yerel alan ağı yöneticisi.

**NTLMv2:** NTLM kimlik doğrulama sistemidir.

**LDAP (Basit İndeks Erişim Protokolü):** TCP/IP üzerinde çalışan indeks servislerini sorgulama ve değiştirme amacıyla kullanılan uygulama katmanı protokolü.

**SSP:** Tedarik tarafı platformu (SSP), yayıncıların reklam gösterimlerinin satışını kolaylaştıran programatik bir yazılımdır.

**Remote Procedure Call (RPC):** esasında sunucu ve istemcilerin başarılı bir iletişim kurabilmesi için dizayn edilmiştir.

**Alt Sistemler:** Alt sistemler, sistemin birbirine dayalı ve bağımlı olan alt parçalarıdır. Alt sistemler, parçası oldukları sistemden ayrı özellikler taşır. Bir örgütün birimleri, alt sistem özelliği gösterebilir.

**Kayıt Defteri:** Microsoft Windows 32-bit, 64-bit, sürümleri ve Windows Mobile'da işletim sisteminin seçeneklerini ve ayarlarını tutan bir dizindir

**Bluetooth:** Çevre birimleri ve diğer cihazların birbirleri ile kablo bağlantısı olmadan görüş doğrultusu dışında bile olsalar haberleşmelerine olanak sağlar.

**Browser:** Bilgisayar kullanıcılarının internet üzerinden sitelere ulaşmasını sağlayan programlara verilen isimdir.

**Map :** Web tasarımında kullanılan, yüklenen grafiğin belirli bölgelerine basıldığında değişik bağlantıları çağırmak için kullanılan sistemdir.

**IIS**: IIS olarak bilinen Internet Information Services esnek yapılı ve genel kullanım için Microsoft tarafından Windows sistemlerde çalışmak üzere geliştirilmiş bir web sunucudur

**Web Sunucu:** İnternet uygulamalarının saklandığı bilgisayarlara web sunucusu adı verilmektedir. Bu server uygulamaların varsayılan olarak belirlenmiş TCP portlarından gelen mesajları işlemektedir.

**Internet Bağlantı Paylaşımı (ICS)**: Windows bilgisayarların yerel alan ağının (LAN) tek bir internet bağlantısını paylaşmasına izin verir.

**Topoloji:** Bir ağdaki bilgisayarların nasıl yerleşebileceğini, nasıl bağlanacağını, veri iletiminin nasıl olacağını belirleyen gene yapıdır.

**Lxss Manager:** Windows kernel sistem çağrılarıyla (calls), Linux kernel sistem çağrılarının birbirine map edilmesine sağlayan bir ara katman

**Dosya Taşıma Protokolü (FTP):** İnternete bağlı iki bilgisayar arasında dosya transferini sağlayan bir protokoldür

**ISCSI:** SCSI tabanlı depolama komutlarını, ağ yapısının her yerinden gönderebilen bir protokoldür (Bunun için LAN yapısı veya VPN bağlantı kullanabilir). iSCSI servisi, hayali bir hard disk belirler (Bir hard disk illüzyonu oluşturur) ve lokal bir bilgisayar üzerinden görülebilir.

**Küçük Bilgisayar Sistemi Arayüzü (SCSI):** Sabit Disk, CD sürücü, tarayıcı, yazıcı gibi aygıtları paralel arabirim standartlarından daha uyumlu ve gelişmiş bir şekilde kontrol eden standarttır.

**SSH:** Kullanıcılara sunucularını internet üzerinden kontrol etmesini ve düzenlemesini sağlayan uzak yönetim protokolüdür

**Eş Adı Çözümlemesi:** Çözüm için hem zaman uyumlu hem de zaman uyumsuz yöntemler dahil olmak üzere bir eş adı ağ uç noktalarıyla çözümleme işlemini tanımlar.

**Eşler Arası Ağ (P2P):** Merkezi bir sunucu gibi bir üçüncü taraf olmadan kullanıcıların doğrudan birbirleri arasında gerçekleştirdiği veri paylaşımını ifade eder

**Peer Networking Identity Manager:** Eş ağ iletişimi için kimlik hizmeti sağlar. Eşler arası bir uygulamada eş kimliklerin oluşturulmasına, numaralandırılmasına ve değiştirilmesine izin verir.

**Eş Ağ Adı Çözümleme Protokolü (PNRP) :** Eşler arası ortamlarda eşlerin adlarından ve diğer tanımlayıcı türlerinden çözülebilmesi için yapılan dağıtılmış (neredeyse sunucusuz), üçüncü tarafı dahil etmeden çalışan, eski adreslerin çözümlenmesine kendini güncelleyerek imkan vermeyen, ayrıca sadece bilgisayarlar için değil hizmetler için de bu çözümlenmeyi sağlayan protokoldür.

**Yazdırma Biriktiricisi (Spooler) :** Yerel ve ağdaki tüm yazdırma işlem ve sıralarını kontrol eden servistir

**Sorun Raporları ve Çözümleri Denetim Masası Desteği :** Sorun Raporları ve Çözümleri Kontrol Paneli için sistem düzeyinde raporların görüntülenmesi, gönderilmesi ve silinmesi için destek sağlayan servistir.

**Uzaktan Erişim Otomatik Bağlantı Yöneticisi (RasAuto) :** Uzak bir ağa veya bilgisayara başarısız bağlanma girişimlerini algılar ve bağlantı için alternatif yöntemler sağlayan hizmettir

**Uzak Masaüstü Yapılandırması (SessionEnv) :**  SYSTEM bağlamı gerektiren tüm Uzak Masaüstü Hizmetleri ve Uzak Masaüstü ile ilgili yapılandırma ve oturum bakım etkinliklerinden sorumlu hizmettir.

**Uzak Masaüstü Hizmetleri (TermService) :** Kullanıcıların uzak bir bilgisayara etkileşimli olarak bağlanmasına olanak tanıyan servistir.

**Uzak Masaüstü Hizmetleri Kullanıcı Modu Bağlantı Noktası Yeniden Yönlendiricisi(UmRDP Service) :** Uzak Masaüstü bağlantıları için yazıcıların, sürücülerin ve bağlantı noktalarının yeniden yönlendirilmesine olanak tanır.

**RPC Locator** : Uzaktan Yordam Çağrısı (RPC) Bulucu hizmeti, RPC sunucularını bulmak için RpcNs\* API'lerini kullanan RPC istemcilerine olanak tanır.

**Uzak Kayıt Defteri ( Remote Registry) :** Uzak Kayıt Defteri hizmeti, uygun izinlere sahip uzak kullanıcıların etki alanı denetleyicisindeki kayıt defteri ayarlarını değiştirmesine olanak tanır.

**Yönlendirme ve Uzaktan Erişim (Remote Access) :** Yönlendirme ve Uzaktan Erişim (Uzaktan Erişim) hizmeti, çok protokollü LAN'dan LAN'a, LAN'dan WAN'a, VPN ve NAT yönlendirme hizmetleri sağlar. Bu hizmet aynı zamanda çevirmeli ağ ve VPN uzaktan erişim hizmetleri de sağlar.

**Sunucu (server) :** Veri merkezlerinde korunaklı bir alan içerisinde tutulan, kapatılması söz konusu olmadığı için geniş güvenlik önemleri ile korunan, jeneratör ve soğutma sistemleri ile desteklenerek çalıştırılan, kesintisiz internet bağlantısına sahip ve dayanıklılığı yüksek bilgisayarlara denir.

**Basit TCP/IP Hizmetleri :** Basit TCP/IP Hizmetleri (simptcp), aşağıdaki protokoller ve bağlantı noktaları için destek uygular:

* Echo, port 7, RFC 862
* Discard, port 9, RFC 863
* Character Generator, port 19, RFC 864
* Daytime, port 13, RFC 867
* Quote of the Day, port 17, RFC 865

**Basit Ağ Yönetim Protokolü(SNMP)** :İsteklerine yerel bilgisayar tarafından hizmet verilmesine izin verir. Bu hizmet, ağ cihazlarındaki etkinliği izleyen ve ağ konsolu iş istasyonuna rapor veren aracıları içerir.

**Özel Yönetim Konsolu Yardımcısı (sacsvr) :** Özel Yönetim Konsolu Yardımcısı (sacsvr) hizmeti, bilgisayarın işlevleri Dur hata mesajı nedeniyle durdurulursa, Windows Server 2008 R2 çalıştıran bir bilgisayarda uzaktan yönetim görevlerini gerçekleştirme yeteneği sağlar.

**SSDP Bulucu (SSDPSRV)** : Evrensel Tak ve Çalıştır (UPnP) aygıtları gibi basit hizmet bulma protokolünü (SSDP) kullanan ağ aygıtlarını ve hizmetlerini keşfeder.

**UPnP :** Bir ağdaki cihazların birbirlerine bağlanabilmesi için gerekli olan portları otomatik olarak açıp kapayan bir protokoldür.

**UPnP Device Host (upnphost) :** UPnP Aygıt Ana Bilgisayarı (upnphost) hizmeti, ağ aygıtları için eşler arası UPnP işlevselliğini destekler. Bu hizmet, aygıt ve ağ hizmeti kurulumunu ve yönetimini basitleştirir ve sürücüsüz, standartlara dayalı protokol mekanizmaları aracılığıyla aygıt ve hizmet keşfini ve kontrolünü gerçekleştirir.

**Web Yönetim Hizmeti (WMSvc) :** Web Yönetim Hizmeti (WMSVC), yöneticilerin bu bilgisayarda bulunan web sunucusunu, siteleri ve uygulamaları yönetebilmesi için uzaktan ve yetki verilmiş yönetim özelliklerini etkinleştirir.

**Windows Hata Raporlama Hizmeti (WerSvc) :** Programlar çalışmayı veya yanıt vermeyi durdurduğunda hataları bildirir ve mevcut çözümlerin teslim edilmesini sağlar.

**Windows Olay Toplayıcısı (WecSvc)** : WS-Management protokolünü destekleyen uzak kaynaklardan gelen olaylara kalıcı abonelikleri yönetir.

**Windows Uzaktan Yönetim (WS Management) :** WS-Management, uzak yazılım ve donanımı yönetmek için kullanılan standart bir Web hizmetleri protokolüdür.

**World Wide Web Yayınlama Servisi (W3SVC) :** IIS ek bileşeni aracılığıyla web bağlantısı ve web sitelerinin yönetimini sağlar.

**Xbox Live :** Microsofta ait oyun yayınlama ve geliştirme platformu.

**Windows Defender :** Windows işletim sistemi kullanan bilgisayarlarda işletim sisteminin kurulmasıyla birlikte yüklenen güvenlik duvarı ve koruma yazılımıdır

**Günlük :** Sisteminizde belirli olaylar meydana geldiğinde, otomatik olarak üretilen bir dosyadır, zaman damgalıdır ve işletim sistemlerinde veya yazılım uygulamalarında perde arkasında gerçekleşen her şeyi pratik olarak kaydedebilir.

**Profil :** Belirli bir kullanıcıyla veya özelleştirilmiş bir masaüstü ortamıyla ilişkili kişisel verilerin görsel bir görüntüsüdür. Bu nedenle bir profil, bir kişinin kimliğinin açık dijital temsilini ifade eder

**PnP(plug and play) :** Genellikle bilgisayarlarda sisteme bağlı olan bir donanımın herhangi bir ayarlamaya ihtiyaç olmaksızın, donanımın sürücüsünün otomatik olarak sisteme yüklenmesi anlamında kullanılan terimdir.

**Süreç(Process) :** Belleğe yüklenmiş ve işlemcide (CPU) yürütülmekte olan bir program olarak tanımlanmaktadır.

**DS Access :** DS Access güvenlik denetim ilkesi ayarları, Active Directory Etki Alanı Hizmetleri'ndeki (AD DS) nesnelere erişme ve bunları değiştirme girişimlerinin ayrıntılı bir denetim izini sağlar.

**Grup İlkesi :** Microsoft Windows Active Directory'nin kullanıcı ve bilgisayar hesaplarına ek denetimler ekleyen bir özelliğidir. BT ortamlarında merkezi yönetimi ve işletim sistemlerini yapılandırmasını sağlar.

**Denetim İlkesi :** Denetlemek istediğiniz güvenlikle ilgili olayların kategorilerini belirler. Windows'un bu sürümü ilk yüklendiğinde, tüm denetim kategorileri devre dışı bırakılır. Farklı denetim olay kategorilerini etkinleştirerek, kuruluşunuzun güvenlik gereksinimlerine uygun bir denetim ilkesi uygulayabilirsiniz.

**Kimlik Doğrulama İlkesi** : Bir varlığın(kurum, kişi ya da sistem) doğruladığı bir veri parçasının doğruluğunun teyit edilmesidir.

**IPSec :** Kullanılarak sağlanan iletişimlerde her paket için doğrulama ve şifreleme kullanarak koruma sağlayan bir protokol paketidir.

**Sistem :** Birbiriyle etkileşen veya ilişkili olan, bir bütün oluşturan cisim veya varlıkların bileşkesidir.

**Yerel Yönetici Parolası Çözümü(LAPS) :** Etki alanına katılmış bilgisayarlar için yerel yönetici hesabı parolalarının yönetimini sağlar.

**Kullanıcı Hesabı Denetimi (UAC) :** Windows işletim sistemlerindeki bir güvenlik bileşenidir. UAC, kullanıcıların sık kullanılan görevleri kullanıcı değiştirmek, oturumu kapatmak veya Farklı Çalıştır özelliğini kullanmak zorunda kalmadan, ister yönetici yetkileri olmadan, ister yönetici olarak gerçekleştirmelerini sağlar.

**Node :** Bilgisayar ağlarında başka birimlerle iletişim kurma yeteneği olan yönlendirici, istemci bilgisayar, sunucu bilgisayar gibi elektronik birimdir.

**Kaynak :** Bir bilgisayar sisteminin eriştiği komponentleri ifade eder

**Encryption :** Verilerin insanlar ve diğer bilgisayarlar tarafından okunmasını engellemek ve içeriğin aslına ulaşılmasının önüne geçmek amacıyla yapılan şifreleme işlemleridir.

**İntern Kontrol Mesajı Protokolü (ICMP) :** Hata mesajları ve TCP/IP yazılımının bir takım kendi mesaj trafiği amaçları için kullanılır

**OSPF (en kısa yola öncelik) :** Bir TCP/IP ağındaki router'ların birbirini otomatik olarak tanımasında kullanılan bir protokoldür

**NetBIOS (Network Basic Input/Output System) :** Bir yerel ağ (LAN) üzerindeki farklı bilgisayarların birbirleriyle iletişim kurmasını sağlayan (veri aktarımı vs.) bir sistemdir

**DOS (Disk İşletim Sistemi) :** Bilgisayarlar için ufak ve basit bir işletim sistemi türü olup, ana görevi disket ve sabit disk gibi saklama ortamlarının yönetimidir.

**DoS (Hizmet Engelleme Saldırısı) :** Belirli bir web sitesini, sunucuyu veya çevrimiçi hizmeti sınırlamak ya da tamamen ortadan kaldırmak için bilgisayar korsanları tarafından yapılan bir saldırıdır.

**DLL :** Aynı anda birden fazla program tarafından kullanılabilen kod ve veriler içeren bir kitaplıktır

**BranchCache :** Windows Server 2008 R2 ve Windows 7 ile birlikte sunulan, Windows Server 2012 ile birlikte ise bazı geliştirmelerin yapıldığı geniş alan ağı (Wide Area Network) bant genişliği optimizasyonunu sağlayan bir teknolojidir.

**Domain İsim Sunucusu (DNS) :** isimlerin IP'ye dönüştürülesi maksadıyla kullanılan ve 256 karaktere kadar da büyüyebilen bir sistemdir.

**HTTPS ( güvenli hiper metin aktarım iletişim protokolü) :** Bir bilgisayar ağı üzerinden güvenli iletişim için internet üzerinde yaygın olarak kullanılan bir HTTP (hiper metin aktarım iletişim protokolü) uzantısıdır.

**HotSpot :** İnternete bağlantımızın bir kablosuz yönlendirici aracılığı ile (WLAN) genellikle Wi-Fi kullanarak sağladığımız fiziksel bir bağlantı türüdür

**Lanman :** Lan Manager

**Topoloji :** Bir ağdaki bilgisayarların nasıl yerleşebileceğini, nasıl bağlanacağını, veri iletiminin nasıl olacağını belirleyen gene yapıdır.

**LLTDIO(Eşleyici G/Ç) :** Bir bilgisayarın bağlı olduğu bir ağın topolojisini keşfetmesini sağlar. Ayrıca, bir bilgisayarın bant genişliği tahmini ve ağ sağlığı analizi gibi Hizmet Kalitesi isteklerini başlatmasına izin verir.

**Ağ köprüsü :** İki TCP/IP ağını birbirine bağlayan bir donanımdır

**Netlogon uzak Protokolü ( MS-NRPColarak da bilinir) :** Yalnızca etki alanına katılmış cihazlarda kullanılan bir RPC arabirimidir.

**Unc Yolu :** Ana bilgisayar adından ile \ ayrılmış bir paylaşım adı. Birlikte, sunucu ve paylaşım adı birimi oluşturur.

**QoS(Quality of Service) :** Hizmet kalitesi verilen görevlere ve uygulamalara ihtiyaç duydukları internet bant genişliği sağlarlar.

**SNMP (Simple Network Management Protocol - Basit Ağ Yönetim Protokolü) :** ağı yönetirken, ağ yöneticisine yardımcı olan basit bir uygulama katmanı protokolüdür

**SSL(Güvenli Yuva Katmanı) :** bir web sitesinin kimliğini doğrulayan ve şifreli bir bağlantı sağlayan dijital bir sertifikadır

**TCP/IP :** TCP (Transmission Control Protocol) ve IP (Internet Protocol) protokollerinin birleştirilmesiyle oluşturulan internet üzerindeki bir iletişim metodudur

**IPv6 :** Internet Protocol'ünün altıncı revizyonudur. IPv6'in görevi de tıpkı IPv4 gibi internete bağlanan cihazlara eşsiz, nümerik bir IP adresi atamak.

**Ethernet :** Kablolu veya kablosuz ağda bilgisayarlar, routerlar ve switchler dahil olmak üzere cihazlara bağlanmak için kullanılan standart iletişim protokolüdür

**Wireless Local Area Network (WLAN):** Kablosuz yerel alan ağ

**Yazdırma biriktiricisi :** Yazıcı bunları yazdırmaya hazır olana kadar yazdırma işlerini geçici olarak bilgisayarın sabit diskinde veya bellekte depolayan bir yazılım / hizmettir.

**Oracle :**  Kompleks ve çok miktardaki verilerin güvenli bir ortamda korunabildiği, bilgilerin parça halinde değil bir bütün şeklinde tutulduğu, hızlı bir şekilde birden çok kullanıcının istenilen bilgiye erişimini sağlayabildiği veri tabanı yazılım programıdır.

**Sanallaştırma teknolojisi :** Fiziksel bir bilgisayar üzerindeki işlemci, bellek ve hafıza gibi kaynakların, birbirinden yalıtılmış olarak birden çok işletim sistemi ile aynı anda kullanım sağlayan bir paylaşım sistemidir.

**Güvenli Önyükleme :**  Kişisel bilgisayar sektörünün üyeleri tarafından geliştirilen ve bir cihazın yalnızca özgün donanım üreticisi (OEM) tarafından güvenilen yazılım kullanarak önyüklendiğinden emin olmaya yardımcı olan bir güvenlik standardıdır.

**önyükleme (İngilizce: booting) :** Bir donanım veya bir yazılım komutu ile elektrik verilen bilgisayarı başlatma işlemidir.

**UEFI :** Daha büyük boyuttaki sabit diskleri ve sürücüleri, daha hızlı önyükleme sürelerini, daha fazla güvenlik özelliğini ve daha fazla grafik ve fare imleci seçeneğini destekleyen bir yazılım biçimidir.

**Öznitelik:** Veri nesnesinin bir özelliğini, niteliğini temsil eden bir veri alanıdır

**Çevre Birimi Bileşen Ara Bağlantısı standardı (PCI):**  Neredeyse tüm masaüstü bilgisayarlarda bulunan endüstri standardı, yüksek hızlı bir veri yoludur.

**Metadata :** Bir kaynağın nerede üretildiği, kim tarafından üretildiği, en son ne zaman erişildiği, ne hakkında olduğu gibi birçok ayrıntı hakkında ek bilgiler taşıyan verilerdir.

**NVMe yeni nesil depolama teknolojisi :** (Non Volatile Express) Hızlı geçici olmayan bellek olarak tanımlanır

**Disk Kotası (web Alanı):** İnternet sitenizi meydana getiren tüm öğeleri içinde barındırır

**Dağıtılmış COM :** Bir ağ üzerine kuruludur. Yazılımla, ağdaki bileşenler arası uyumluluk ve kullanıcı açısından saydamlık sağlanır.

**Anahtar Dağıtım Merkezi ( Key-Distribution-Center/KDC) :** Kullanıcı ve hesabı İstenilen servisi sağlayan sunucu.

**Pano :** Kısa süreli veri depolama, kesme, kopyalama ve yapıştırma işlemleri tarafından kullanılan, işletim sistemi tarafından sağlanan belgeler veya uygulamalar arasında veri aktarımı için kullanılan bir veri arabelleğidir.

**PIN :** Kendi seçtiğiniz bir sayı kümesi veya harf ve sayıların bileşimidir.

**Endpoint :** API üzerinde belirli bir amaç için oluşturulmuş metodunuza verilen isim

**Microsoft Destek Tanı Aracı (MSDT) :** Microsoft Destek göndermek için bilgi toplar. Microsoft Destek sonra bu bilgileri analiz ve bilgisayarınızda yaşıyor olabilirsiniz herhangi bir soruna çözünürlüğünü belirlemek için kullanacaktır.

**NTP :** Fazlalık kapasitesi olan bir sıralı zaman dağıtım sistemidir. Ağdaki ve de hedef makinedeki algoritmaları, gecikmeleri ölçer. Bu teknikleri kullanarak saatleri saliselere kadar senkronize edebilir

**Active Directory :** Microsoft ağlarında kullanılan dizin hizmetidir. Bu veritabanı, kullanıcılar, bilgisayarlar, mekanlar, yazıcılar gibi organizasyonun tüm bilgilerini saklar.

**ActiveX :** Microsoft'un Microsoft Windows platformları için geliştirdiği bir nesne bileşeni modelidir

**API :** İki uygulamanın birbiriyle konuşmasına olanak tanıyan bir yazılım aracısı olan Uygulama Programlama Arayüzü'nün kısaltmasıdır.

**Biyometri :** Parmak izleri, parmak damarı, yüz ölçümleri, avuç içi, avuç içi damarı gibi kişiye özgün biyolojik ölçümlemelere denir.

**Adres sahteciliği :** Bir e-posta iletisinin Gönderen adresinin sahte olduğu saldırı türüdür. Sahte adresli bir ileti, kimliğine bürünülmüş bir kuruluştan veya alandan geliyormuş gibi görünüyor.

**Sabit disk ya da Hard disk kısaca HDD ya da (sabit disk sürücüsü) :** veri depolanması amacı ile kullanılan manyetik kayıt ortamlarıdır.

**Active Directory Domain Services :** Veri tabanı, kullanıcı hesapları, bilgisayar hesapları ve gruplar gibi tüm nesnelerin (Object) deposudur

**Aygıt Yöneticisi :** İşletim sistemlerinde korumalı mod mimarisinde uygulamaların işletim sisteminden bağımsız olarak donanıma erişiminin kısıtlandığı durumlarda donanımla veya işletim sistemi çekirdeği ile haberleşebilmek maksadı ile yazılan kodlardır.

**Bulut bilişim (İngilizce: cloud computing)** : Bilgisayarlar ve diğer cihazlar için, istendiği zaman kullanılabilen ve kullanıcılar arasında paylaşılan bilgisayar kaynakları sağlayan, internet tabanlı bilişim hizmetlerinin genel adıdır.

**Tanılama Verileri :** Cihazınız, cihazının ayarları, özellikleri ve düzgün çalışıp çalışmadığı hakkındaki bilgilerdir.

**Proxy :** Bağlanmak istediğiniz siteye başka bir kanal kullanarak geçmenize yarayan bir araçtır.

**Windows Insider :** Kullanıcıların tüm Windows güncellemelerini önceden alarak deneyimlemesine ve geri beslemeler iletebilmesine olanak sağlayan geniş çaplı bir program

**Gadget :** Bir yazılım, script, işletim sistemi, GUI veya web sayfasına ekstra özellikler kazandırmak, kullanıcı deneyimini olumlu yönde arttırmak için eklenen özellikler veya araçlardır.

**Cihaz kaydı :** Bir programcının cihazı bir işletim sistemi veya ek ekipman parçası ile kurmak ve kullanmak için kullanabileceği bilgileri sağlayan elektronik cihaz üzerindeki programlanabilir bir alandır

**Olay Görüntüleyicisi :** Microsoft'un Windows NT işletim sistemlerinin yöneticilerinin ve kullanıcıların olay günlüklerini yerel veya uzak bir makinede görmelerini sağlayan bir bileşendir.

**Aile Koruması :** Microsoft Windows tarafından 2007 Yılında geliştirilen aile ebeveynlerinin çocuklarını zararlı internet sitelerinden ve bilgisayar kullanım şeklinden koruma amacıyla sunulan bir Windows yazılımıdır.

**Explorer (Dosya Yöneticisi) :** Microsoft'un Windows, 95'den bu yana çıkarılan tüm işletim sistemi sürümlerinde yer alan dosya yöneticisidir.

**Veri Yürütme Engellemesi (DEP) :** Bilgisayarınızın virüsler veya başka güvenlik tehditleri nedeniyle hasar görmesini önleyebilen bir güvenlik özelliğidir.

**Ev grubu:** Bir ev ağı üzerinde dosyaları ve yazıcıları paylaşabilen bir bilgisayar grubudur.

**Mobil Cihaz Yönetimi (MDM) :** İşletmelerde kullanılan dizüstü bilgisayar, akıllı telefon ve tablet gibi mobil cihazların izlenmesi, yönetilmesi ve güvenliğinin sağlanarak kurumsal veri güvenliğinin artırılması sürecidir.

**Saldırı yüzeyi :** Yetkisiz bir kullanıcının bir sisteme erişebileceği ve veri ihlaline sebep olabileceği tüm olası noktalar veya saldırı vektörleri, kısaca saldırganlara açık olan tüm alanlardır.

**Otomatik Konuşma Tanıma(OSR) :** Bir programın insan konuşmasını yazılı biçime dönüştürebilme yeteneğidir.

**Karantina :** Herhangi bir program dosyasına virüs bulaşmış olabilir. Anti virüs programı bu dosyayı karantina bölgesine alır ve sana bildirir. Yani senin iznin olmadan bu dosyayı silmez. Virüs dosyasını zarar vermeyecek şekilde hapseder. Bu olaya denir.

**Watson :** IBM tarafından geliştirilen ve doğal dilde sorulan sorulara cevap vermek için tasarlanan bir yapay zekâ programıdır

**Güvenlik İstihbaratı :** Elektronik ortamlardan toplanmış ve zenginleştirilmiş verilerin bir süreçten geçirilerek analiz edilmesi sonucu saldırganların amaçları, metotları ya da saldırı türleri tespit edilerek erken önlem alınmasına olanak sağlayan bir istihbarat türüdür.

**Microsoft Defender Application Guard :** Güvenilmeyen web sitelerini yalıtılmış bir Microsoft Edge göz atma penceresinde açarak cihazınızın gelişmiş saldırılara karşı korunmasına yardımcı olan yazılımdır.

**Microsoft NetMeeting :** Microsoft tarafından geliştirilen ve Microsoft Windows'un birçok sürümünde (Windows 95 OSR2'den Windows XP'ye kadar) dahil edilen, durdurulan bir VoIP ve çok noktalı video konferans istemcisidir.

**Out-of-box Experience (OOBE):** Kutu açılımından sonra dijital dağıtım için veya bir ürünü alırken bir son kullanıcı için bir ekrandır

**RemoteFX :** Kullanıcıların Windows 7 masaüstü ve uygulama deneyimlerini sanallaştırılmış bir ortamda çalıştırmayı sağlar ve 3D hızlandırılmış grafik ile fiziksel bir bilgisayar deneyimi sunar.

**Kullanıcı Arayüzü Tasarımı(UI) :** Dokunsal, işitsel ya da görsel iletişim köprüsü kurarak etkileşimi kolaylaştıran tasarımlara verilen bir addır.

**Paralel port veya paralel kapı :** Bilgisayarın kasasının arkasında bulunan 25 pinlik D şeklindeki konnektördür. Genellikle yazıcı bağlanmak için kullanılır.

**RSS (Really Simple Syndication) Gerçekten Basit Dağıtım :** Haber sağlayan siteler, bloglar veya podcastler gibi sıklıkla güncellenen sitelerin güncellemelerinden geri kalmamanızı sağlayan bir web sitesi bildirimcisidir.

**OCR (Optical Character Recognition - Optik Karakter Tanıma) :** Taranmış kağıt evraklar, PDF dosyalar veya dijital kamerayla çekilen resimler gibi belge türlerinin düzenlenebilir ve aranabilir verilere dönüştürülmesine olanak sağlayan bir teknolojidir.

**Cortana :** Microsoft tarafından bir akıllı kişisel asistan.

**Ağ Bilgi Servisi, ( The Network Information Service ya da NIS ( Normalde Yellow Pages (YS) diye adlandırılır.)):** Kullanıcı ve host adları gibi sistem konfigürasyonu bilgilerinin dağıtımını yapan sunucu-istemci rehberi hizmeti protokolüdür.

**Windows Hello :** Yüzünüzü, parmak izinizi veya PIN kodu kullanarak oturum açmanın daha kişisel bir yoludur.

**Windows kabuğu :** Microsoft Windows işletim sisteminin grafik kullanıcı arabirimidir.

**Windows Sandbox :** Windows'ta şüphelendiğiniz, güvenmediğiniz programları ve uygulamaları test edebilmeniz için Sanallaştırma Teknolojisi aracılığıyla sanal bir Windows 10 oluşturmamıza olanak tanır ve burada şüpheli dosya ve programlar ile çalışmanıza olanak tanır.

**Ek Yöneticisi :** Bilgisayarınızı, e-posta iletileriyle alabileceğiniz güvenli olmayan eklerden veya internetten kaydedebileceğiniz güvenli olmayan dosyalardan korumaya yardımcı olur.

Windows Spotlight varsayılan olarak Windows 10'da bulunan, resimleri ve reklamları Bing'den otomatik olarak indiren ve Windows 10 kilit ekranı çalıştıran bir bilgisayarda kilit ekranı gösterildiğinde görüntüleyen bir özelliktir.

**Codec bileşenleri :** Dosya veya verideki dijital sinyalleri kodlayan ve kodları çözen küçük dosyalardır.

1. **SORUMLULUKLAR**
2. **UYGULAMA**

[**1 Hesap İlkeleri**](#bir)

**[1.1 Parola İlkesi](#birbir)**

* [1.1.1 (L1) 'Parola geçmişini zorla' seçeneği '24 veya daha fazla şifre' olarak ayarlanmalıdır.](#birbirbir)
* [1.1.2 (L1) Maximum parola süresi seçeneği '365 gün veya daha az, ama 0 olamaz' olarak ayarlanmalıdır.](#birbiiki)
* [1.1.3 (L1)'Minimum parola süresi' seçeneği '1 gün veya daha fazla' olarak ayarlanmalıdır.](#birbirüç)
* [1.1.4 (L1) 'Minimum parola uzunluğu' seçeneği '14 veya daha fazla karakter' olarak ayarlanmalıdır.](#birbirdört)
* [1.1.5 (L1) 'Parola karışıklık gereksinimlerini karşılamalıdır' seçeneği 'Etkin' olarak ayarlanmalıdır.](#birbirbeş)
* [1.1.6 (L1) 'Minimum şifre uzunluğu limiti esnektir' seçeneği 'Etkin' olarak ayarlanmalıdır.](#a116)
* [1.1.7 (L1) 'Parolaları geri döndürülebilir şifreleme kullanarak depolama' seçeneği 'Devre Dışı' olarak ayarlanmalıdır.](#a117)

[**1.2 Hesap Kilitleme İlkesi**](#a12)

* [1.2.1 (L1) 'Hesap kilitleme süresi' seçeneği '15 dakika veya daha fazla' olarak ayarlanmalıdır.](#a121)
* [1.2.2 (L1) 'Hesap kilitleme eşiği' seçeneği '5 veya daha az geçersiz oturum açma girişimi ancak 0 değil' olarak ayarlanmalıdır.](#a122)
* [1.2.3 (L1) 'Hesap kilitleme sayacını şu süreden sonra sıfırla' seçeneği '15 dakika veya daha fazla' olarak ayarlanmalıdır.](#a123)

[**2 Yerel İlkeler**](#a2)

[**2.1 Denetim İlkeleri**](#a21)

[**2.2 Kullanıcı Hakları Atamaları**](#a22)

* [2.2.1 (L1) 'Kimlik Bilgileri Yöneticisi’ne güvenilir kullanıcı olarak eriş' seçeneği 'Hiç Kimse' olarak ayarlanmalıdır.](#a221)
* [2.2.2 (L1) 'Bu bilgisayara ağdan eriş' seçeneği 'Yöneticiler, Uzak Masaüstü Kullanıcıları' olarak ayarlanmalıdır.](#a222)
* [2.2.3 (L1) 'İşletim sisteminin bir parçası olarak görün' seçeneği 'Hiç Kimse' olarak ayarlanmalıdır.](#a223)
* [2.2.4 (L1) 'İşlem için bellek kotalarını ayarla' seçeneği 'Yöneticiler, Yerel Servis, Ağ Servisi' olarak ayarlanmalıdır.](#a224)
* [2.2.5 (L1) 'Yerel olarak oturum açmaya izin ver' seçeneği 'Yöneticiler, Kullanıcılar' olarak ayarlanmalıdır.](#a225)
* [2.2.6 (L1) 'Uzak Masaüstü Hizmetleri ile oturum açmaya izin ver' seçeneği 'Yöneticiler, Uzak Masaüstü Kullanıcıları' olarak ayarlanmalıdır.](#a226)
* [2.2.7 (L1) 'Dosyaları ve dizinleri yedekle' seçeneği 'Yöneticiler' olarak ayarlanmalıdır.](#a227)
* [2.2.8 (L1) 'Sistem saatini değiştir' seçeneği 'Yöneticiler, Yerel Servis' olarak ayarlanmalıdır.](#a228)
* [2.2.9 (L1) 'Saat dilimini değiştir' seçeneği 'Yöneticiler, Yerel Servis, Kullanıcılar' olarak ayarlanmalıdır.](#a229)
* [2.2.10 (L1) 'Disk belleği dosyası oluştur' seçeneği 'Yöneticiler' olarak ayarlanmalıdır.](#a2211)
* [2.2.11 (L1) 'Belirteç nesnesi oluştur' seçeneği 'Hiç Kimse' olarak ayarlanmalıdır.](#a2211)
* [2.2.12 (L1) 'Genel nesneler oluştur' seçeneği 'Yöneticiler, Yerel Servis, Ağ Servisi, Servis' olarak ayarlanmalıdır.](#a2212)
* [2.2.13 (L1) 'Kalıcı paylaşılan nesneler oluştur' seçeneği 'Hiç Kimse' olarak ayarlanmalıdır.](#a2213)
* [2.2.15 (L1) 'Programlarda hata ayıklama' seçeneği 'Yöneticiler' olarak ayarlanmalıdır.](#a2215)
* [2.2.16 (L1) 'Bu bilgisayara ağdan erişimi reddet' seçeneği 'Konuklar, Yerel Hesaplar' olarak ayarlanmalıdır.](#a2216)
* [2.2.17 (L1) 'Toplu iş olarak oturum açmayı reddet' seçeneği 'Konuklar' olarak ayarlanmalıdır.](#a2217)
* [2.2.18 (L1) 'Servis olarak oturum açmayı reddet' seçeneği 'Konuklar' olarak ayarlanmalıdır.](#a2218)
* [2.2.19 (L1) 'Yerel olarak oturum açmayı reddet' seçeneği 'Konuklar' olarak ayarlanmalıdır.](#a2219)
* [2.2.20 (L1) 'Uzak Masaüstü Servisleri aracılığıyla oturum açmayı reddet' seçeneği 'Konuklar, Yerel hesaplar' olarak ayarlanmalıdır.](#a2220)
* [2.2.21 (L1) 'Bilgisayar ve kullanıcı hesaplarını yetkilendirme için güvenilir olacak şekilde etkinleştir' seçeneği 'Hiç Kimse' olarak ayarlanmalıdır.](#a2221)
* [2.2.22 (L1) 'Uzak sistemden kapanmaya zorla' seçeneği 'Yöneticiler' olarak ayarlanmalıdır.](#a2222)
* [2.2.23 (L1) 'Güvenlik denetimleri oluştur' seçeneği 'Yerel Servis, Ağ Servisi' olarak ayarlanmalıdır.](#a2223)
* [2.2.24 (L1) 'Kimlik doğrulamasından sonra istemci kimliğine bürün' seçeneği 'Yöneticiler, Yerel Servis, Ağ Servisi, Servis' olarak ayarlanmalıdır.](#a2224)
* [2.2.25 'Zamanlama önceliğini arttır' seçeneği 'Yöneticiler, Window Yöneticisi/ Window Yöneticisi Grubu' olarak ayarlanmalıdır.](#a2225)
* [2.2.26 (L1) 'Aygıt sürücüsü yükle ve kaldır' seçeneği 'Yöneticiler' olarak ayarlanmalıdır.](#a2226)
* [2.2.27 (L1) 'Sayfaları belleğe kilitle' seçeneği 'Hiç Kimse' olarak ayarlanmalıdır.](#a2227)
* [2.2.28 (L2) 'Toplu iş olarak oturum aç' seçeneği 'Yöneticiler' olarak ayarlanmalıdır.](#a2228)
* [2.2.29 (L2) 'Servis olarak oturum aç' seçeneği 'NT Servis, Tüm Servisler' olarak ayarlanmalıdır.](#a2229)
* [2.2.30 (L1) 'Denetim ve güvenlik günlüğünü yönet' seçeneği 'Yöneticiler' olarak ayarlanmalıdır.](#a2230)
* [2.2.31 (L1) 'Nesne etiketini değiştir' seçeneği 'Hiç Kimse' olarak ayarlanmalıdır.](#a2231)
* [2.2.32 (L1) 'Ürün yazılımı ortam değerlerini değiştir' seçeneği 'Yöneticiler' olarak ayarlanmalıdır.](#a2232)
* [2.2.33 (L1) 'Toplu bakım görevleri gerçekleştir' seçeneği 'Yöneticiler' olarak ayarlanmalıdır.](#a2233)
* [2.2.34 (L1) 'Tekil İşlemi Göster' seçeneği ' Yöneticiler' olarak ayarlanmalıdır.](#a2234)
* [2.2.35 (L1) 'Sistem performansını göster' seçeneği 'Yöneticiler, NT SERVICE\WdiServiceHost' (Otomatik) olarak ayarlanmalıdır.](#a2235)
* [2.2.36 (L1) 'İşlem düzeyi belirtecini değiştir' seçeneği 'YEREL SERVİS, AĞ SERVİSİ' (Otomatik) olarak ayarlanmalıdır.](#a2236)
* [2.2.37 (L1) 'Dosyaları ve dizinleri geri yükle' seçeneği 'Yöneticiler' (Otomatik) olarak ayarlanmalıdır.](#a2237)
* [2.2.38 (L1) 'Sistemi kapat' seçeneği 'Yöneticiler, Kullanıcılar' (Otomatik) olarak ayarlanmalıdır.](#a2238)
* [2.2.39 (L1) 'Dosyaların veya diğer nesnelerin sahipliğini al' seçeneği 'Yöneticiler' (Otomatik) olarak ayarlanmalıdır.](#a2239)

[**2.3 Güvenlik Seçenekleri**](#a23)

[**2.3.1 Hesaplar**](#a231)

* [2.3.1.1 (L1) 'Hesaplar: Yönetici hesabı durumu' 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a231a1)
* [2.3.1.2 (L1) 'Hesaplar: Microsoft hesaplarını engelle' seçeneği 'Kullanıcılar Microsoft hesapları ekleyemez veya bu hesaplarla oturum açamaz' olarak ayarlanmalıdır.](#a231a2)
* [2.3.1.3 (L1) 'Hesaplar: Konuk hesabı durumu' 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a231a3)
* [2.3.1.4 (L1) 'Hesaplar: Yerel hesaplarda boş parola kullanımını yalnızca konsolda oturum açma ile sınırla' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a231a4)
* [2.3.1.5 (L1) 'Hesaplar: Yönetici hesabını yeniden adlandır' seçeneği 'Yönetici' olarak ayarlanmalıdır. (Otomatik)](#a2315)
* [2.3.1.6 (L1)'Hesaplar: Konuk hesabını yeniden adlandır' seçeneği Konuk hesaplar devre dışı olduğu için hiçbir önem göstermemektedir.](#a2316)

[**2.3.2 Denetim**](#a232)

* [2.3.2.1 (L1) 'Denetim: Denetim ilkesi alt kategori ayarlarını (Windows Vista veya üzeri) denetim ilkesi kategorisi ayarlarını geçersiz kılmaya zorla' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a2321)
* [2.3.2.2 (L1) 'Denetim: Güvenlik denetimleri kaydedilemiyorsa sistemi hemen kapat' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a2322)

[**2.3.4 Cihazlar**](#a234)

* [2.3.4.1 (L1) 'Cihazlar: Çıkarılabilir medyayı biçimlendirmesine ve çıkarmasına izin verildi' seçeneği 'Yöneticiler ve Etkileşimli Kullanıcılar' (Otomatik) olarak ayarlanmalıdır.](#a2341)
* [2.3.4.2 (L2) 'Cihazlar: Kullanıcıların yazıcı sürücülerini yüklemesini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a2342)

[**2.3.6 Domain üyesi**](#a236)

* [2.3.6.1 (L1) 'Etki Alanı Üyesi: Güvenli kanal verilerini dijital olarak şifreleyin veya imzalayın (her zaman)' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a2361)
* [2.3.6.2 (L1) 'Etki Alanı Üyesi: Güvenli kanal verilerini şifreleme (mümkünse)' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a2362)
* [2.3.6.3 (L1) 'Etki Alanı üyesi: Güvenli kanal verilerini dijital olarak imzala (mümkünse)' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a2363)
* [2.3.6.4 (L1) 'Etki alanı üyesi: Makine hesabı şifre değişikliklerini devre dışı bırak' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a2364)
* [2.3.6.5 (L1) 'Etki Alanı üyesi: Maksimum makine hesabı şifre yaşı' seçeneği '30 veya daha az gün, ancak 0 değil' olarak ayarlanmalıdır. (Otomatik)](#a2365)
* [2.3.6.6 (L1) 'Etki Alanı üyesi: Güçlü (Windows 2000 veya üzeri) oturum anahtarı gerektir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a2366)

[**2.3.7 İnteraktif oturum açma**](#a237)

* [2.3.7.1 (L1) 'Etkileşimli oturum açma: CTRL+ALT+DEL tuşlarına basmayın' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a2371)
* [2.3.7.2 (L1) 'Etkileşimli oturum açma: Son oturum açılanları görüntüleme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a2372)
* [2.3.7.3 (BL) 'Etkileşimli oturum açma: Makine hesabı kilitleme eşiği' seçeneği '10 veya daha az geçersiz oturum açma girişimi, ancak 0 değil' olarak ayarlanmalıdır.](#a2373)
* [2.3.7.4 (L1) 'Etkileşimli oturum açma: Makine hareketsizlik sınırı' seçeneği '900 veya daha az saniye, ancak 0 değil' olarak ayarlanmalıdır. (Otomatik)](#a2374)
* [2.3.7.5 (L1) 'Etkileşimli oturum açma: Oturum açmaya çalışan kullanıcılar için ileti metni' seçeneği 'Mesaj yok' olarak ayarlanmalıdır. (Otomatik)](#a2375)
* [2.3.7.6 (L1) 'Etkileşimli oturum açma: Oturum açmaya çalışan kullanıcılar için ileti başlığı' seçeneği 'Mesaj Yok' olarak ayarlanmalıdır. (Otomatik)](#a2376)
* [2.3.7.7 (L2) 'Etkileşimli oturum açma: Önbelleğe alınacak önceki oturum açma sayısı (etki alanı denetleyicisinin kullanılamaması durumunda)' ifadesi '4 veya daha az oturum açma' (Otomatik) olarak ayarlanmalıdır.](#a2377)
* [2.3.7.8 (L1) 'Etkileşimli oturum açma: Kullanıcıdan süre dolmadan önce parolayı değiştirmesini iste' seçeneği '5 ila 14 gün arasında' olarak ayarlanmalıdır. (Otomatik)](#a2378)
* [2.3.7.9 (L1) 'Etkileşimli oturum açma: Akıllı kart çıkarma davranışı' seçeneği 'İş İstasyonunu Kilitle' veya üstü (Otomatik) olarak ayarlanmalıdır.](#a2379)

[**2.3.8 Microsoft ağ istemcisi**](#a238)

* [2.3.8.1 (L1) 'Microsoft ağ istemcisi: İletişimi dijital olarak imzala (her zaman)' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a2381)
* [2.3.8.2 (L1) 'Microsoft ağ istemcisi: İletişimi dijital olarak imzala (sunucu kabul ederse)' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a2382)
* [2.3.8.3 (L1) 'Microsoft ağ istemcisi: Üçüncü taraf SMB sunucularına şifrelenmemiş parola gönder' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a2383)

[**2.3.9 Microsoft ağ sunucusu**](#a239)

* [2.3.9.1 (L1) 'Microsoft ağ sunucusu: Oturumu askıya almadan önce gereken boşta kalma süresi' seçeneği '15 dakika veya daha az' olarak ayarlanmalıdır. (Otomatik)](#a2391)
* [2.3.9.2 (L1) 'Microsoft ağ sunucusu: İletişimi dijital olarak imzala (her zaman)' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a2392)
* [2.3.9.3 (L1) 'Microsoft ağ sunucusu: İletişimi dijital olarak imzala (istemci kabul ederse)' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a2393)
* [2.3.9.4 (L1) 'Microsoft ağ sunucusu: Oturum açma saatleri sona erdiğinde istemcilerin bağlantısını kes' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a2394)
* [2.3.9.5 (L1) 'Microsoft ağ sunucusu: Sunucu SPN hedef adı doğrulama düzeyi' seçeneği 'İstemci tarafından sağlanıyorsa kabul et' veya üstü (Otomatik) olarak ayarlanmalıdır.](#a2395)

[**2.3.10 Ağ erişimi**](#a23a10)

* [2.3.10.1 (L1) 'Ağ erişimi: Anonim SID/İsim çevirisine izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a23101)
* [2.3.10.2 (L1) 'Ağ erişimi: SAM hesaplarının anonim numaralandırılmasına izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a23102)
* [2.3.10.3 (L1) 'Ağ erişimi: SAM hesaplarının ve paylaşımlarının anonim numaralandırılmasına izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a23103)
* [2.3.10.4 (L1) 'Ağ erişimi: Ağ kimlik doğrulaması için şifrelerin ve kimlik bilgilerinin depolanmasına izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a23104)
* [2.3.10.5 (L1) 'Ağ erişimi: Herkes izinlerinin anonim kullanıcılara uygulanmasına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a23105)
* [2.3.10.6 (L1) 'Ağ erişimi: Adlandırılmış Kanallar anonim olarak ulaşılabilir' seçeneği 'Hiçbiri' (Otomatik) olarak ayarlanmalıdır.](#a23106)
* [2.3.10.7 (L1) 'Ağ erişimi: Uzaktan erişilebilir kayıt defteri yolları' yapılandırıldığından emin olun (Otomatik)](#a23107)
* [2.3.10.8 (L1) 'Ağ erişimi: Uzaktan erişilebilir kayıt defteri yolları ve alt yolları' yapılandırıldığından emin olun (Otomatik)](#a23108)
* [2.3.10.9 (L1) 'Ağ erişimi: Adlandırılmış Kanallar ve Paylaşımlara anonim erişimi kısıtla' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a23109)
* [2.3.10.10 (L1) 'Ağ erişimi: İstemcilerin SAM'a uzaktan arama yapmasına izin verilmesini kısıtla' seçeneği 'Yöneticiler: Uzaktan Erişim: İzin Ver' (Otomatik) olarak ayarlanmalıdır.](#a231010)
* [2.3.10.11 (L1) 'Ağ erişimi: Paylaşımlar anonim olarak erişilebilir' seçeneği 'Hiçbiri' (Otomatik) olarak ayarlanmalıdır.](#a231011)
* [2.3.10.12 (L1) 'Ağ erişimi: Yerel hesaplar için paylaşım ve güvenlik modeli' seçeneği 'Klasik - yerel kullanıcılar kendileri gibi kimlik doğrulaması yapar' olarak ayarlanmalıdır. (Otomatik)](#a231012)

[**2.3.11 Ağ güvenliği**](#a2311)

* [2.3.11.1 (L1) 'Ağ güvenliği: Yerel Sistemin NTLM için bilgisayar kimliğini kullanmasına izin ver' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a23111)
* [2.3.11.2 (L1) 'Ağ güvenliği: Yerel sistemin NULL oturum geri dönüşüne izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a23112)
* [2.3.11.3 (L1) 'Ağ Güvenliği: Bu bilgisayara yapılan PKU2U kimlik doğrulama isteklerinin çevrimiçi kimlikleri kullanmasına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a23113)
* [2.3.11.4 (L1) 'Ağ güvenliği: Kerberos için izin verilen şifreleme türlerini yapılandır' seçeneği 'AES128\_HMAC\_SHA1, AES256\_HMAC\_SHA1, Gelecekteki şifreleme türleri' (Otomatik) olarak ayarlanmalıdır.](#a23114)
* [2.3.11.5 (L1) 'Ağ güvenliği: Bir sonraki parola değişikliğinde LAN Manager karma değerini saklamayın' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a23115)
* [2.3.11.6 (L1) 'Ağ güvenliği: Oturum açma saatleri sona erdiğinde oturumu kapatmaya zorla' seçeneği 'Etkin' olarak ayarlandığından emin olun (Manuel)](#a23116)
* [2.3.11.7 (L1) 'Ağ güvenliği: LAN Manager kimlik doğrulama düzeyi' seçeneği 'Yalnızca NTLMv2 yanıtı gönder. LM & NTLM’i reddet' olarak ayarlanmalıdır. (Otomatik)](#a23117)
* [2.3.11.8 (L1) 'Ağ güvenliği: LDAP istemcisi imzalama gereksinimleri' seçeneği 'İmzalama anlaşması yap veya üstü '(Otomatik) olarak ayarlanmalıdır.](#a23118)
* [2.3.11.9 (L1) 'Ağ güvenliği: NTLM SSP tabanlı (güvenli RPC dahil) istemciler için minimum oturum güvenliği' seçeneği 'NTLMv2 oturum güvenliği gerektir, 128 bit şifreleme gerektir' (Otomatik) olarak ayarlanmalıdır.](#a23119)
* [2.3.11.10 (L1) 'Ağ güvenliği: NTLM SSP tabanlı (güvenli RPC dahil) sunucular için minimum oturum güvenliği' seçeneği 'NTLMv2 oturum güvenliği gerektir, 128 bit şifreleme gerektir' (Otomatik) olarak ayarlanmalıdır.](#a231110)

[**2.3.14 Kriptografik sistemler**](#a2314)

* [2.3.14.1 (L2) 'Sistem şifrelemesi: Bilgisayarda depolanan kullanıcı anahtarları için güçlü anahtar korumasını zorla' seçeneği 'Anahtar ilk kullanıldığında kullanıcıya sorulur veya üstü’ (Otomatik) olarak ayarlanmalıdır.](#a23141)

[**2.3.15 Sistem nesneleri**](#a2315)

* [2.3.15.1 (L1) 'Sistem nesneleri: Windows dışı alt sistemler için büyük/küçük harf duyarsızlığı gerektir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a23151)
* [2.3.15.2 (L1) 'Sistem nesneleri: Dahili sistem nesnelerinin (ör. Sembolik Bağlantılar) varsayılan izinlerini güçlendir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a23151)

[**2.3.17 Kullanıcı Hesabı Kontrolü**](#a2317)

* [2.3.17.1 (L1) 'Kullanıcı Hesabı Denetimi: Yerleşik Yönetici hesabı için Yönetici Onay Modu' seçeneği ‘Etkin' (Otomatik) olarak ayarlanmalıdır.](#a23171)
* [2.3.17.2(L1) 'Kullanıcı Hesabı Denetimi: Yönetici Onay Modu'nda yöneticiler için yükseltme isteminin davranışı’ seçeneği 'Güvenli masaüstünde onay istemi' (Otomatik) olarak ayarlanmalıdır.](#a23172)
* [2.3.17.3 (L1) 'Kullanıcı Hesabı Denetimi: Standart kullanıcılar için yükseltme isteminin davranışı' seçeneği 'Yükseltme isteklerini otomatik olarak reddet' (Otomatik) olarak ayarlanmalıdır.](#a23173)
* [2.3.17.4 (L1) 'Kullanıcı Hesabı Denetimi: Uygulama yüklemelerini algıla ve yükseltme istemi' seçeneği 'Etkin' (Otomatik) olarak ayarlandığından emin olun](#a23174)
* [2.3.17.5 (L1) 'Kullanıcı Hesabı Denetimi: Yalnızca güvenli konumlara yüklenen UIAccess uygulamalarını yükselt' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a23175)
* [2.3.17.6 (L1) 'Kullanıcı Hesabı Denetimi: Tüm yöneticileri Yönetici Onay Modunda çalıştır' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a23176)
* [2.3.17.7 (L1) 'Kullanıcı Hesabı Denetimi: Yükseltme istendiğinde güvenli masaüstüne geç' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a23177)
* [2.3.17.8 (L1) 'Kullanıcı Hesabı Denetimi: Dosya ve kayıt defteri yazma hatalarını kullanıcı başına konumlara sanallaştır' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a23178)

[**5 Sistem Hizmetleri**](#a5)

* [5.1 (L2) 'Bluetooth Ses Ağ Geçidi Hizmeti (BTAGService)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a51)
* [5.2 (L2) 'Bluetooth Destek Hizmeti (bthserv)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a52)
* [5.3 (L1) 'Bilgisayar Tarayıcısı (Browser)' seçeneği 'Devre Dışı' veya 'Yüklü Değil' (Otomatik) olarak ayarlanmalıdır.](#a53)
* [5.4 (L2) 'İndirilen Haritalar Yöneticisi (MapsBroker)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a54)
* [5.5 (L2) 'Coğrafi Konum Hizmeti (lfsvc)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a55)
* [5.6 (L1) 'IIS Yönetim Hizmeti (IISADMIN)' seçeneği 'Devre Dışı' veya 'Yüklenmemiş' (Otomatik) olarak ayarlanmalıdır.](#a56)
* [5.7 (L1) 'Kızılötesi monitör hizmeti (irmon)' seçeneği 'Devre Dışı' veya 'Yüklü Değil' (Otomatik) olarak ayarlanmalıdır.](#a57)
* [5.8 (L1) 'İnternet Bağlantısı Paylaşımı (ICS) (SharedAccess)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a58)
* [5.9 (L2) 'Bağlantı Katmanı Topolojisi Keşif Eşleştiricisi' (lltdsvc)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a59)
* [5.10 (L1) 'LxssManager (LxssManager)' seçeneği 'Devre Dışı' veya 'Yüklenmedi' (Otomatik) olarak ayarlanmalıdır.](#a510)
* [5.11 (L1) 'Microsoft FTP Hizmeti (FTPSVC)' seçeneği 'Devre Dışı' veya 'Yüklü Değil' (Otomatik) olarak ayarlanmalıdır.](#a511)
* [5.12 (L2) 'Microsoft iSCSI Başlatıcı Hizmeti (MSiSCSI)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a512)
* [5.13 (L1) 'OpenSSH SSH Sunucusu (sshd)' seçeneği 'Devre Dışı' veya 'Yüklü Değil' (Otomatik) olarak ayarlanmalıdır.](#a513)
* [5.14 (L2) 'Eş Adı Çözümleme Protokolü (PNRPsvc)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a514)
* [5.15 (L2) 'Eş Ağ Gruplaması (p2psvc)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a515)
* [5.16 (L2) 'Peer Networking Identity Manager (p2pimsvc)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a516)
* [5.17 (L2) 'PNRP Machine Name Publication Service (PNRPAutoReg)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a517)
* [5,18 (L2) 'Yazdırma Biriktiricisi (Spooler)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a518)
* [5.19 (L2) 'Sorun Raporları ve Çözümleri Denetim Masası Desteği (wercplsupport)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a519)
* [5.20 (L2) 'Uzaktan Erişim Otomatik Bağlantı Yöneticisi (RasAuto)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a520)
* [5.21 (L2) 'Uzak Masaüstü Yapılandırması (SessionEnv)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a521)
* [5.22 (L2) 'Uzak Masaüstü Hizmetleri (TermService)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a522)
* [5.23 (L2) 'Uzak Masaüstü Hizmetleri Kullanıcı Modu Bağlantı Noktası Yeniden Yönlendiricisi (UmRdpService)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a523)
* [5,24 (L1) 'Uzaktan Yordam Çağrısı (RPC) Konum Belirleyicisi (RpcLocator)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a524)
* [5.25 (L2) 'Uzak Kayıt Defteri (RemoteRegistry)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a525)
* [5.26 (L1) 'Yönlendirme ve Uzaktan Erişim (RemoteAccess)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a526)
* [5.27 (L2) 'Sunucu (LanmanServer)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a527)
* [5.28 (L1) 'Basit TCP/IP Hizmetleri (simptcp)' seçeneği 'Devre Dışı' veya 'Yüklenmemiş' (Otomatik) olarak ayarlanmalıdır.](#a528)
* [5,29 (L2) 'SNMP Hizmeti (SNMP)' seçeneği 'Devre Dışı' veya 'Yüklenmemiş' (Otomatik) olarak ayarlanmalıdır.](#a529)
* [5.30 (L1) 'Özel Yönetim Konsol Yardımcısı (sacsvr)' seçeneği 'Devre Dışı' veya 'Yüklenmemiş' (Otomatik) olarak ayarlanmalıdır.](#a530)
* [5,31 (L1) 'SSDP Bulma (SSDPSRV)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a531)
* [5,32 (L1) 'UPnP Device Host (upnphost)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a532)
* [5.33 (L1) 'Web Yönetim Hizmeti (WMSvc)' seçeneği 'Devre Dışı' veya 'Yüklü Değil' (Otomatik) olarak ayarlanmalıdır.](#a533)
* [5.34 (L2) 'Windows Hata Raporlama Hizmeti (WerSvc)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a534)
* [5,35 (L2) 'Windows Olay Toplayıcısı (Wecsvc)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a535)
* [5.36 (L1) 'Windows Media Player Ağ Paylaşım Hizmeti (WMPNetworkSvc)' seçeneği 'Devre Dışı' veya 'Yüklü Değil' (Otomatik) olarak ayarlanmalıdır.](#a536)
* [5.37 (L1) 'Windows Mobile Etkin Nokta Hizmeti (icssvc)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a537)
* [5.38 (L2) 'Windows Bildirim Gönderme Sistemleri Servisi (WpnService)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a538)
* [5,39 (L2) 'Windows PushToInstall Hizmeti (PushToInstall)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a539)
* [5,40 (L2) 'Windows Uzaktan Yönetim (WSManagement) (WinRM)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a540)
* [5.41 (L1) 'World Wide Web Yayımlama Servisi (W3SVC)' seçeneği 'Devre Dışı' veya 'Yüklü Değil' (Otomatik) olarak ayarlanmalıdır.](#a541)
* [5.42 (L1) 'Xbox Aksesuar Yönetim Hizmeti (XboxGipSvc)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a542)
* [5.43 (L1) 'Xbox Live Kimlik Doğrulama Yöneticisi (XblAuthManager)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a543)
* [5.44 (L1) 'Xbox Live Oyun Kaydetme (XblGameSave)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a544)
* [5,45 (L1) 'Xbox Live Ağ Hizmeti (XboxNetApiSvc)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a545)

[**9 Gelişmiş Güvenlik Özellikli Windows Defender Güvenlik Duvarı (eski adıyla Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı)**](#a9)

[**9.1 Domain Profili**](#a91)

* [9.1.1 (L1) ‘Windows Güvenlik Duvarı: Etki Alanı: Güvenlik duvarı durumu' seçeneği 'Açık (önerilen)' (Otomatik) olarak ayarlanmalıdır.](#a911)
* [9.1.2 (L1) ‘Windows Güvenlik Duvarı: Etki Alanı: Gelen bağlantılar' seçeneği 'Engelle (varsayılan)' (Otomatik) olarak ayarlanmalıdır.](#a912)
* [9.1.3 (L1) ‘Windows Güvenlik Duvarı: Etki Alanı: Giden bağlantılar' seçeneği 'İzin Ver (varsayılan)' (Otomatik) olarak ayarlanmalıdır.](#a913)
* [9.1.4 (L1) ‘Windows Güvenlik Duvarı: Etki Alanı: Ayarlar: Bildirim görüntüle' seçeneği 'Hayır' (Otomatik) olarak ayarlanmalıdır.](#a914)
* [9.1.5 (L1) ‘Windows Güvenlik Duvarı: Etki Alanı: Günlüğe Kaydetme: Ad' seçeneği '%SystemRoot%\System32\logfiles\firewall\domainfw.log' (Otomatik) olarak ayarlanmalıdır.](#a915)
* [9.1.6 (L1) 'Windows Güvenlik Duvarı: Etki Alanı: Günlüğe Kaydetme: Boyut sınırı (KB)' ifadesi '16.384 KB veya üzeri' (Otomatik) olarak ayarlanmalıdır.](#a916)
* [9.1.7 (L1) 'Windows Güvenlik Duvarı: Etki Alanı: Günlük bırakılan paketler' seçeneği 'Evet' (Otomatik) olarak ayarlanmalıdır.](#a917)
* [9.1.8 (L1) 'Windows Güvenlik Duvarı: Etki Alanı: Günlük başarılı bağlantılar' seçeneği 'Evet' (Otomatik) olarak ayarlanmalıdır.](#a918)

[**9.2 Özel Profil**](#a92)

* [9.2.1 (L1) 'Windows Güvenlik Duvarı: Özel: Güvenlik duvarı durumu' seçeneği 'Açık (önerilen)' (Otomatik) olarak ayarlanmalıdır.](#a921)
* [9.2.2 (L1) 'Windows Güvenlik Duvarı: Özel: Gelen bağlantılar' seçeneği 'Engelle (varsayılan)' (Otomatik) olarak ayarlanmalıdır.](#a922)
* [9.2.3 (L1) 'Windows Güvenlik Duvarı: Özel: Giden bağlantılar' seçeneği 'İzin Ver (varsayılan)' (Otomatik) olarak ayarlanmalıdır.](#a923)
* [9.2.4 (L1) 'Windows Güvenlik Duvarı: Özel: Ayarlar: Bildirim görüntüle' seçeneği 'Hayır' (Otomatik) olarak ayarlanmalıdır.](#a924)
* [9.2.5 (L1) 'Windows Güvenlik Duvarı: Özel: Günlüğe Kaydetme: Ad' seçeneği '%SystemRoot%\System32\logfiles\firewall\privatefw.log' (Otomatik) olarak ayarlanmalıdır.](#a925)
* [9.2.6 (L1) 'Windows Güvenlik Duvarı: Özel: Günlüğe kaydetme: Boyut sınırı (KB)' ifadesi '16.384 KB veya üzeri' (Otomatik) olarak ayarlanmalıdır.](#a926)
* [9.2.7 (L1) 'Windows Güvenlik Duvarı: Özel: Günlüğe bırakılan paketler' seçeneği 'Evet' (Otomatik) olarak ayarlanmalıdır.](#a927)
* [9.2.8 (L1) 'Windows Güvenlik Duvarı: Özel: Günlüğe kaydetme: Başarılı bağlantılar' seçeneği 'Evet' (Otomatik) olarak ayarlanmalıdır.](#a928)

[**9.3 Genel Profil**](#a93)

* [9.3.1 (L1) 'Windows Güvenlik Duvarı: Genel: Güvenlik duvarı durumu' seçeneği 'Açık (önerilen)' (Otomatik) olarak ayarlanmalıdır.](#a931)
* [9.3.2 (L1) 'Windows Güvenlik Duvarı: Genel: Gelen bağlantılar' seçeneği 'Engelle (varsayılan)' (Otomatik) olarak ayarlanmalıdır.](#a932)
* [9.3.3 (L1) 'Windows Güvenlik Duvarı: Genel: Giden bağlantılar' seçeneği 'İzin Ver (varsayılan)' (Otomatik) olarak ayarlanmalıdır.](#a933)
* [9.3.4 (L1) 'Windows Güvenlik Duvarı: Genel: Ayarlar: Bildirim görüntüle' seçeneği 'Hayır' (Otomatik) olarak ayarlanmalıdır.](#a934)
* [9.3.5 (L1) 'Windows Güvenlik Duvarı: Genel: Ayarlar: Yerel güvenlik duvarı kurallarını uygula' seçeneği 'Hayır' (Otomatik) olarak ayarlanmalıdır.](#a935)
* [9.3.6 (L1) 'Windows Güvenlik Duvarı: Genel: Ayarlar: Yerel bağlantı güvenliği kurallarını uygula' seçeneği 'Hayır' (Otomatik) olarak ayarlanmalıdır.](#a936)
* [9.3.7 (L1) 'Windows Güvenlik Duvarı: Ortak: Günlüğe Kaydetme: Ad' seçeneği '%SystemRoot%\System32\logfiles\firewall\publicfw.log' (Otomatik) olarak ayarlanmalıdır.](#a937)
* [9.3.8 (L1) 'Windows Güvenlik Duvarı: Genel: Günlüğe kaydetme: Boyut sınırı (KB)' seçeneği '16.384 KB veya daha büyük' (Otomatik) olarak ayarlanmalıdır.](#a938)
* [9.3.9 (L1) 'Windows Güvenlik Duvarı: Genel: Günlük bırakılan paketler' seçeneği 'Evet' (Otomatik) olarak ayarlanmalıdır.](#a939)
* [9.3.10 (L1) 'Windows Güvenlik Duvarı: Genel: Günlüğe kaydetme: Başarılı bağlantılar' seçeneği 'Evet' (Otomatik) olarak ayarlanmalıdır.](#a9310)

[**17 Gelişmiş Denetim İlkesi Yapılandırması**](#a17)

[**17.1 Hesapta Oturum Açma**](#a171)

* [17.1.1 (L1) 'Kimlik Bilgileri Doğrulamasını Denetle' seçeneği 'Başarılı ve Başarısız' (Otomatik) olarak ayarlanmalıdır.](#a1711)

[**17.2 Hesap Yönetimi**](#a172)

* [17.2.1 (L1) 'Uygulama Grubu Yönetimini Denetle' seçeneği 'Başarı ve Başarısızlık' (Otomatik) olarak ayarlanmalıdır.](#a1721)
* [17.2.2 (L1) 'Güvenlik Grubu Yönetimini Denetle' seçeneği 'Başarılı' (Otomatik) içerecek şekilde ayarlanmalıdır.](#a1722)
* [17.2.3 (L1) 'Kullanıcı Hesabı Yönetimini Denetle' seçeneği 'Başarı ve Başarısızlık' (Otomatik) olarak ayarlanmalıdır.](#a1723)

[**17.3 Ayrıntılı İzleme**](#a173)

* [17.3.1 (L1) 'PNP Etkinliğini Denetle' seçeneği 'Başarı' (Otomatik) içerecek şekilde ayarlanmalıdır.](#a1731)
* [17.3.2 (L1) 'Süreç Oluşturmayı Denetle' seçeneği 'Başarılı' (Otomatik) içerecek şekilde ayarlanmalıdır.](#a1732)

[**17.4 DS Access**](#a174)

[**17.5 Oturum Açma/Oturumu Kapatma**](#a175)

* [17.5.1 (L1) 'Hesap Oturumu Kapatmayı Denetle' seçeneği 'Hata' (Otomatik) içerecek şekilde ayarlanmalıdır.](#a1751)
* [17.5.2 (L1) 'Grup Üyeliğini Denetle' seçeneği 'Başarılı' (Otomatik) içerecek şekilde ayarlanmalıdır.](#a1752)
* [17.5.3 (L1) 'Oturum Kapatmayı Denetle' seçeneği 'Başarılı' (Otomatik) içerecek şekilde ayarlanmalıdır.](#a1753)
* [17.5.4 (L1) 'Oturum Açmayı Denetle' seçeneği 'Başarılı ve Başarısız' (Otomatik) olarak ayarlanmalıdır.](#a1754)
* [17.5.5 (L1) 'Diğer Oturum Açma/Oturum Kapatma Olaylarını Denetle' seçeneği 'Başarılı ve Hatalı' (Otomatik) olarak ayarlanmalıdır.](#a1755)
* [17.5.6 (L1) 'Özel Oturum Açmayı Denetle' seçeneği 'Başarılı' (Otomatik) içerecek şekilde ayarlanmalıdır.](#a1756)

[**17.6 Nesne Erişimi**](#a176)

* [17.6.1 (L1) 'Ayrıntılı Dosya Paylaşımını Denetle' seçeneği 'Hata' (Otomatik) içerecek şekilde ayarlanmalıdır.](#a1761)
* [17.6.2 (L1) 'Dosya Paylaşımını Denetle' seçeneği 'Başarılı ve Başarısız' (Otomatik) olarak ayarlanmalıdır.](#a1762)
* [17.6.3 (L1) 'Diğer Nesne Erişim Olaylarını Denetle' seçeneği 'Başarı ve Başarısızlık' (Otomatik) olarak ayarlanmalıdır.](#a1763)
* [17.6.4 (L1) ‘Çıkarılabilir Depolamayı Denetle' seçeneği 'Başarılı ve Hatalı' (Otomatik) olarak ayarlanmalıdır.](#a1764)

[**17.7 İlke Değişikliği**](#a177)

* [17.7.1 (L1) 'Denetim İlkesi Değişikliğini Denetle' seçeneği 'Başarı' (Otomatik) içerecek şekilde ayarlanmalıdır.](#a1771)
* [17.7.2 (L1) 'Kimlik Doğrulama İlkesi Değişikliğini Denetle' seçeneği 'Başarılı' (Otomatik) içerecek şekilde ayarlanmalıdır.](#a1772)
* [17.7.3 (L1) 'Yetkilendirme İlkesi Değişikliğini Denetle' seçeneği 'Başarılı' (Otomatik) içerecek şekilde ayarlanmalıdır.](#a1773)
* [17.7.4 (L1) 'MPSSVC Kural Düzeyinde İlke Değişikliğini Denetle' seçeneği 'Başarılı ve Başarısız' (Otomatik) olarak ayarlanmalıdır.](#a1774)
* [17.7.5 (L1) 'Diğer İlke Değişikliği Olaylarını Denetle' seçeneği 'Hata' (Otomatik) içerecek şekilde ayarlanmalıdır.](#a1775)

[**17.8 Ayrıcalık Kullanımı**](#a178)

* [17.8.1 (L1) 'Hassas Ayrıcalık Kullanımını Denetle' seçeneği 'Başarılı ve Başarısız' (Otomatik) olarak ayarlanmalıdır.](#a1781)

[**17.9 Sistem**](#a179)

* [17.9.1 (L1) 'IPsec Sürücüsünü Denetle' seçeneği 'Başarılı ve Hatalı' (Otomatik) olarak ayarlanmalıdır.](#a1791)
* [17.9.2 (L1) 'Diğer Sistem Olaylarını Denetle' seçeneği 'Başarı ve Başarısızlık' (Otomatik) olarak ayarlanmalıdır.](#a1792)
* [17.9.3 (L1) 'Güvenlik Durumu Değişikliğini Denetle' seçeneği 'Başarılı' (Otomatik) içerecek şekilde ayarlanmalıdır.](#a1793)
* [17.9.4 (L1) 'Güvenlik Sistemi Uzantısını Denetle' seçeneği 'Başarılı' (Otomatik) içerecek şekilde ayarlanmalıdır.](#a1794)
* [17.9.5 (L1) 'Sistem Bütünlüğünü Denetle' seçeneği 'Başarı ve Başarısızlık' (Otomatik) olarak ayarlanmalıdır.](#a1795)

[**18 Yönetim Şablonları (Bilgisayar)**](#a18)

[**18.1 Kontrol Paneli**](#a181)

[**18.1.1 Kişiselleştirme**](#a1811)

* [18.1.1.1 (L1) 'Kilit ekranı kamerasının etkinleştirilmesini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18111)
* [18.1.1.2 (L1) 'Kilit ekranı slayt gösterisinin etkinleştirilmesini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18112)

[**18.1.2 Bölge ve Dil Seçenekleri**](#a1812)

* [18.1.2.1 El yazısı kişiselleştirme](#a18121)
* [18.1.2.2 (L1) 'Kullanıcıların çevrimiçi konuşma tanıma hizmetlerini etkinleştirmesine izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18122)

[**18.1.3 (L2) 'Çevrimiçi İpuçlarına İzin Ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**](#a1813)

[**18.2 LAPS ( Yerel Yöneticiler içim Parola Çözümleyici)**](#a182)

* [18.2.1 (L1) LAPS AdmPwd GPO Uzantısı / CSE'nin yüklü olmalıdır. (Otomatik)](#a1821)
* [18.2.2 (L1) 'Politikanın gerektirdiğinden daha uzun parola süre sonlarına izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1822)
* [18.2.3 (L1) 'Yerel Yönetici Şifre Yönetimini Etkinleştir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1823)
* [18.2.4 (L1) 'Parola Ayarları: Parola Karmaşıklığı' seçeneği 'Etkin: Büyük harfler + küçük harfler + sayılar + özel karakterler' olarak ayarlanmalıdır. (Otomatik)](#a1824)
* [18.2.5 (L1) 'Şifre Ayarları: Şifre Uzunluğu' seçeneği 'Etkin: 15 veya daha fazla' (Otomatik) olarak ayarlanmalıdır.](#a1825)
* [18.2.6 (L1) 'Şifre Ayarları: Şifre Yaşı (Gün)' seçeneği 'Etkin: 30 veya daha az' (Otomatik) olarak ayarlandığından emin olun](#a1826)

[**18.3 MS Güvenlik Kılavuzu**](#a183)

* [18.3.1 (L1) 'Ağda oturum açarken yerel hesaplara UAC (Kullanıcı Hesap Denetimi) kısıtlamaları uygula' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1831)
* [18.3.2 (L1) 'SMB v1 istemci sürücüsünü yapılandır' seçeneği 'Etkin: Sürücüyü devre dışı bırak (önerilen)' (Otomatik) olarak ayarlanmalıdır.](#a1832)
* [18.3.3 (L1) 'SMB v1 sunucusunu yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1833)
* [18.3.4 (L1) 'Yapılandırılmış İstisna İşleme Üzerine Yazma Korumasını (SEHOP) Etkinleştir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1834)
* [18.3.5 (L1) 'Yazıcı sürücüsü yüklemesini Yöneticilerle sınırlar' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1835)
* [18.3.6 (L1) 'NetBT NodeType yapılandırması' seçeneği 'Etkin: P-düğümü (önerilen)' (Otomatik) olarak ayarlanmalıdır.](#a1836)
* [18.3.7 (L1) 'WDigest Kimlik Doğrulaması' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1837)

[**18.4 MSS (Eski)**](#a184)

* [18.4.1 (L1) 'MSS: Otomatik Oturum Açmayı Etkinleştir (önerilmez)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1841)
* [18.4.2 (L1) 'MSS: IP kaynak yönlendirme koruma düzeyi (paket sahteciliğine karşı korur)' seçeneği 'Etkin: En yüksek koruma, kaynak yönlendirme tamamen devre dışı' (Otomatik) olarak ayarlanmalıdır.](#a1842)
* [18.4.3 (L1) 'MSS: IP kaynak yönlendirme koruma düzeyi (paket sahteciliğine karşı korur)' seçeneği 'Etkin: En yüksek koruma, kaynak yönlendirme tamamen devre dışı' (Otomatik) olarak ayarlanmalıdır.](#a1843)
* [18.4.4 (L2) 'MSS: Çevirmeli ağ şifresinin kaydedilmesini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1844)
* [18.4.5 (L1) 'MSS: ICMP yönlendirmelerinin OSPF tarafından oluşturulan yolları geçersiz kılmasına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1845)
* [18.4.6 (L2) 'MSS: Canlı tutma paketlerinin milisaniye cinsinden ne sıklıkta gönderildiği' seçeneği 'Etkin: 300.000 veya 5 dakika (önerilen)' olarak ayarlanmalıdır. (Otomatik)](#a1846)
* [18.4.7 (L1) 'MSS: Bilgisayarın WINS sunucuları dışındaki NetBIOS ad bırakma isteklerini yok saymasına izin ver' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1847)
* [18.4.8 (L2) 'MSS: IRDP'nin Varsayılan Ağ Geçidi adreslerini algılamasına ve yapılandırmasına izin ver (DoS'a yol açabilir)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1848)
* [18.4.9 (L1) 'MSS: Güvenli DLL arama modunu etkinleştir (önerilen)' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1849)
* [18.4.10 (L1) 'MSS: Ekran koruyucu yetkisiz kullanım süresinin sona ermesinden önceki saniye cinsinden süre (0 önerilir)' seçeneği 'Etkin: 5 veya daha az saniye' (Otomatik) olarak ayarlanmalıdır.](#a18410)
* [18.4.11 (L2) 'MSS : Onaylanmamış verilerin kaç kez yeniden iletildiği' seçeneği 'Etkin: 3' (Otomatik) olarak ayarlanmalıdır.](#a18411)
* [18.4.12 (L2) 'MSS: Onaylanmamış verilerin kaç kez yeniden iletildiği' seçeneği 'Etkin: 3' (Otomatik) olarak ayarlanmalıdır.](#a18412)
* [18.4.13 (L1) 'MSS: Sistemin uyarı oluşturacağı güvenlik olay günlüğü için yüzde eşiği' seçeneği 'Etkin: %90 veya daha az' (Otomatik) olarak ayarlanmalıdır.](#a18413)

[**18.5 Ağ**](#a185)

[**18.5.1 Arka Plan Akıllı Aktarım Hizmeti (BITS)**](#a1851)

[**18.5.2 BranchCache**](#a1852)

[**18.5.3 DirectAccess İstemci Deneyimi Ayarları**](#a1853)

[**18.5.4 DNS İstemcisi**](#a1854)

* [18.5.4.1 (L1) 'HTTPS üzerinden DNS yapılandırma (DoH) ad çözümlemesi' seçeneği 'Etkin: DoH'ye İzin Ver' veya üstü (Otomatik) olarak ayarlanmalıdır.](#a18541)
* [18.5.4.2 (L1) 'Çok noktaya yayın adı çözünürlüğünü kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18542)

[**18.5.5 Fontlar**](#a1855)

* [18.5.5.1 (L2) 'Font Sağlayıcılarını Etkinleştir' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18551)

[**18.5.6 Hotspot Kimlik Doğrulaması**](#a1856)

[**18.5.7 Lanman Sunucusu**](#a1857)

[**18.5.8 Lanman İş İstasyonu**](#a1858)

* [18.5.8.1 (L1) 'Güvenli olmayan misafir oturum açmalarını etkinleştir' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18581)

[**18.5.9 Bağlantı Katmanı Topolojisi Keşfi**](#a1859)

* [18.5.9.1 (L2) 'Eşleyici G/Ç (LLTDIO) sürücüsünü aç' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18591)
* [18.5.9.2 (L2) 'Yanıtlayıcı Aç (RSPNDR) sürücüsünü aç' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18592)

[**18.5.10 Microsoft Eşler Arası Ağ Hizmetleri**](#a18510)

* [18.5.10.1 Eş Adı Çözümleme Protokolü](#a185101)
* [18.5.10.2 (L2) 'Microsoft Eşler Arası Ağ Hizmetlerini Kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a185102)

[**18.5.11 Ağ Bağlantıları**](#a18511)

* [18.5.11.1 Windows Defender Güvenlik Duvarı (eski adıyla Windows Güvenlik Duvarı)](#a185111)
* [18.5.11.2 (L1) 'DNS etki alanı ağınızda Ağ Köprüsü'nün yüklenmesini ve yapılandırılmasını yasakla' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a185112)
* [18.5.11.3 (L1) 'DNS alan adı ağınızda İnternet Bağlantısı Paylaşımının kullanımını yasakla' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a185113)
* [18.5.11.4 (L1) 'Bir ağın konumunu ayarlarken alan adı kullanıcılarının yükselmesini iste' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a185114)

[**18.5.12 Ağ Bağlantısı Durum Göstergesi**](#a18512)

[**18.5.13 Ağ İzolasyonu**](#a18513)

[**18.5.14 Ağ Sağlayıcı**](#a18514)

* [18.5.14.1 (L1) Tüm NETLOGON ve SYSVOL paylaşımları için 'Sağlamlaştırılmış UNC Yolları' seçeneği 'Etkin, 'Karşılıklı Kimlik Doğrulaması İste' ve 'Bütünlük İste' olarak ayarlanmalıdır. (Otomatik)](#a185141)

[**18.5.15 Çevrimdışı Dosyalar**](#a18515)

[**18.5.16 QoS Paket Zamanlayıcı**](#a18516)

[**18.5.17 SNMP**](#a18517)

[**18.5.18 SSL Yapılandırma Ayarları**](#a18518)

[**18.5.19 TCPIP Ayarları**](#a18519)

[**18.5.19.1 IPv6 Geçiş Teknolojileri**](#a185191)

[**18.5.19.2 Parametreler**](#a185192)

* [18.5.19.2.1 (L2) IPv6'yı Devre Dışı Bırak (TCPIP6) sçeneğinin 'DisabledComponents'ın '0xff (255)' olarak ayarlanmalıdır. (Otomatik)](#a1851921)

[**18.5.20 Windows Şimdi Bağlan**](#a18520)

* [18.5.20.1 (L2) 'Windows Connect Now kullanılarak kablosuz ayarların yapılandırılması' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır](#a185201)
* [18.5.20.2 (L2) 'Windows Connect Now sihirbazlarına erişimi engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a185202)

[**18.5.21 Windows Bağlantı Yöneticisi**](#a18521)

* [18.5.21.1 (L1) 'İnternet veya Windows Etki Alanına eşzamanlı bağlantı sayısını en aza indir' seçeneği 'Etkin: 3 = Ethernet üzerindeyken Wi-Fi'yi engelle' olarak ayarlanmalıdır. (Otomatik)](#a185211)
* [18.5.21.2 (L1) 'Etki alanı kimliği doğrulanmış ağa bağlanıldığında etki alanı olmayan ağlara bağlantıyı yasakla' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a185212)

[**18.5.22 Kablosuz Ekran**](#a18522)

[**18.5.23 WLAN Servis Kontrolü**](#a18523)

[**18.5.23.1 WLAN Medya Maliyeti**](#a185231)

[**18.5.23.2 WLAN Ayarları**](#a185232)

* [18.5.23.2.1 (L1) 'Windows'un önerilen açık erişim noktalarına, kişiler tarafından paylaşılan ağlara ve ücretli hizmetler sunan erişim noktalarına otomatik olarak bağlanmasına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1852321)

[**18.6 Yazıcılar**](#a186)

* [18.6.1 (L1) 'Yazdırma Biriktiricisinin istemci bağlantılarını kabul etmesine izin ver' seçeneği 'Devre Dışı' olarak ayarlanmalıdır (Otomatik)](#a1861)
* [18.6.2 (L1) 'Nokta ve Yazdırma Kısıtlamaları: Yeni bir bağlantı için sürücüleri yüklerken' seçeneği 'Etkin: Uyarı ve yükseltme istemini göster' olarak ayarlanmalıdır. (Otomatik)](#a1862)
* [18.6.3 (L1) 'Nokta ve Yazdırma Kısıtlamaları: Mevcut bir bağlantı için sürücüleri güncellerken' seçeneği 'Etkin: Uyarı ve yükseltme istemini göster' olarak ayarlanmalıdır. (Otomatik)](#a1863)

[**18.7 Başlat Menüsü ve Görev Çubuğu**](#a187)

[**18.7.1 Bildirimler**](#a1871)

* [18.7.1.1 (L2) 'Ağ kullanımı bildirimlerini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18711)

[**18.8 Sistem**](#a188)

[**18.8.1 Erişim Reddedilen Yardım**](#a1881)

[**18.8.2 Uygulama-V**](#a1882)

[**18.8.3 Denetim Sürecinin Oluşturulması**](#a1883)

* [18.8.3.1 (L1) 'İşlem oluşturma olaylarına komut satırını dahil et' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18831)

[**18.8.4 Kimlik Bilgileri Delegasyonu**](#a1884)

* [18.8.4.1 (L1) 'Oracle Düzeltme Şifrelemesi' seçeneği 'Etkin: Güncellenen İstemcileri Zorla' (Otomatik) olarak ayarlanmalıdır.](#a18841)
* [18.8.4.2 (L1) 'Uzak ana bilgisayar, dışa aktarılamayan kimlik bilgilerinin devredilmesine izin veriyor' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18842)

[**18.8.5 Cihaz Koruması**](#a1885)

* [18.8.5.1 (NG) 'Sanallaştırma Tabanlı Güvenliği Aç' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18851)
* [18.8.5.2 (NG) 'Sanallaştırma Tabanlı Güvenliği Aç: Platform Güvenlik Düzeyini Seç' seçeneği 'Güvenli Önyükleme ve DMA Koruması' (Otomatik) olarak ayarlanmalıdır.](#a18852)
* [18.8.5.3 (NG) 'Sanallaştırma Tabanlı Güvenliği Aç: Kod Bütünlüğünün Sanallaştırma Tabanlı Koruması' seçeneği 'UEFI kilidi ile etkin' (Otomatik) olarak ayarlanmalıdır.](#a18853)
* [18.8.5.4 (NG) 'Sanallaştırma Tabanlı Güvenliği Aç: UEFI Bellek Öznitelikleri Tablosunu Gerektir' seçeneği 'Doğru (işaretli)' (Otomatik) olarak ayarlanmalıdır.](#a18854)
* [18.8.5.5 (NG) 'Sanallaştırma Tabanlı Güvenliği Aç: Kimlik Bilgileri Koruma Yapılandırması' seçeneği 'UEFI kilidi ile etkin' (Otomatik) olarak ayarlanmalıdır.](#a18855)
* [18.8.5.6 (NG) 'Sanallaştırma Tabanlı Güvenliği Aç: Güvenli Başlatma Yapılandırması' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18856)

[**18.8.6 Cihaz Sağlığı Tasdik Hizmeti**](#a1886)

[**18.8.7 Cihaz Kurulumu**](#a1887)

[**18.8.7.1 Cihaz Yükleme Kısıtlamaları**](#a18871)

* [18.8.7.1.1 (BL) 'Bu cihaz kimliklerinden herhangi biriyle eşleşen cihazların yüklenmesini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a188711)
* [18.8.7.1.2 (BL) 'Bu cihaz kimliklerinden herhangi biriyle eşleşen cihazların yüklenmesini engelle: Bu cihaz kimliklerinden herhangi biriyle eşleşen cihazların yüklenmesini engelle' seçeneği 'PCI\CC\_0C0A' (Otomatik) olarak ayarlanmalıdır.](#a188712)
* [18.8.7.1.3 (BL) 'Bu cihaz kimliklerinden herhangi biriyle eşleşen cihazların yüklenmesini engelle: Zaten yüklü olan eşleşen cihazlara da uygulanır.' seçeneği 'Doğru' (işaretli) (Otomatik) olarak ayarlanmalıdır.](#a188713)
* [18.8.7.1.4 (BL) 'Bu aygıt kurulum sınıflarıyla eşleşen sürücüleri kullanarak aygıtların yüklenmesini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a188714)
* [18.8.7.1.5 (BL) 'Bu aygıt kurulum sınıflarıyla eşleşen sürücüleri kullanarak aygıtların yüklenmesini engelle: Bu aygıt kurulumu için sürücüleri kullanarak aygıtların yüklenmesini engelle' seçeneği 'IEEE 1394 aygıt kurulum sınıfları' (Otomatik) olarak ayarlanmalıdır.](#a188715)
* [18.8.7.1.6 (BL) 'Bu aygıt kurulum sınıflarıyla eşleşen sürücüleri kullanarak aygıtların yüklenmesini engelle: Zaten yüklü olan eşleşen aygıtlara da uygulanır.' seçeneği 'Doğru' (işaretli) (Otomatik) olarak ayarlanmalıdır.](#a188716)

[**18.8.7.2 (L1) 'İnternetten cihaz meta verilerinin alınmasını engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**](#a18872)

[**18.8.8 Cihaz Yeniden Yönlendirme**](#a1888)

[**18.8.9 Disk NV Önbelleği**](#a1889)

[**18.8.10 Disk Kotaları**](#a18810)

[**18.8.11 Ekran**](#a18811)

[**18.8.12 Dağıtılmış COM**](#a18812)

[**18.8.13 Sürücü Kurulumu**](#a18813)

[**18.8.14 Erken Başlatma Kötü Amaçlı Yazılımdan Koruma**](#a18814)

* [18.8.14.1 (L1) 'Boot-Start Driver Initialization Policy' (Önyükleme-Başlat Sürücüsü Başlatma İlkesi) seçeneği 'Etkin: İyi, bilinmeyen ve kötü ama kritik' (Otomatik) olarak ayarlanmalıdır.](#a188141)

[**18.8.15 Gelişmiş Depolama Erişimi**](#a18815)

[**18.8.16 Dosya Sınıflandırma Altyapısı**](#a18816)

[**18.8.17 Dosya Paylaşımı Gölge Kopya Aracısı**](#a18817)

[**18.8.18 Dosya Paylaşımı Gölge Kopya Sağlayıcısı**](#a18818)

[**18.8.19 Dosya Sistemi (eski adıyla NTFS Dosya Sistemi)**](#a18819)

[**18.8.20 Klasör Yeniden Yönlendirme**](#a18820)

[**18.8.21 Grup İlkesi**](#a18821)

* [18.8.21.1 Günlüğe kaydetme ve izleme](#a188211)
* [18.8.21.2 (L1) 'Kayıt defteri ilkesi işlemeyi yapılandır: Periyodik arka plan işleme sırasında uygulamayın' seçeneği 'Etkin: YANLIŞ' (Otomatik) olarak ayarlanmalıdır.](#a188212)
* [18.8.21.3 (L1) 'Kayıt defteri politikası işlemeyi yapılandır: Grup İlkesi nesneleri değişmemiş olsa bile işle' seçeneği 'Etkin: DOĞRU' (Otomatik) olarak ayarlanmalıdır.](#a188213)
* [18.8.21.4 (L1) 'Bu cihazda deneyimlere devam et' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a188214)
* [18.8.21.5 (L1) 'Grup İlkesi arka plan yenilemesini kapat' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a188215)

[**18.8.22 İnternet İletişim Yönetimi**](#a18822)

[**18.8.22.1 İnternet İletişimi ayarları**](#a18822a1)

* [18.8.22.1.1 (L2) 'Mağazaya erişimi kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1882211)
* [18.8.22.1.2 (L1) 'HTTP üzerinden yazdırma sürücülerinin indirilmesini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1882212)
* [18.8.22.1.3 (L2) 'El yazısı kişiselleştirme veri paylaşımını kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1882213)
* [18.8.22.1.4 (L2) 'El yazısı tanıma hata bildirimini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1882214)
* [18.8.22.1.5 (L2) 'URL bağlantısı Microsoft.com atıfta bulunuyorsa İnternet Bağlantı Sihirbazını kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1882215)
* [18.8.22.1.6 (L1) 'Web yayıncılığı ve çevrimiçi sipariş sihirbazları için İnternet'ten indirmeyi kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1882216)
* [18.8.22.1.7 (L2) 'HTTP üzerinden yazdırmayı kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1882217)
* [18.8.22.1.8 (L2) 'URL bağlantısı Microsoft.com atıfta bulunuyorsa Kaydı kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1882218)
* [18.8.22.1.9 (L2) 'Arama Yardımcısı içerik dosyası güncellemelerini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1882219)
* [18.8.22.1.10 (L2) ''Baskı Siparişi Ver' resim görevini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18822110)
* [18.8.22.1.11 (L2) 'Dosya ve klasörler için 'Web'de Yayınla' görevini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18822111)
* [18.8.22.1.12 (L2) 'Windows Messenger Müşteri Deneyimini Geliştirme Programı'nı kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18822112)
* [18.8.22.1.13 (L2) 'Windows Müşteri Deneyimini Geliştirme Programını Kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18822113)
* [18.8.22.1.14 (L2) 'Windows Hata Bildirimini Kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18822114)

[**18.8.23 iSCSI**](#a18823)

[**18.8.24 KDC**](#a18824)

[**18.8.25 Kerberos**](#a18825)

* [18.8.25.1 (L2) 'Sertifika kullanarak cihaz kimlik doğrulamasını destekle' seçeneği 'Etkin: Otomatik' (Otomatik) olarak ayarlanmalıdır.3](#a188251)

[**18.8.26 Çekirdek DMA Koruması**](#a18826)

* [18.8.26.1 (BL) 'Çekirdek DMA Koruması ile uyumlu olmayan harici cihazlar için numaralandırma politikası' seçeneği 'Etkin: Tümünü engelle' (Otomatik) olarak ayarlanmalıdır.](#a18826)

[**18.8.27 Yerel Hizmetler**](#a18827)

* [18.8.27.1 (L2) 'Oturum açma için kullanıcı giriş yöntemlerinin sistem hesabına kopyalanmasına izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a188271)

[**18.8.28 Oturum açma**](#a18828)

* [18.8.28.1 (L1) 'Kullanıcının oturum açarken hesap ayrıntılarını göstermesini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a188281)
* [18.8.28.2 (L1) 'Ağ seçimi kullanıcı arayüzünü görüntüleme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a188282)
* [18.8.28.3 (L1) 'Etki alanına katılmış bilgisayarlarda bağlı kullanıcıları numaralandırma' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a188283)
* [18.8.28.4 (L1) 'Etki alanına katılmış bilgisayarlarda yerel kullanıcıları numaralandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a188284)
* [18.8.28.5 (L1) 'Kilit ekranında uygulama bildirimlerini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a188285)
* [18.8.28.6 (L1) 'Resimli şifre ile oturum açmayı kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a188286)
* [18.8.28.7 (L1) 'Kolay PIN ile oturum açmayı aç' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a188287)

[**18.8.29 Azaltma Seçenekleri**](#a18829)

[**18.8.30 Net Oturum Açma**](#a18830)

[**18.8.31 İşletim Sistemi Politikaları**](#a18831)

* [18.8.31.1 (L2) 'Cihazlar arasında Pano senkronizasyonuna izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a188311)
* [18.8.31.2 (L2) 'Kullanıcı Etkinliklerinin yüklenmesine izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a188312)

[**18.8.32 Performans Kontrol Paneli**](#a18832)

[**18.8.33 PIN Karmaşıklığı**](#a1833)

[**18.8.34 Güç Yönetimi**](#a18834)

[**18.8.34.1 Düğme Ayarları**](#a188341)

[**18.8.34.2 Enerji Tasarrufu Ayarları**](#a188342)

[**18.8.34.3 Sabit Disk Ayarları**](#a188343)

[**18.8.34.4 Bildirim Ayarları**](#a188344)

[**18.8.34.5 Güç Azaltma Ayarları**](#a188345)

[**18.8.34.6 Uyku Ayarları**](#a188346)

* [18.8.34.6.1 (L1) 'Bağlı bekleme sırasında ağ bağlantısına izin ver (pilde)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1883461)
* [18.8.34.6.2 (L1) 'Bağlı bekleme sırasında ağ bağlantısına izin ver (prize takılı)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1883462)
* [18.8.34.6.3 (BL) 'Uyurken (pilde) bekleme durumlarına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1883463)
* [18.8.34.6.4 (BL) 'Uyurken bekleme durumlarına izin ver (S1-S3))' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1883464)
* [18.8.34.6.5 (L1) 'Bilgisayar uyandığında (pille olduğunda) parola iste' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1883465)
* [18.8.34.6.6 (L1) 'Bilgisayar uyandığında parola iste (prize takılı)' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1883466)

[**18.8.35 Kurtarma**](#a18835)

[**18.8.36 Uzaktan Yardım**](#a18836)

* [18.8.36.1 (L1) 'Uzaktan Yardım Teklifini Yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a188361)
* [18.8.36.2 (L1) 'İstenen Uzaktan Yardımı Yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a188362)

[**18.8.37 Uzaktan Prosedür Çağrısı (RPC)**](#a18837)

* [18.8.37.1 (L1) 'RPC Endpoint Eşleştiricisi İstemci Kimlik Doğrulamasını Etkinleştir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a188371)
* [18.8.37.2 (L1) 'Kimliği Doğrulanmamış RPC istemcilerini kısıtla' seçeneği 'Etkin: Kimliği Doğrulanmış' (Otomatik) olarak ayarlanmalıdır.](#a188372)

[**18.8.38 Çıkarılabilir Depolama Birimi Erişimi**](#a18838)

[**18.8.39 Komut Dosyaları**](#a18839)

[**18.8.40 Güvenlik Hesabı Yöneticisi**](#a18840)

[**18.8.41 Sunucu Yöneticisi**](#a188a41)

[**18.8.42 Hizmet Denetim Yöneticisi Ayarları**](#a188a42)

[**18.8.43 Kapatma**](#a188a43)

[**18.8.44 Kapatma Seçenekleri**](#a18844)

[**18.8.45 Depolama Sağlığı**](#a18845)

[**18.8.46 Akıllı Depolama**](#a18846)

[**18.8.47 Sistem Geri Yükleme**](#a18847)

[**18.8.48 Sorun Giderme ve Tanılama**](#a18848)

[**18.8.48.1 Uygulama Uyumluluğu Tanılaması**](#a188481)

[**18.8.48.2 Bozuk Dosya Kurtarma**](#a188482)

[**18.8.48.3 Disk Tanılama**](#a188483)

[**18.8.48.4 Hataya Dayanıklı Yığın**](#a188484)

[**18.8.48.5 Microsoft Destek Tanılama**](#a188485)

* [Araç 18.8.48.5.1 (L2) 'Microsoft Destek Tanılama Aracı: Destek sağlayıcısıyla MSDT etkileşimli iletişimini aç' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1884851)

[**18.8.48.6 MSI Bozuk Dosya Kurtarma**](#a188486)

[**18.8.48.7 Planlı Bakım**](#a188487)

[**18.8.48.8 Yazılı Tanılama**](#a188488)

[**18.8.48.9 Windows Önyükleme Performansı Tanılama**](#a188489)

[**18.8.48.10 Windows Bellek Sızıntısı Teşhisi**](#a1884810)

[**18.8.48.11 Windows Performans (PerfTrack)**](#a1884811)

* [18.8.48.11.1 (L2) 'PerfTrack'i Etkinleştir/Devre Dışı Bırak' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18848111)

[**18.8.49 Güvenilir Platform Modülü Hizmetleri**](#a18849)

[**18.8.50 Kullanıcı Profiller**i](#a18850)

* [18.8.50.1 (L2) 'Reklam kimliğini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a188501)

[**18.8.51 Windows Dosya Koruması**](#a188a51)

[**18.8.52 Windows HotStart**](#a188a52)

[**18.8.53 Windows Saati Hizmeti**](#a188a53)

[**18.8.53.1 Zaman Sağlayıcılar**](#a188a531)

* [18.8.53.1.1 (L2) 'Windows NTP İstemcisini Etkinleştir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a188a5311)
* [18.8.53.1.2 (L2) 'Windows NTP Server'ı Etkinleştir' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a188a5312)

[**18.9 Windows Bileşenleri**](#a189)

[**18.9.1 Active Directory Federasyon Hizmetleri**](#a1891)

[**18.9.2 ActiveX Yükleyici Hizmeti**](#a1892)

[**18.9.3 Windows 8 / 8.1 / 10'a özellikler ekleme (eski adıyla Windows Anytime Upgrade)**](#a1893)

[**18.9.4 Uygulama Paketi Dağıtımı**](#a1894)

* [18.9.4.1 (L2) 'Bir Windows uygulamasının uygulama verilerini kullanıcılar arasında paylaşmasına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18941)
* [18.9.4.2 (L1) 'Yönetici olmayan kullanıcıların paketlenmiş Windows uygulamalarını yüklemesini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18942)

[**18.9.5 Uygulama Gizliliği**](#a1895)

* [18.9.5.1 (L1) 'Sistem kilitliyken Windows uygulamalarının sesle etkinleştirilmesine izin ver' seçeneği 'Etkin: Reddetmeye Zorla' (Otomatik) olarak ayarlanmalıdır.](#a18951)

[**18.9.6 Uygulama çalışma zamanı**](#a1896)

* [18.9.6.1 (L1) 'Microsoft hesaplarının isteğe bağlı olmasına izin ver' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18961)
* [18.9.6.2 (L2) 'Barındırılan içerikten Windows Çalışma Zamanı API erişimi olan Evrensel Windows uygulamalarının başlatılmasını engelle.' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18962)

[**18.9.7 Uygulama Uyumluluğu**](#a1897)

[**18.9.8 Otomatik Oynatma Politikaları**](#a1898)

* [18.9.8.1 (L1) 'Ses düzeyi olmayan cihazlar için Otomatik Oynatmaya İzin Verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18981)
* [18.9.8.2 (L1) 'Otomatik Çalıştır için varsayılan davranışı ayarla' seçeneği 'Etkin: Otomatik çalıştırma komutu yürütme' (Otomatik) olarak ayarlanmalıdır.](#a18982)
* [18.9.8.3 (L1) 'Otomatik Oynatmayı kapat' seçeneği 'Etkin: Tüm sürücüler' (Otomatik) olarak ayarlanmalıdır.](#a18983)

[**18.9.9 Yedekleme**](#a1899)

[**18.9.10 Biyometri**](#a18910)

[**18.9.10.1 Yüz Özellikleri**](#a189101)

* [18.9.10.1.1 (L1) 'Gelişmiş adres sahteciliği önleme yapılandır' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1891011)

[**18.9.11 BitLocker Sürücü Şifrelemesi**](#a18911)

[**18.9.11.1 Sabit Veri Sürücüleri**](#a189111)

* [18.9.11.1.1 (BL) 'Windows'un önceki sürümlerinden BitLocker korumalı sabit veri sürücülerine erişime izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1891111)
* [18.9.11.1.2 (BL) 'BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçin' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1891112)
* [18.9.11.1.3 (BL) 'BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçin: Veri kurtarma aracısına izin ver' seçeneği 'Etkin: Doğru' (Otomatik) olarak ayarlanmalıdır.](#a1891113)
* [18.9.11.1.4 (BL) 'BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçme: Kurtarma Parolası' seçeneği 'Etkin: 48 basamaklı kurtarma parolasına izin ver' (Otomatik) olarak ayarlanmalıdır.](#a1891114)
* [18.9.11.1.5 (BL) 'BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçin: Kurtarma Anahtarı' seçeneği 'Etkin: 256 bit kurtarma anahtarına izin ver' (Otomatik) olarak ayarlanmalıdır.](#a1891115)
* [18.9.11.1.6 (BL) 'BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçme: BitLocker kurulum sihirbazından kurtarma seçeneklerini çıkar' seçeneği 'Etkin: Doğru' (Otomatik) olarak ayarlanmalıdır.](#a1891116)
* [18.9.11.1.7 (BL) 'BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçin: BitLocker kurtarma bilgilerini sabit veri sürücüleri için AD DS'ye kaydet' seçeneği 'Etkin: Yanlış' (Otomatik) olarak ayarlanmalıdır.](#a1891117)
* [18.9.11.1.8 (BL) 'BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçin: BitLocker kurtarma bilgilerinin depolanmasını AD DS'ye yapılandır' seçeneği 'Etkin: Kurtarma parolalarını ve anahtar paketlerini yedekle' (Otomatik) olarak ayarlanmalıdır.](#a1891118)
* [18.9.11.1.9 (BL) 'BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçin: Kurtarma bilgileri sabit veri sürücüleri için AD DS'de depolanana kadar BitLocker'ı etkinleştirmeyin' seçeneği 'Etkin: Yanlış' (Otomatik) olarak ayarlanmalıdır.](#a1891119)
* [18.9.11.1.10 (BL) 'Sabit veri sürücüleri için donanım tabanlı şifreleme kullanımını yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18911110)
* [18.9.11.1.11 (BL) 'Sabit veri sürücüleri için parola kullanımını yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18911111)
* [18.9.11.1.12 (BL) 'Sabit veri sürücülerinde akıllı kart kullanımını yapılandır' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18911112)
* [18.9.11.1.13 (BL) 'Sabit veri sürücülerinde akıllı kart kullanımını yapılandırma: Sabit veri sürücülerinde akıllı kart kullanımını gerektir' seçeneği 'Etkin: Doğru' (Otomatik) olarak ayarlanmalıdır.](#a18911113)

[**18.9.11.2 İşletim Sistemi Sürücüleri**](#a189112)

* [18.9.11.2.1 (BL) 'Başlangıç için geliştirilmiş PIN'lere izin ver' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1891121)
* [18.9.11.2.2 (BL) 'Bütünlük doğrulaması için Güvenli Önyüklemeye İzin Ver' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1891122)
* [18.9.11.2.3 (BL) 'BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılabileceğini seçin' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1891123)
* [18.9.11.2.4 (BL) 'BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılabileceğini seçin: Veri kurtarma aracısına izin ver' seçeneği 'Etkin: Yanlış' (Otomatik) olarak ayarlanmalıdır.](#a1891124)
* [18.9.11.2.5 (BL) 'BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılabileceğini seçin: Kurtarma Parolası' seçeneği 'Etkin: 48 basamaklı kurtarma parolası iste' (Otomatik) olarak ayarlanmalıdır.](#a1891125)
* [18.9.11.2.6 (BL) 'BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılabileceğini seçin: Kurtarma Anahtarı' seçeneği 'Etkin: 256 bit kurtarma anahtarına izin verme' (Otomatik) olarak ayarlanmalıdır.](#a1891126)
* [18.9.11.2.7 (BL) 'BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılabileceğini seçin: BitLocker kurulum sihirbazından kurtarma seçeneklerini çıkar' seçeneği 'Etkin: Doğru' (Otomatik) olarak ayarlanmalıdır.](#a1891128)
* [18.9.11.2.8 (BL) 'BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılabileceğini seçin: BitLocker kurtarma bilgilerini işletim sistemi sürücüleri için AD DS'ye kaydet' seçeneği 'Etkin: Doğru' (Otomatik) olarak ayarlanmalıdır.](#a1891128)
* [18.9.11.2.9 (BL) 'BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılabileceğini seçin: BitLocker kurtarma bilgilerinin depolanmasını AD DS'ye yapılandırın:' seçeneği 'Etkin: Kurtarma parolalarını ve anahtar paketlerini depola' (Otomatik) olarak ayarlanmalıdır.](#a1891129)
* [18.9.11.2.10 (BL) 'BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılabileceğini seçin: Kurtarma bilgileri işletim sistemi sürücüleri için AD DS'de depolanana kadar BitLocker'ı etkinleştirmeyin' seçeneği 'Etkin: Doğru' (Otomatik) olarak ayarlanmalıdır.](#a18911210)
* [18.9.11.2.11 (BL) 'İşletim sistemi sürücüleri için donanım tabanlı şifreleme kullanımını yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18911211)
* [18.9.11.2.12 (BL) 'İşletim sistemi sürücüleri için parola kullanımını yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18911212)
* [18.9.11.2.13 (BL) 'Başlangıçta ek kimlik doğrulaması gerektir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18911213)
* [18.9.11.2.14 (BL) 'Başlangıçta ek kimlik doğrulaması gerektir: BitLocker'a uyumlu TPM olmadan izin ver' seçeneği 'Etkin: Yanlış' (Otomatik) olarak ayarlanmalıdır.](#a18911214)

[**18.9.11.3 Çıkarılabilir Veri Sürücüleri**](#a189113)

* [18.9.11.3.1 (BL) 'Windows'un önceki sürümlerinden BitLocker korumalı çıkarılabilir veri sürücülerine erişime izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1891131)
* [18.9.11.3.2 (BL) 'BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılabileceğini seçin' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1891132)
* [18.9.11.3.3 (BL) 'BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılabileceğini seçin: Veri kurtarma aracısına izin ver' seçeneği 'Etkin: Doğru' (Otomatik) olarak ayarlanmalıdır.](#a1891133)
* [18.9.11.3.4 (BL) 'BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılabileceğini seçme: Kurtarma Parolası' seçeneği 'Etkin: 48 basamaklı kurtarma parolasına izin verme' olarak ayarlanmalıdır. (Otomatik)](#a1891134)
* [18.9.11.3.5 (BL) 'BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılabileceğini seçin: Kurtarma Anahtarı' seçeneği 'Etkin: 256 bit kurtarma anahtarına izin verme' (Otomatik) olarak ayarlanmalıdır.](#a1891135)
* [18.9.11.3.6 (BL) 'BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılabileceğini seçin: Kurtarma seçeneklerini BitLocker kurulum sihirbazından çıkar' seçeneği 'Etkin: Doğru' (Otomatik) olarak ayarlandığından emin olun](#a1891136)
* [18.9.11.3.7 (BL) 'BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılabileceğini seçin: BitLocker kurtarma bilgilerini çıkarılabilir veri sürücüleri için AD DS'ye kaydet' seçeneği 'Etkin: Yanlış' (Otomatik) olarak ayarlanmalıdır.](#a1891137)6566
* [18.9.11.3.8 (BL) 'BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılabileceğini seçin: BitLocker kurtarma bilgilerinin depolanmasını AD DS'ye yapılandırın:' seçeneği 'Etkin: Kurtarma parolalarını ve anahtar paketlerini yedekle' (Otomatik) olarak ayarlanmalıdır.](#a1891138)
* [18.9.11.3.9 (BL) 'BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılabileceğini seçin: Kurtarma bilgileri çıkarılabilir veri sürücüleri için AD DS'de depolanana kadar BitLocker'ı etkinleştirmeyin' seçeneği 'Etkin: Yanlış' (Otomatik) olarak ayarlanmalıdır.](#a1891139)
* [18.9.11.3.10 (BL) 'Çıkarılabilir veri sürücüleri için donanım tabanlı şifreleme kullanımını yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18911310)
* [18.9.11.3.11 (BL) 'Çıkarılabilir veri sürücüleri için parola kullanımını yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18911311)
* [18.9.11.3.12 (BL) 'Çıkarılabilir veri sürücülerinde akıllı kart kullanımını yapılandır' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18911312)
* [18.9.11.3.13 (BL) 'Çıkarılabilir veri sürücülerinde akıllı kart kullanımını yapılandırma: Çıkarılabilir veri sürücülerinde akıllı kart kullanımını gerektir' seçeneği 'Etkin: Doğru' (Otomatik) olarak ayarlanmalıdır.](#a18911313)
* [18.9.11.3.14 (BL) 'BitLocker tarafından korunmayan çıkarılabilir sürücülere yazma erişimini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18911314)
* [18.9.11.3.15 (BL) 'BitLocker tarafından korunmayan çıkarılabilir sürücülere yazma erişimini reddet: Başka bir kuruluşta yapılandırılmış cihazlara yazma erişimine izin verme' seçeneği 'Etkin: Yanlış' (Otomatik) olarak ayarlanmalıdır.](#a18911315)

[**18.9.11.4 (BL) 'Bu bilgisayar kilitliyken yeni DMA aygıtlarını devre dışı bırak' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**](#a189114)

[**18.9.12 Kamera**](#a18912)

* [18.9.12.1 (L2) 'Kamera Kullanımına İzin Ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189121)

[**18.9.13 Sohbet**](#a18913)

[**18.9.14 Bulut İçeriği**](#a18914)

* [18.9.14.1 (L1) 'Bulut kullanıcı hesabı durum içeriğini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a189141)
* [18.9.14.2 (L2) 'Bulut için optimize edilmiş içeriği kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a189142)
* [18.9.14.3 (L1) 'Microsoft tüketici deneyimlerini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a189143)

[**18.9.15 Bağlantı**](#a18915)

* [18.9.15.1 (L1) 'Eşleştirme için pin iste' seçeneği 'Etkin: İlk kez' VEYA 'Etkin: Her Zaman' (Otomatik) olarak ayarlanmalıdır.](#a189151)

[**18.9.16 Kimlik Bilgileri Kullanıcı Arayüzü**](#a18916)

* [18.9.16.1 (L1) 'Parola göster düğmesini görüntüleme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a189161)
* [18.9.16.2 (L1) 'Yönetici hesaplarını yükseklikte numaralandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189162)
* [18.9.16.3 (L1) 'Yerel hesaplar için güvenlik sorularının kullanılmasını engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a189163)

[**18.9.17 Veri toplama ve önizleme yapıları**](#a18917)

* [18.9.17.1 (L1) 'Tanılama Verilerine İzin Ver' seçeneği 'Etkin: Tanılama verileri kapalı (önerilmez)' veya 'Etkin: Gerekli tanılama verilerini gönder' (Otomatik) olarak ayarlanmalıdır.](#a189171)
* [18.9.17.2 (L2) 'Bağlı Kullanıcı Deneyimi ve Telemetri hizmeti için Kimliği Doğrulanmış Proxy kullanımını yapılandır' seçeneği 'Etkin: Kimliği Doğrulanmış Proxy kullanımını devre dışı bırak' (Otomatik) olarak ayarlanmalıdır.](#a189172)
* [18.9.17.3 (L1) ‘OneSettings indirmelerini devre dışı bırak’ seçeneği ‘Etkin’(Otomatik) olarak ayarlanmalıdır.](#a189173)
* [18.9.17.4 (L1) 'Geri bildirim bildirimlerini gösterme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a189174)
* [18.9.17.5 (L1) 'OneSettings Denetimini Etkinleştir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a189175)
* [18.9.17.6 (L1) 'Tanılama Günlüğü Toplamayı Sınırla' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a189176)
* [18.9.17.7 (L1) 'Limit Dump Collection' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a189177)
* [18.9.17.8 (L1) 'Insider derlemeleri üzerinde kullanıcı denetimini değiştir' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189178)

[**18.9.18 Teslimat Optimizasyonu**](#a18918)

* [18.9.18.1 (L1) 'İndirme Modu' seçeneği 'Etkin: İnternet' (Otomatik) olarak ayarlanmalıdır.](#a189181)

[**18.9.19 Masaüstü Gadget'ları**](#a18919)

[**18.9.20 Masaüstü Pencere Yöneticisi**](#a18920)

[**18.9.21 Aygıt ve Sürücü Uyumluluğu**](#a18921)

[**18.9.22 Cihaz kaydı (eski adıyla Workplace Join)**](#a18922)

[**18.9.23 Dijital Dolap**](#a18923)

[**18.9.24 Uç kullanıcı arayüzü**](#a18924)

[**18.9.25 NUMBER**](#a18925)

[**18.9.26 Etkinlik Yönlendirme**](#a18926)

[**18.9.27 Olay Günlüğü Hizmeti**](#a18927)

[**18.9.27.1 Uygulama**](#a189271)

* [18.9.27.1.1 (L1) 'Uygulama: Günlük dosyası maksimum boyutuna ulaştığında Olay Günlüğü davranışını denetle' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1892711)
* [18.9.27.1.2 (L1) 'Uygulama: Maksimum günlük dosyası boyutunu belirtin' seçeneği 'Etkin: 32.768 veya üzeri' (Otomatik) olarak ayarlanmalıdır.](#a1892712)

[**18.9.27.2 Güvenlik**](#a189272)

* [18.9.27.2.1 (L1) 'Güvenlik: Günlük dosyası maksimum boyutuna ulaştığında Olay Günlüğü davranışını denetle' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1892721)
* [18.9.27.2.2 (L1) 'Güvenlik: Maksimum günlük dosyası boyutunu belirtin (KB)' seçeneği 'Etkin: 196.608 veya üzeri' (Otomatik) olarak ayarlanmalıdır.](#a1892722)

[**18.9.27.3 Kurulum**](#a189273)

* [18.9.27.3.1 (L1) 'Kurulum: Günlük dosyası maksimum boyutuna ulaştığında Olay Günlüğü davranışını denetle' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1892731)
* [18.9.27.3.2 (L1) 'Kurulum: Maksimum günlük dosyası boyutunu belirtin' seçeneği 'Etkin: 32.768 veya üzeri' (Otomatik) olarak ayarlanmalıdır.](#a1892732)

[**18.9.27.4 Sistem**](#a189274)

* [18.9.27.4.1 (L1) 'Sistem: Günlük dosyası maksimum boyutuna ulaştığında Olay Günlüğü davranışını kontrol et' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1892741)
* [18.9.27.4.2 (L1) 'Sistem: Maksimum günlük dosyası boyutunu belirtin' seçeneği 'Etkin: 32.768 veya üzeri' (Otomatik) olarak ayarlanmalıdır.](#a1892742)

[**18.9.28 Etkinlik Kaydı**](#a18928)

[**18.9.29 Olay Görüntüleyicisi**](#a18929)

[**18.9.30 Aile Koruması (eski adıyla Ebeveyn Denetimleri)**](#a18930)

[**18.9.31 Dosya Gezgini (eski adıyla Windows Gezgini)**](#a18931)

* [18.9.31.2 (L1) 'Explorer için Veri Yürütme Engellemesini Kapat' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189312)
* [18.9.31.3 (L1) 'Bozulmada yığın sonlandırmayı kapat' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189313)
* [18.9.31.4 (L1) 'Kabuk protokolü korumalı modunu kapat' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189314)

[**18.9.32 Dosya Geçmişi**](#a18932)

[**18.9.33 Cihazımı Bul**](#a18933)

[**18.9.34 Oyun Gezgini**](#a18934)

[**18.9.35 El yazısı**](#a18935)

[**18.9.36 Ev Grubu**](#a18936)

* [18.9.36.1 (L1) 'Bilgisayarın ev grubuna katılmasını engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a189361)

[**18.9.37 İnsan Varlığı**](#a18937)

[**18.9.38 Video İçe Aktar**](#a18938)

[**18.9.39 Internet Explorer**](#a18939)

[**18.9.40 İnternet Bilgi Hizmetleri**](#a18940)

[**18.9.41 Konum ve Sensörler**](#a189a41)

* [18.9.41.1 (L2) 'Konumu kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a189a411)

[**18.9.42 Bakım Zamanlayıcı**](#a189a42)

[**18.9.43 Haritalar**](#a189a43)

[**18.9.44 MDM**](#a189a44)

[**18.9.45 Mesajlaşma**](#a189a45)

* [18.9.45.1 (L2) 'Message Service Cloud Senkronizasyonuna İzin Ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189451)

[**18.9.46 Microsoft hesabı**](#a18946)

* [18.9.46.1 (L1) 'Tüm tüketiciler için Microsoft hesabı kullanıcı kimlik doğrulamasını engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a189461)

[**18.9.47 Microsoft Defender Antivirüs (eski adıyla Windows Defender ve Windows Defender Antivirus)**](#a18947)

[**18.9.47.1 İstemci Arayüzü**](#a189471)

[**18.9.47.2 Cihaz Kontrolü**](#a189472)

[**18.9.47.3 İstisnalar**](#a189473)

[**18.9.47.4 MAPS**](#a189474)

* [18.9.47.4.1 (L1) 'Microsoft MAPS'e raporlama için yerel ayar geçersiz kılma özelliğini yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1894741)
* [18.9.47.4.2 (L2) 'Microsoft MAPS'e Katıl' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1894742)

[**18.9.47.5 Microsoft Defender Exploit Guard (eski adıyla Windows Defender Exploit**  **Guard)**](#a189475)

[**18.9.47.5.1 Saldırı Yüzeyinin Azaltılması**](#a1894751)

* [18.9.47.5.1.1 (L1) 'Saldırı Yüzeyi Azaltma kurallarını yapılandır' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18947511)
* [18.9.47.5.1.2 (L1) 'Saldırı Yüzeyi Azaltma kurallarını yapılandır: Her ASR kuralı için durumu ayarla' olarak yapılandır.(Otomatik)](#a18947512)

[**18.9.47.5.2 Kontrollü Klasör Erişimi**](#a1894752)

[**18.9.47.5.3 Ağ Koruması**](#a1894753)

* [18.9.47.5.3.1 (L1) 'Kullanıcıların ve uygulamaların tehlikeli web sitelerine erişmesini engelle' seçeneği 'Etkin: Engelle' (Otomatik) olarak ayarlanmalıdır.](#a18947531)

[**18.9.47.6 MpEngine**](#a189476)

* [18.9.47.6.1 (L2) 'Dosya karması hesaplama özelliğini etkinleştir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1894761)

[**18.9.47.7 Ağ Denetim Sistemi**](#a189477)

[**18.9.47.8 Karantina**](#a189478)

[**18.9.47.9 Gerçek zamanlı koruma**](#a189479)

* [18.9.47.9.1 (L1) 'İndirilen tüm dosyaları ve ekleri tara' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1894791)
* [18.9.47.9.2 (L1) 'Gerçek zamanlı korumayı kapat' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1894792)
* [18.9.47.9.3 (L1) 'Davranış izlemeyi aç' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1894793)
* [18.9.47.9.4 (L1) 'Komut dosyası taramasını aç' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1894794)

[**18.9.47.10 İyileştirme**](#a1894710)

[**18.9.47.11 Raporlama**](#a1894711)

* [18.9.47.11.1 (L2) 'Watson olaylarını yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18947111)

[**18.9.47.12 Tarama**](#a1894712)

* [18.9.47.12.1 (L1) 'Çıkarılabilir sürücüleri tara' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18947121)
* [18.9.47.12.2 (L1) 'E-posta taramasını aç' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18947122)

[**18.9.47.13 Güvenlik İstihbaratı Güncellemeleri (eski adıyla İmza Güncellemeleri)**](#a1894713)

[**18.9.47.14 Tehditler**](#a1894714)

* [18.9.47.15 (L1) 'İstenmeyen türden olabilecek uygulamalar için algılamayı yapılandır' seçeneği 'Etkin: Engelle' (Otomatik) olarak ayarlanmalıdır.](#a1894715)
* [18.9.47.16 (L1) 'Microsoft Defender Antivirüs'ü kapat' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1894716)

[**18.9.48 Microsoft Defender Application Guard (eski adıyla Windows Defender Application Guard)**](#a18948)

* [18.9.48.1 (NG) 'Microsoft Defender Application Guard'da olayların denetlenmesine izin ver' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a189481)
* [18.9.48.2 (NG) 'Microsoft Defender Application Guard'da kamera ve mikrofon erişimine izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189482)
* [18.9.48.3 (NG) 'Microsoft Defender Application Guard için veri kalıcılığına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189483)
* [18.9.48.4 (NG) 'Dosyaların Microsoft Defender Application Guard'dan ana bilgisayar işletim sistemine indirilmesine ve kaydedilmesine izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189484)
* [18.9.48.5 (NG) 'Microsoft Defender Application Guard pano ayarlarını yapılandırma: Pano davranış ayarı' seçeneği 'Etkin: Pano işlemini yalıtılmış bir oturumdan ana bilgisayara etkinleştir' (Otomatik) olarak ayarlanmalıdır.](#a189485)
* [18.9.48.6 (NG) 'Microsoft Defender Application Guard'ı Yönetilen Mod'da Aç' seçeneği 'Etkin: 1' (Otomatik) olarak ayarlanmalıdır.](#a189486)

[**18.9.49 Microsoft Defender Exploit Guard (eski adıyla Windows Defender Exploit Guard)**](#a18949)

[**18.9.50 Microsoft Edge**](#a18950)

[**18.9.51 Microsoft FIDO Kimlik Doğrulaması**](#a189a51)

[**18.9.52 Microsoft İkincil Kimlik Doğrulama Faktörü**](#a189a52)

[**18.9.53 Microsoft Kullanıcı Deneyimi Sanallaştırma**](#a189a53)

[**18.9.54 NetMeeting**](#a189a54)

[**18.9.55 Ağ Erişim Koruması**](#a189a55)

[**18.9.56 Ağ Projektörü**](#a189a56)

[**18.9.57 Haberler ve ilgi alanları**](#a18957)

* [18.9.57.1 (L2) 'Görev çubuğunda haberleri ve ilgi alanlarını etkinleştir' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189571)

[**18.9.58 OneDrive (eski adıyla SkyDrive)**](#a18958)

* [18.9.58.1 (L1) 'Dosya depolama alanı için OneDrive kullanımını engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a189581)

[**18.9.59 Çevrimiçi Yardım**](#a18959)

[**18.9.60 OOBE**](#a18960)

[**18.9.61 Parola Senkronizasyonu**](#a18961)

[**18.9.62 Taşınabilir İşletim Sistemi**](#a18962)

[**18.9.63 Sunum Ayarları**](#a18963)

[**18.9.64 Yüklemeye Zorla**](#a18964)

* [18.9.64.1 (L2) 'Yüklemeye Zorla hizmetini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a189641)

[**18.9.65 Uzak Masaüstü Hizmetleri (eski adıyla Terminal Hizmetleri)**](#a18965)

[**18.9.65.1 RD Lisansı (eski adıyla TH Lisansı)**](#a189651)

[**18.9.65.2 Uzak Masaüstü Bağlantısı İstemcisi**](#a189652)

* [18.9.65.2.1 RemoteFX USB Aygıt Yeniden Yönlendirme](#a1896521)
* [18.9.65.2.2 (L1) 'Şifrelerin kaydedilmesine izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1896522)

[**18.9.65.3 Uzak Masaüstü Oturum Ana Bilgisayarı (eski adıyla Terminal Server)**](#a189653)

[**18.9.65.3.1 Uygulama Uyumluluğu**](#a1896531)

[**18.9.65.3.2 Bağlantılar**](#a1896532)

* [18.9.65.3.2.1 (L2) 'Kullanıcıların Uzak Masaüstü Hizmetleri'ni kullanarak uzaktan bağlanmasına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18965321)

[**18.9.65.3.3 Cihaz ve Kaynak Yeniden Yönlendirme**](#a1896533)

* [18.9.65.3.3.1 (L2) 'UI Otomasyonu yeniden yönlendirmesine izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18965331)
* [18.9.65.3.3.2 (L2) 'COM bağlantı noktası yeniden yönlendirmesine izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18965332)
* [18.9.65.3.3.3 (L1) 'Sürücü yeniden yönlendirmesine izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18965333)
* [18.9.65.3.3.4 (L2) 'Konum yeniden yönlendirmeye izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18965334)
* [18.9.65.3.3.5 (L2) 'LPT bağlantı noktası yeniden yönlendirmesine izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18965335)
* [18.9.65.3.3.6 (L2) 'Desteklenen Tak ve Kullan cihaz yeniden yönlendirmesine izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18965336)

[**18.9.65.3.4 Lisanslama**](#a1896534)

[**18.9.65.3.5 Yazıcı Yeniden Yönlendirme**](#a1896535)

[**18.9.65.3.6 Profiller**](#a1896536)

[**18.9.65.3.7 RD Bağlantı Aracısı (eski adıyla TH Bağlantı Aracısı)**](#a1896537)

[**18.9.65.3.8 Uzak Oturum Ortamı**](#a1896538)

[**18.9.65.3.9 Güvenlik**](#a1896539)

* [18.9.65.3.9.1 (L1) 'Bağlantı sırasında her zaman parola sor' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18965391)
* [18.9.65.3.9.2 (L1) 'Güvenli RPC iletişimi gerektir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18965392)
* [18.9.65.3.9.3 (L1) 'Uzak (RDP) bağlantılar için belirli güvenlik katmanının kullanılmasını gerektir' seçeneği 'Etkin: SSL' (Otomatik) olarak ayarlanmalıdır.](#a18965393)
* [18.9.65.3.9.4 (L1) 'Ağ Düzeyinde Kimlik Doğrulama kullanarak uzak bağlantılar için kullanıcı kimlik doğrulaması gerektir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18965394)
* [18.9.65.3.9.5 (L1) 'İstemci bağlantısı şifreleme düzeyini ayarla' seçeneği 'Etkin: Yüksek Düzey' (Otomatik) olarak ayarlanmalıdır.](#a18965395)

[**18.9.65.3.10 Oturum Süresi Sınırları**](#a18965310)

* [18.9.65.3.10.1 (L2) 'Etkin ancak boşta olan Uzak Masaüstü Hizmetleri oturumları için zaman sınırı ayarla' seçeneği 'Etkin: 15 dakika veya daha az, ancak Hiçbir Zaman (0)’ olarak ayarlanmalıdır. (Otomatik)](#a189653101)
* [18.9.65.3.10.2 (L2) 'Bağlantısı kesilmiş oturumlar için süre sınırı ayarla' seçeneği 'Etkin: 1 dakika' (Otomatik) olarak ayarlanmalıdır.](#a189653102)

[**18.9.65.3.11 Geçici klasörler**](#a18965311)

* [18.9.65.3.11.1 (L1) 'Çıkışta geçici klasörleri silme' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189653111)

[**18.9.66 RSS Beslemeleri**](#a18966)

* [18.9.66.1 (L1) 'Kasaların indirilmesini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a189661)

[**18.9.67 Arama**](#a18967)

* [18.9.67.1 OCR](#a189671)
* [18.9.67.2 (L2) 'Cloud Search'e İzin Ver' seçeneği 'Etkin: Cloud Search'ü Devre Dışı Bırak' (Otomatik) olarak ayarlanmalıdır.](#a189672)
* [18.9.67.3 (L1) 'Cortana'ya izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189673)
* [18.9.67.4 (L1) 'Cortana'nın kilit ekranının üzerinde olmasına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189674)
* [18.9.67.5 (L1) 'Şifrelenmiş dosyaların dizine eklenmesine izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189675)
* [18.9.67.6 (L1) 'Aramanın ve Cortana'nın konumu kullanmasına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189676)

[**18.9.68 Güvenlik Merkezi**](#a18968)

[**18.9.69 NIS Sunucusu**](#a18969)

[**18.9.70 Kapatma Seçenekleri**](#a18970)

[**18.9.71 Akıllı Kart**](#a18971)

[**18.9.72 Yazılım Koruma Platformu**](#a18972)

* [18.9.72.1 (L2) 'KMS Client Online AVS Doğrulamasını Kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a189721)

[**18.9.73 Ses Kaydedici**](#a18973)

[**18.9.74 Konuşma**](#a18974)

[**18.9.75 Mağaza**](#a18975)

* [18.9.75.1 (L2) 'Microsoft Store'daki tüm uygulamaları devre dışı bırak' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189751)
* [18.9.75.2 (L1) 'Yalnızca Microsoft Store'daki özel mağazayı göster' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a189752)
* [18.9.75.3 (L1) 'Güncellemelerin Otomatik İndirilmesini ve Yüklenmesini Kapat' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189753)
* [18.9.75.4 (L1) 'Windows'un en son sürümüne güncelleme teklifini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a189754)
* [18.9.75.5 (L2) 'Mağaza uygulamasını kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a189755)

[**18.9.76 Ayarlarınızı senkronize edin**](#a18976)

[**18.9.77 Tablet PC**](#a18977)

[**18.9.78 Görev Zamanlayıcı**](#a18978)

[**18.9.79 Kiracı Kısıtlamaları**](#a18979)

[**18.9.80 Metin Girişi**](#a18980)

[**18.9.81 Widget'lar**](#a189a81)

* 18.9.81.1 (L1) 'Widget'lara izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlandığından emin olun

[**18.9.82 Windows Takvim**](#a189a82)

[**18.9.83 Windows Renk Sistemi**](#a189a83)

[**18.9.84 Windows Müşteri Deneyimini Geliştirme Programı**](#a189a84)

[**18.9.85 Windows Defender Akıllı Ekran**](#a189a85)

[**18.9.85.1 Gezgin**](#a189851)

* [18.9.85.1.1 (L1) 'Windows Defender SmartScreen'i Yapılandır' seçeneği 'Etkin: Uyar ve atlamayı önle' (Otomatik) olarak ayarlanmalıdır.](#a1898511)

[**18.9.85.2 Microsoft Edge**](#a189852)

* [18.9.85.2.1 (L1) 'Windows Defender SmartScreen'i Yapılandır' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1898521)
* [18.9.85.2.2 (L1) 'Siteler için Windows Defender SmartScreen istemlerinin atlanmasını engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1898522)

[**18.9.86 Windows Hata Bildirimi**](#a18986)

[**18.9.87 Windows Oyun Kaydı ve Yayını**](#a18987)

* [18.9.87.1 (L1) 'Windows Oyun Kaydını ve Yayınını etkinleştirir veya devre dışı bırakır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189871)

[**18.9.88 İş için Windows Hello (eski adıyla Microsoft Passport for Work)**](#a18988)

[**18.9.89 Windows Ink Çalışma Alanı**](#a18989)

* [18.9.89.1 (L2) 'Windows Ink Çalışma Alanı'nda önerilen uygulamalara izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189891)
* [18.9.89.2 (L1) ' Windows Ink Çalışma Alanına İzin Ver' seçeneği 'Etkin: Açık, ancak kilidin üstünde erişime izin verme' veya ‘Devre Dışı’ olarak ayarlanmalıdır, ‘Etkin’ yapılmamalıdır.](#a189892)

[**18.9.90 Windows Installer**](#a18990)

* [18.9.90.1 (L1) 'Yüklemeler üzerinde kullanıcı kontrolüne izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189901)
* [18.9.90.2 (L1) 'Her zaman yükseltilmiş ayrıcalıklarla yükle' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189902)
* [18.9.90.3 (L2) 'Windows Installer komut dosyaları için Internet Explorer güvenlik istemini engelle' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189903)

[**18.9.91 Windows Oturum Açma Seçenekleri**](#a18991)

* [18.9.91.1 (L1) 'Yeniden başlatmadan sonra oturum aç ve son etkileşimli kullanıcıyı otomatik olarak kilitle' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189911)

[**18.9.92 Windows Mail**](#a18992)

[**18.9.93 Windows Media Center**](#a18993)

[**18.9.94 Windows Media Dijital Hak Yönetimi**](#a18994)

[**18.9.95 Windows Media Player**](#a18995)

[**18.9.96 Windows Toplantı Alanı**](#a18996)

[**18.9.97 Windows Messenger**](#a18997)

[**18.9.98 Windows Mobility Center**](#a18998)

[**18.9.99 Windows Movie Maker**](#a18999)

[**18.9.100 Windows PowerShell**](#a189100)

* [18.9.100.1 (L1) 'PowerShell Betik Blok Günlüğünü Aç' seçeneği 'Etkin' (Otomatik) olarak ayarlanlanmalıdır.](#a1891001)
* [18.9.100.2 (L1) 'PowerShell Transkripsiyonunu Aç' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a189a1002)

[**18.9.101 Windows Güvenilirlik Analizi**](#a189a101)

[**18.9.102 Windows Uzaktan Yönetim (WinRM)**](#a189a102)

[**18.9.102.1 WinRM İstemcisi**](#a1891021)

* [18.9.102.1.1 (L1) 'Temel kimlik doğrulamasına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18910211)
* [18.9.102.1.2 (L1) 'Şifrelenmemiş trafiğe izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18910212)
* [18.9.102.1.3 (L1) 'Özet kimlik doğrulamasına izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18910213)

[**18.9.102.2 WinRM Hizmeti**](#a1891022)

* [18.9.102.2.1 (L1) 'Temel kimlik doğrulamasına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlandığından emin olun](#a18910221)
* [18.9.102.2.2 (L2) 'WinRM aracılığıyla uzaktan sunucu yönetimine izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18910222)
* [18.9.102.2.3 (L1) 'Şifrelenmemiş trafiğe izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18910223)
* [18.9.102.2.4 (L1) 'WinRM'nin RunAs kimlik bilgilerini depolamasına izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18910224)

[**18.9.103 Windows Uzak Kabuk**](#a189103)

* [18.9.103.1 (L2) 'Uzaktan Kabuk Erişimine İzin Ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1891031)

[**18.9.104 Windows Sandbox**](#a189104)

* [18.9.104.1 (L1) 'Windows Sandbox ile pano paylaşımına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1891041)
* [18.9.104.2 (L1) 'Windows Sandbox'ta ağa izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a1891042)

[**18.9.105 Windows Güvenliği (eski adıyla Windows Defender Güvenlik Merkezi)**](#a189105)

[**18.9.105.1 Hesap koruması**](#a1891051)

[**18.9.105.2 Uygulama ve tarayıcı koruması**](#a1891052)

* [18.9.105.2.1 (L1) 'Kullanıcıların ayarları değiştirmesini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18910521)

[**18.9.106 Windows SideShow**](#a189106)

[**18.9.107 Windows Sistem Kaynağı Yöneticisi**](#a189107)

[**18.9.108 Windows Güncelleme**](#a189108)

[**18.9.108.1 Eski Politikalar**](#a1891081)

* [18.9.108.1.1 (L1) 'Zamanlanmış otomatik güncelleştirme yüklemeleri için oturum açmış kullanıcılarla otomatik yeniden başlatma yok' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18910811)

[**18.9.108.2 Son kullanıcı deneyimini yönetme**](#a1891082)

* [18.9.108.2.1 (L1) 'Otomatik Güncelleştirmeleri Yapılandır' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18910821)
* [18.9.108.2.2 (L1) 'Otomatik Güncellemeleri Yapılandır: Zamanlanmış yükleme günü' seçeneği '0 - Her gün' (Otomatik) olarak ayarlanmalıdır.](#a18910822)
* [18.9.108.2.3 (L1) 'Güncellemeleri duraklat özelliğine erişimi kaldır' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a18910823)

[**18.9.108.3 Windows Server Update Service'ten sunulan güncellemeleri yönetme**](#a1891083)

[**18.9.108.4 Windows Update'ten (eski adıyla Windows Güncelleştirmelerini ve İş için Windows Update'i Ertele) sunulan güncelleştirmeleri yönetme**](#a1891084)

* [18.9.108.4.1 (L1) 'Önizleme yapılarını yönet' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a18910841)
* [18.9.108.4.2 (L1) 'Önizleme Derlemeleri ve Özellik Güncelleştirmelerinin ne zaman alınacağını seç' seçeneği 'Etkin: 180 gün veya daha fazla' (Otomatik) olarak ayarlanmalıdır.](#a18910842)
* [18.9.108.4.3 (L1) 'Kalite Güncellemelerinin ne zaman alınacağını seç' seçeneği 'Etkin: 0 gün' (Otomatik) olarak ayarlanmalıdır.](#a18910843)

[**19 Yönetim Şablonları (Kullanıcı)**](#a19)

[**19.1 Denetim Masası**](#a191)

[**19.1.1 Program Ekle veya Kaldır**](#a1911)

[**19.1.2 Ekran**](#a1912)

[**19.1.3 Kişiselleştirme (eski adıyla Masaüstü Temaları)**](#a1913)

* [19.1.3.1 (L1) 'Ekran koruyucuyu etkinleştir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a19131)
* [19.1.3.2 (L1) 'Ekran koruyucuyu parola ile koru' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a19132)
* [19.1.3.3 (L1) 'Ekran koruyucu zaman aşımı' seçeneği 'Etkin: 900 saniye veya daha az, ancak 0 değil' olarak ayarlanmalıdır. (Otomatik)](#a19133)

[**19.2 Masaüstü**](#a192)

[**19.3 Ağ**](#a193)

[**19.4 Paylaşılan Klasörler**](#a194)

[**19.5 Başlat Menüsü ve Görev Çubuğu**](#a195)

[**19.5.1 Bildirimler**](#a1951)

* [19.5.1.1 (L1) 'Kilit ekranında toast bildirimlerini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a19511)

[**19.6 Sistem**](#a196)

[**19.6.1 Ctrl+Alt+Del Seçenekleri**](#a1961)

[**19.6.2 Ekran**](#a1962)

[**19.6.3 Sürücü Kurulumu**](#a1963)

[**19.6.4 Klasör Yeniden Yönlendirme**](#a1964)

[**19.6.5 Grup İlkesi**](#a1965)

[**19.6.6 İnternet İletişim Yönetimi**](#a1966)

[**19.6.6.1 İnternet İletişimi ayarları**](#a19661)

* [19.6.6.1.1 (L2) 'Yardım Deneyimini Geliştirme Programını Kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a196611)

[**19.7 Windows Bileşenleri**](#a197)

[**19.7.1 Windows 8 / 8.1 / 10'a özellikler ekleme (eski adıyla Windows Anytime Upgrade)**](#a1971)

[**19.7.2 Uygulama çalışma zamanı**](#a1972)

[**19.7.3 Uygulama Uyumluluğu**](#a1973)

[**19.7.4 Ek Yöneticisi**](#a1974)

* [19.7.4.1 (L1) 'Dosya eklerindeki bölge bilgilerini koruma' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a19741)
* [19.7.4.2 (L1) 'Ekleri açarken virüsten koruma programlarını bilgilendir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a19742)

[**19.7.5 Otomatik Oynatma Politikaları**](#a1975)

[**19.7.6 Yedekleme**](#a1976)

[**19.7.7 Hesap Makinesi**](#a1977)

[**19.7.8 Bulut İçeriği**](#a1978)

* [19.7.8.1 (L1) 'Windows spot ışığını kilit ekranında yapılandır' seçeneği Devre Dışı' (Otomatik) olarak ayarlanmalıdır.](#a19781)
* [19.7.8.2 (L1) 'Windows spot ışığında üçüncü taraf içeriği önerme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a19782)
* [19.7.8.3 (L2) 'Tanılama verilerini uyarlanmış deneyimler için kullanma' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a19783)
* [19.7.8.4 (L2) 'Tüm Windows spot ışığı özelliklerini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a19784)
* [19.7.8.5 (L1) 'Masaüstünde Spotlight koleksiyonunu kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a19785)

[**19.7.9 Kimlik Bilgileri Kullanıcı Arayüzü**](#a1979)

[**19.7.10 Veri toplama ve önizleme derlemeleri**](#a19710)

[**19.7.11 Masaüstü Araçları**](#a19711)

[**19.7.12 Masaüstü Pencere Yöneticisi**](#a19712)

[**19.7.13 Dijital Dolap**](#a19713)

[**19.7.14 Uç kullanıcı arayüzü**](#a19714)

[**19.7.15 Dosya Gezgini (eski adıyla Windows Gezgini)**](#a19715)

[**19.7.16 Dosya İptali**](#a19716)

[**19.7.17 İSİM**](#a19717)

[**19.7.18 Video İçe Aktar**](#a19718)

[**19.7.19 Anlık Arama**](#a19719)

[**19.7.20 Internet Explorer**](#a19720)

[**19.7.21 Konum ve Sensörler**](#a19721)

[**19.7.22 Microsoft Edge**](#a19722)

[**19.7.23 Microsoft Yönetim Konsolu**](#a19723)

[**19.7.24 Microsoft Kullanıcı Deneyimi Sanallaştırma**](#a19724)

[**19.7.25 Çoklu görev**](#a19725)

[**19.7.26 NetMeeting**](#a19726)

[**19.7.27 Ağ Projektörü**](#a19727)

[**19.7.28 Ağ Paylaşımı**](#a19728)

* [19.7.28.1 (L1) 'Kullanıcıların profillerinde dosya paylaşmasını engelle.' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a197281)

[**19.7.29 OOBE**](#a19729)

[**19.7.30 Sunum Ayarları**](#a19730)

[**19.7.31 Uzak Masaüstü Hizmetleri (eski adıyla Terminal Hizmetleri)**](#a19731)

[**19.7.32 RSS Beslemeleri**](#a19732)

[**19.7.33 Arama**](#a19733)

[**19.7.34 Ses Kaydedici**](#a19734)

[**19.7.35 Mağaza**](#a19735)

[**19.7.36 Tablet PC**](#a19736)

[**19.7.37 Görev Zamanlayıcı**](#a19737)

[**19.7.38 Windows Takvim**](#a19738)

[**19.7.39 Windows Renk Sistemi**](#a19739)

[**19.7.40 Windows Defender Akıllı Ekran**](#a19740)

[**19.7.41 Windows Hata Bildirimi**](#a19741)

[**19.7.42 İş için Windows Hello (eski adıyla Microsoft Passport for Work)**](#a19742)

[**19.7.43 Windows Installer**](#a19743)

* [19.7.43.1 (L1) 'Her zaman yükseltilmiş ayrıcalıklarla yükle' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlandığından emin olun](#a197431)

[**19.7.44 Windows Oturum Açma Seçenekleri**](#a19744)

[**19.7.45 Windows Posta**](#a19745)

[**19.7.46 Windows Media Center**](#a19746)

[**19.7.47 Windows Media Player**](#a19747)

[**19.7.47.1 Ağ İletişimi**](#a197471)

[**19.7.47.2 Oynatma**](#a197472)

* [19.7.47.2.1 (L2) 'Codec Bileşeninin İndirilmesini Engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.](#a1974721)

**5.Uygulama**

**1 Hesap İlkeleri**

**1.1 Parola İlkesi**

**1.1.1 (L1) 'Parola geçmişini zorla' seçeneği '24 veya daha fazla şifre' olarak ayarlanmalıdır.**

**Açıklama :**

Bu ilke ayarı, eski bir parolayı yeniden kullanabilmeniz için bir kullanıcı hesabıyla ilişkilendirilmesi gereken yenilenen benzersiz parolaların sayısını belirler. Bu ilke ayarının değeri 0 ile 24 parola arasında olmalıdır. Windows Vista için varsayılan değer 0 paroladır, ancak bir etki alanındaki varsayılan ayar 24 paroladır. Bu ilke ayarının etkinliğini korumak için, kullanıcıların parolalarını tekrar tekrar değiştirmesini önlemek için Minimum parola yaşı ayarını kullanın.

Bu ayar için önerilen durum: 24 veya daha fazla parola

**Not**: Parola İlkesi ayarları (bölüm 1.1) ve Hesap Kilitleme İlkesi ayarları (bölüm 1.2), varsayılan davranış olarak etki alanı kullanıcı hesaplarında global olarak geçerli olmak için Varsayılan Etki Alanı İlkesi GPO'su aracılığıyla uygulanmalıdır. Bu ayarlar başka bir GPO'da yapılandırılırsa, yalnızca GPO'yu alan bilgisayarlardaki yerel kullanıcı hesaplarını etkiler. Ancak, belirli etki alanı kullanıcıları ve/veya grupları için varsayılan parola ilkesine ve hesap kilitleme ilkesi kurallarına özel istisnalar, Grup İlkesinden tamamen ayrı olan ve en kolay şekilde Active Directory Yönetim Merkezi kullanılarak yapılandırılan Parola Ayarları Nesneleri (PSO'lar) kullanılarak tanımlanabilir.

**Gerekçe:**

Bir kullanıcı aynı parolayı ne kadar uzun süre kullanırsa, saldırganın kaba kuvvet saldırıları yoluyla parolayı belirleme şansı o kadar artar. Ayrıca, güvenliği ihlal edilmiş olabilecek hesaplar, parola değiştirilmediği sürece kötüye kullanılabilir durumda kalacaktır. Parola değişiklikleri gerekliyse ancak parolanın yeniden kullanımı engellenmiyorsa veya kullanıcılar sürekli olarak az sayıda parolayı yeniden kullanıyorsa, iyi bir parola politikasının etkinliği büyük ölçüde azalır. Bu ilke ayarı için düşük bir sayı belirtirseniz, kullanıcılar aynı az sayıda parolayı art arda kullanabilecektir. Minimum parola yaşı ayarını da yapılandırmazsanız, kullanıcılar orijinal parolalarını yeniden kullanana kadar parolalarını art arda değiştirebilir.

**Etki:**

Bu yapılandırmanın en büyük etkisi, kullanıcıların eski parolalarını her değiştirmeleri gerektiğinde yeni bir parola oluşturmaları gerektiğidir. Kullanıcıların parolalarını yeni benzersiz değerlerle değiştirmeleri gerekiyorsa, kullanıcıların parolalarını unutmamak için bir yere yazma riski artar. Diğer bir risk, kullanıcıların ezberlemeyi kolaylaştırmak, ancak tahmin edilmelerini kolaylaştırmak için kademeli olarak değişen (örneğin, password01, password02 vb.) şifreler oluşturmalarıdır. Ayrıca, Minimum parola yaşı ayarı için aşırı derecede düşük bir değer, parolalarını unutan kullanıcılar yardım masasından sık sık sıfırlamasını isteyebileceklerinden, yönetim yükünü artıracaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme**:

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu 24 veya daha fazla parolaya ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Hesap İlkeleri\Parola Politikası\Parola geçmişini uygula*

**1.1.2 (L1) Maximum parola süresi seçeneği '365 gün veya daha az, ama 0 olamaz' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir kullanıcının parolasının süresi dolmadan önce ne kadar süreyle kullanabileceğini tanımlar. Bu ilke ayarının değerleri 0 ile 999 gün arasında değişir. Değeri 0 olarak ayarlarsanız, parolanın süresi asla dolmaz. Saldırganlar şifreleri kırabildiğinden, şifreyi ne kadar sık değiştirirseniz, saldırganın kırılmış bir şifre kullanma şansı o kadar az olur. Ancak, bu değer ne kadar düşük ayarlanırsa, kullanıcıların parolalarını değiştirmeleri veya hangi parolanın geçerli olduğunu unutmaları nedeniyle yardım masası desteğine yapılan çağrıların artması olasılığı o kadar yüksek olur. Bu ayar için önerilen durum 365 veya daha az gündür, ancak 0 değildir.

**Not:** Parola İlkesi ayarları (bölüm 1.1) ve Hesap Kilitleme İlkesi ayarları (bölüm 1.2), varsayılan davranış olarak etki alanı kullanıcı hesaplarında global olarak geçerli olmak için Varsayılan Etki Alanı İlkesi GPO'su aracılığıyla uygulanmalıdır. Bu ayarlar başka bir GPO'da yapılandırılırsa, yalnızca GPO'yu alan bilgisayarlardaki yerel kullanıcı hesaplarını etkiler. Ancak, belirli etki alanı kullanıcıları ve/veya grupları için varsayılan parola ilkesine ve hesap kilitleme ilkesi kurallarına özel istisnalar, Grup İlkesinden tamamen ayrı olan ve en kolay şekilde Active Directory Yönetim Merkezi kullanılarak yapılandırılan Parola Ayarları Nesneleri (PSO'lar) kullanılarak tanımlanabilir.

**Gerekçe:**

Bir parola ne kadar uzun olursa, bir kaba kuvvet saldırısı, bir saldırganın kullanıcı hakkında genel bilgi edinmesi veya parolayı paylaşan kullanıcı tarafından ele geçirilme olasılığı o kadar yüksek olur. Kullanıcıların hiçbir zaman parolalarını değiştirmek zorunda kalmamaları için Maksimum parola yaşı ayarını 0 olarak yapılandırmak büyük bir güvenlik riskidir, çünkü bu, geçerli kullanıcının yetkilendirilmiş erişimi olduğu sürece, güvenliği ihlal edilmiş bir parolanın kötü niyetli kullanıcı tarafından kullanılmasına izin verir.

**Etki:**

Maksimum parola yaşı ayarı çok düşükse, kullanıcıların parolalarını çok sık değiştirmeleri gerekir. Bu tür bir yapılandırma, kullanıcılar parolalarını güvenli olmayan bir yere yazabileceği veya kaybedebileceği için kuruluştaki güvenliği azaltabilir. Bu ilke ayarının değeri çok yüksekse, potansiyel saldırganların kullanıcı parolalarını keşfetmeleri veya güvenliği ihlal edilmiş hesapları kullanmaları için daha fazla zaman sağladığından bir kuruluş içindeki güvenlik düzeyi azalır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu 365 veya daha az güne ayarlayın, ancak 0'a değil:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Hesap İlkeleri\Parola İlkesi\Maksimum parola yaşı*

**1.1.3 (L1)'Minimum parola süresi' seçeneği '1 gün veya daha fazla' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, parolayı değiştirebilmeniz için kaç gün kullanmanız gerektiğini belirler. Bu ilke ayarının değer aralığı 1 ile 999 gün arasındadır. (Ayrıca, anında parola değişikliklerine izin vermek için değeri 0 olarak ayarlayabilirsiniz.) Bu ayar için varsayılan değer 0 gündür. Bu ayar için önerilen durum: 1 veya daha fazla gün).

**Not:** Parola İlkesi ayarları (bölüm 1.1) ve Hesap Kilitleme İlkesi ayarları (bölüm 1.2), varsayılan davranış olarak etki alanı kullanıcı hesaplarında global olarak geçerli olmak için Varsayılan Etki Alanı İlkesi GPO'su aracılığıyla uygulanmalıdır. Bu ayarlar başka bir GPO'da yapılandırılırsa, yalnızca GPO'yu alan bilgisayarlardaki yerel kullanıcı hesaplarını etkiler. Ancak, belirli etki alanı kullanıcıları ve/veya grupları için varsayılan parola ilkesine ve hesap kilitleme ilkesi kurallarına özel istisnalar, Grup İlkesinden tamamen ayrı olan ve en kolay şekilde Active Directory Yönetim Merkezi kullanılarak yapılandırılan Parola Ayarları Nesneleri (PSO'lar) kullanılarak tanımlanabilir.

**Gerekçe:**

Kullanıcıların, hatırlamaları kolay olduğu ve parola seçimlerinin tehlikeye atılmaya karşı güvenli olduğuna inandıkları için kullanmayı sevdikleri favori parolaları olabilir. Ne yazık ki, parolalar tehlikeye girer ve bir saldırgan belirli bir kişinin kullanıcı hesabını hedef alıyorsa, o kullanıcıyla ilgili verileri önceden bilerek, eski parolaların yeniden kullanılması bir güvenlik ihlaline neden olabilir. Parolayı yeniden kullanmak için güvenlik ayarlarının bir kombinasyonu gereklidir. Bu ilke ayarının Parola geçmişini uygula ayarıyla birlikte kullanılması, eski parolaların kolayca yeniden kullanılmasını engeller. Örneğin, Parola geçmişini uygula ayarını, kullanıcıların son 12 parolalarından hiçbirini yeniden kullanamayacaklarından emin olmak için yapılandırırsanız, Minimum parolayı da yapılandırmadığınız sürece parolalarını birkaç dakika içinde 13 kez değiştirebilir ve başladıkları parolayı yeniden kullanabilirler. yaş ayarını 0'dan büyük bir sayıya ayarlayın. Parola geçmişini uygula ayarının etkili olması için bu ilke ayarını 0'dan büyük bir sayıya yapılandırmanız gerekir.

**Etki:**

Bir yönetici bir kullanıcı için bir parola belirlerse ancak kullanıcı ilk oturum açtığında bu kullanıcının parolayı değiştirmesini isterse, yöneticinin Kullanıcı bir sonraki oturum açmada parolayı değiştirmeli onay kutusunu seçmesi gerekir, aksi takdirde kullanıcı parolayı değiştiremez ertesi güne kadar şifre.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu 1 veya daha fazla güne ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Hesap İlkeleri\Parola İlkesi\Minimum parola yaşı*

**1.1.4 (L1) 'Minimum parola uzunluğu' seçeneği '14 veya daha fazla karakter' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir kullanıcı hesabı için parola oluşturan en az karakter sayısını belirler. Bir kuruluş için en iyi parola uzunluğunun nasıl belirleneceği konusunda birçok farklı teori vardır, ancak belki de "passphrase", "password"dan daha iyi bir terimdir. Microsoft Windows 2000 ve daha yeni sürümlerde, parolalar oldukça uzun olabilir ve boşluk içerebilir. Bu nedenle, "5 dolarlık milkshake içmek istiyorum" gibi bir ifade geçerli bir paroladır; 8 veya 10 karakterlik rastgele sayı ve harflerden çok daha güçlü bir paroladır ve yine de hatırlanması daha kolaydır. Kullanıcılar, özellikle şifre uzunluğu ile ilgili olarak, şifrelerin doğru seçimi ve bakımı konusunda eğitilmelidir. Kurumsal ortamlarda, Minimum parola uzunluğu ayarı için ideal değer 14 karakterdir, ancak bu değeri kuruluşunuzun iş gereksinimlerini karşılayacak şekilde ayarlamanız gerekir. Bu ayar için önerilen durum: 14 veya daha fazla karakterdir.

**Not:** Windows Server 2016 ve Windows Server'ın daha eski sürümlerinde, Yerel Güvenlik İlkesi (LSP), Yerel Grup İlkesi Düzenleyicisi (LGPE) ve Grup İlkesi Yönetimi Düzenleyicisi'nin (GPME) GUI'si bu değeri 14 karakterden daha yüksek bir değere ayarlamanıza izin vermez. . Ancak, Windows Server 2019'dan başlayarak Microsoft, GUI'yi minimum 20 karakterlik bir parola uzunluğuna izin verecek şekilde değiştirdi.

**Not 2:** Parola İlkesi ayarları (bölüm 1.1) ve Hesap Kilitleme İlkesi ayarları (bölüm 1.2), etki alanı kullanıcı hesaplarında varsayılan davranışları olarak global olarak geçerli olmak için Varsayılan Etki Alanı İlkesi GPO aracılığıyla uygulanmalıdır. Bu ayarlar başka bir GPO'da yapılandırılırsa, yalnızca GPO'yu alan bilgisayarlardaki yerel kullanıcı hesaplarını etkiler. Ancak, belirli etki alanı kullanıcıları ve/veya grupları için varsayılan parola ilkesine ve hesap kilitleme ilkesi kurallarına özel istisnalar, Grup İlkesinden tamamen ayrı olan ve en kolay şekilde Active Directory Yönetim Merkezi kullanılarak yapılandırılan Parola Ayarları Nesneleri (PSO'lar) kullanılarak tanımlanabilir.

**Gerekçe:**

Parola saldırı türleri arasında sözlük saldırıları (yaygın sözcükleri ve tümcecikleri kullanmaya çalışan) ve kaba kuvvet saldırıları (olası her karakter kombinasyonunu deneyen) bulunur. Ayrıca, saldırganlar bazen hesapları ve parolaları keşfetmek için araçları kullanabilmeleri için hesap veritabanını elde etmeye çalışırlar.

**Etki:**

Çok uzun parolalar için gereksinimler, kullanıcılar bilgileri güvenli olmayan bir yerde bırakabileceği veya kaybedebileceği için aslında bir kuruluşun güvenliğini azaltabilir. Çok uzun parolalar gerekliyse, yanlış yazılan parolalar hesapların kilitlenmesine neden olabilir ve yardım masası aramalarının hacmini artırabilir. Kuruluşunuz parola uzunluğu gereksinimleri nedeniyle unutulan parolalarla ilgili sorunlar yaşıyorsa, kullanıcılarınıza genellikle hatırlaması daha kolay olan ve daha fazla sayıda karakter kombinasyonu nedeniyle keşfetmesi çok daha zor olan parolaları öğretmeyi düşünün. Not: Windows 98 ve Windows NT 4.0 gibi daha eski Windows sürümleri, 14 karakterden uzun parolaları desteklemez. Bu eski işletim sistemlerini çalıştıran bilgisayarlar, uzun parolalar gerektiren hesapları kullanan bilgisayarlarda veya etki alanlarında kimlik doğrulaması yapamaz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:** GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu 14 veya daha fazla karaktere ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Hesap İlkeleri\Parola Politikası\Minimum parola uzunluğu*

**1.1.5 (L1) 'Parola karışıklık gereksinimlerini karşılamalıdır' seçeneği 'Etkin' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, güçlü parolalar için temel gereksinimleri karşıladıklarından emin olmak için tüm yeni parolaları kontrol eder. Bu politika etkinleştirildiğinde, parolalar aşağıdaki minimum gereksinimleri karşılamalıdır:

* Kullanıcının hesap adını veya kullanıcının tam adının ardışık iki karakteri aşan kısımlarını içermemelidir.
* En az altı karakter uzunluğunda olun
* Aşağıdaki kategorilerin üçünden karakterler içerir:
  + İngilizce büyük harfler (A'dan Z'ye)
  + İngilizce küçük harfler (a'dan z'ye)
  + 10 basamaklı taban (0 - 9)
  + Alfabetik olmayan karakterler (örneğin, !, $, #, %
  + Önceki dört kategoriye girmeyen herhangi bir Unicode karakterinin tümünü yakalama kategorisi. Bu beşinci kategori bölgesel olarak spesifik olabilir.

Paroladaki her ek karakter, karmaşıklığını katlanarak artırır. Örneğin, yedi karakterli, tamamı küçük harfli bir alfabetik parola 267 (yaklaşık 8 x 109 veya 8 milyar) olası kombinasyona sahip olacaktır. Saniyede 1.000.000 denemede (birçok şifre kırma yardımcı programının özelliği), kırılması yalnızca 133 dakika sürer. Büyük/küçük harf duyarlılığına sahip yedi karakterli alfabetik bir parola 527 kombinasyona sahiptir. Yedi karakterli, büyük/küçük harf duyarlı, noktalama işareti olmayan alfasayısal bir parolanın 627 kombinasyonu vardır. Sekiz karakterli bir parolanın 268 (veya 2 x 1011) olası kombinasyonu vardır. Bu çok büyük bir sayı gibi görünse de, saniyede 1.000.000 denemede tüm olası parolaları denemek yalnızca 59 saat sürer. Unutmayın, ALT karakterleri ve "!" gibi diğer özel klavye karakterlerini kullanan şifreler için bu süreler önemli ölçüde artacaktır. veya "@". Parola ayarlarının doğru kullanımı, bir kaba kuvvet saldırısı gerçekleştirmeyi zorlaştırmaya yardımcı olabilir. Bu ayar için önerilen durum: Etkin.

**Not:** Parola İlkesi ayarları (bölüm 1.1) ve Hesap Kilitleme İlkesi ayarları (bölüm 1.2), varsayılan davranış olarak etki alanı kullanıcı hesaplarında global olarak geçerli olmak için Varsayılan Etki Alanı İlkesi GPO'su aracılığıyla uygulanmalıdır. Bu ayarlar başka bir GPO'da yapılandırılırsa, yalnızca GPO'yu alan bilgisayarlardaki yerel kullanıcı hesaplarını etkiler. Ancak, belirli etki alanı kullanıcıları ve/veya grupları için varsayılan parola ilkesine ve hesap kilitleme ilkesi kurallarına özel istisnalar, Grup İlkesinden tamamen ayrı olan ve en kolay şekilde Active Directory Yönetim Merkezi kullanılarak yapılandırılan Parola Ayarları Nesneleri (PSO'lar) kullanılarak tanımlanabilir.

**Gerekçe:**

Yalnızca alfasayısal karakterler içeren parolaların, herkese açık çeşitli araçlarla keşfedilmesi son derece kolaydır.

**Etki:**

Varsayılan parola karmaşıklığı yapılandırması korunursa, kullanıcılar alfabetik olmayan karakterler içeren parolalara alışık olmayabileceğinden, kilitli hesaplar için ek yardım masası çağrıları yapılabilir. Bununla birlikte, tüm kullanıcılar, karmaşıklık gereksinimini minimum zorlukla karşılayabilmelidir. Kuruluşunuzun daha katı güvenlik gereksinimleri varsa, Passfilt.dll dosyasının rastgele karmaşık parola gücü kurallarının kullanımına izin veren özel bir sürümünü oluşturabilirsiniz. Örneğin, özel bir parola filtresi, üst satır olmayan karakterlerin kullanılmasını gerektirebilir. (Üst satır karakterleri, SHIFT tuşunu basılı tutmanızı ve 1 ile 0 arasındaki rakamlardan herhangi birine basmanızı gerektiren karakterlerdir.) Özel bir parola filtresi, önerilen parolanın ortak sözlük sözcükleri içermediğini doğrulamak için bir sözlük denetimi de yapabilir veya parça. Ayrıca, ALT tuş karakter kombinasyonlarının kullanılması, bir parolanın karmaşıklığını büyük ölçüde artırabilir. Ancak, bu tür katı parola gereksinimleri, mutsuz kullanıcılar ve son derece meşgul bir yardım masası ile sonuçlanabilir. Alternatif olarak, kuruluşunuz tüm yönetici parolalarının 0128 - 0159 aralığında ALT karakterlerini kullanma gereksinimini değerlendirebilir. (Bu aralığın dışındaki ALT karakterler, parolaya ek karmaşıklık eklemeyen standart alfasayısal karakterleri temsil edebilir.)

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Hesap İlkeleri\Parola İlkesi\Parola karmaşıklık gereksinimlerini karşılamalıdır*

**1.1.6 (L1) 'Minimum şifre uzunluğu limiti esnektir' seçeneği 'Etkin' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, minimum parola uzunluğu ayarının eski 14 karakterlik sınırın ötesine yükseltilip yükseltilemeyeceğini belirler. Daha fazla bilgi için lütfen aşağıdaki [Microsoft Güvenlik Bloguna](https://techcommunity.microsoft.com/t5/microsoft-security-baselines/security-baseline-draft-windows-10-and-windows-server-version/ba-p/1419213) bakın. Bu ayar için önerilen durum: Etkin.

**Not:** Bu ayar yalnızca bilgisayardaki yerel hesapları etkiler. Etki alanı hesapları, etki alanı hesaplarının depolandığı yer olduğundan, yalnızca Etki Alanı Denetleyicilerindeki ayarlardan etkilenir. Gerekçe: Bu ayar, MFA'nın kullanılmadığı durumlarda daha uzun ve genellikle daha güçlü parolaların veya parolaların uygulanmasını sağlar.

**Etki:**

Minimum parola uzunluğu ayarı 14 karakterden daha uzun yapılandırılabilir. Çok uzun parolalar gerekliyse, yanlış yazılan parolalar hesapların kilitlenmesine neden olabilir ve yardım masası aramalarının hacmini artırabilir. Kuruluşunuz parola uzunluğu gereksinimleri nedeniyle unutulan parolalarla ilgili sorunlar yaşıyorsa, kullanıcılarınıza genellikle hatırlaması daha kolay olan ve daha fazla sayıda karakter kombinasyonu nedeniyle keşfetmesi çok daha zor olan parolaları öğretmeyi düşünün.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Control\SAM:RelaxMinimumPasswordL engthLimits*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Hesap İlkeleri\Parola Politikası\Relax minimum parola uzunluğu sınırları*

**Not:** Bu ayar yalnızca Windows 10 Sürüm 2004 ve Server 2022'nin (veya daha yenisi) yerleşik işletim sistemi güvenlik şablonunda mevcuttur ve işletim sisteminin eski sürümleri veya indirilebilir Yönetim Şablonları (ADMX/ADML) aracılığıyla kullanılamaz. Bu nedenle, bu ayarı Grup İlkesi Yönetim Konsolu (GPMC) veya Grup İlkesi Yönetim Düzenleyicisi (GPME) ile görüntülemek veya düzenlemek için Windows 10 Sürüm 2004 veya Server 2022 sistemi (veya daha yenisi) kullanmanız gerekir.

**1.1.7 (L1) 'Parolaları geri döndürülebilir şifreleme kullanarak depolama' seçeneği 'Devre Dışı' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, işletim sisteminin parolaları, kimlik doğrulama amacıyla kullanıcının parolası hakkında bilgi gerektiren uygulama protokolleri için destek sağlayan, tersine çevrilebilir şifreleme kullanan bir şekilde depolayıp depolamayacağını belirler. Tersinir şifreleme ile saklanan şifreler, esasen şifrelerin düz metin versiyonları ile aynıdır. Bu ayar için önerilen durum: Devre Dışı.

**Not:** Parola İlkesi ayarları (bölüm 1.1) ve Hesap Kilitleme İlkesi ayarları (bölüm 1.2), varsayılan davranış olarak etki alanı kullanıcı hesaplarında global olarak geçerli olmak için Varsayılan Etki Alanı İlkesi GPO'su aracılığıyla uygulanmalıdır. Bu ayarlar başka bir GPO'da yapılandırılırsa, yalnızca GPO'yu alan bilgisayarlardaki yerel kullanıcı hesaplarını etkiler. Ancak, belirli etki alanı kullanıcıları ve/veya grupları için varsayılan parola ilkesine ve hesap kilitleme ilkesi kurallarına özel istisnalar, Grup İlkesinden tamamen ayrı olan ve en kolay şekilde Active Directory Yönetim Merkezi kullanılarak yapılandırılan Parola Ayarları Nesneleri (PSO'lar) kullanılarak tanımlanabilir.

**Gerekçe:**

Bu ilke ayarını etkinleştirmek, işletim sisteminin parolaları, tehlikeye atılmaya çok daha açık olan ve sistem güvenliğinizi zayıflatan daha zayıf bir biçimde depolamasına olanak tanır.

**Etki:**

Kuruluşunuz, uzaktan erişim veya IAS hizmetleri aracılığıyla CHAP kimlik doğrulama protokolünü veya IIS'de Özet Kimlik Doğrulamayı kullanıyorsa, bu ilke ayarını Etkin olarak yapılandırmanız gerekir. Active Directory Kullanıcıları ve Bilgisayarlarında uygun kullanıcı hesabı nesnesinin açılmasını gerektirdiğinden, bu ayarın her kullanıcı için Grup İlkesi aracılığıyla uygulanması son derece tehlikelidir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Hesap İlkeleri\Parola İlkesi\Geri dönüşümlü şifreleme kullanarak parolaları saklayın*

**1.2 Hesap Kilitleme İlkesi**

**1.2.1 (L1) 'Hesap kilitleme süresi' seçeneği '15 dakika veya daha fazla' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kilitli bir hesabın kilidinin açılması ve kullanıcının yeniden oturum açmayı deneyebilmesi için geçmesi gereken süreyi belirler. Ayar bunu, kilitli bir hesabın kullanılamayacağı dakika sayısını belirterek yapar. Bu ilke ayarının değeri 0 olarak yapılandırılırsa, kilitlenen hesaplar, bir yönetici bunları manuel olarak açana kadar kilitli kalır. Bu ilke ayarının değerini yüksek bir değere yapılandırmak iyi bir fikir gibi görünse de, böyle bir yapılandırma, yanlışlıkla kilitlenen hesapların kilidini açmak için yardım masasının aldığı çağrıların sayısını büyük olasılıkla artıracaktır. Kullanıcılar, bir kilidin yerinde kaldığı sürenin uzunluğunun farkında olmalıdır, böylece yalnızca bilgisayarlarına yeniden erişim sağlamak için son derece acil bir ihtiyaçları varsa yardım masasını aramaları gerektiğini anlarlar. Bu ayar için önerilen durum: 15 veya daha fazla dakika.

**Not:** Parola İlkesi ayarları (bölüm 1.1) ve Hesap Kilitleme İlkesi ayarları (bölüm 1.2), varsayılan davranış olarak etki alanı kullanıcı hesaplarında global olarak geçerli olmak için Varsayılan Etki Alanı İlkesi GPO'su aracılığıyla uygulanmalıdır. Bu ayarlar başka bir GPO'da yapılandırılırsa, yalnızca GPO'yu alan bilgisayarlardaki yerel kullanıcı hesaplarını etkiler. Ancak, belirli etki alanı kullanıcıları ve/veya grupları için varsayılan parola ilkesine ve hesap kilitleme ilkesi kurallarına özel istisnalar, Grup İlkesinden tamamen ayrı olan ve en kolay şekilde Active Directory Yönetim Merkezi kullanılarak yapılandırılan Parola Ayarları Nesneleri (PSO'lar) kullanılarak tanımlanabilir.

**Gerekçe:**

Bir saldırgan Hesap kilitleme eşiğini kötüye kullanırsa ve tekrar tekrar belirli bir hesapla oturum açmaya çalışırsa bir hizmet reddi (DoS) koşulu oluşturulabilir. Hesap kilitleme eşiği ayarını yapılandırdıktan sonra, belirtilen sayıda başarısız denemeden sonra hesap kilitlenecektir. Hesap kilitleme süresi ayarını 0 olarak yapılandırırsanız, bir yönetici manuel olarak kilidi açana kadar hesap kilitli kalır.

**Etki:**

Bu ilke ayarını hiçbir zaman otomatik olarak bir hesabın kilidini açmayacak şekilde yapılandırmak iyi bir fikir gibi görünse de, böyle bir yapılandırma, kuruluşunuzun yardım masasının yanlışlıkla kilitlenen hesapların kilidini açmak için aldığı isteklerin sayısını artırabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu 15 veya daha fazla dakikaya ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Hesap İlkeleri\Hesap Kilitleme İlkesi\Hesap kilitleme süresi*

**1.2.2 (L1) 'Hesap kilitleme eşiği' seçeneği '5 veya daha az geçersiz oturum açma girişimi ancak 0 değil' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, hesap kilitlenmeden önce başarısız oturum açma girişimlerinin sayısını belirler. Bu politikayı 0'a ayarlamak, karşılaştırmaya uymaz, çünkü bunu yapmak hesap kilitleme eşiğini devre dışı bırakır. Bu ayar için önerilen durum şudur: 5 veya daha az geçersiz oturum açma girişimi(ler), ancak 0 değil.

**Not:** Parola İlkesi ayarları (bölüm 1.1) ve Hesap Kilitleme İlkesi ayarları (bölüm 1.2), varsayılan davranış olarak etki alanı kullanıcı hesaplarında global olarak geçerli olmak için Varsayılan Etki Alanı İlkesi GPO'su aracılığıyla uygulanmalıdır. Bu ayarlar başka bir GPO'da yapılandırılırsa, yalnızca GPO'yu alan bilgisayarlardaki yerel kullanıcı hesaplarını etkiler. Ancak, belirli etki alanı kullanıcıları ve/veya grupları için varsayılan parola ilkesine ve hesap kilitleme ilkesi kurallarına özel istisnalar, Grup İlkesinden tamamen ayrı olan ve en kolay şekilde Active Directory Yönetim Merkezi kullanılarak yapılandırılan Parola Ayarları Nesneleri (PSO'lar) kullanılarak tanımlanabilir.

**Gerekçe:**

Bir hesap kilitleme eşiği belirlemek, çevrimiçi parola kaba kuvvet saldırısının başarılı olma olasılığını azaltır. Hesap kilitleme eşiğinin çok düşük ayarlanması, yanlışlıkla artan kilitlenme ve/veya kötü niyetli bir aktörün hesapları kasten kilitleme riskini ortaya çıkarır.

**Etki:**

Bu ilke ayarı etkinleştirilirse, kilitlenmiş bir hesap, bir yönetici tarafından sıfırlanana veya hesap kilitleme süresi sona erene kadar kullanılamaz. Bu ayar, ek yardım masası çağrıları oluşturabilir. Bu ayarı uygularsanız, bir saldırgan birden çok kullanıcı için kasıtlı olarak başarısız oturum açmalar oluşturarak hizmet reddi durumuna neden olabilir, bu nedenle Hesap Kilitleme Süresi'ni de nispeten düşük bir değere yapılandırmanız gerekir. Hesap Kilitleme Eşiği'ni 0 olarak yapılandırırsanız, sağlam bir denetim mekanizması mevcut değilse, bir saldırganın kaba kuvvet parola saldırısıyla parolaları keşfetme girişiminin algılanmama olasılığı vardır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu 5 veya daha az geçersiz oturum açma girişimine/denemesine ayarlayın, ancak 0 değil:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Hesap İlkeleri\Hesap Kilitleme İlkesi\Hesap kilitleme eşiği*

**1.2.3 (L1) 'Hesap kilitleme sayacını şu süreden sonra sıfırla' seçeneği '15 dakika veya daha fazla' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Hesap kilitleme eşiğinin sıfırlanmasından önce geçecek süreyi belirler. Bu ilke ayarının varsayılan değeri Tanımlanmadı'dır. Hesap kilitleme eşiği tanımlanmışsa, bu sıfırlama süresi Hesap kilitleme süresi ayarının değerinden küçük veya ona eşit olmalıdır. Bu ilke ayarını varsayılan değerinde bırakırsanız veya değeri çok uzun bir aralıkta yapılandırırsanız, ortamınız bir DoS saldırısına karşı savunmasız olabilir. Saldırgan, kuruluştaki tüm kullanıcılar üzerinde hesaplarını kilitleyecek bir dizi başarısız oturum açma girişiminde bulunabilir. Hesap kilitlemeyi sıfırlamak için herhangi bir politika belirlenmediyse, bu yöneticiler için manuel bir görev olacaktır. Tersine, bu ilke ayarı için makul bir zaman değeri yapılandırılırsa, kullanıcılar tüm hesapların kilidi otomatik olarak açılana kadar belirli bir süre boyunca kilitlenir. Bu ayar için önerilen durum: 15 veya daha fazla dakika.

**Not:** Parola İlkesi ayarları (bölüm 1.1) ve Hesap Kilitleme İlkesi ayarları (bölüm 1.2), varsayılan davranış olarak etki alanı kullanıcı hesaplarında global olarak geçerli olmak için Varsayılan Etki Alanı İlkesi GPO'su aracılığıyla uygulanmalıdır. Bu ayarlar başka bir GPO'da yapılandırılırsa, yalnızca GPO'yu alan bilgisayarlardaki yerel kullanıcı hesaplarını etkiler. Ancak, belirli etki alanı kullanıcıları ve/veya grupları için varsayılan parola ilkesine ve hesap kilitleme ilkesi kurallarına özel istisnalar, Grup İlkesinden tamamen ayrı olan ve en kolay şekilde Active Directory Yönetim Merkezi kullanılarak yapılandırılan Parola Ayarları Nesneleri (PSO'lar) kullanılarak tanımlanabilir.

**Gerekçe:**

Kullanıcılar, parolalarını birden çok kez yanlış yazarlarsa, yanlışlıkla kendilerini hesaplarından kilitleyebilirler. Bu tür yanlışlıkla kilitlenme olasılığını azaltmak için, Hesap kilitleme sayacını sıfırla ayarı, başarısız oturum açma girişimlerini izleyen ve kilitlemeleri tetikleyen sayacın sıfırlanmasından önce geçmesi gereken dakika sayısını belirler.

**Etki:**

Bu ilke ayarını yapılandırmazsanız veya değer çok uzun bir aralığa yapılandırılırsa bir DoS saldırısı meydana gelebilir. Saldırgan, önceki paragraflarda açıklandığı gibi, kötü niyetli olarak her kullanıcının hesabında defalarca oturum açmaya ve hesaplarını kilitlemeye çalışabilir. Ayarladıktan sonra Hesap kilitleme sayacını sıfırla'yı yapılandırmazsanız, yöneticilerin tüm hesapların kilidini manuel olarak açması gerekir. Bu ilke ayarını makul bir değere yapılandırırsanız, kullanıcılar belirli bir süre için kilitlenir ve ardından hesaplarının kilidi otomatik olarak açılır. Kullanıcıları, oturum açamamaları konusunda yardım masasını aramadan önce, kilitleme zamanlayıcısının süresinin dolmasını bekleyecekleri şekilde, bu ilke ayarı için kullanılan değerler konusunda bilgilendirdiğinizden emin olun.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu 15 veya daha fazla dakikaya ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Hesap İlkeleri\Hesap Kilitleme İlkesi\Sonra hesap kilitleme sayacını sıfırla*

**2 Yerel İlkeler**

**2.1 Denetim İlkeleri**

**2.2 Kullanıcı Hakları Atamaları**

**2.2.1 (L1) 'Kimlik Bilgileri Yöneticisi’ne güvenilir kullanıcı olarak eriş' seçeneği 'Hiç Kimse' olarak ayarlanmalıdır.**

**Açıklama:**

Bu güvenlik ayarı, Yedekleme ve Geri Yükleme sırasında Kimlik Bilgileri Yöneticisi tarafından kullanılır. Yalnızca Winlogon'a atandığından hiçbir hesap bu kullanıcı hakkına sahip olmamalıdır. Bu kullanıcı hakkı başka varlıklara atanırsa, kullanıcıların kayıtlı kimlik bilgileri tehlikeye girebilir. Bu ayar için önerilen durum: Hiç Kimse.

**Gerekçe:**

Bir hesaba bu hak verilirse, hesabın kullanıcısı, Kimlik Bilgisi Yöneticisi'ni çağıran ve başka bir kullanıcının kimlik bilgilerini döndüren bir uygulama oluşturabilir.

**Etki:**

Yok - bu varsayılan davranıştır. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Hiç Kimse olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Güvenilir arayan olarak Kimlik Bilgileri Yöneticisine Erişim*

**2.2.2 (L1) 'Bu bilgisayara ağdan eriş' seçeneği 'Yöneticiler, Uzak Masaüstü Kullanıcıları' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, ağdaki diğer kullanıcıların bilgisayara bağlanmasına izin verir ve Sunucu İleti Bloğu (SMB) tabanlı protokoller, NetBIOS, Ortak İnternet Dosya Sistemi (CIFS) ve Bileşen Nesne Modeli Plus'ı içeren çeşitli ağ protokolleri için gereklidir. (COM+). Bu ayar için önerilen durum: Yöneticiler, Uzak Masaüstü Kullanıcıları.

**Gerekçe:**

Bilgisayarlarından ağa bağlanabilen kullanıcılar, izinleri olan hedef bilgisayarlardaki kaynaklara erişebilir. Örneğin, kullanıcıların paylaşılan yazıcılara ve klasörlere bağlanması için Bu bilgisayara ağdan eriş kullanıcı hakkı gereklidir. Bu kullanıcı hakkı Herkes grubuna atanırsa, bu paylaşılan klasörlerdeki dosyaları herkes okuyabilir. Ancak, Windows Server 2003'teki varsayılan paylaşım ve NTFS izinleri Herkes grubunu içermediğinden, Service Pack 1 (SP1) içeren yeni Windows Server 2003 yüklemeleri için bu durum olası değildir. Bu güvenlik açığı, Windows NT 4.0 veya Windows 2000'den yükselttiğiniz bilgisayarlar için daha yüksek bir risk düzeyine sahip olabilir, çünkü bu işletim sistemlerine yönelik varsayılan izinler, Windows Server 2003'teki varsayılan izinler kadar kısıtlayıcı değildir.

**Etki:**

Tüm kullanıcılar için Etki Alanı Denetleyicileri üzerindeki Bu bilgisayara eriş kullanıcı hakkını ağdan kaldırırsanız, hiç kimse etki alanında oturum açamaz veya ağ kaynaklarını kullanamaz. Üye Sunucularda bu kullanıcı hakkını kaldırırsanız, kullanıcılar ağ üzerinden bu sunuculara bağlanamazlar. IPsec bağlantılarının başarılı anlaşması, başlatan makinenin bu hakka sahip olmasını gerektirir, bu nedenle IPsec kullanılıyorsa, Authenticated Users grubuna atanması önerilir. ASP.NET veya Internet Information Services (IIS) gibi isteğe bağlı bileşenler yüklediyseniz, bu kullanıcı hakkını bu bileşenlerin gerektirdiği ek hesaplara atamanız gerekebilir. Yetkili kullanıcılara, ağa erişmeleri gereken bilgisayarlar için bu kullanıcı hakkının atandığını doğrulamak önemlidir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Yöneticiler, Uzak Masaüstü Kullanıcıları olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Bu bilgisayara ağdan erişin*

**2.2.3 (L1) 'İşletim sisteminin bir parçası olarak görün' seçeneği 'Hiç Kimse' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir işlemin herhangi bir kullanıcının kimliğini üstlenmesine ve böylece kullanıcının erişim yetkisine sahip olduğu kaynaklara erişmesine olanak tanır. Bu ayar için önerilen durum: Hiç Kimse.

**Not:** Bu kullanıcı hakkı, denetim amacıyla "hassas bir ayrıcalık" olarak kabul edilir. Gerekçe: İşletim sistemi kullanıcı hakkının bir parçası olarak Kanun son derece güçlüdür. Bu kullanıcı hakkına sahip olan herkes bilgisayarın kontrolünü tamamen ele geçirebilir ve etkinliklerinin kanıtlarını silebilir.

**Etki:**

Çok az veya hiç etkisi olmamalıdır, çünkü İşletim sistemi kullanıcı hakkının bir parçası olarak Yasası'na, dolaylı olarak bu hakka sahip olan Yerel Sistem hesabı dışındaki herhangi bir hesap nadiren ihtiyaç duyar.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Hiç Kimse olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\İşletim sisteminin bir parçası olarak hareket edin*

**2.2.4 (L1) 'İşlem için bellek kotalarını ayarla' seçeneği 'Yöneticiler, Yerel Servis, Ağ Servisi' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcının bir işlem için kullanılabilen maksimum bellek miktarını ayarlamasına olanak tanır. Bellek kotalarını ayarlama yeteneği, sistem ayarı için kullanışlıdır, ancak kötüye kullanılabilir. Yanlış ellerde, bir hizmet reddi (DoS) saldırısı başlatmak için kullanılabilir. Bu ayar için önerilen durum: Yöneticiler, YEREL HİZMET, AĞ HİZMETİ.

**Gerekçe:**

Bir işlem için bellek kotalarını ayarla kullanıcı hakkı olan bir kullanıcı, herhangi bir işlem için kullanılabilen bellek miktarını azaltabilir, bu da iş açısından kritik ağ uygulamalarının yavaşlamasına veya başarısız olmasına neden olabilir. Yanlış ellerde, bu ayrıcalık bir hizmet reddi (DoS) saldırısı başlatmak için kullanılabilir.

**Etki:**

Kullanıcıları sınırlı ayrıcalıklara sahip rollerle sınırlamayan kuruluşlar, bu karşı önlemi uygulamakta zorlanacaklardır. Ayrıca, ASP.NET veya IIS gibi isteğe bağlı bileşenler yüklediyseniz, bu bileşenlerin gerektirdiği ek hesaplara bir işlem kullanıcı hakkı için Bellek kotalarını ayarla'yı atamanız gerekebilir. Aksi takdirde, bu önlemin çoğu bilgisayarda hiçbir etkisi olmayacaktır. Bu kullanıcı hakkı bir kullanıcı hesabı için gerekliyse, bir etki alanı hesabı yerine yerel bir bilgisayar hesabına atanabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Yöneticiler, YEREL HİZMET, AĞ HİZMETİ olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Bir işlem için bellek kotalarını ayarlayın*

**2.2.5 (L1) 'Yerel olarak oturum açmaya izin ver' seçeneği 'Yöneticiler, Kullanıcılar' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, hangi kullanıcıların ortamınızdaki bilgisayarlarda etkileşimli olarak oturum açabileceğini belirler. İstemci bilgisayar klavyesinde CTRL+ALT+DEL tuş dizisine basılarak başlatılan oturum açma işlemleri bu kullanıcı hakkını gerektirir. Terminal Hizmetleri / Uzak Masaüstü Hizmetleri veya IIS üzerinden oturum açmaya çalışan kullanıcılar da bu kullanıcı hakkına ihtiyaç duyar. Bu ayar için önerilen durum: Yöneticiler, Kullanıcılar.

**Not:** Konuk hesabına da varsayılan olarak bu kullanıcı hakkı atanmıştır. Bu hesap varsayılan olarak devre dışı bırakılmış olsa da, bu ayarı Grup İlkesi aracılığıyla yapılandırmanız önerilir. Ancak, bu kullanıcı hakkı genellikle Yöneticiler ve Kullanıcılar gruplarıyla sınırlandırılmalıdır. Kuruluşunuz bu yeteneğe sahip olmasını gerektiriyorsa, bu kullanıcı hakkını Backup Operators grubuna atayın. Gerekçe: Yerel olarak oturum açmaya izin ver kullanıcı hakkına sahip herhangi bir hesap, bilgisayarın konsolunda oturum açabilir. Bu kullanıcı hakkını, bilgisayarın konsolunda oturum açması gereken meşru kullanıcılarla kısıtlamazsanız, yetkisiz kullanıcılar ayrıcalıklarını yükseltmek için kötü amaçlı yazılımları indirebilir ve çalıştırabilir.

**Etki:**

Bu varsayılan grupları kaldırırsanız, ortamınızda belirli yönetim rollerine atanan kullanıcıların yeteneklerini sınırlayabilirsiniz. Yerel olarak oturum açmaya izin ver kullanıcı hakkı üzerinde yaptığınız değişikliklerden temsilci etkinliklerin olumsuz etkilenmeyeceğini onaylamanız gerekir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Yöneticiler, Kullanıcılar olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Yerel olarak oturum açmaya izin ver*

**2.2.6 (L1) 'Uzak Masaüstü Hizmetleri ile oturum açmaya izin ver' seçeneği 'Yöneticiler, Uzak Masaüstü Kullanıcıları' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, hangi kullanıcıların veya grupların Uzak Masaüstü Hizmetleri istemcisi olarak oturum açma hakkına sahip olduğunu belirler. Kuruluşunuz, yardım masası stratejisinin bir parçası olarak Uzaktan Yardım kullanıyorsa, bir grup oluşturun ve bu kullanıcıyı doğrudan Grup İlkesi aracılığıyla atayın. Kuruluşunuzdaki yardım masası Uzaktan Yardım kullanmıyorsa, bu kullanıcı hakkını yalnızca Yöneticiler grubuna atayın veya hiçbir kullanıcı hesabının Uzak Masaüstü Kullanıcıları grubunun parçası olmadığından emin olmak için Kısıtlı Gruplar özelliğini kullanın. İstenmeyen kullanıcıların Uzaktan Yardım özelliği aracılığıyla ağınızdaki bilgisayarlara erişmesini önlemek için bu kullanıcı hakkını Administrators grubuyla ve muhtemelen Remote Desktop Users grubuyla sınırlayın. Bu ayar için önerilen durum: Yöneticiler, Uzak Masaüstü Kullanıcıları.

**Not:** Yukarıdaki liste, bir beyaz liste olarak ele alınmalıdır; bu, bu tavsiyenin değerlendirilmesi için yukarıdaki ilkelerin mevcut olması gerekmediği anlamına gelir. Not #2: Windows 7'den önceki tüm Windows sürümlerinde, Uzak Masaüstü Hizmetleri Terminal Hizmetleri olarak biliniyordu, bu nedenle daha eski bir işletim sistemiyle karşılaştırırken eski terimi değiştirmelisiniz.

**Gerekçe:**

Uzak Masaüstü Hizmetleri aracılığıyla oturum açmaya izin ver kullanıcı hakkına sahip herhangi bir hesap, bilgisayarın uzak konsolunda oturum açabilir. Bu kullanıcı hakkını bilgisayarın konsolunda oturum açması gereken meşru kullanıcılarla kısıtlamazsanız, yetkisiz kullanıcılar ayrıcalıklarını yükseltmek için kötü amaçlı yazılımları indirebilir ve çalıştırabilir.

**Etki:**

Uzak Masaüstü Hizmetleri aracılığıyla oturum açmaya izin ver kullanıcı hakkının diğer gruplardan kaldırılması veya bu varsayılan gruplardaki üyelik değişiklikleri, ortamınızda belirli yönetim rollerini gerçekleştiren kullanıcıların yeteneklerini sınırlayabilir. Temsil edilen faaliyetlerin olumsuz etkilenmeyeceğini onaylamanız gerekir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Yöneticiler, Uzak Masaüstü Kullanıcıları olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Uzak Masaüstü Hizmetleri aracılığıyla oturum açmaya izin ver*

**2.2.7 (L1) 'Dosyaları ve dizinleri yedekle' seçeneği 'Yöneticiler' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların sistemi yedeklemek için dosya ve dizin izinlerini atlatmasına olanak tanır. Bu kullanıcı hakkı, yalnızca bir uygulama (NTBACKUP gibi) NTFS dosya sistemi yedekleme uygulaması programlama arabirimi (API) aracılığıyla bir dosyaya veya dizine erişmeye çalıştığında etkinleştirilir. Aksi takdirde, atanan dosya ve dizin izinleri geçerlidir. Bu ayar için önerilen durum: Yöneticiler.

**Not:** Bu kullanıcı hakkı, denetim amacıyla "hassas bir ayrıcalık" olarak kabul edilir. Gerekçe: Bir bilgisayardan veri yedekleyebilen kullanıcılar, yedekleme ortamını yönetici ayrıcalıklarına sahip oldukları etki alanı olmayan bir bilgisayara alabilir ve verileri geri yükleyebilir. Dosyaların sahipliğini alabilir ve yedekleme kümesinde bulunan şifrelenmemiş verileri görüntüleyebilirler.

**Etki:**

Dosyaları ve dizinleri yedekle kullanıcı hakkına sahip grupların üyeliğindeki değişiklikler, ortamınızda belirli yönetim rollerine atanan kullanıcıların yeteneklerini sınırlayabilir. Yetkili yedekleme yöneticilerinin hala yedekleme işlemlerini gerçekleştirebildiğini onaylamanız gerekir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Yöneticiler olarak ayarlayın.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Dosyaları ve dizinleri yedekleyin*

**2.2.8 (L1) 'Sistem saatini değiştir' seçeneği 'Yöneticiler, Yerel Servis' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, ortamınızdaki bilgisayarların dahili saatinde hangi kullanıcıların ve grupların saat ve tarihi değiştirebileceğini belirler. Bu kullanıcı hakkının atandığı kullanıcılar, olay günlüklerinin görünümünü etkileyebilir. Bir bilgisayarın zaman ayarı değiştirildiğinde, günlüğe kaydedilen olaylar, olayların meydana geldiği gerçek zamanı değil, yeni zamanı yansıtır. Bu ayar için önerilen durum: Yöneticiler, YEREL HİZMET.

**Not:**

Yerel bilgisayar ve ortamınızdaki Etki Alanı Denetleyicileri arasındaki zaman farklılıkları, Kerberos kimlik doğrulama protokolü için sorunlara neden olabilir; bu, kullanıcıların etki alanında oturum açmasını veya etki alanı kaynaklarına erişim izni almasını engelledikten sonra olanaksız hale getirebilir. oturum açıldı. Ayrıca, sistem saati Etki Alanı Denetleyicileri ile eşitlenmemişse, istemci bilgisayarlara Grup İlkesi uygulandığında sorunlar ortaya çıkacaktır.

**Gerekçe:**

Bir bilgisayarda saati değiştirebilen kullanıcılar çeşitli sorunlara neden olabilir. Örneğin, olay günlüğü girişlerindeki zaman damgaları hatalı yapılabilir, oluşturulan veya değiştirilen dosya ve klasörlerdeki zaman damgaları yanlış olabilir ve bir etki alanına ait bilgisayarlar kendilerinin veya oturum açmaya çalışan kullanıcıların kimliğini doğrulayamayabilir. onlardan etki alanına. Ayrıca, Kerberos kimlik doğrulama protokolü, istekte bulunan ve kimlik doğrulayıcının saatlerinin yönetici tarafından tanımlanan bir çarpıklık süresi içinde eşitlenmesini gerektirdiğinden, bilgisayarın saatini değiştiren bir saldırgan, o bilgisayarın Kerberos biletleri alamamasına veya vermemesine neden olabilir. Bu tür olaylardan kaynaklanan risk, çoğu Etki Alanı Denetleyicisi, Üye Sunucusu ve son kullanıcı bilgisayarında azaltılır, çünkü Windows Saati hizmeti Etki Alanı Denetleyicileri ile zamanı aşağıdaki şekillerde otomatik olarak eşitler:

* Tüm istemci masaüstü bilgisayarlar ve Üye Sunucular, gelen zaman ortağı olarak kimlik doğrulaması yapan Etki Alanı Denetleyicisini kullanır.
* Bir etki alanındaki tüm Etki Alanı Denetleyicileri, gelen zaman ortağı olarak Birincil Etki Alanı Denetleyicisi (PDC) Öykünücüsü işlem yöneticisini aday gösterir.
* Tüm PDC Öykünücüsü işlem yöneticileri, gelen zaman ortağı seçiminde etki alanlarının hiyerarşisini takip eder.
* Etki alanının kökündeki PDC Öykünücüsü işlem yöneticisi, kuruluş için yetkilidir. Bu nedenle, bu bilgisayarı güvenilir bir harici zaman sunucusuyla eşitlenecek şekilde yapılandırmanız önerilir.

Saldırgan sistem saatini değiştirip ardından Windows Saati hizmetini durdurabilir veya doğru olmayan bir saat sunucusuyla eşitlenecek şekilde yeniden yapılandırabilirse, bu güvenlik açığı çok daha ciddi hale gelir.

**Etki:**

Etkisi olmamalıdır, çünkü çoğu kuruluş için zaman senkronizasyonu, etki alanına ait tüm bilgisayarlar için tam otomatik olmalıdır. Etki alanına ait olmayan bilgisayarlar, harici bir kaynakla senkronize olacak şekilde yapılandırılmalıdır.

**Denetim:** Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme :**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Yöneticiler, YEREL HİZMET olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Sistem saatini değiştirin*

**2.2.9 (L1) 'Saat dilimini değiştir' seçeneği 'Yöneticiler, Yerel Servis, Kullanıcılar' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, hangi kullanıcıların bilgisayarın saat dilimini değiştirebileceğini belirler. Bu yetenek bilgisayar için büyük bir tehlike oluşturmaz ve mobil çalışanlar için faydalı olabilir. Bu ayar için önerilen durum: Yöneticiler, YEREL HİZMET, Kullanıcılar.

**Gerekçe:**

Sistem saati etkilenmediği için saat diliminin değiştirilmesi çok az güvenlik açığı anlamına gelir. Bu ayar, kullanıcıların yalnızca farklı saat dilimlerindeki Etki Alanı Denetleyicileri ile senkronize edilirken tercih ettikleri saat dilimini görüntülemelerini sağlar.

**Etki:**

Yok - bu varsayılan davranıştır. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Yöneticiler, YEREL HİZMET, Kullanıcılar olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Saat dilimini değiştir*

**2.2.10 (L1) 'Disk belleği dosyası oluştur' seçeneği 'Yöneticiler' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların sayfa dosyasının boyutunu değiştirmesine olanak tanır. Bir saldırgan, sayfa dosyasını çok büyük veya çok küçük yaparak, güvenliği ihlal edilmiş bir bilgisayarın performansını kolayca etkileyebilir. Bu ayar için önerilen durum: Yöneticiler.

**Gerekçe:**

Sayfa dosyasının boyutunu değiştirebilen kullanıcılar, sayfayı çok küçültebilir veya dosyayı çok parçalı bir depolama birimine taşıyabilir ve bu da bilgisayar performansının düşmesine neden olabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Yöneticiler olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Bir sayfa dosyası oluştur*

**2.2.11 (L1) 'Belirteç nesnesi oluştur' seçeneği 'Hiç Kimse' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir işlemin hassas verilere erişim için yükseltilmiş haklar sağlayabilecek bir erişim belirteci oluşturmasına olanak tanır. Bu ayar için önerilen durum: Hiç Kimse. Not: Bu kullanıcı hakkı, denetim amacıyla "hassas bir ayrıcalık" olarak kabul edilir.

**Gerekçe:**

Bu kullanıcı hakkı verilen bir kullanıcı hesabı, sistem üzerinde tam kontrole sahiptir ve sistemin güvenliğinin ihlal edilmesine neden olabilir. Bu hakkı herhangi bir kullanıcı hesabına atamamanız şiddetle tavsiye edilir. İşletim sistemi, kullanıcının ayrıcalıklarının düzeyini belirlemek için bir kullanıcının erişim belirtecini inceler. Erişim belirteçleri, kullanıcılar yerel bilgisayarda oturum açtığında veya bir ağ üzerinden uzak bir bilgisayara bağlandığında oluşturulur. Bir ayrıcalığı iptal ettiğinizde, değişiklik hemen kaydedilir, ancak değişiklik, kullanıcının bir sonraki oturum açmasına veya bağlanmasına kadar kullanıcının erişim belirtecine yansıtılmaz. Belirteç oluşturma veya değiştirme yeteneğine sahip kullanıcılar, şu anda oturum açmış herhangi bir hesabın erişim düzeyini değiştirebilir. Kendi ayrıcalıklarını yükseltebilir veya bir DoS koşulu oluşturabilirler.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Hiç Kimse olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Bir belirteç nesnesi oluştur*

**2.2.12 (L1) 'Genel nesneler oluştur' seçeneği 'Yöneticiler, Yerel Servis, Ağ Servisi, Servis' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların tüm oturumlarda kullanılabilen genel nesneler oluşturup oluşturamayacağını belirler. Kullanıcılar, bu kullanıcı hakkına sahip değillerse, yine de kendi oturumlarına özgü nesneler oluşturabilirler. Genel nesneler oluşturabilen kullanıcılar, diğer kullanıcıların oturumları altında çalışan işlemleri etkileyebilir. Bu yetenek, uygulama hatası veya veri bozulması gibi çeşitli sorunlara yol açabilir. Bu ayar için önerilen durum: Yöneticiler, YEREL HİZMET, AĞ HİZMETİ, HİZMET.

**Gerekçe:**

Genel nesneler oluşturabilen kullanıcılar, diğer kullanıcı veya sistem hesapları altında çalışan Windows hizmetlerini ve işlemlerini etkileyebilir. Bu yetenek, uygulama hatası, veri bozulması ve ayrıcalık yükselmesi gibi çeşitli sorunlara yol açabilir.

**Etki:**

Yok - bu varsayılan davranıştır. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Yöneticiler, YEREL HİZMET, AĞ HİZMETİ, HİZMET olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Genel nesneler oluştur*

**2.2.13 (L1) 'Kalıcı paylaşılan nesneler oluştur' seçeneği 'Hiç Kimse' olarak ayarlanmalıdır.**

**Açıklama:**

Bu kullanıcı hakkı, nesne ad alanını genişleten çekirdek modu bileşenleri için yararlıdır. Ancak, çekirdek modunda çalışan bileşenler bu kullanıcı hakkına doğal olarak sahiptir. Bu nedenle, genellikle bu kullanıcı hakkının özel olarak atanması gerekli değildir. Bu ayar için önerilen durum: Hiç Kimse.

**Gerekçe:**

Kalıcı paylaşılan nesneler oluştur kullanıcı hakkına sahip kullanıcılar, yeni paylaşılan nesneler oluşturabilir ve hassas verileri ağa gösterebilir.

**Etki:** Yok - bu varsayılan davranıştır.

**Denetim:** Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:** GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Hiç Kimse olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Kalıcı paylaşılan nesneler oluştur*

**2.2.15 (L1) 'Programlarda hata ayıklama' seçeneği 'Yöneticiler' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, hangi kullanıcı hesaplarının herhangi bir işleme veya hassas ve kritik işletim sistemi bileşenlerine tam erişim sağlayan çekirdeğe hata ayıklayıcı ekleme hakkına sahip olacağını belirler. Kendi uygulamalarında hata ayıklayan geliştiricilere bu kullanıcı hakkının atanması gerekmez; ancak, yeni sistem bileşenlerinde hata ayıklayan geliştiricilerin buna ihtiyacı olacaktır. Bu ayar için önerilen durum: Yöneticiler.

**Not:** Bu kullanıcı hakkı, denetim amacıyla "hassas bir ayrıcalık" olarak kabul edilir. Gerekçe: Hata ayıklama programları kullanıcı hakkından, sistem belleğinden hassas bilgisayar bilgilerini yakalamak veya çekirdek veya uygulama yapılarına erişmek ve bunları değiştirmek için kullanılabilir. Bazı saldırı araçları, bu kullanıcı hakkından karma parolaları ve diğer özel güvenlik bilgilerini çıkarmak veya rootkit kodu eklemek için yararlanır. Varsayılan olarak, Hata Ayıklama programları kullanıcı hakkı yalnızca yöneticilere atanır ve bu, bu güvenlik açığından kaynaklanan riski azaltmaya yardımcı olur.

**Etki:**

Bu kullanıcı hakkını iptal ederseniz, hiç kimse programlarda hata ayıklayamaz. Ancak, tipik koşullar, üretim bilgisayarlarında nadiren bu yeteneği gerektirir. Bir üretim sunucusunda bir uygulamanın hatalarının ayıklanmasını gerektiren bir sorun ortaya çıkarsa, sunucuyu geçici olarak farklı bir OU'ya taşıyabilir ve Hata Ayıklama programları kullanıcı hakkını o OU için ayrı bir Grup İlkesi'ne atayabilirsiniz. Küme hizmeti için kullanılan hizmet hesabı, Hata Ayıklama programları kullanıcı hakkına ihtiyaç duyar; yoksa, Windows Kümeleme başarısız olur. Süreçleri yönetmek için kullanılan araçlar, araçları çalıştıran kişiye ait olmayan süreçleri etkileyemez. Örneğin, Windows Server 2003 Kaynak Seti aracı Kill.exe, yöneticilerin başlatmadıkları işlemleri sonlandırmaları için bu kullanıcı hakkını gerektirir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Yöneticiler olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Hata Ayıklama programları*

**2.2.16 (L1) 'Bu bilgisayara ağdan erişimi reddet' seçeneği 'Konuklar, Yerel Hesaplar' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların ağ üzerinden bir bilgisayara bağlanmasını yasaklar; bu, kullanıcıların verilere uzaktan erişmesine ve potansiyel olarak bunları değiştirmesine olanak tanır. Yüksek güvenlikli ortamlarda, uzak kullanıcıların bir bilgisayardaki verilere erişmesine gerek kalmamalıdır. Bunun yerine, dosya paylaşımı ağ sunucuları kullanılarak gerçekleştirilmelidir. Bir hesap her iki ilkeye de tabiyse, bu kullanıcı hakkı Bu bilgisayara ağdan eriş kullanıcı hakkının yerini alır. Bu ayar için önerilen durum şunları içerir: Misafirler, Yerel hesap.

**Dikkat:** Yukarıda açıklandığı gibi bağımsız (etki alanına katılmamış) bir iş istasyonunun yapılandırılması, iş istasyonunun uzaktan yönetilememesiyle sonuçlanabilir.

**Not:** Güvenlik tanımlayıcısı Yerel hesabı, MSKB 2871997 yüklenmediği sürece Windows 7 ve Windows 8.0'da kullanılamaz. Gerekçe: Bilgisayarda ağ üzerinden oturum açabilen kullanıcılar, hesap adları, grup adları ve paylaşılan kaynakların listelerini sıralayabilir. Paylaşılan klasörlere ve dosyalara erişim izni olan kullanıcılar, ağ üzerinden bağlanabilir ve muhtemelen verileri görüntüleyebilir veya değiştirebilir.

**Etki:**

Diğer gruplar için bu bilgisayara ağ kullanıcı hakkından erişimi engelle seçeneğini yapılandırırsanız, ortamınızda belirli yönetim rollerine atanan kullanıcıların yeteneklerini sınırlayabilirsiniz. Temsil edilen görevlerin olumsuz etkilenmeyeceğini doğrulamanız gerekir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için Misafirler, Yerel hesabı içerecek şekilde aşağıdaki UI yolunu ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Ağdan bu bilgisayara erişimi engelle*

**2.2.17 (L1) 'Toplu iş olarak oturum açmayı reddet' seçeneği 'Konuklar' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, hangi hesapların toplu iş olarak bilgisayarda oturum açamayacağını belirler. Toplu iş, bir toplu iş (.bat) dosyası değil, bir toplu iş kuyruğu tesisidir. İşleri zamanlamak için Görev Zamanlayıcı'yı kullanan hesapların bu kullanıcı hakkına ihtiyacı vardır. Bu kullanıcı hakkı, hesapların aşırı sistem kaynakları tüketen işleri planlamasına izin vermek için kullanılabilecek toplu iş olarak oturum aç kullanıcı hakkının yerini alır. Böyle bir olay bir DoS durumuna neden olabilir. Bu kullanıcı hakkının önerilen hesaplara atanamaması bir güvenlik riski oluşturabilir. Bu ayar için önerilen durum şunları içerir: Misafirler.

**Gerekçe:**

Toplu iş olarak oturum açma kullanıcı hakkına sahip hesaplar, aşırı bilgisayar kaynaklarını tüketebilecek ve bir DoS durumuna neden olabilecek işleri zamanlamak için kullanılabilir.

**Etki:**

Oturum açmayı bir toplu iş kullanıcı hakkı olarak diğer hesaplara atarsanız, belirli yönetim rollerine atanan kullanıcıların gerekli iş etkinliklerini gerçekleştirmelerini engelleyebilirsiniz. Temsil edilen görevlerin olumsuz etkilenmeyeceğini onaylamanız gerekir. Örneğin, bu kullanıcı hakkını IWAM\_(BilgisayarAdı) hesabına atarsanız, MSM Yönetim Noktası başarısız olur. Windows Server 2003 çalıştıran yeni yüklenen bir bilgisayarda bu hesap, Misafirler grubuna ait değildir, ancak Windows 2000'den yükseltilmiş bir bilgisayarda bu hesap, Misafirler grubunun bir üyesidir. Bu nedenle, bir toplu iş kullanıcı hakkı olarak Oturum açmayı Reddet'i atadığınız herhangi bir gruba hangi hesapların ait olduğunu anlamanız önemlidir.

**Denetim:** Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için Misafirleri dahil etmek için aşağıdaki kullanıcı arayüzü yolunu ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Toplu iş olarak oturum açmayı reddet*

**2.2.18 (L1) 'Servis olarak oturum açmayı reddet' seçeneği 'Konuklar' olarak ayarlanmalıdır.**

**Açıklama:**

Bu güvenlik ayarı, hangi hizmet hesaplarının bir işlemi hizmet olarak kaydetmesinin engelleneceğini belirler. Bu kullanıcı hakkı, bir hesap her iki ilkeye de tabiyse, Hizmet olarak oturum aç kullanıcı hakkının yerini alır. Bu ayar için önerilen durum şunları içerir: Misafirler.

**Not:** Bu güvenlik ayarı Sistem, Yerel Hizmet veya Ağ Hizmeti hesapları için geçerli değildir.

**Gerekçe:**

Hizmet olarak oturum açabilen hesaplar, keylogger veya diğer kötü amaçlı yazılımlar gibi yeni yetkisiz hizmetleri yapılandırmak ve başlatmak için kullanılabilir. Belirtilen karşı önlemin yararı, yalnızca yönetici ayrıcalıklarına sahip kullanıcıların hizmetleri yükleyip yapılandırabilmesi ve bu erişim düzeyine zaten erişmiş bir saldırganın hizmeti Sistem hesabıyla çalışacak şekilde yapılandırabilmesi gerçeğiyle bir ölçüde azalır.

**Etki:**

Belirli hesaplara hizmet kullanıcı hakkı olarak oturum açmayı reddet seçeneğini atarsanız, hizmetler başlatılamayabilir ve bir DoS durumu ortaya çıkabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için Misafirleri dahil etmek için aşağıdaki kullanıcı arayüzü yolunu ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Hizmet olarak oturum açmayı reddet*

**2.2.19 (L1) 'Yerel olarak oturum açmayı reddet' seçeneği 'Konuklar' olarak ayarlanmalıdır.**

**Açıklama:**

Bu güvenlik ayarı, hangi kullanıcıların bilgisayarda oturum açmasının engelleneceğini belirler. Bu ilke ayarı, bir hesap her iki ilkeye de tabiyse, yerel olarak oturum açmaya izin ver ilke ayarının yerini alır. Bu ayar için önerilen durum şunları içerir: Misafirler.

**Önemli:**

Bu güvenlik ilkesini Herkes grubuna uygularsanız, hiç kimse yerel olarak oturum açamaz.

**Gerekçe:**

Yerel olarak oturum açabilen herhangi bir hesap, bilgisayarın konsolunda oturum açmak için kullanılabilir. Bu kullanıcı hakkı, bilgisayarın konsolunda oturum açması gereken meşru kullanıcılarla sınırlı değilse, yetkisiz kullanıcılar ayrıcalıklarını yükselten kötü amaçlı yazılımları indirebilir ve çalıştırabilir.

**Etki:**

Yerel olarak oturum açmayı reddet kullanıcı hakkını ek hesaplara atarsanız, ortamınızda belirli rollere atanan kullanıcıların yeteneklerini sınırlayabilirsiniz. Ancak, bu kullanıcı hakkı, IIS 6.0 çalıştıran bilgisayarlarda ASPNET hesabına açıkça atanmalıdır. Temsil edilen faaliyetlerin olumsuz etkilenmeyeceğini onaylamanız gerekir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için Misafirleri dahil etmek için aşağıdaki kullanıcı arayüzü yolunu ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Yerel olarak oturum açmayı reddet*

**2.2.20 (L1) 'Uzak Masaüstü Servisleri aracılığıyla oturum açmayı reddet' seçeneği 'Konuklar, Yerel hesaplar' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların Uzak Masaüstü istemcileri olarak oturum açıp açamayacağını belirler. Temel iş istasyonu bir etki alanı ortamına katıldıktan sonra, iş istasyonuna ağdan erişmek için yerel hesapları kullanmaya gerek yoktur. Etki alanı hesapları, yönetim ve son kullanıcı işlemleri için iş istasyonuna erişebilir. Bu kullanıcı hakkı, bir hesap her iki ilkeye de tabiyse, Uzak Masaüstü Hizmetleri aracılığıyla oturum açmaya izin ver kullanıcı hakkının yerini alır. Bu ayar için önerilen durum şunları içerir: Misafirler, Yerel hesap.

**Dikkat:** Yukarıda açıklandığı gibi bağımsız (etki alanına katılmamış) bir iş istasyonunun yapılandırılması, iş istasyonunun uzaktan yönetilememesiyle sonuçlanabilir.

**Not:** Güvenlik tanımlayıcısı Yerel hesabı, MSKB 2871997 yüklenmediği sürece Windows 7 ve Windows 8.0'da kullanılamaz.

**Not #2:** Windows 7'den önceki tüm Windows sürümlerinde, Uzak Masaüstü Hizmetleri Terminal Hizmetleri olarak biliniyordu, bu nedenle daha eski bir işletim sistemiyle karşılaştırırken eski terimi değiştirmelisiniz.

**Gerekçe:**

Uzak Masaüstü Hizmetleri aracılığıyla oturum açma hakkına sahip herhangi bir hesap, bilgisayarın uzak konsolunda oturum açmak için kullanılabilir. Bu kullanıcı hakkı, bilgisayarın konsolunda oturum açması gereken meşru kullanıcılarla sınırlı değilse, yetkisiz kullanıcılar ayrıcalıklarını yükselten kötü amaçlı yazılımları indirebilir ve çalıştırabilir.

**Etki:**

Uzak Masaüstü Hizmetleri aracılığıyla oturum açmayı reddet kullanıcı hakkını diğer gruplara atarsanız, ortamınızda belirli yönetim rollerine atanan kullanıcıların yeteneklerini sınırlayabilirsiniz. Bu kullanıcı hakkına sahip hesaplar, Uzak Masaüstü Hizmetleri veya Uzaktan Yardım aracılığıyla bilgisayara bağlanamaz. Temsil edilen görevlerin olumsuz etkilenmeyeceğini onaylamanız gerekir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için Misafirler, Yerel hesabı içerecek şekilde aşağıdaki UI yolunu ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Uzak Masaüstü Hizmetleri aracılığıyla oturum açmayı reddet*

**2.2.21 (L1) 'Bilgisayar ve kullanıcı hesaplarını yetkilendirme için güvenilir olacak şekilde etkinleştir' seçeneği 'Hiç Kimse' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların Active Directory'deki bir bilgisayar nesnesindeki Temsilci için Güvenilir ayarını değiştirmesine olanak tanır. Bu ayrıcalığın kötüye kullanılması, yetkisiz kullanıcıların ağdaki diğer kullanıcıları taklit etmesine izin verebilir. Bu ayar için önerilen durum: Hiç Kimse.

**Not:** Bu kullanıcı hakkı, denetim amacıyla "hassas bir ayrıcalık" olarak kabul edilir.

**Gerekçe:**

Yetkilendirme kullanıcı hakkı için bilgisayar ve kullanıcı hesaplarına güvenilmesini etkinleştir öğesinin yanlış kullanımı, yetkisiz kullanıcıların ağdaki diğer kullanıcıların kimliğine bürünmesine izin verebilir. Saldırgan, ağ kaynaklarına erişmek ve bir güvenlik olayından sonra ne olduğunu belirlemeyi zorlaştırmak için bu ayrıcalıktan yararlanabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Hiç Kimse olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Delegasyon için bilgisayar ve kullanıcı hesaplarının güvenilmesini etkinleştirin*

**2.2.22 (L1) 'Uzak sistemden kapanmaya zorla' seçeneği 'Yöneticiler' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların Windows Vista tabanlı ve daha yeni bilgisayarları ağdaki uzak konumlardan kapatmalarına olanak tanır. Bu kullanıcı hakkının atandığı herkes, bilgisayarın kullanıcı isteklerine hizmet edememesine neden olacak bir hizmet reddi (DoS) durumuna neden olabilir. Bu nedenle, bu kullanıcı hakkının yalnızca son derece güvenilir yöneticilere atanması önerilir. Bu ayar için önerilen durum: Yöneticiler.

**Gerekçe:**

Bir bilgisayarı kapatabilen herhangi bir kullanıcı, bir DoS koşulunun oluşmasına neden olabilir. Bu nedenle, bu kullanıcı hakkı sıkı bir şekilde kısıtlanmalıdır.

**Etki:**

Sunucu Operatörleri grubundan uzak bir sistem kullanıcısından Kapatmaya zorla seçeneğini kaldırırsanız, ortamınızda belirli yönetim rollerine atanan kullanıcıların yeteneklerini sınırlayabilirsiniz. Temsil edilen faaliyetlerin olumsuz etkilenmeyeceğini onaylamanız gerekir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Yöneticiler olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Uzak bir sistemden kapatmaya zorlama*

**2.2.23 (L1) 'Güvenlik denetimleri oluştur' seçeneği 'Yerel Servis, Ağ Servisi' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Güvenlik günlüğünde hangi kullanıcıların veya işlemlerin denetim kayıtları oluşturabileceğini belirler. Bu ayar için önerilen durum: YEREL SERVİS, AĞ SERVİSİ.

**Not:** Bu kullanıcı hakkı, denetim amacıyla "hassas bir ayrıcalık" olarak kabul edilir.

**Gerekçe:**

Saldırgan, bu özelliği, bir sistem yöneticisinin herhangi bir yasa dışı etkinliği bulmasını zorlaştıracak şekilde çok sayıda denetlenen olay oluşturmak için kullanabilir. Ayrıca, olay günlüğü gerektiğinde olayların üzerine yazılacak şekilde yapılandırılırsa, çok sayıda alakasız olay, yetkisiz etkinliklerin herhangi bir kanıtının üzerine yazılabilir.

**Etki:**

Çoğu bilgisayarda bu varsayılan yapılandırmadır ve olumsuz bir etkisi olmayacaktır. Ancak, Web Sunucusu (IIS) kurduysanız, bu kullanıcı hakkının verilmesi için IIS uygulama havuzuna/havuzlarına izin vermeniz gerekecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:** GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu YEREL HİZMET, AĞ HİZMETİ olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Güvenlik denetimleri oluştur*

**2.2.24 (L1) 'Kimlik doğrulamasından sonra istemci kimliğine bürün' seçeneği 'Yöneticiler, Yerel Servis, Ağ Servisi, Servis' olarak ayarlanmalıdır.**

**Açıklama:**

İlke ayarı, bir kullanıcı adına çalışan programların, kullanıcı adına hareket edebilmeleri için o kullanıcının (veya belirtilen başka bir hesabın) kimliğine bürünmesine izin verir. Bu tür bir kimliğe bürünme için bu kullanıcı hakkı gerekiyorsa, yetkisiz bir kullanıcı, bir istemciyi, örneğin, uzaktan yordam çağrısı (RPC) veya adlandırılmış kanallar aracılığıyla, bu hizmetin kimliğine bürünmek için oluşturdukları bir hizmete bağlanmaya ikna edemez. yetkisiz kullanıcının izinlerini yönetim veya sistem seviyelerine yükseltebilecek istemci. Hizmet Denetim Yöneticisi tarafından başlatılan hizmetler, varsayılan olarak erişim belirteçlerine eklenen yerleşik Hizmet grubuna sahiptir. COM altyapısı tarafından başlatılan ve belirli bir hesap altında çalışacak şekilde yapılandırılan COM sunucularında, erişim belirteçlerine Hizmet grubu da eklenir. Sonuç olarak, bu işlemler başlatıldığında bu kullanıcıya atanır. Ayrıca, aşağıdaki koşullardan herhangi biri mevcutsa, bir kullanıcı bir erişim belirtecinin kimliğine bürünebilir:

* Kimliğine bürünülmekte olan erişim belirteci bu kullanıcı içindir.
* Kullanıcı, bu oturum açma oturumunda, erişim belirtecini oluşturmak için açık kimlik bilgileriyle ağda oturum açtı.
* İstenen düzey, Anonim veya Tanımla gibi Kimliğe bürünme'den daha azdır.

Kimlik doğrulamadan sonra istemcinin kimliğine bürünme kullanıcı hakkına sahip bir saldırgan, bir hizmet oluşturabilir, hizmete bağlanması için bir istemciyi kandırabilir ve ardından saldırganın erişim düzeyini istemcinin erişim düzeyine yükseltmek için o istemcinin kimliğine bürünebilir. Bu ayar için önerilen durum: Yöneticiler, YEREL HİZMET, AĞ HİZMETİ, HİZMET.

**Not:** Bu kullanıcı hakkı, denetim amacıyla "hassas bir ayrıcalık" olarak kabul edilir

**Gerekçe:**

Kimlik doğrulamadan sonra istemcinin kimliğine bürünme kullanıcı hakkına sahip bir saldırgan, bir hizmet oluşturabilir, hizmete bağlanması için bir istemciyi kandırabilir ve ardından saldırganın erişim düzeyini istemcinin erişim düzeyine yükseltmek için o istemcinin kimliğine bürünebilir.

**Etki:** Çoğu durumda bu yapılandırmanın hiçbir etkisi olmaz. Web Sunucusu (IIS) kurduysanız, kullanıcı hakkını da IIS\_IUSRS'ye atamanız gerekecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Yöneticiler, YEREL HİZMET, AĞ HİZMETİ, HİZMET olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Kimlik doğrulamadan sonra bir istemcinin kimliğine bürünme*

**2.2.25 'Zamanlama önceliğini arttır' seçeneği 'Yöneticiler, Window Yöneticisi/ Window Yöneticisi Grubu' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların bir işlemin temel öncelik sınıfını artırıp artıramayacağını belirler. (Bir öncelik sınıfı içinde göreli önceliği artırmak ayrıcalıklı bir işlem değildir.) Bu kullanıcı hakkı, işletim sistemiyle birlikte sağlanan yönetim araçları tarafından gerekli değildir, ancak yazılım geliştirme araçları tarafından gerekli olabilir. Bu ayar için önerilen durum: Yöneticiler, Pencere Yöneticisi\Pencere Yöneticisi Grubu.

**Gerekçe:**

Bu kullanıcı hakkının atandığı bir kullanıcı, bir işlemin zamanlama önceliğini Gerçek Zamana yükseltebilir, bu da diğer tüm işlemler için çok az işlem süresi bırakır ve bir DoS koşuluna yol açabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Yöneticiler, Pencere Yöneticisi\Pencere Yöneticisi Grubu olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Zamanlama önceliğini artır*

**2.2.26 (L1) 'Aygıt sürücüsü yükle ve kaldır' seçeneği 'Yöneticiler' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların bir sisteme dinamik olarak yeni bir aygıt sürücüsü yüklemesine olanak tanır. Saldırgan, aygıt sürücüsü gibi görünen kötü amaçlı kod yüklemek için bu özelliği kullanabilir. Bu kullanıcı hakkı, kullanıcıların Windows Vista'da yerel yazıcılar veya yazıcı sürücüleri eklemeleri için gereklidir. Bu ayar için önerilen durum: Yöneticiler.

**Not:** Bu kullanıcı hakkı, denetim amacıyla "hassas bir ayrıcalık" olarak kabul edilir. Gerekçe: Aygıt sürücüleri yüksek ayrıcalıklı kod olarak çalışır. Aygıt sürücülerini yükle ve kaldır kullanıcı hakkına sahip bir kullanıcı, istemeden bir aygıt sürücüsü gibi görünen kötü amaçlı kod yükleyebilir. Yöneticiler daha fazla özen göstermeli ve yalnızca doğrulanmış dijital imzalara sahip sürücüleri yüklemelidir.

**Etki:**

Yazdırma Operatörleri grubundan veya diğer hesaplardan Aygıt sürücülerini yükle ve kaldır kullanıcı hakkını kaldırırsanız, ortamınızda belirli yönetim rollerine atanan kullanıcıların yeteneklerini sınırlayabilirsiniz. Temsil edilen görevlerin olumsuz etkilenmeyeceğinden emin olmalısınız.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Yöneticiler olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Aygıt sürücülerini yükleyin ve kaldırın*

**2.2.27 (L1) 'Sayfaları belleğe kilitle' seçeneği 'Hiç Kimse' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir işlemin verileri fiziksel bellekte tutmasına izin verir, bu da sistemin verileri diskteki sanal belleğe sayfalamasını engeller. Bu kullanıcı hakkı atanırsa, sistem performansında önemli bir düşüş meydana gelebilir. Bu ayar için önerilen durum: Hiç Kimse.

**Gerekçe:**

Sayfaları bellekte kilitle kullanıcı hakkına sahip kullanıcılar, birkaç işleme fiziksel bellek atayabilir, bu da diğer işlemler için çok az RAM bırakabilir veya hiç RAM bırakmayabilir ve bir DoS durumuna neden olabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Hiç Kimse olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Bellekteki sayfaları kilitle*

**2.2.28 (L2) 'Toplu iş olarak oturum aç' seçeneği** 'Yöneticiler' **olarak ayarlanmalıdır.**

**Açıklama**:

Bu ilke ayarı, hesapların görev zamanlayıcı hizmetini kullanarak oturum açmasına olanak tanır. Görev zamanlayıcı genellikle yönetim amaçları için kullanıldığından, kurumsal ortamlarda gerekli olabilir. Ancak, sistem kaynaklarının kötüye kullanılmasını önlemek veya saldırganların bir bilgisayara kullanıcı düzeyinde erişim sağladıktan sonra kötü amaçlı kod başlatma hakkını kullanmasını önlemek için kullanımı yüksek güvenlikli ortamlarda kısıtlanmalıdır. Bu ayar için önerilen durum: Yöneticiler.

**Gerekçe:**

Toplu iş olarak oturum açma kullanıcı hakkı, düşük riskli bir güvenlik açığı sunar. Çoğu kuruluş için varsayılan ayarlar yeterlidir.

**Etki:**

Etki alanı tabanlı Grup İlkeleri aracılığıyla toplu iş olarak oturum açma ayarını yapılandırırsanız, bilgisayar, Görev Zamanlayıcı'da zamanlanmış işler için kullanılan hesaplara kullanıcı hakkı atayamaz. ASP.NET veya IIS gibi isteğe bağlı bileşenler yüklerseniz, bu kullanıcı hakkını bu bileşenler için gerekli olan ek hesaplara atamanız gerekebilir. Örneğin, IIS, bu kullanıcı hakkının IIS\_WPG grubuna ve IUSR\_(BilgisayarAdı), ASPNET ve IWAM\_(BilgisayarAdı) hesaplarına atanmasını gerektirir. Bu kullanıcı hakkı bu gruba ve bu hesaplara atanmamışsa, IIS düzgün işlevsellik için gerekli olan bazı COM nesnelerini çalıştıramaz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Yöneticiler olarak ayarlayın:

*Bilgisayar Yapılandırması\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Toplu iş olarak oturum açma*

**2.2.29 (L2) 'Servis olarak oturum aç' seçeneği 'NT Servis, Tüm Servisler' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, hesapların ağ hizmetlerini başlatmasına veya sistemde çalışan bir hizmet olarak bir işlemi kaydetmesine olanak tanır. Bu kullanıcı hakkı, yüksek güvenlikli bir ortamda herhangi bir bilgisayarda kısıtlanmalıdır, ancak birçok uygulama bu ayrıcalığı gerektirebileceğinden, bir kurumsal ortamda yapılandırılmadan önce dikkatlice değerlendirilmeli ve test edilmelidir. Windows Vista tabanlı (ve daha yeni) bilgisayarlarda, varsayılan olarak hiçbir kullanıcı veya grup bu ayrıcalığa sahip değildir. Bu ayar için önerilen durum: Hiçbiri veya (Hyper-V özelliği yüklendiğinde) NT VIRTUAL MACHINE\Virtual Machines.

**Not:** Hyper-V özelliği ilk olarak Windows 8.0'ın 64-bit sürümüne sahip Windows iş istasyonlarında kullanıma sunulmuştur, bu nedenle NT VIRTUAL MACHINE\Virtual Machines seçeneği Windows'un Windows 7 (veya daha eski) sürümleri için geçerli değildir. Daha eski işletim sistemleri yalnızca No One için yapılandırılmalıdır.

**Gerekçe:**

Hizmet olarak oturum açma, güçlü bir kullanıcı hakkıdır, çünkü hesapların, konsolda kimse oturum açmadığında bile, bir bilgisayarda sürekli olarak çalışan ağ hizmetlerini veya hizmetleri başlatmasına izin verir. Yalnızca yönetici ayrıcalıklarına sahip kullanıcıların hizmetleri yükleyip yapılandırabilmesi, riskleri azaltır. Bu erişim düzeyine zaten ulaşmış bir saldırgan, hizmeti Yerel Sistem hesabıyla çalışacak şekilde yapılandırabilir.

**Etki:**

ASP.NET veya IIS gibi isteğe bağlı bileşenler yüklediyseniz, bu bileşenlerin gerektirdiği ek hesaplara hizmet olarak oturum açma kullanıcı hakkını atamanız gerekebilir. IIS, bu kullanıcı hakkının ASPNET kullanıcı hesabına açıkça verilmesini gerektirir. Hyper-V özelliğinin kurulu olduğu Windows İş İstasyonlarında, bu kullanıcı hakkı ayrıca NT VIRTUAL MACHINE\Virtual Machines özel grubuna da verilmelidir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu ayarlayın:

*Bilgisayar Yapılandırması\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Hizmet olarak oturum açma*

**2.2.30 (L1) 'Denetim ve güvenlik günlüğünü yönet' seçeneği 'Yöneticiler' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, hangi kullanıcıların dosyalar ve dizinler için denetleme seçeneklerini değiştirebileceğini ve Güvenlik günlüğünü temizleyebileceğini belirler. Bu ayar için önerilen durum: Yöneticiler.

**Not:** Bu kullanıcı hakkı, denetim amacıyla "hassas bir ayrıcalık" olarak kabul edilir. Gerekçe: Güvenlik olay günlüğünü yönetme yeteneği, güçlü bir kullanıcı hakkıdır ve yakından korunmalıdır. Bu kullanıcı hakkına sahip olan herkes, yetkisiz etkinliğin önemli kanıtlarını silmek için Güvenlik günlüğünü temizleyebilir.

**Etki:** Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Yöneticiler olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Denetim ve güvenlik günlüğünü yönet*

**2.2.31 (L1) 'Nesne etiketini değiştir' seçeneği 'Hiç Kimse' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayrıcalık, hangi kullanıcı hesaplarının dosyalar, kayıt defteri anahtarları veya diğer kullanıcılara ait işlemler gibi nesnelerin bütünlük etiketini değiştirebileceğini belirler. Bir kullanıcı hesabı altında çalışan işlemler, o kullanıcının sahip olduğu bir nesnenin etiketini bu ayrıcalık olmadan daha düşük bir düzeye değiştirebilir. Bu ayar için önerilen durum: Hiç Kimse.

**Gerekçe:**

Kötü niyetli bir kullanıcı, başka bir kullanıcının sahip olduğu bir nesnenin bütünlük etiketini değiştirerek, amaçlanandan daha yüksek bir ayrıcalık düzeyinde kod yürütmelerine neden olabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Hiç Kimse olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Bir nesne etiketini değiştirme*

**2.2.32 (L1) 'Ürün yazılımı ortam değerlerini değiştir' seçeneği 'Yöneticiler' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların donanım yapılandırmasını etkileyen sistem genelindeki ortam değişkenlerini yapılandırmasına olanak tanır. Bu bilgiler genellikle Bilinen Son İyi Yapılandırma'da saklanır. Bu değerlerin değiştirilmesi ve hizmet reddi durumuna neden olacak bir donanım arızasına neden olabilir. Bu ayar için önerilen durum: Yöneticiler.

**Not:** Bu kullanıcı hakkı, denetim amacıyla "hassas bir ayrıcalık" olarak kabul edilir.

**Gerekçe:**

Ürün yazılımı ortam değerlerini değiştir kullanıcı hakkı atanan herkes, bir donanım bileşeninin ayarlarını, veri bozulmasına veya bir DoS durumuna yol açabilecek şekilde başarısız olmasına neden olacak şekilde yapılandırabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Yöneticiler olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Firmware ortam değerlerini değiştir*

**2.2.33 (L1) 'Toplu bakım görevleri gerçekleştir' seçeneği 'Yöneticiler' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların sistemin birimini veya disk yapılandırmasını yönetmesine olanak tanır; bu, bir kullanıcının bir birimi silmesine ve veri kaybının yanı sıra bir hizmet reddi koşuluna neden olmasına olanak verebilir. Bu ayar için önerilen durum: Yöneticiler.

**Not:** Microsoft SQL Server'ın kurulu olduğu bir iş istasyonu, SQL Server hizmetini çalıştıran hesaba bu kullanıcı hakkının verilmesi için bu öneriye özel bir istisna gerektirir.

**Gerekçe:**

Birim bakım görevlerini gerçekleştir kullanıcı hakkı atanan bir kullanıcı, bir birimi silebilir ve bu da veri kaybına veya bir DoS koşuluna neden olabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Yöneticiler olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Birim bakım görevlerini gerçekleştirin*

**2.2.34 (L1) 'Tekil İşlemi Göster' seçeneği ' Yöneticiler' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, sistem dışı işlemlerin performansını izlemek için hangi kullanıcıların araçları kullanabileceğini belirler. Genellikle, Microsoft Yönetim Konsolu (MMC) Performans ek bileşenini kullanmak için bu kullanıcı hakkını yapılandırmanız gerekmez. Ancak, Sistem Monitörü Windows Yönetim Araçları (WMI) kullanarak veri toplamak üzere yapılandırılmışsa bu kullanıcı hakkına ihtiyacınız vardır. Profil tek işlemli kullanıcı hakkının kısıtlanması, izinsiz giriş yapanların sisteme bir saldırı başlatmak için kullanılabilecek ek bilgiler edinmesini engeller. Bu ayar için önerilen durum: Yöneticiler.

**Gerekçe:**

Profil tek işlemli kullanıcı hakkı, orta düzeyde bir güvenlik açığı sunar. Bu kullanıcı hakkına sahip bir saldırgan, doğrudan saldırmak isteyebilecekleri kritik süreçleri belirlemeye yardımcı olmak için bir bilgisayarın performansını izleyebilir. Saldırgan ayrıca, virüsten koruma yazılımı, izinsiz giriş algılama sistemi veya başka hangi kullanıcıların bilgisayarda oturum açtığı gibi kaçınmaları gerekebilecek karşı önlemleri belirleyebilmek için bilgisayarda hangi işlemlerin çalıştığını belirleyebilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Yöneticiler olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Profil tek işlem*

**2.2.35 (L1) 'Sistem performansını göster' seçeneği 'Yöneticiler, NT SERVICE\WdiServiceHost' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların, saldırganların bir sistemin etkin işlemlerini belirlemesine ve bilgisayarın olası saldırı yüzeyine ilişkin öngörü sağlamasına olanak tanımak için kötüye kullanılabilecek farklı sistem işlemlerinin performansını görüntülemeye yönelik araçları kullanmalarına olanak tanır. Bu ayar için önerilen durum: Yöneticiler, NT SERVICE\WdiServiceHost.

**Gerekçe:**

Profil sistem performansı kullanıcı hakkı, orta düzeyde bir güvenlik açığı oluşturur. Bu kullanıcı hakkına sahip saldırganlar, doğrudan saldırmak isteyebilecekleri kritik süreçleri belirlemeye yardımcı olmak için bir bilgisayarın performansını izleyebilir. Saldırganlar ayrıca, virüsten koruma yazılımı veya izinsiz giriş tespit sistemi gibi kaçınmaları gerekebilecek karşı önlemleri belirleyebilmek için bilgisayarda hangi işlemlerin etkin olduğunu belirleyebilirler.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Yöneticiler, NT SERVICE\WdiServiceHost olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Profil sistem performansı*

**2.2.36 (L1) 'İşlem düzeyi belirtecini değiştir' seçeneği 'YEREL SERVİS, AĞ SERVİSİ' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:** Bu ilke ayarı, bir işlemin veya hizmetin, o alt işlemin güvenlik erişim belirtecini değiştirmek için kullanılabilen ve ayrıcalıkların yükselmesine neden olan farklı bir güvenlik erişim belirteciyle başka bir hizmet veya işlem başlatmasına izin verir. Bu ayar için önerilen durum: YEREL SERVİS, AĞ SERVİSİ.

**Not:** Bu kullanıcı hakkı, denetim amacıyla "hassas bir ayrıcalık" olarak kabul edilir.

**Gerekçe:**

Bir işlem düzeyinde belirteci değiştir ayrıcalığına sahip kullanıcılar, kimlik bilgilerini bildikleri diğer kullanıcılar gibi işlemleri başlatabilir. Bilgisayardaki yetkisiz eylemlerini gizlemek için bu yöntemi kullanabilirler. (Windows 2000 tabanlı bilgisayarlarda, Bir işlem düzeyi belirtecini değiştir kullanıcı hakkının kullanılması, kullanıcının bu bölümde daha önce açıklanan bir işlem için Bellek kotalarını ayarla kullanıcı hakkına sahip olmasını gerektirir.)

**Etki:**

Çoğu bilgisayarda bu, varsayılan yapılandırmadır ve olumsuz bir etkisi olmayacaktır. Ancak, Web Sunucusu (IIS) kurduysanız, bu Kullanıcı Hakkı Atamasının verilmesi için IIS uygulama havuzuna/havuzlarına izin vermeniz gerekir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki kullanıcı arabirimi yolunu YEREL HİZMET, AĞ HİZMETİ olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\İşlem düzeyi belirtecini değiştirin*

**2.2.37 (L1) 'Dosyaları ve dizinleri geri yükle' seçeneği 'Yöneticiler' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, ortamınızda Windows Vista (veya daha yenisi) çalıştıran bilgisayarlarda yedeklenen dosyaları ve dizinleri geri yüklerken hangi kullanıcıların dosya, dizin, kayıt defteri ve diğer kalıcı nesne izinlerini atlayabileceğini belirler. Bu kullanıcı hakkı, hangi kullanıcıların geçerli güvenlik ilkelerini nesne sahipleri olarak ayarlayabileceğini de belirler; Dosyaları ve dizinleri yedekle kullanıcı hakkına benzer. Bu ayar için önerilen durum: Yöneticiler.

**Not:** Bu kullanıcı hakkı, denetim amacıyla "hassas bir ayrıcalık" olarak kabul edilir.

**Gerekçe:**

Dosyaları ve dizinleri geri yükle kullanıcı hakkına sahip bir saldırgan, hassas verileri bir bilgisayara geri yükleyebilir ve daha yeni olan verilerin üzerine yazabilir; bu da önemli verilerin kaybolmasına, verilerin bozulmasına veya hizmet reddine neden olabilir. Saldırganlar, kendilerine yükseltilmiş ayrıcalıklar vermek, verileri tehlikeye atmak veya bilgisayara sürekli erişim için arka kapılar yüklemek için kötü amaçlı yazılım içeren sürümlerle meşru yöneticiler veya sistem hizmetleri tarafından kullanılan yürütülebilir dosyaların üzerine yazabilir.

**Not:** Aşağıdaki önlem yapılandırılmış olsa bile, bir saldırgan yine de saldırgan tarafından kontrol edilen bir etki alanındaki bir bilgisayara verileri geri yükleyebilir. Bu nedenle, kuruluşların verileri yedeklemek için kullanılan medyayı dikkatli bir şekilde koruması çok önemlidir.

**Etki:**

Dosyaları ve dizinleri geri yükle kullanıcı hakkını Yedekleme Operatörleri grubundan ve diğer hesaplardan kaldırırsanız, belirli görevler verilmiş olan kullanıcıların bu görevleri gerçekleştirmesini imkansız hale getirebilirsiniz. Bu değişikliğin kuruluşunuzun personelinin işlerini yapma becerisini olumsuz etkilemeyeceğini doğrulamanız gerekir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için Yöneticiler olarak şu kullanıcı arabirimi yolunu ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Dosyaları ve dizinleri geri yükleyin*

**2.2.38 (L1) 'Sistemi kapat' seçeneği 'Yöneticiler, Kullanıcılar' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, ortamınızdaki bilgisayarlarda yerel olarak oturum açan hangi kullanıcıların Kapat komutuyla işletim sistemini kapatabileceğini belirler. Bu kullanıcı hakkının kötüye kullanılması, hizmet reddi durumuna neden olabilir. Bu ayar için önerilen durum: Yöneticiler, Kullanıcılar.

**Gerekçe:**

Hizmet Reddi saldırısını önlemek için, bir iş istasyonunu kapatma yeteneği, genel olarak Yöneticiler ve o iş istasyonunun yetkili kullanıcıları tarafından kullanılabilir olmalı, ancak misafirler veya yetkisiz kullanıcılar için izin verilmemelidir.

**Etki:**

Sistemi kapat kullanıcı hakkından bu varsayılan grupları kaldırmanın etkisi, ortamınızda atanan rollerin devredilen yeteneklerini sınırlayabilir. Temsil edilen faaliyetlerin olumsuz etkilenmeyeceğini teyit etmelisiniz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için Yöneticiler, Kullanıcılar olarak şu kullanıcı arabirimi yolunu ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Sistemi kapatın*

**2.2.39 (L1) 'Dosyaların veya diğer nesnelerin sahipliğini al' seçeneği 'Yöneticiler' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların dosyaların, klasörlerin, kayıt defteri anahtarlarının, işlemlerin veya iş parçacıklarının sahipliğini almasına olanak tanır. Bu kullanıcı hakkı, mülkiyeti belirtilen kullanıcıya vermek için nesneleri korumak için mevcut tüm izinleri atlar. Bu ayar için önerilen durum: Yöneticiler.

**Not:** Bu kullanıcı hakkı, denetim amacıyla "hassas bir ayrıcalık" olarak kabul edilir.

**Gerekçe:**

Dosyaların veya diğer nesnelerin sahipliğini al kullanıcı hakkına sahip herhangi bir kullanıcı, o nesne üzerindeki izinlerden bağımsız olarak herhangi bir nesnenin kontrolünü ele geçirebilir ve sonra o nesnede dilediği değişiklikleri yapabilir. Bu tür değişiklikler, verilerin açığa çıkmasına, verilerin bozulmasına veya bir DoS koşuluna neden olabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için Yöneticiler olarak şu kullanıcı arabirimi yolunu ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Kullanıcı Hakları Ataması\Dosyaların veya diğer nesnelerin sahipliğini alın*

**2.3 Güvenlik Seçenekleri**

**2.3.1 Hesaplar**

**2.3.1.1 (L1) 'Hesaplar: Yönetici hesabı durumu' 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, normal çalışma sırasında Yönetici hesabını etkinleştirir veya devre dışı bırakır. Bir bilgisayar güvenli modda başlatıldığında, bu ayarın nasıl yapılandırıldığına bakılmaksızın Yönetici hesabı her zaman etkinleştirilir. Etki Alanı Denetleyicileri yerel hesap veritabanına sahip olmadığı için, bu ayarın Grup ilkesi aracılığıyla Etki Alanı Denetleyicileri kuruluş birimine uygulandığında hiçbir etkisi olmayacağını unutmayın. Hesap kilitleme ve parola ilkesi ayarlarına benzer şekilde, grup ilkesi aracılığıyla etki alanı düzeyinde yapılandırılabilir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bazı kuruluşlarda, yerel hesaplar için periyodik parola değişiklikleri için düzenli bir program sürdürmek göz korkutucu bir yönetim zorluğu olabilir. Bu nedenle, saldırılara karşı korumak için düzenli parola değişikliklerine güvenmek yerine yerleşik Yönetici hesabını devre dışı bırakmak isteyebilirsiniz. Bu yerleşik hesabı devre dışı bırakmanın bir başka nedeni, ne kadar başarısız oturum açarsa açsın kilitlenememesidir, bu da onu parolaları tahmin etmeye çalışan kaba kuvvet saldırıları için ana hedef haline getirir. Ayrıca, bu hesabın iyi bilinen bir güvenlik tanımlayıcısı (SID) vardır ve hesap adı yerine SID'yi kullanarak kimlik doğrulamaya izin veren üçüncü taraf araçlar vardır. Bu yetenek, Yönetici hesabını yeniden adlandırsanız bile, bir saldırganın oturum açmak için SID'yi kullanarak bir kaba kuvvet saldırısı başlatabileceği anlamına gelir.

**Etki:**

Yönetici hesabını devre dışı bırakırsanız, belirli koşullar altında bakım sorunları ortaya çıkabilir. Örneğin, bir üye bilgisayar ile Etki Alanı Denetleyicisi arasındaki güvenli kanal herhangi bir nedenle etki alanı ortamında başarısız olursa ve başka bir yerel Yönetici hesabı yoksa, güvenli kanalı bozan sorunu gidermek için güvenli modda yeniden başlatmanız gerekir. Geçerli Yönetici parolası parola gereksinimlerini karşılamıyorsa, Yönetici hesabını devre dışı bırakıldıktan sonra yeniden etkinleştiremezsiniz. Bu durum oluşursa, Yöneticiler grubunun başka bir üyesi, Yerel Kullanıcılar ve Gruplar aracıyla Yönetici hesabındaki parolayı belirlemelidir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Hesaplar: Yönetici hesabı durumu*

**2.3.1.2 (L1) 'Hesaplar: Microsoft hesaplarını engelle' seçeneği 'Kullanıcılar Microsoft hesapları ekleyemez veya bu hesaplarla oturum açamaz' olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların bu bilgisayara yeni Microsoft hesapları eklemesini engeller. Bu ayar için önerilen durum şudur: Kullanıcılar Microsoft hesapları ekleyemez veya bu hesaplarla oturum açamaz.

**Gerekçe:**

Kimlik yönetimi ilkelerini etkin bir şekilde uygulamak ve bilgisayarlarında oturum açmak için hangi hesapların kullanıldığını sıkı bir şekilde kontrol etmek isteyen kuruluşlar, muhtemelen Microsoft hesaplarını engellemek isteyeceklerdir. Kuruluşların ayrıca bilgi sistemleri için geçerli olan uyumluluk standartlarının gereksinimlerini karşılamak için Microsoft hesaplarını engellemesi gerekebilir.

**Etki:**

Kullanıcılar, Microsoft hesaplarıyla bilgisayarda oturum açamayacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: NoConnectedUser*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Kullanıcılar ekleyemiyor veya oturum açamıyor olarak ayarlayın Microsoft hesaplarıyla açık:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Hesaplar: Microsoft hesaplarını engelle*

**2.3.1.3 (L1) 'Hesaplar: Konuk hesabı durumu' 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Konuk hesabının etkinleştirilip etkinleştirilmeyeceğini belirler. Konuk hesabı, kimliği doğrulanmamış ağ kullanıcılarının sisteme erişmesine izin verir. Bu ayar için önerilen durum: Devre Dışı.

**Not:** Etki Alanı Denetleyicileri yerel hesap veritabanına sahip olmadığı için, bu ayarın Etki Alanı Denetleyicileri kuruluş birimine grup ilkesi aracılığıyla uygulandığında hiçbir etkisi olmaz. Hesap kilitleme ve parola ilkesi ayarlarına benzer şekilde, grup ilkesi aracılığıyla etki alanı düzeyinde yapılandırılabilir.

**Gerekçe:**

Varsayılan Konuk hesabı, kimliği doğrulanmamış ağ kullanıcılarının parola olmadan Misafir olarak oturum açmasına izin verir. Bu yetkisiz kullanıcılar, Konuk hesabının ağ üzerinden erişebildiği tüm kaynaklara erişebilir. Bu özellik, Konuk hesabına, Misafirler grubuna veya Herkes grubuna erişime izin veren izinlere sahip tüm ağ paylaşımlarının ağ üzerinden erişilebilir olacağı ve bu da verilerin açığa çıkmasına veya bozulmasına yol açabileceği anlamına gelir.

**Etki:**

Tüm ağ kullanıcılarının, paylaşılan kaynaklara erişebilmeleri için kimlik doğrulaması yapması gerekecek. Konuk hesabını devre dışı bırakırsanız ve Ağ Erişimi: Paylaşım ve Güvenlik Modeli seçeneği Yalnızca Konuk olarak ayarlanırsa, Microsoft Ağ Sunucusu (SMB Hizmeti) tarafından gerçekleştirilenler gibi ağ oturum açma işlemleri başarısız olur. Bu ilke ayarı, Microsoft Windows 2000, Windows XP ve Windows Server™ 2003'te varsayılan ayar olduğundan, çoğu kuruluş üzerinde çok az etkiye sahip olmalıdır.

**Denetim:**

Düzeltme bölümünde belirtilen Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Hesaplar: Konuk hesabı durumu*

**2.3.1.4 (L1) 'Hesaplar: Yerel hesaplarda boş parola kullanımını yalnızca konsolda oturum açma ile sınırla' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, fiziksel bilgisayar konsolu dışındaki konumlardan oturum açmak için parola korumalı olmayan yerel hesapların kullanılıp kullanılamayacağını belirler. Bu ilke ayarını etkinleştirirseniz, parolaları boş olan yerel hesaplar, uzak istemci bilgisayarlardan ağda oturum açamaz. Bu tür hesaplar sadece bilgisayarın klavyesinden oturum açabilecektir. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Boş parolalar bilgisayar güvenliği için ciddi bir tehdittir ve hem kurumsal politika hem de uygun teknik önlemler yoluyla yasaklanmalıdır. Aslında, Active Directory etki alanları için varsayılan ayarlar, en az yedi karakterden oluşan karmaşık parolalar gerektirir. Ancak, yeni hesap oluşturma becerisine sahip kullanıcılar, etki alanına dayalı şifre politikalarınızı atlarsa, boş şifrelerle hesap oluşturabilirler. Örneğin, bir kullanıcı bağımsız bir bilgisayar oluşturabilir, boş parolalarla bir veya daha fazla hesap oluşturabilir ve ardından bilgisayarı etki alanına katabilir. Boş parolalara sahip yerel hesaplar çalışmaya devam edecektir. Bu korumasız hesaplardan birinin adını bilen herkes, oturum açmak için bu hesabı kullanabilir. Etki: Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:LimitBlankPasswordUse*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Hesaplar: Yerel hesapta boş parola kullanımını yalnızca konsol oturum açmayla sınırlayın*

**2.3.1.5 (L1) 'Hesaplar: Yönetici hesabını yeniden adlandır' seçeneği 'Yönetici' olarak ayarlanmalıdır. (Otomatik)**

**Açıklama:**

Yerleşik yerel yönetici hesabı, saldırganların hedef alacağı iyi bilinen bir hesap adıdır. Bu hesap için başka bir ad seçmeniz ve yönetici veya yüksek erişim hesaplarını ifade eden adlardan kaçınmanız önerilir. Yerel yönetici için varsayılan açıklamayı da değiştirdiğinizden emin olun (Bilgisayar Yönetimi konsolu aracılığıyla).

**Gerekçe:**

Yönetici hesabı, Windows 2000 veya daha yeni işletim sistemlerini çalıştıran tüm bilgisayarlarda bulunur. Bu hesabı yeniden adlandırırsanız, yetkisiz kişilerin bu ayrıcalıklı kullanıcı adı ve şifre kombinasyonunu tahmin etmesi biraz daha zorlaşır. Yerleşik Yönetici hesabı, bir saldırganın hatalı parolayı kaç kez kullanabileceğinden bağımsız olarak kilitlenemez. Bu yetenek, Yönetici hesabını parolaları tahmin etmeye çalışan kaba kuvvet saldırıları için popüler bir hedef haline getirir. Bu hesabın iyi bilinen bir SID'si olduğundan ve hesap adı yerine SID'yi kullanarak kimlik doğrulamaya izin veren üçüncü taraf araçlar bulunduğundan bu önlemin değeri azalır. Bu nedenle, Yönetici hesabını yeniden adlandırsanız bile, bir saldırgan oturum açmak için SID'yi kullanarak bir kaba kuvvet saldırısı başlatabilir.

**Etki:**

Bu hesabı kullanma yetkisi olan kullanıcılara yeni hesap adını bildirmeniz gerekecek. (Bu ayar için kılavuz, bu bölümün önceki bölümlerinde önerilen Yönetici hesabının devre dışı bırakılmadığını varsayar.)

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu yapılandırın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Hesaplar: Yönetici hesabını yeniden adlandırın*

**2.3.1.6 (L1)'Hesaplar: Konuk hesabını yeniden adlandır' seçeneği Konuk hesaplar devre dışı olduğu için hiçbir önem göstermemektedir.**

**Açıklama:**

Yerleşik yerel konuk hesabı, saldırganlar tarafından iyi bilinen bir başka addır. Bu hesabın amacını belirtmeyen bir adla yeniden adlandırılması önerilir. Önerilen bu hesabı devre dışı bıraksanız bile, ek güvenlik için yeniden adlandırdığınızdan emin olun.

**Gerekçe:**

Konuk hesabı, Windows 2000 veya daha yeni işletim sistemlerini çalıştıran tüm bilgisayarlarda bulunur. Bu hesabı yeniden adlandırırsanız, yetkisiz kişilerin bu ayrıcalıklı kullanıcı adı ve şifre kombinasyonunu tahmin etmesi biraz daha zorlaşır.

**Etki:**

Konuk hesabı varsayılan olarak devre dışı bırakıldığından çok az etkisi olmalıdır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu yapılandırın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Hesaplar: Konuk hesabını yeniden adlandırın*

**2.3.2 Denetim**

**2.3.2.1 (L1) 'Denetim: Denetim ilkesi alt kategori ayarlarını (Windows Vista veya üzeri) denetim ilkesi kategorisi ayarlarını geçersiz kılmaya zorla' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, yöneticilerin Windows Vista'da bulunan daha kesin denetim özelliklerini etkinleştirmesine olanak tanır. Windows Server 2003 Active Directory'de bulunan Denetim İlkesi ayarları, henüz yeni denetim alt kategorilerini yönetmeye yönelik ayarları içermez. Bu temel çizgide belirtilen denetim ilkelerini düzgün bir şekilde uygulamak için, Denetim: Denetim ilkesi alt kategori ayarlarını (Windows Vista veya üstü) denetim ilkesi kategori ayarlarını geçersiz kılmaya zorla ayarının Etkin olarak yapılandırılması gerekir. Bu ayar için önerilen durum: Etkin.

**Önemli**: Büyük miktarda trafik oluşturabilecek denetim ayarları konusunda çok dikkatli olun. Örneğin, tüm Ayrıcalık Kullanımı alt kategorileri için başarı veya başarısızlık denetimini etkinleştirirseniz, oluşturulan yüksek hacimli denetim olayları, Güvenlik günlüğünde diğer giriş türlerini bulmayı zorlaştırabilir. Böyle bir yapılandırma, sistem performansı üzerinde de önemli bir etkiye sahip olabilir.

**Gerekçe:**

Windows Vista'da denetim alt kategorilerinin tanıtılmasından önce, olayları sistem başına veya kullanıcı başına düzeyde izlemek zordu. Daha büyük olay kategorileri çok fazla olay yarattı ve denetlenmesi gereken temel bilgileri bulmak zordu.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:** Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:SCENoApplyLegacyAudit Policy*

**Düzeltme**:

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\ Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Denetim: Denetim ilkesi kategori ayarlarını geçersiz kılmak için denetim ilkesi alt kategori ayarlarını (Windows Vista veya üstü) zorla*

**2.3.2.2 (L1) 'Denetim: Güvenlik denetimleri kaydedilemiyorsa sistemi hemen kapat' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Güvenlik olaylarını günlüğe kaydedemezse sistemin kapanıp kapanmayacağını belirler. Denetim sistemi bunları günlüğe kaydedemiyorsa, denetlenebilir olayların oluşmasını önlemek için Güvenilir Bilgisayar Sistemi Değerlendirme Ölçütleri (TCSEC)-C2 ve Ortak Ölçütler sertifikası için bir gerekliliktir. Microsoft, bu gereksinimi, sistemi durdurarak ve denetim sistemi bir hatayla karşılaşırsa bir dur mesajı görüntüleyerek karşılamayı seçmiştir. Bu ilke ayarı etkinleştirildiğinde, herhangi bir nedenle bir güvenlik denetimi günlüğe kaydedilemezse sistem kapatılacaktır.

Güvenlik denetimleri kaydedilemiyorsa sistemi hemen kapat ayarı etkinleştirilirse, planlanmamış sistem hataları meydana gelebilir. Yönetim yükü, özellikle Güvenlik günlüğü için Tutma yöntemini Olayların üzerine yazma (günlüğü manuel olarak temizle) olarak da yapılandırırsanız önemli olabilir. Bu yapılandırma, bir reddetme tehdidinin (bir yedekleme operatörü, verileri yedeklediğini veya geri yüklediğini reddedebilir), bir hizmet reddi (DoS) güvenlik açığı haline gelmesine neden olur, çünkü bir sunucu, oturum açma olayları ve diğer güvenlik önlemleriyle boğulursa kapanmaya zorlanabilir. Güvenlik günlüğüne yazılan olaylar. Ayrıca, kapatma işlemi uygun olmadığı için işletim sisteminde, uygulamalarda veya verilerde onarılamaz hasarlar meydana gelebilir. NTFS dosya sistemi, uygun olmayan bir bilgisayar kapanması meydana geldiğinde bütünlüğünü garanti etse de, bilgisayar yeniden başlatıldığında her uygulama için her veri dosyasının hala kullanılabilir bir biçimde olacağını garanti edemez. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bilgisayar olayları Güvenlik günlüğüne kaydedemezse, bir güvenlik olayının ardından kritik kanıtlar veya önemli sorun giderme bilgileri gözden geçirilmek üzere mevcut olmayabilir. Ayrıca, bir saldırgan, bilgisayarı kasıtlı olarak kapatmaya zorlamak için büyük miktarda Güvenlik günlüğü olayı oluşturabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:CrashOnAuditFail*

**Düzeltme**:

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarlar\Yerel İlkeler\Güvenlik Seçenekleri\Denetim: Güvenlik denetimlerini günlüğe kaydedemiyorsa sistemi hemen kapatın*

**2.3.4 Cihazlar**

**2.3.4.1 (L1) 'Cihazlar: Çıkarılabilir medyayı biçimlendirmesine ve çıkarmasına izin verildi' seçeneği 'Yöneticiler ve Etkileşimli Kullanıcılar' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kimlerin çıkarılabilir NTFS ortamını biçimlendirmesine ve çıkarmasına izin verileceğini belirler. Yetkisiz kullanıcıların yerel yönetici ayrıcalıklarına sahip oldukları başka bir bilgisayarda erişmek için bir bilgisayardaki verileri kaldırmasını önlemek için bu ilke ayarını kullanabilirsiniz. Bu ayar için önerilen durum şudur: Yöneticiler ve Etkileşimli Kullanıcılar.

**Gerekçe:**

Kullanıcılar çıkarılabilir disklerdeki verileri yönetici ayrıcalıklarına sahip oldukları farklı bir bilgisayara taşıyabilir. Kullanıcı daha sonra herhangi bir dosyanın sahipliğini alabilir, kendilerine tam kontrol verebilir ve herhangi bir dosyayı görüntüleyebilir veya değiştirebilir. Çoğu çıkarılabilir depolama aygıtının medyayı mekanik bir düğmeye basarak çıkarması, bu ilke ayarının avantajını azaltır.

**Etki:**

Yok - varsayılan değer yalnızca Yöneticiler'dir. Yöneticiler ve Etkileşimli Kullanıcılar, çıkarılabilir NTFS ortamını biçimlendirebilir ve çıkarabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon:AllocateDASD*

**Düzeltme:** GP aracılığıyla önerilen yapılandırmayı oluşturmak için, Yöneticiler ve Etkileşimli Kullanıcılar olarak aşağıdaki UI yolunu ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Aygıtlar: Çıkarılabilir medyayı biçimlendirme ve çıkarma izni var*

**2.3.4.2 (L2) 'Cihazlar: Kullanıcıların yazıcı sürücülerini yüklemesini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bir bilgisayarın paylaşılan bir yazıcıya yazdırması için, o paylaşılan yazıcının sürücüsünün yerel bilgisayara yüklenmesi gerekir. Bu güvenlik ayarı, paylaşılan bir yazıcıya bağlanmanın bir parçası olarak kimlerin yazıcı sürücüsü yüklemesine izin verileceğini belirler. Bu ayar için önerilen durum: Etkin.

**Not:** Bu ayar, yerel yazıcı ekleme özelliğini etkilemez. Bu ayar Yöneticileri etkilemez.

**Gerekçe:**

Bazı kuruluşlarda, kullanıcıların yazıcı sürücülerini kendi iş istasyonlarına yüklemelerine izin vermek uygun olabilir. Ancak, yüksek güvenlikli bir ortamda, kullanıcıların değil, yalnızca Yöneticilerin bunu yapmasına izin vermelisiniz, çünkü yazıcı sürücüsü yüklemesi istemeden bilgisayarın daha az kararlı olmasına neden olabilir. Kötü niyetli bir kullanıcı, kasıtlı olarak bilgisayara zarar verme girişiminde bulunarak uygun olmayan yazıcı sürücüleri yükleyebilir veya bir kullanıcı yanlışlıkla bir yazıcı sürücüsü gibi görünen kötü amaçlı yazılımlar yükleyebilir. Bir saldırganın bir Truva atı programını yazıcı sürücüsü olarak gizlemesi mümkündür. Program, kullanıcılara yazdırmak için kullanmaları gerekiyormuş gibi görünebilir, ancak böyle bir program bilgisayar ağınızda kötü amaçlı kodlar açığa çıkarabilir.

**Etki:**

Yalnızca Yöneticiler, paylaşılan bir yazıcıya bağlanmanın bir parçası olarak bir yazıcı sürücüsü yükleyebilir. Yerel yazıcı ekleme özelliği etkilenmeyecektir.

**Denetim:** Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Print\Providers\LanMan Print Services\Servers:AddPrinterDrivers*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Aygıtlar: Kullanıcıların yazıcı sürücülerini yüklemesini engelle*

**2.3.6 Domain üyesi**

**2.3.6.1 (L1) 'Etki Alanı Üyesi: Güvenli kanal verilerini dijital olarak şifreleyin veya imzalayın (her zaman)' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, etki alanı üyesi tarafından başlatılan tüm güvenli kanal trafiğinin imzalanması mı yoksa şifrelenmesi mi gerektiğini belirler. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bir bilgisayar bir etki alanına katıldığında, bir bilgisayar hesabı oluşturulur. Etki alanına katıldıktan sonra, bilgisayar her yeniden başlatıldığında etki alanı için Etki Alanı Denetleyicisi ile güvenli bir kanal oluşturmak üzere bu hesabın parolasını kullanır. Güvenli kanaldan gönderilen isteklerin kimliği doğrulanır ve parolalar gibi hassas bilgiler şifrelenir, ancak kanal bütünlük denetimine tabi tutulmaz ve tüm bilgiler şifrelenmez. Dijital şifreleme ve güvenli kanalın imzalanması, desteklendiği yerlerde iyi bir fikirdir. Güvenli kanal, etki alanı kimlik bilgilerini Etki Alanı Denetleyicisine gönderilirken korur.

**Etki:** Yok - bu varsayılan davranıştır. Ancak, yalnızca Service Pack 6a (SP6a) içeren Windows NT 4.0 ve Windows işletim sisteminin sonraki sürümleri, güvenli kanalın dijital şifrelemesini ve imzalanmasını destekler. Windows 98 Second Edition istemcileri, Dsclient'in kurulu olmadığı sürece bunu desteklemez. Bu nedenle, Etki Alanı üyesini etkinleştiremezsiniz: Etki alanının üyeleri olarak Windows 98 istemcilerini destekleyen Etki Alanı Denetleyicilerinde Güvenli kanal verilerini dijital olarak şifrele veya imzala (her zaman) ayarını. Olası etkiler aşağıdakileri içerebilir:

* Windows'un SP6a ile Windows NT 4.0'dan önceki sürümlerini çalıştıran istemcilerle güven ilişkileri oluşturma veya silme yeteneği devre dışı bırakılır.
* SP6a ile Windows NT 4.0'dan önceki Windows sürümlerini çalıştıran istemcilerden oturum açma işlemleri devre dışı bırakılacaktır.
* Güvenilir bir etki alanında SP6a ile Windows NT 4.0'dan önceki bir Windows sürümünü çalıştıran bir Etki Alanı Denetleyicisinden diğer etki alanlarının kullanıcılarının kimliğini doğrulama yeteneği devre dışı bırakılacaktır.

Bu ilke ayarını etki alanından tüm Windows 9x istemcilerini kaldırdıktan ve tüm Windows NT 4.0 sunucularını ve Etki Alanı Denetleyicilerini güvenilen/güvenilen etki alanlarından SP6a ile Windows NT 4.0'a yükselttikten sonra etkinleştirebilirsiniz.

**Denetim:** Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:Requ ireSignOrSeal*

**Düzeltme**:

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarlar\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Etki Alanı üyesi: Güvenli kanal verilerini dijital olarak şifreleyin veya imzalayın (her zaman)*

**2.3.6.2 (L1) 'Etki Alanı Üyesi: Güvenli kanal verilerini şifreleme (mümkünse)' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir etki alanı üyesinin başlattığı tüm güvenli kanal trafiği için şifreleme anlaşması yapmaya çalışıp çalışmayacağını belirler. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bir bilgisayar bir etki alanına katıldığında, bir bilgisayar hesabı oluşturulur. Etki alanına katıldıktan sonra, bilgisayar her yeniden başlatıldığında etki alanı için Etki Alanı Denetleyicisi ile güvenli bir kanal oluşturmak üzere bu hesabın parolasını kullanır. Güvenli kanaldan gönderilen isteklerin kimliği doğrulanır ve parolalar gibi hassas bilgiler şifrelenir, ancak kanal bütünlük denetimine tabi tutulmaz ve tüm bilgiler şifrelenmez. Dijital şifreleme ve güvenli kanalın imzalanması, desteklendiği yerlerde iyi bir fikirdir. Güvenli kanal, etki alanı kimlik bilgilerini Etki Alanı Denetleyicisine gönderilirken korur.

**Etki:**

Yok - bu varsayılan davranıştır. Ancak, yalnızca Windows NT 4.0 Service Pack 6a (SP6a) ve Windows işletim sisteminin sonraki sürümleri, güvenli kanalın dijital şifrelemesini ve imzalanmasını destekler. Windows 98 Second Edition istemcileri, Dsclient'in kurulu olmadığı sürece bunu desteklemez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:Seal SecureChannel*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Etki Alanı üyesi: Güvenli kanal verilerini dijital olarak şifreleyin (mümkün olduğunda)*

**2.3.6.3 (L1) 'Etki Alanı üyesi: Güvenli kanal verilerini dijital olarak imzala (mümkünse)' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir etki alanı üyesinin başlattığı tüm güvenli kanal trafiğinin dijital olarak imzalanması gerekip gerekmediği konusunda anlaşmaya çalışıp çalışmayacağını belirler. Dijital imzalar, trafiği ağda dolaşırken verileri yakalayan herkes tarafından değiştirilmekten korur. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bir bilgisayar bir etki alanına katıldığında, bir bilgisayar hesabı oluşturulur. Etki alanına katıldıktan sonra, bilgisayar her yeniden başlatıldığında etki alanı için Etki Alanı Denetleyicisi ile güvenli bir kanal oluşturmak üzere bu hesabın parolasını kullanır. Güvenli kanaldan gönderilen isteklerin kimliği doğrulanır ve parolalar gibi hassas bilgiler şifrelenir, ancak kanal bütünlük denetimine tabi tutulmaz ve tüm bilgiler şifrelenmez. Dijital şifreleme ve güvenli kanalın imzalanması, desteklendiği yerlerde iyi bir fikirdir. Güvenli kanal, etki alanı kimlik bilgilerini Etki Alanı Denetleyicisine gönderilirken korur.

**Etki:**

Yok - bu varsayılan davranıştır. Ancak, yalnızca Service Pack 6a (SP6a) içeren Windows NT 4.0 ve Windows işletim sisteminin sonraki sürümleri, güvenli kanalın dijital şifrelemesini ve imzalanmasını destekler. Windows 98 Second Edition istemcileri, Dsclient'in kurulu olmadığı sürece bunu desteklemez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:Sign SecureChannel*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Etki Alanı üyesi: Güvenli kanal verilerini dijital olarak imzala (mümkün olduğunda)*

**2.3.6.4 (L1) 'Etki alanı üyesi: Makine hesabı şifre değişikliklerini devre dışı bırak' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir etki alanı üyesinin bilgisayar hesabı parolasını düzenli aralıklarla değiştirip değiştiremeyeceğini belirler. Bir saldırgan sistemin etki alanı hesabının parolasını belirleyebileceğinden, hesap parolalarını otomatik olarak değiştiremeyen bilgisayarlar potansiyel olarak savunmasızdır. Bu ayar için önerilen durum: Devre Dışı.

**Not:** Makine hesabı parolasının süresinin dolmasının bir sonucu olarak, özellikle bir makine, sanal makinelerde yaygın olduğu gibi, önceki bir zaman noktasındaki durumuna döndürülürse, bazı sorunlar oluşabilir. Geri döndürmenin ne kadar geriye gittiğine bağlı olarak, makinede depolanan eski makine hesabı parolası artık etki alanı denetleyicileri tarafından tanınmayabilir ve bu nedenle bilgisayar etki alanı güvenini kaybeder. Bu, kalıcı olmayan VDI uygulamalarını ve işletim sistemi biriminde kalıcı değişikliklere izin vermeyen yazma filtreleri olan cihazları da bozabilir. Bazı kuruluşlar, kendilerini bu öneriden muaf tutmayı seçebilir ve bu durumlar için makine hesabı parola süresinin dolmasını devre dışı bırakabilir.

**Gerekçe:**

Bir etki alanına ait olan Windows Server 2003 tabanlı bilgisayarlar için varsayılan yapılandırma, hesaplarının parolalarını her 30 günde bir otomatik olarak değiştirmelerinin gerekmesidir. Bu ilke ayarını devre dışı bırakırsanız, Windows Server 2003 çalıştıran bilgisayarlar, bilgisayar hesaplarıyla aynı parolaları korur. Artık hesap parolalarını otomatik olarak değiştiremeyen bilgisayarlar, bilgisayarın etki alanı hesabının parolasını belirleyebilen bir saldırganın tehdidi altındadır.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:Disa blePasswordChange*

**Düzeltme:** GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarlar\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Etki Alanı üyesi: Makine hesabı parola değişikliklerini devre dışı bırakın*

**2.3.6.5 (L1) 'Etki Alanı üyesi: Maksimum makine hesabı şifre yaşı' seçeneği '30 veya daha az gün, ancak 0 değil' olarak ayarlanmalıdır. (Otomatik)**

**Açıklama:**

Bu ilke ayarı, bir bilgisayar hesabı parolası için izin verilen maksimum yaşı belirler. Varsayılan olarak, alan üyeleri, alan parolalarını her 30 günde bir otomatik olarak değiştirir. Bilgisayarların artık parolalarını değiştirmemesi için bu aralığı önemli ölçüde artırırsanız, saldırganın bilgisayar hesaplarından birine kaba kuvvet saldırısı gerçekleştirmek için daha fazla zamanı olur. Bu ayar için önerilen durum: 30 veya daha az gün, ancak 0 değil.

**Not:** 0 değeri, maksimum parola yaşını devre dışı bıraktığı için karşılaştırmaya uymaz.

**Not #2:** Makine hesabı parolasının süresinin dolmasının bir sonucu olarak, özellikle bir makine, sanal makinelerde yaygın olduğu gibi, bir önceki zaman noktasına döndürülürse, bazı sorunlar oluşabilir. Geri döndürmenin ne kadar geriye gittiğine bağlı olarak, makinede depolanan eski makine hesabı parolası artık etki alanı denetleyicileri tarafından tanınmayabilir ve bu nedenle bilgisayar etki alanı güvenini kaybeder. Bu, kalıcı olmayan VDI uygulamalarını ve işletim sistemi biriminde kalıcı değişikliklere izin vermeyen yazma filtreleri olan cihazları da bozabilir. Bazı kuruluşlar, kendilerini bu öneriden muaf tutmayı seçebilir ve bu durumlar için makine hesabı parola süresinin dolmasını devre dışı bırakabilir.

**Gerekçe:**

Active Directory tabanlı etki alanlarında, her bilgisayarın tıpkı her kullanıcı gibi bir hesabı ve parolası vardır. Varsayılan olarak, etki alanı üyeleri, etki alanı parolalarını her 30 günde bir otomatik olarak değiştirir. Bu aralığı önemli ölçüde artırırsanız veya bilgisayarların artık parolalarını değiştirmemesi için 0'a ayarlarsanız, saldırganın bir veya daha fazla bilgisayar hesabının parolasını tahmin etmek için kaba kuvvet saldırısı gerçekleştirmesi için daha fazla zamanı olacaktır.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:** Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\System\CurrentControlSet\Services\Netlogon\Parameters:Maxi mumPasswordAge*

**Düzeltme:** GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu 30 veya daha az güne ayarlayın, ancak 0 değil :

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Etki Alanı üyesi: Maksimum makine hesabı parolası yaşı*

**2.3.6.6 (L1) 'Etki Alanı üyesi: Güçlü (Windows 2000 veya üzeri) oturum anahtarı gerektir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı etkinleştirildiğinde, yalnızca güçlü bir (128 bit) oturum anahtarıyla güvenli kanal verilerini şifreleyebilen Etki Alanı Denetleyicileri ile güvenli bir kanal oluşturulabilir. Bu ilke ayarını etkinleştirmek için, etki alanındaki tüm Etki Alanı Denetleyicileri, güvenli kanal verilerini güçlü bir anahtarla şifreleyebilmelidir; bu, tüm Etki Alanı Denetleyicilerinin Microsoft Windows 2000 veya daha yenisini çalıştırması gerektiği anlamına gelir. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Etki Alanı Denetleyicileri ile üye bilgisayarlar arasında güvenli kanal iletişimi kurmak için kullanılan oturum anahtarları, Windows 2000'de önceki Microsoft işletim sistemlerinde olduğundan çok daha güçlüdür. Mümkün olduğunda, güvenli kanal iletişimlerini ağ oturumlarını ele geçirmeye ve gizlice dinlemeye çalışan saldırılardan korumaya yardımcı olmak için bu daha güçlü oturum anahtarlarından yararlanmalısınız. (Dinleme, ağ verilerinin aktarım sırasında okunduğu veya değiştirildiği bir bilgisayar korsanlığı biçimidir. Veriler, göndereni gizlemek veya değiştirmek veya yeniden yönlendirilmek üzere değiştirilebilir.)

**Etki:**

Yok - bu varsayılan davranıştır. Ancak, bilgisayarlar Windows NT 4.0 etki alanlarına katılamaz ve Active Directory etki alanları ile Windows NT stili etki alanları arasındaki güvenler düzgün çalışmayabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Netlogon\Parameters:Requ ireStrongKey*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Etki Alanı üyesi: Güçlü (Windows 2000 veya üstü) oturum anahtarı gerektir*

**2.3.7 İnteraktif oturum açma**

**2.3.7.1 (L1) 'Etkileşimli oturum açma: CTRL+ALT+DEL tuşlarına basmayın' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların oturum açmadan önce CTRL+ALT+DEL tuşlarına basıp basmayacağını belirler. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Microsoft bu özelliği, belirli türde fiziksel engelleri olan kullanıcıların Windows çalıştıran bilgisayarlarda oturum açmasını kolaylaştırmak için geliştirmiştir. Kullanıcıların CTRL+ALT+DEL tuşlarına basması gerekmiyorsa, parolalarını ele geçirmeye çalışan saldırılara açıktırlar. Oturum açmadan önce CTRL+ALT+DEL gerekliyse, kullanıcı parolaları güvenilir bir yol aracılığıyla iletilir. Saldırgan, standart Windows oturum açma iletişim kutusuna benzeyen bir Truva atı programı yükleyebilir ve kullanıcının parolasını yakalayabilir. Saldırgan daha sonra, kullanıcının sahip olduğu ayrıcalık düzeyi ne olursa olsun, güvenliği ihlal edilmiş hesapta oturum açabilir.

**Etki:**

Kullanıcılar, Windows oturumu açmak için akıllı kart kullanmıyorlarsa, Windows'ta oturum açmadan önce CTRL+ALT+DEL tuşlarına basmalıdır. Akıllı kart, güvenlik bilgilerini saklayan, kurcalamaya karşı korumalı bir cihazdır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: DisableCAD*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Etkileşimli oturum açma: CTRL+ALT+DEL gerektirmez*

**2.3.7.2 (L1) 'Etkileşimli oturum açma: Son oturum açılanları görüntüleme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kuruluşunuzdaki istemci bilgisayarlarda oturum açan son kullanıcının hesap adının her bilgisayarın ilgili Windows oturum açma ekranında görüntülenip görüntülenmeyeceğini belirler. Davetsiz misafirlerin kuruluşunuzdaki masaüstü veya dizüstü bilgisayarların ekranlarından hesap adlarını görsel olarak toplamasını önlemek için bu ilke ayarını etkinleştirin. Bu ayar için önerilen durum: Etkin.

**Gerekçe**:

Konsola erişimi olan bir saldırgan (örneğin, fiziksel erişimi olan veya sunucuya Uzak Masaüstü Hizmetleri aracılığıyla bağlanabilen biri) sunucuda oturum açan son kullanıcının adını görebilir. Saldırgan daha sonra parolayı tahmin etmeye çalışabilir, bir sözlük kullanabilir veya oturum açmayı denemek için bir kaba kuvvet saldırısı kullanabilir.

**Etki:**

Başarılı bir şekilde oturum açan son kullanıcının adı, Windows oturum açma ekranında görüntülenmeyecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: DontDisplayLastUserName*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Etkileşimli oturum açma: Son oturum açmayı gösterme*

**2.3.7.3 (BL) 'Etkileşimli oturum açma: Makine hesabı kilitleme eşiği' seçeneği '10 veya daha az geçersiz oturum açma girişimi, ancak 0 değil' olarak ayarlanmalıdır.**

**Açıklama:**

Bu güvenlik ayarı, makinenin kilitlenmesine neden olan başarısız oturum açma girişimlerinin sayısını belirler. CTRL+ALT+DELETE veya parola korumalı ekran koruyucular kullanılarak kilitlenen iş istasyonlarına veya üye sunuculara yönelik başarısız parola girişimleri, başarısız oturum açma girişimleri olarak sayılır. Makine kilitleme ilkesi, yalnızca işletim sistemi birimlerini korumak için BitLocker'ın etkinleştirildiği makinelerde uygulanır. Lütfen uygun kurtarma parolası yedekleme ilkelerinin etkinleştirildiğinden emin olun. Bu ayar için önerilen durum: 10 veya daha az geçersiz oturum açma girişimidir, ancak 0 değil.

**Not:** 0 değeri, makine hesabı kilitleme eşiğini devre dışı bıraktığı için karşılaştırmaya uymaz. 1'den 3'e kadar olan değerler 4 olarak yorumlanacaktır.

**Gerekçe:**

Bir makine kaybolursa veya çalınırsa ya da içeriden bir tehdit bilgisayara karşı bir kaba kuvvet parola saldırısı girişiminde bulunursa, BitLocker'ın bilgisayarı kilitleyeceğinden emin olmak önemlidir ve bu nedenle başarılı bir saldırı.

**Etki:**

Kullanıcılar parolalarını birkaç kez yanlış yazabilecekler, ancak bir kaba kuvvet parola saldırısı gerçekleşirse makine hesabı kilitlenecek. Kilitlenen bir makine yalnızca konsolda BitLocker kurtarma anahtarı sağlanarak kurtarılabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: MaxDevicePasswordFailedAttempts*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu 10 veya daha az geçersiz oturum açma girişimi olarak ayarlayın, ancak 0 değil:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Etkileşimli oturum açma: Makine hesabı kilitleme eşiği*

**2.3.7.4 (L1) 'Etkileşimli oturum açma: Makine hareketsizlik sınırı' seçeneği '900 veya daha az saniye, ancak 0 değil' olarak ayarlanmalıdır. (Otomatik)**

**Açıklama:**

Windows, bir oturum açma oturumunun etkin olmadığını fark eder ve etkin olmayan süre, etkinlik dışı kalma sınırını aşarsa, ekran koruyucu çalışarak oturumu kilitler. Bu ayar için önerilen durum: 900 veya daha az saniyedir, ancak 0 değil.

**Not:** 0 değeri, makine hareketsizlik sınırını devre dışı bıraktığı için kıyaslama ile uyumlu değildir.

**Gerekçe:**

Bir kullanıcı, uzaklaşırken bilgisayarını kilitlemeyi unutursa, yoldan geçen birinin onu ele geçirmesi olasıdır.

**Etki:**

Belirtilen süre boyunca bilgisayar başında kimse olmadığında ekran koruyucu otomatik olarak etkinleşir. Ekran koruyucu varsayılan olarak etkinleştirildiğinden etki minimum düzeyde olmalıdır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: InactivityTimeoutSecs*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu 900 veya daha az saniyeye ayarlayın, ancak 0:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Etkileşimli oturum açma: Makine hareketsizlik sınırı*

**2.3.7.5 (L1) 'Etkileşimli oturum açma: Oturum açmaya çalışan kullanıcılar için ileti metni' seçeneği 'Mesaj yok' olarak ayarlanmalıdır. (Otomatik)**

**Açıklama:**

Bu ilke ayarı, oturum açtıklarında kullanıcılara görüntülenen bir metin mesajını belirtir. Aşağıdaki grup ilkesini, kuruluşunuzun güvenlik ve operasyonel gereksinimleriyle tutarlı bir değere ayarlayın.

**Gerekçe:**

Oturum açmadan önce bir uyarı mesajının görüntülenmesi, saldırganı yanlış davranışının sonuçları hakkında daha gerçekleşmeden önce uyararak saldırıyı önlemeye yardımcı olabilir. Ayrıca, oturum açma işlemi sırasında çalışanları uygun politika konusunda bilgilendirerek şirket politikasını güçlendirmeye yardımcı olabilir. Bu metin genellikle yasal nedenlerle kullanılır; örneğin, kullanıcıları şirket bilgilerini kötüye kullanmanın sonuçları hakkında uyarmak veya eylemlerinin denetlenebileceği konusunda onları uyarmak.

**Not:** Gösterdiğiniz herhangi bir uyarı, öncelikle kuruluşunuzun yasal ve insan kaynakları temsilcileri tarafından onaylanmalıdır.

**Etki:**

Kullanıcıların bilgisayarda oturum açabilmeleri için yapılandırılmış metni içeren bir iletişim kutusunu onaylamaları gerekir.

**Not:** Windows Vista ve Windows XP Professional, uzunluğu 512 karakteri geçebilen ve satır başı satır besleme dizileri içerebilen oturum açma başlıklarını destekler. Ancak, Windows 2000 tabanlı istemciler bu iletileri yorumlayamaz ve görüntüleyemez. Windows 2000 tabanlı bilgisayarlar için geçerli olan bir oturum açma iletisi ilkesi oluşturmak için Windows 2000 tabanlı bir bilgisayar kullanmanız gerekir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: LegalNoticeText*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, kuruluşunuzun güvenlik ve işletim gereksinimleriyle tutarlı bir değere göre aşağıdaki UI yolunu yapılandırın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\ Etkileşimli oturum açma: Oturum açmaya çalışan kullanıcılar için mesaj metni*

**2.3.7.6 (L1) 'Etkileşimli oturum açma: Oturum açmaya çalışan kullanıcılar için ileti başlığı' seçeneği 'Mesaj Yok' olarak ayarlanmalıdır. (Otomatik)**

**Açıklama:**

Bu ilke ayarı, kullanıcıların sistemde oturum açtıklarında gördükleri pencerenin başlık çubuğunda görüntülenen metni belirtir. Bu ayarı, kuruluşunuzun güvenlik ve işletim gereksinimleriyle tutarlı olacak şekilde yapılandırın.

**Gerekçe:**

Oturum açmadan önce bir uyarı mesajının görüntülenmesi, saldırganı yanlış davranışının sonuçları hakkında daha gerçekleşmeden önce uyararak saldırıyı önlemeye yardımcı olabilir. Ayrıca, oturum açma işlemi sırasında çalışanları uygun politika konusunda bilgilendirerek şirket politikasını güçlendirmeye yardımcı olabilir.

**Etki:**

Kullanıcıların bilgisayarda oturum açabilmeleri için önce yapılandırılmış başlık içeren bir iletişim kutusunu onaylamaları gerekir.

**Denetim**:

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: LegalNoticeCaption*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu aşağıdakiyle tutarlı bir değere yapılandırın: kuruluşunuzun güvenlik ve operasyonel gereksinimleri:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Etkileşimli oturum açma: Oturum açmaya çalışan kullanıcılar için ileti başlığı*

**2.3.7.7 (L2) 'Etkileşimli oturum açma: Önbelleğe alınacak önceki oturum açma sayısı (etki alanı denetleyicisinin kullanılamaması durumunda)' ifadesi '4 veya daha az oturum açma' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir kullanıcının önbelleğe alınmış hesap bilgilerini kullanarak bir Windows etki alanında oturum açıp açamayacağını belirler. Etki alanı hesapları için oturum açma bilgileri, bir Etki Alanı Denetleyicisi ile bağlantı kurulamasa bile kullanıcıların oturum açmasına izin vermek için yerel olarak önbelleğe alınabilir. Bu ilke ayarı, oturum açma bilgilerinin yerel olarak önbelleğe alındığı benzersiz kullanıcıların sayısını belirler. Bu değer 0 olarak ayarlanırsa, oturum açma önbelleği özelliği devre dışı bırakılır. Sunucunun dosya sistemine erişebilen bir saldırgan, bu önbelleğe alınmış bilgileri bulabilir ve kullanıcı parolalarını belirlemek için kaba kuvvet saldırısı kullanabilir. Bu ayar için önerilen durum: 4 veya daha az oturum açma.

**Gerekçe:**

Bu ilke ayarına atanan sayı, bilgisayarın oturum açma bilgilerini yerel olarak önbelleğe alacağı kullanıcıların sayısını belirtir. Sayı 4 olarak ayarlanırsa, bilgisayar 4 kullanıcı için oturum açma bilgilerini önbelleğe alır. 5. bir kullanıcı bilgisayarda oturum açtığında, sunucu önbelleğe alınmış en eski oturum açma oturumunun üzerine yazar. Bilgisayar konsoluna erişen kullanıcıların oturum açma kimlik bilgileri o bilgisayarda önbelleğe alınır. Bilgisayarın dosya sistemine erişebilen bir saldırgan, bu önbelleğe alınmış bilgileri bulabilir ve kullanıcı parolalarını belirlemeye çalışmak için kaba kuvvet saldırısı kullanabilir. Bu tür bir saldırıyı azaltmak için Windows bilgileri şifreler ve fiziksel konumunu gizler.

**Etki:**

Kimliklerini doğrulayacak bir Etki Alanı Denetleyicisi yoksa, kullanıcılar hiçbir bilgisayarda oturum açamaz. Kuruluşlar, özellikle mobil kullanıcılar için son kullanıcı bilgisayarları için bu değeri 2 olarak yapılandırmak isteyebilir. 2 yapılandırma değeri, BT departmanının bir üyesi sistem bakımını gerçekleştirmek için bilgisayarında yakın zamanda oturum açmış olsa bile, kullanıcının oturum açma bilgilerinin önbellekte kalacağı anlamına gelir. Bu yöntem, kullanıcıların kuruluşun ağına bağlı olmadıklarında bilgisayarlarında oturum açmalarına olanak tanır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon:CachedLogonsCount*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu 4 veya daha az oturum açmaya ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Etkileşimli oturum açma: Önbelleğe alınacak önceki oturum açma sayısı (etki alanı denetleyicisi kullanılamıyorsa)*

**2.3.7.8 (L1) 'Etkileşimli oturum açma: Kullanıcıdan süre dolmadan önce parolayı değiştirmesini iste' seçeneği '5 ila 14 gün arasında' olarak ayarlanmalıdır. (Otomatik)**

**Açıklama:**

Bu ilke ayarı, kullanıcıların parolalarının süresinin dolacağı konusunda ne kadar önceden uyarılacağını belirler. Kullanıcıları parolalarının süresi dolduğunda yeterince uyarmak için bu ilke ayarını en az 5 gün, en fazla 14 gün olacak şekilde yapılandırmanız önerilir. Bu ayar için önerilen durum: 5 ila 14 gün arasındadır.

**Gerekçe:**

Kullanıcıların parolalarının süresinin dolacağı konusunda uyarılması gerekir veya parolaları sona erdiğinde yanlışlıkla bilgisayardan kilitlenebilirler. Bu durum, ağa yerel olarak erişen kullanıcılar için kafa karışıklığına neden olabilir veya kullanıcıların çevirmeli veya sanal özel ağ (VPN) bağlantıları aracılığıyla kuruluşunuzun ağına erişmesini imkansız hale getirebilir.

**Etki:**

Kullanıcılar, parolalarının süresi 5 ila 14 gün arasında sona erecek şekilde yapılandırıldığında etki alanında her oturum açtıklarında parolalarını değiştirmeleri için bir iletişim kutusu istemi görür.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon:PasswordExpiryWarning*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu 5 ila 14 gün arasında bir değere ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Etkileşimli oturum açma: Süre dolmadan önce kullanıcıdan parolayı değiştirmesini isteyin*

**2.3.7.9 (L1) 'Etkileşimli oturum açma: Akıllı kart çıkarma davranışı' seçeneği 'İş İstasyonunu Kilitle' veya üstü (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, oturum açmış bir kullanıcının akıllı kartı akıllı kart okuyucusundan kaldırıldığında ne olacağını belirler. Bu ayar için önerilen durum şudur: İş İstasyonunu Kilitle. Bir Uzak Masaüstü Hizmetleri oturumu da karşılaştırmaya uyuyorsa, bu ayarı Oturumu Kapatmaya veya Bağlantıyı Kesmeye Zorlayacak şekilde yapılandırma.

**Gerekçe:**

Kullanıcılar bazen kendilerinden uzaktayken iş istasyonlarını kilitlemeyi unutarak kötü niyetli kullanıcıların bilgisayarlarına erişmesine olanak tanır. Kimlik doğrulama için akıllı kartlar kullanılıyorsa, kart çıkarıldığında, yalnızca akıllı karta sahip kullanıcının bu kimlik bilgilerini kullanarak kaynaklara erişmesini sağlamak için bilgisayar kendini otomatik olarak kilitlemelidir.

**Etki:**

İş İstasyonunu Kilitle'yi seçerseniz, akıllı kart çıkarıldığında iş istasyonu kilitlenir ve kullanıcıların alandan ayrılmalarına, akıllı kartlarını yanlarına almalarına ve yine de korumalı bir oturum sürdürmelerine olanak tanır. Zorla Oturumu Kapat'ı seçerseniz, akıllı kartları çıkarıldığında kullanıcıların oturumları otomatik olarak kapatılır. Uzak Masaüstü Hizmetleri oturumunda Bağlantıyı Kes'i seçerseniz, akıllı kartın kaldırılması, kullanıcıların oturumunu kapatmadan oturumun bağlantısını keser. Bu, kullanıcının akıllı kartı takmasına ve oturumu daha sonra veya akıllı kart okuyucusu olan başka bir bilgisayarda, yeniden oturum açmak zorunda kalmadan sürdürmesine olanak tanır. Oturum yerelse, bu politika İş İstasyonunu Kilitle ile aynı şekilde çalışır. Görevlerini yerine getirmek için birden fazla bilgisayarda oturum açması gereken kişiler tarafından kullanılan bilgisayarlarda bu ayarın uygulanması sinir bozucu olabilir ve üretkenliği azaltabilir. Örneğin, ağ yöneticileri tek bir hesapla sınırlıysa, ancak ağı etkin bir şekilde yönetmek için aynı anda birkaç bilgisayarda oturum açmaları gerekiyorsa, bu ayarı uygulamak onları bir seferde bir bilgisayarda oturum açmakla sınırlayacaktır. Bu nedenlerle, bu ayarın yalnızca belge oluşturma ve e-posta gibi tipik kullanıcılarla yaygın olarak ilişkilendirilen amaçlar için kullanılan iş istasyonlarında uygulanması önerilir.

**Denetim:**

İyileştirme bölümünde belirtilen Kullanıcı Arabirimi Yoluna gidin ve bir Uzak Masaüstü Hizmetleri oturumu varsa Oturumu Kapatmaya Zorla veya Bağlantıyı Kes değerlerinin de kabul edilebilir ayarlar olduğuna dikkat ederek, belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon:ScRemoveOption*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu İş İstasyonunu Kilitle olarak ayarlayın (veya ortamınız, Uzak Masaüstü Hizmetleri oturumuysa Oturumu Kapatmaya Zorla veya Bağlantıyı Kes):

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Etkileşimli oturum açma: Akıllı kart kaldırma davranışı*

**2.3.8 Microsoft ağ istemcisi**

**2.3.8.1 (L1) 'Microsoft ağ istemcisi: İletişimi dijital olarak imzala (her zaman)' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, SMB istemci bileşeni tarafından paket imzalamanın gerekli olup olmadığını belirler.

**Not:** Windows Vista tabanlı bilgisayarlarda bu ilke ayarı etkinleştirildiğinde ve uzak sunuculardaki dosya veya yazdırma paylaşımlarına bağlandıklarında, ayarın tamamlayıcı ayarı olan Microsoft ağ sunucusu: İletişimleri dijital olarak imzala (her zaman) ile eşitlenmesi önemlidir. bu sunucular. Bu ayarlar hakkında daha fazla bilgi için, Tehditler ve Önlemler kılavuzunun 5. Bölümündeki "**Microsoft ağ istemcisi ve sunucusu: İletişimleri dijital olarak imzala (ilgili dört ayar)**" bölümüne bakın. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Oturum kaçırma, istemci veya sunucu ile aynı ağa erişimi olan saldırganların devam eden bir oturumu kesmesine, sonlandırmasına veya çalmasına izin veren araçları kullanır. Saldırganlar potansiyel olarak imzasız SMB paketlerini yakalayabilir ve değiştirebilir ve ardından trafiği değiştirebilir ve sunucunun istenmeyen eylemler gerçekleştirebilmesi için iletebilir. Alternatif olarak, saldırgan meşru kimlik doğrulamasından sonra sunucu veya istemci gibi davranabilir ve verilere yetkisiz erişim elde edebilir. SMB, birçok Windows işletim sistemi tarafından desteklenen kaynak paylaşım protokolüdür. NetBIOS ve diğer birçok protokolün temelidir. SMB imzaları, hem kullanıcıların hem de verileri barındıran sunucuların kimliğini doğrular. Her iki taraf da kimlik doğrulama sürecinde başarısız olursa, veri aktarımı gerçekleşmeyecektir.

**Etki:**

Microsoft ağ istemcisi, bu sunucu SMB paket imzalamayı kabul etmedikçe bir Microsoft ağ sunucusuyla iletişim kurmayacaktır. SMB dosya ve baskı paylaşım protokolünün Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional ve Windows Vista uygulamaları, karşılıklı kimlik doğrulamayı destekler, bu da oturum ele geçirme saldırılarını önler ve ortadaki adamı önlemek için mesaj kimlik doğrulamasını destekler saldırılar. SMB imzalama, her SMB'ye dijital imza yerleştirerek bu kimlik doğrulamasını sağlar ve bu imza daha sonra hem istemci hem de sunucu tarafından doğrulanır. Her paketin imzalanması ve doğrulanması gerektiğinden, SMB imzalamanın uygulanması performansı olumsuz etkileyebilir. Bu ayarlar, Etki Alanı Denetleyicisi olarak hizmet veren küçük işletme sunucusu gibi birden çok rol gerçekleştiren bir sunucuda etkinleştirilirse, dosya sunucusu, yazdırma sunucusu ve uygulama sunucusu performansı önemli ölçüde yavaşlayabilir. Ayrıca, bilgisayarları tüm imzasız SMB iletişimlerini yok sayacak şekilde yapılandırırsanız, eski uygulamalar ve işletim sistemleri bağlanamaz. Ancak, tüm SMB imzalamayı tamamen devre dışı bırakırsanız, bilgisayarlar oturum ele geçirme saldırılarına karşı savunmasız kalır. Windows Server 2003 çalıştıran Etki Alanı Denetleyicilerinde ve Windows Vista SP1 veya Windows Server 2008 çalıştıran üye bilgisayarlarda SMB imzalama ilkeleri etkinleştirildiğinde grup ilkesi işleme başarısız olur. Microsoft'tan bu sorunu çözen bir düzeltme bulunmaktadır; daha fazla ayrıntı için 950876 numaralı Microsoft Bilgi Bankası makalesine bakın: [Belirli SMB imzalama ilkeleri etkinleştirildiğinde, Windows Server 2008 veya Windows Vista SP1 çalıştıran üye bilgisayarlarda Grup İlkesi ayarları uygulanmaz.](https://support.microsoft.com/en-us/kb/950876)

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters:RequireSecuritySignature*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarlar\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Microsoft ağ istemcisi: İletişimleri dijital olarak imzala (her zaman)*

**2.3.8.2 (L1) 'Microsoft ağ istemcisi: İletişimi dijital olarak imzala (sunucu kabul ederse)' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, SMB istemcisinin SMB paket imzalama konusunda anlaşmaya çalışıp çalışmayacağını belirler.

**Not:** Ağınızdaki SMB istemcilerinde bu ilke ayarını etkinleştirmek, onları ortamınızdaki tüm istemciler ve sunucularla paket imzalama için tamamen etkili hale getirir. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Oturum kaçırma, istemci veya sunucu ile aynı ağa erişimi olan saldırganların devam eden bir oturumu kesmesine, sonlandırmasına veya çalmasına izin veren araçları kullanır. Saldırganlar potansiyel olarak imzasız SMB paketlerini yakalayabilir ve değiştirebilir ve ardından trafiği değiştirebilir ve sunucunun istenmeyen eylemler gerçekleştirebilmesi için iletebilir. Alternatif olarak, saldırgan meşru kimlik doğrulamasından sonra sunucu veya istemci gibi davranabilir ve verilere yetkisiz erişim elde edebilir. SMB, birçok Windows işletim sistemi tarafından desteklenen kaynak paylaşım protokolüdür. NetBIOS ve diğer birçok protokolün temelidir. SMB imzaları, hem kullanıcıların hem de verileri barındıran sunucuların kimliğini doğrular. Her iki taraf da kimlik doğrulama sürecinde başarısız olursa, veri aktarımı gerçekleşmeyecektir.

**Etki:**

Yok - bu varsayılan davranıştır. SMB dosya ve baskı paylaşım protokolünün Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional ve Windows Vista uygulamaları, karşılıklı kimlik doğrulamayı destekler, bu da oturum ele geçirme saldırılarını önler ve ortadaki adamı önlemek için mesaj kimlik doğrulamasını destekler saldırılar. SMB imzalama, her SMB'ye dijital imza yerleştirerek bu kimlik doğrulamasını sağlar ve bu imza daha sonra hem istemci hem de sunucu tarafından doğrulanır. Her paketin imzalanması ve doğrulanması gerektiğinden, SMB imzalamanın uygulanması performansı olumsuz etkileyebilir. Bu ayarlar, Etki Alanı Denetleyicisi olarak hizmet veren küçük işletme sunucusu gibi birden çok rol gerçekleştiren bir sunucuda etkinleştirilirse, dosya sunucusu, yazdırma sunucusu ve uygulama sunucusu performansı önemli ölçüde yavaşlayabilir. Ayrıca, bilgisayarları tüm imzasız SMB iletişimlerini yok sayacak şekilde yapılandırırsanız, eski uygulamalar ve işletim sistemleri bağlanamaz. Ancak, tüm SMB imzalamayı tamamen devre dışı bırakırsanız, bilgisayarlar oturum ele geçirme saldırılarına karşı savunmasız kalır. Windows Server 2003 çalıştıran Etki Alanı Denetleyicilerinde ve Windows Vista SP1 veya Windows Server 2008 çalıştıran üye bilgisayarlarda SMB imzalama ilkeleri etkinleştirildiğinde grup ilkesi işleme başarısız olur. Microsoft'tan bu sorunu çözen bir düzeltme bulunmaktadır; daha fazla ayrıntı için 950876 numaralı Microsoft Bilgi Bankası makalesine bakın: [Belirli SMB imzalama ilkeleri etkinleştirildiğinde, Windows Server 2008 veya Windows Vista SP1 çalıştıran üye bilgisayarlarda Grup İlkesi ayarları uygulanmaz.](https://support.microsoft.com/en-us/kb/950876)

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters:EnableSecuritySignature*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarlar\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Microsoft ağ istemcisi: İletişimleri dijital olarak imzala (sunucu kabul ederse)*

**2.3.8.3 (L1) 'Microsoft ağ istemcisi: Üçüncü taraf SMB sunucularına şifrelenmemiş parola gönder' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, SMB yeniden yönlendiricisinin, kimlik doğrulaması sırasında parola şifrelemesini desteklemeyen üçüncü taraf SMB sunucularına düz metin parolaları gönderip göndermeyeceğini belirler. Etkinleştirmek için güçlü bir iş gerekçesi olmadığı sürece bu ilke ayarını devre dışı bırakmanız önerilir. Bu ilke ayarı etkinleştirilirse, ağ genelinde şifrelenmemiş parolalara izin verilir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bu ilke ayarını etkinleştirirseniz, sunucu, önemli bir güvenlik riski olan SMB hizmetleri sunan diğer bilgisayarlara ağ üzerinden düz metin olarak parolalar iletebilir. Bu diğer bilgisayarlar, Windows Server 2003'te bulunan SMB güvenlik mekanizmalarından hiçbirini kullanamaz.

**Etki:**

Yok - bu varsayılan davranıştır. MS-DOS, Windows for Workgroups 3.11 ve Windows 95a gibi bazı çok eski uygulamalar ve işletim sistemleri, SMB protokolü aracılığıyla kuruluşunuzdaki sunucularla iletişim kuramıyor olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanWorkstation\Parameters:EnablePlainTextPassword*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Microsoft ağ istemcisi: Üçüncü taraf SMB sunucularına şifrelenmemiş parola gönder*

**2.3.9 Microsoft ağ sunucusu**

**2.3.9.1 (L1) 'Microsoft ağ sunucusu: Oturumu askıya almadan önce gereken boşta kalma süresi' seçeneği '15 dakika veya daha az' olarak ayarlanmalıdır. (Otomatik)**

**Açıklama:**

Bu ilke ayarı, etkinlik olmaması nedeniyle oturum askıya alınmadan önce bir SMB oturumunda geçmesi gereken sürekli boşta kalma süresini belirtmenize olanak tanır. Yöneticiler, bir bilgisayarın etkin olmayan bir SMB oturumunu ne zaman askıya alacağını kontrol etmek için bu ilke ayarını kullanabilir. İstemci etkinliği devam ederse, oturum otomatik olarak yeniden kurulur. Maksimum değer, 69 günden fazla olan 99999'dur; aslında bu değer ayarı devre dışı bırakır. Bu ayar için önerilen durum: 15 veya daha az dakika.

**Gerekçe:**

Her SMB oturumu sunucu kaynaklarını tüketir ve çok sayıda boş oturum sunucuyu yavaşlatır veya muhtemelen başarısız olmasına neden olur. Saldırgan, sunucunun SMB hizmetleri yavaşlayana veya yanıt vermemeye başlayana kadar art arda SMB oturumları oluşturabilir.

**Etki:**

İstemci faaliyete devam ederse SMB oturumları otomatik olarak yeniden kurulacağından çok az etki olacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters: AutoDisconnect*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu 15 veya daha az dakikaya ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Microsoft ağ sunucusu: Boşta kalma miktarı oturumu askıya almadan önce gereken süre*

**2.3.9.2 (L1) 'Microsoft ağ sunucusu: İletişimi dijital olarak imzala (her zaman)' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, SMB sunucu bileşeni tarafından paket imzalamanın gerekli olup olmadığını belirler. Aşağı akış istemcilerinin iş istasyonunu bir ağ sunucusu olarak kullanmasını önlemek için bu ilke ayarını karma bir ortamda etkinleştirin. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Oturum kaçırma, istemci veya sunucu ile aynı ağa erişimi olan saldırganların devam eden bir oturumu kesmesine, sonlandırmasına veya çalmasına izin veren araçları kullanır. Saldırganlar potansiyel olarak imzasız SMB paketlerini yakalayabilir ve değiştirebilir ve ardından trafiği değiştirebilir ve sunucunun istenmeyen eylemler gerçekleştirebilmesi için iletebilir. Alternatif olarak, saldırgan meşru kimlik doğrulamasından sonra sunucu veya istemci gibi davranabilir ve verilere yetkisiz erişim elde edebilir. SMB, birçok Windows işletim sistemi tarafından desteklenen kaynak paylaşım protokolüdür. NetBIOS ve diğer birçok protokolün temelidir. SMB imzaları, hem kullanıcıların hem de verileri barındıran sunucuların kimliğini doğrular. Her iki taraf da kimlik doğrulama sürecinde başarısız olursa, veri aktarımı gerçekleşmeyecektir.

**Etki:**

Microsoft ağ sunucusu, bu istemci SMB paket imzalamayı kabul etmedikçe bir Microsoft ağ istemcisiyle iletişim kurmayacaktır. SMB dosya ve baskı paylaşım protokolünün Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional ve Windows Vista uygulamaları, karşılıklı kimlik doğrulamayı destekler, bu da oturum ele geçirme saldırılarını önler ve ortadaki adamı önlemek için mesaj kimlik doğrulamasını destekler saldırılar. SMB imzalama, her SMB'ye dijital imza yerleştirerek bu kimlik doğrulamasını sağlar ve bu imza daha sonra hem istemci hem de sunucu tarafından doğrulanır. Her paketin imzalanması ve doğrulanması gerektiğinden, SMB imzalamanın uygulanması performansı olumsuz etkileyebilir. Bu ayarlar, Etki Alanı Denetleyicisi olarak hizmet veren küçük işletme sunucusu gibi birden çok rol gerçekleştiren bir sunucuda etkinleştirilirse, dosya sunucusu, yazdırma sunucusu ve uygulama sunucusu performansı önemli ölçüde yavaşlayabilir. Ayrıca, bilgisayarları tüm imzasız SMB iletişimlerini yok sayacak şekilde yapılandırırsanız, eski uygulamalar ve işletim sistemleri bağlanamaz. Ancak, tüm SMB imzalamayı tamamen devre dışı bırakırsanız, bilgisayarlar oturum ele geçirme saldırılarına karşı savunmasız kalır. Windows Server 2003 çalıştıran Etki Alanı Denetleyicilerinde ve Windows Vista SP1 veya Windows Server 2008 çalıştıran üye bilgisayarlarda SMB imzalama ilkeleri etkinleştirildiğinde grup ilkesi işleme başarısız olur. Microsoft'tan bu sorunu çözen bir düzeltme bulunmaktadır; daha fazla ayrıntı için 950876 numaralı Microsoft Bilgi Bankası makalesine bakın: [Belirli SMB imzalama ilkeleri etkinleştirildiğinde, Windows Server 2008 veya Windows Vista SP1 çalıştıran üye bilgisayarlarda Grup İlkesi ayarları uygulanmaz.](https://support.microsoft.com/en-us/kb/950876)

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters: RequireSecuritySignature*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları \Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Microsoft ağ sunucusu: İletişimleri dijital olarak imzala (her zaman)*

**2.3.9.3 (L1) 'Microsoft ağ sunucusu: İletişimi dijital olarak imzala (istemci kabul ederse)' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, SMB sunucusunun, onu isteyen istemcilerle SMB paket imzalama konusunda anlaşıp anlaşmayacağını belirler. İstemciden herhangi bir imzalama isteği gelmezse, Microsoft ağ sunucusu: İletişimleri dijital olarak imzala (her zaman) ayarı etkinleştirilmemişse imza olmadan bağlantıya izin verilir.

**Not:** Ortamınızdaki tüm istemciler ve sunucularla paket imzalama için tam olarak etkili olmaları için ağınızdaki SMB istemcilerinde bu ilke ayarını etkinleştirin. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Oturum kaçırma, istemci veya sunucu ile aynı ağa erişimi olan saldırganların devam eden bir oturumu kesmesine, sonlandırmasına veya çalmasına izin veren araçları kullanır. Saldırganlar potansiyel olarak imzasız SMB paketlerini yakalayabilir ve değiştirebilir ve ardından trafiği değiştirebilir ve sunucunun istenmeyen eylemler gerçekleştirebilmesi için iletebilir. Alternatif olarak, saldırgan meşru kimlik doğrulamasından sonra sunucu veya istemci gibi davranabilir ve verilere yetkisiz erişim elde edebilir. SMB, birçok Windows işletim sistemi tarafından desteklenen kaynak paylaşım protokolüdür. NetBIOS ve diğer birçok protokolün temelidir. SMB imzaları, hem kullanıcıların hem de verileri barındıran sunucuların kimliğini doğrular. Her iki taraf da kimlik doğrulama sürecinde başarısız olursa, veri aktarımı gerçekleşmeyecektir.

**Etki:**

Microsoft ağ sunucusu, istemci tarafından istendiği gibi SMB paket imzalama konusunda anlaşır. Diğer bir deyişle, istemcide paket imzalama etkinleştirildiyse, paket imzalama konusunda anlaşmaya varılacaktır. SMB dosya ve baskı paylaşım protokolünün Windows 2000 Server, Windows 2000 Professional, Windows Server 2003, Windows XP Professional ve Windows Vista uygulamaları, karşılıklı kimlik doğrulamayı destekler, bu da oturum ele geçirme saldırılarını önler ve ortadaki adamı önlemek için mesaj kimlik doğrulamasını destekler saldırılar. SMB imzalama, her SMB'ye dijital imza yerleştirerek bu kimlik doğrulamasını sağlar ve bu imza daha sonra hem istemci hem de sunucu tarafından doğrulanır. Her paketin imzalanması ve doğrulanması gerektiğinden, SMB imzalamanın uygulanması performansı olumsuz etkileyebilir. Bu ayarlar, Etki Alanı Denetleyicisi olarak hizmet veren küçük işletme sunucusu gibi birden çok rol gerçekleştiren bir sunucuda etkinleştirilirse, dosya sunucusu, yazdırma sunucusu ve uygulama sunucusu performansı önemli ölçüde yavaşlayabilir. Ayrıca, bilgisayarları tüm imzasız SMB iletişimlerini yok sayacak şekilde yapılandırırsanız, eski uygulamalar ve işletim sistemleri bağlanamaz. Ancak, tüm SMB imzalamayı tamamen devre dışı bırakırsanız, bilgisayarlar oturum ele geçirme saldırılarına karşı savunmasız kalır. Windows Server 2003 çalıştıran Etki Alanı Denetleyicilerinde ve Windows Vista SP1 veya Windows Server 2008 çalıştıran üye bilgisayarlarda SMB imzalama ilkeleri etkinleştirildiğinde grup ilkesi işleme başarısız olur. Microsoft'tan bu sorunu çözen bir düzeltme bulunmaktadır; daha fazla ayrıntı için 950876 numaralı Microsoft Bilgi Bankası makalesine bakın: [Belirli SMB imzalama ilkeleri etkinleştirildiğinde, Windows Server 2008 veya Windows Vista SP1 çalıştıran üye bilgisayarlarda Grup İlkesi ayarları uygulanmaz.](https://support.microsoft.com/en-us/kb/950876)

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters: EnableSecuritySignature*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları \Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Microsoft ağ sunucusu: İletişimleri dijital olarak imzalayın (istemci kabul ederse)*

**2.3.9.4 (L1) 'Microsoft ağ sunucusu: Oturum açma saatleri sona erdiğinde istemcilerin bağlantısını kes' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu güvenlik ayarı, yerel bilgisayara kendi kullanıcı hesaplarının geçerli oturum açma saatleri dışında bağlanan kullanıcıların bağlantısının kesilip kesilmeyeceğini belirler. Bu ayar, Sunucu İleti Bloğu (SMB) bileşenini etkiler. Bu ilke ayarını etkinleştirirseniz, Ağ güvenliğini de etkinleştirmelisiniz: **Oturum açma saatleri sona erdiğinde oturumu kapatmaya zorla (Kural 2.3.11.6).** Kuruluşunuz kullanıcılar için oturum açma saatlerini yapılandırıyorsa, bunların etkili olduğundan emin olmak için bu ilke ayarı gereklidir. Bu ayar için önerilen durum: Etkin. **Gerekçe:**

Kuruluşunuz kullanıcılar için oturum açma saatlerini yapılandırıyorsa, bu ilke ayarını etkinleştirmek mantıklıdır. Aksi takdirde, oturum açma saatleri dışında ağ kaynaklarına erişimi olmaması gereken kullanıcılar, izin verilen saatlerde kurulan oturumlarla bu kaynakları kullanmaya devam edebilirler.

**Etki**:

Yok - bu varsayılan davranıştır. Kuruluşunuzda oturum açma saatleri kullanılmıyorsa, bu ilke ayarının hiçbir etkisi olmaz. Oturum açma saatleri kullanılırsa, oturum açma saatleri sona erdiğinde mevcut kullanıcı oturumları zorla sonlandırılır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters: enableforcedlogoff*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Microsoft ağ sunucusu: Oturum açma saatleri sona erdiğinde istemcilerin bağlantısını kesin*

**2.3.9.5 (L1) 'Microsoft ağ sunucusu: Sunucu SPN hedef adı doğrulama düzeyi' seçeneği 'İstemci tarafından sağlanıyorsa kabul et' veya üstü (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, paylaşılan klasörlere veya yazıcılara (sunucu) sahip bir bilgisayarın, sunucu ileti bloğunu (SMB) kullanarak bir oturum oluşturduğunda istemci bilgisayar tarafından sağlanan hizmet asıl adı (SPN) üzerinde gerçekleştirdiği doğrulama düzeyini denetler. Sunucu mesaj bloğu (SMB) protokolü, dosya ve yazıcı paylaşımı ve uzak Windows yönetimi gibi diğer ağ işlemleri için temel sağlar. SMB protokolü, SMB geçiş saldırıları olarak adlandırılan SMB sunucularına yönelik bir saldırı sınıfını önlemek için bir SMB istemcisi tarafından sağlanan kimlik doğrulama bloğu içindeki SMB sunucusu hizmet asıl adının (SPN) doğrulanmasını destekler. Bu ayar hem SMB1 hem de SMB2'yi etkiler. Bu ayar için önerilen durum şudur: İstemci tarafından sağlandıysa kabul et. Bu ayarın İstemciden gerekli olarak yapılandırılması da kıyaslamayla uyumludur.

**Gerekçe:**

Bir bilgisayarın kimliği, ağ kaynaklarına yetkisiz erişim elde etmek için sahte olabilir.

**Etki:**

Tüm Windows işletim sistemleri, hem istemci tarafı SMB bileşenini hem de sunucu tarafı SMB bileşenini destekler. Bu ayar, sunucu SMB davranışını etkiler ve dosya ve baskı sunma yeteneklerinde kesintileri önlemek için uygulanması dikkatli bir şekilde değerlendirilmeli ve test edilmelidir. İstemci tarafından sağlandıysa Kabul Et olarak yapılandırılırsa, SMB sunucusu, SMB istemcisi tarafından sağlanan SPN'yi kabul eder ve doğrular ve kendisi için SMB sunucusunun SPN listesiyle eşleşirse bir oturumun kurulmasına izin verir. SPN eşleşmezse, o SMB istemcisi için oturum isteği reddedilir. İstemciden gerekli olarak yapılandırılırsa, SMB istemcisi oturum kurulumunda bir SPN adı GÖNDERMELİDİR ve sağlanan SPN adı, bağlantı kurmak için istenen SMB sunucusuyla eşleşmelidir ZORUNLU. İstemci tarafından hiçbir SPN sağlanmazsa veya sağlanan SPN eşleşmezse oturum reddedilir.

**Denetim:** Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters: SMBServerNameHardeningLevel*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, istemci tarafından sağlandıysa aşağıdaki UI yolunu Kabul Et olarak ayarlayın (yapılandırma Gerekli olarak istemciden de kıyaslama ile uyumludur):

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Microsoft ağ sunucusu: Sunucu SPN hedef adı doğrulama düzeyi*

**2.3.10 Ağ erişimi**

**2.3.10.1 (L1) 'Ağ erişimi: Anonim SID/İsim çevirisine izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, anonim bir kullanıcının başka bir kullanıcı için güvenlik tanımlayıcısı (SID) öznitelikleri isteyip isteyemeyeceğini veya karşılık gelen kullanıcı adını almak için bir SID kullanıp kullanamayacağını belirler. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bu ilke ayarı etkinleştirilirse, yerel erişimi olan bir kullanıcı, yeniden adlandırılmış olsa bile yerleşik Yönetici hesabının gerçek adını öğrenmek için iyi bilinen Yöneticinin SID'sini kullanabilir. Bu kişi daha sonra bir parola tahmin saldırısı başlatmak için hesap adını kullanabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Ağ erişimi: Anonim SID/Ad çevirisine izin ver*

**2.3.10.2 (L1) 'Ağ erişimi: SAM hesaplarının anonim numaralandırılmasına izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, anonim kullanıcıların Güvenlik Hesapları Yöneticisi'ndeki (SAM) hesapları numaralandırma yeteneğini kontrol eder. Bu ilke ayarını etkinleştirirseniz, anonim bağlantıları olan kullanıcılar, ortamınızdaki sistemlerde etki alanı hesabı kullanıcı adlarını numaralandıramaz. Bu ilke ayarı, anonim bağlantılarda ek kısıtlamalara da izin verir. Bu ayar için önerilen durum: Etkin.

**Not:** Bu politikanın Etki Alanı Denetleyicileri üzerinde hiçbir etkisi yoktur.

**Gerekçe:**

Yetkisiz bir kullanıcı, hesap adlarını anonim olarak listeleyebilir ve bu bilgileri parolaları tahmin etmeye veya sosyal mühendislik saldırıları gerçekleştirmeye çalışmak için kullanabilir. (Sosyal mühendislik saldırıları, parolaları veya bir tür güvenlik bilgisi elde etmek için kullanıcıları bir şekilde aldatmaya çalışır.)

**Etki:**

Yok - bu varsayılan davranıştır. Windows NT 4.0 tabanlı etki alanları ile güven oluşturmak imkansız olacaktır. Ayrıca, Windows NT 3.51 ve Windows 95 gibi Windows işletim sisteminin eski sürümlerini çalıştıran istemci bilgisayarlar, sunucudaki kaynakları kullanmaya çalıştıklarında sorunlarla karşılaşacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:RestrictAnonymousSAM*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Ağ erişimi: SAM hesaplarının anonim olarak numaralandırılmasına izin verme*

**2.3.10.3 (L1) 'Ağ erişimi: SAM hesaplarının ve paylaşımlarının anonim numaralandırılmasına izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, anonim kullanıcıların paylaşımların yanı sıra SAM hesaplarını da numaralandırma yeteneğini kontrol eder. Bu ilke ayarını etkinleştirirseniz, anonim kullanıcılar, ortamınızdaki sistemlerde etki alanı hesabı kullanıcı adlarını ve ağ paylaşımı adlarını numaralandıramaz. Bu ayar için önerilen durum: Etkin.

**Not:** Bu politikanın Etki Alanı Denetleyicileri üzerinde hiçbir etkisi yoktur.

**Gerekçe:**

Yetkisiz bir kullanıcı, hesap adlarını ve paylaşılan kaynakları anonim olarak listeleyebilir ve bilgileri parolaları tahmin etmeye veya sosyal mühendislik saldırıları gerçekleştirmeye çalışmak için kullanabilir. (Sosyal mühendislik saldırıları, parolaları veya bir tür güvenlik bilgisi elde etmek için kullanıcıları bir şekilde aldatmaya çalışır.)

**Etki:**

Windows NT 4.0 tabanlı etki alanları ile güven oluşturmak imkansız olacaktır. Ayrıca, Windows NT 3.51 ve Windows 95 gibi Windows işletim sisteminin eski sürümlerini çalıştıran istemci bilgisayarlar, sunucudaki kaynakları kullanmaya çalıştıklarında sorunlarla karşılaşacaktır. Dosya ve yazıcı sunucularına anonim olarak erişen kullanıcılar, bu sunuculardaki paylaşılan ağ kaynaklarını listeleyemez; kullanıcıların paylaşılan klasörler ve yazıcılar listelerini görebilmeleri için önce kimlik doğrulaması yapmaları gerekecektir. Ancak, bu ilke ayarı etkinleştirilse bile, anonim kullanıcılar, yerleşik grup olan ANONYMOUS LOGON'u açıkça içeren izinlere sahip kaynaklara erişebilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:RestrictAnonymous*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Ağ erişimi: SAM hesaplarının ve paylaşımlarının anonim olarak numaralandırılmasına izin verme*

**2.3.10.4 (L1) 'Ağ erişimi: Ağ kimlik doğrulaması için şifrelerin ve kimlik bilgilerinin depolanmasına izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Kimlik Bilgileri Yöneticisi'nin (önceden Depolanan Kullanıcı Adları ve Parolalar olarak adlandırılırdı) parolaları veya kimlik bilgilerini, etki alanı kimlik doğrulaması aldığında daha sonra kullanmak üzere kaydedip kaydetmeyeceğini belirler. Bu ayar için önerilen durum: Etkin.

**Not:** Bu ayarda yapılan değişiklikler, Windows yeniden başlatılıncaya kadar geçerli olmayacaktır.

**Gerekçe:**

Önbelleğe alınan parolalara, kullanıcı bilgisayarda oturum açtığında erişilebilir. Bu bilgiler kulağa açık gibi gelse de, kullanıcı bilmeden şifreleri okuyan ve bunları başka bir yetkisiz kullanıcıya ileten düşmanca kod yürütürse bir sorun ortaya çıkabilir.

**Etki:**

Kimlik Bilgisi Yöneticisi, bilgisayarda parolaları ve kimlik bilgilerini saklamaz. Kullanıcılar, Passport hesaplarında veya etki alanı hesaplarına erişilemeyen diğer ağ kaynaklarında her oturum açtıklarında parola girmeye zorlanırlar. Testler, Windows Vista veya Windows Server 2008 çalıştıran istemcilerin güvenilmeyen etki alanlarındaki Dağıtılmış Dosya Sistemi (DFS) paylaşımlarına bağlanamayacaklarını göstermiştir. Bu ayarın etkinleştirilmesi, zamanlanmış görevler için alternatif kimlik bilgilerinin belirtilmesini de imkansız hale getirir; bu, çeşitli sorunlara neden olabilir. Örneğin, bazı üçüncü taraf yedekleme ürünleri artık çalışmayacaktır. Bu ilke ayarının, Active Directory tabanlı etki alanı hesaplarıyla erişime izin verecek şekilde yapılandırılmış ağ kaynaklarına erişen kullanıcılar üzerinde hiçbir etkisi olmamalıdır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:DisableDomainCreds*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Ağ erişimi: Ağ için parolaların ve kimlik bilgilerinin depolanmasına izin verme kimlik doğrulama*

**2.3.10.5 (L1) 'Ağ erişimi: Herkes izinlerinin anonim kullanıcılara uygulanmasına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bilgisayara anonim bağlantılar için hangi ek izinlerin atanacağını belirler. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Yetkisiz bir kullanıcı, hesap adlarını ve paylaşılan kaynakları anonim olarak listeleyebilir ve bilgileri parolaları tahmin etmeye, sosyal mühendislik saldırıları gerçekleştirmeye veya DoS saldırıları başlatmaya çalışmak için kullanabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:EveryoneIncludesAnony mous*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\ Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Ağ erişimi: Herkes izinlerinin anonim kullanıcılara uygulanmasına izin ver*

**2.3.10.6 (L1) 'Ağ erişimi: Adlandırılmış Kanallar anonim olarak ulaşılabilir' seçeneği 'Hiçbiri' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, hangi iletişim oturumlarının veya borularının anonim erişime izin veren niteliklere ve izinlere sahip olacağını belirler. Bu ayar için önerilen durum: (yani Yok).

**Gerekçe:**

Anonim olarak erişilebilen adlandırılmış kanalları sınırlamak, sistemin saldırı yüzeyini azaltacaktır.

**Etki:**

Bu yapılandırma, adlandırılmış kanallar üzerinden boş oturum erişimini devre dışı bırakacak ve bu özelliğe veya adlandırılmış kanallara kimlik doğrulamasız erişime dayanan uygulamalar artık çalışmayacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters: NullSessionPipes*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu (yani Yok):

*Bilgisayar Yapılandırması\İlkeler olarak ayarlayın. \Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Ağ erişimi: Anonim olarak erişilebilen Adlandırılmış Kanallar*

**2.3.10.7 (L1) 'Ağ erişimi: Uzaktan erişilebilir kayıt defteri yolları' yapılandırıldığından emin olun (Otomatik)**

**Açıklama:**

Bu ilke ayarı, winreg kayıt defteri anahtarının erişim denetim listesinde (ACL) listelenen kullanıcılar veya gruplardan bağımsız olarak ağ üzerinden hangi kayıt defteri yollarına erişilebileceğini belirler.

**Not:** Bu ayar Windows XP'de mevcut değildir. Windows XP'de bu ada sahip bir ayar vardı, ancak buna Windows Server 2003, Windows Vista ve Windows Server 2008'de (R2 olmayan) "Ağ erişimi: Uzaktan erişilebilir kayıt defteri yolları ve alt yollar" denir.

**Not #2:** Bu ayarı yapılandırdığınızda, bir veya daha fazla nesnenin bir listesini belirtirsiniz. Listeye girerken kullanılan sınırlayıcı bir satır besleme veya satır başıdır, yani listedeki ilk nesneyi yazın, Enter düğmesine basın, sonraki nesneyi yazın, tekrar Enter'a basın vb. Ayar değeri virgül olarak kaydedilir. grup ilkesi güvenlik şablonlarında sınırlandırılmış liste. Ayrıca Grup İlkesi Düzenleyicisi'nin görüntü bölmesinde ve Sonuç İlke Kümesi konsolunda virgülle ayrılmış bir liste olarak işlenir. Kayıt defterine, REG\_MULTI\_SZ değerinde satır beslemeyle ayrılmış bir liste olarak kaydedilir. Bu ayar için önerilen durum: *System\CurrentControlSet\Control\ProductOptions*

*System\CurrentControlSet\Control\Server Applications*

*Software\Microsoft\Windows NT\CurrentVersion*

**Gerekçe:**

Kayıt defteri, bilgisayar yapılandırma bilgilerini içeren bir veritabanıdır ve bilgilerin çoğu duyarlı. Saldırgan, yetkisiz etkinlikleri kolaylaştırmak için bu bilgileri kullanabilir. Bu tür bir saldırı riskini azaltmak için, kayıt defterinin yetkisiz kullanıcıların erişimine karşı korunmasına yardımcı olmak için kayıt defteri genelinde uygun ACL'ler atanır.

**Etki:**

Yok - bu varsayılan davranıştır. Ancak, erişilebilir olanlar listesinden varsayılan kayıt defteri yollarını kaldırırsanız, bilgisayarları düzgün bir şekilde izlemek ve yönetmek için kayıt defterine uzaktan erişim gerektirdiklerinden Microsoft Baseline Security Analyzer ve Microsoft Systems Management Server gibi uzaktan yönetim araçları başarısız olabilir.

**Not**: Uzaktan erişime izin vermek istiyorsanız, Uzak Kayıt hizmetini de etkinleştirmeniz gerekir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg\ AllowedExactPaths:Machine*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu şu şekilde ayarlayın: *System\CurrentControlSet\Control\ ProductOptions*

*System\CurrentControlSet\Control\Server Applications*

*SOFTWARE\Microsoft\Windows NT\CurrentVersion*

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Ağ erişimi: Uzaktan erişilebilir kayıt yolları*

**2.3.10.8 (L1) 'Ağ erişimi: Uzaktan erişilebilir kayıt defteri yolları ve alt yolları' yapılandırıldığından emin olun (Otomatik)**

**Açıklama:**

Bu ilke ayarı, winreg kayıt defteri anahtarının erişim denetim listesinde (ACL) listelenen kullanıcılar veya gruplardan bağımsız olarak, ağ üzerinden hangi kayıt defteri yollarına ve alt yollarına erişilebileceğini belirler.

**Not:** Windows XP'de bu ayar "Ağ erişimi: Uzaktan erişilebilir kayıt yolları" olarak adlandırılır; Windows Vista, Windows Server 2008 (R2 olmayan) ve Windows Server 2003'te aynı ada sahip ayar Windows XP'de yoktur. Not #2: Bu ayarı yapılandırdığınızda, bir veya daha fazla nesnenin bir listesini belirtirsiniz. Listeye girerken kullanılan sınırlayıcı bir satır besleme veya satır başıdır, yani listedeki ilk nesneyi yazın, Enter düğmesine basın, sonraki nesneyi yazın, tekrar Enter'a basın vb. Ayar değeri virgül olarak kaydedilir. grup ilkesi güvenlik şablonlarında sınırlandırılmış liste. Ayrıca Grup İlkesi Düzenleyicisi'nin görüntü bölmesinde ve Sonuç İlke Kümesi konsolunda virgülle ayrılmış bir liste olarak işlenir. Kayıt defterine, REG\_MULTI\_SZ değerinde satır beslemeyle ayrılmış bir liste olarak kaydedilir. Bu ayar için önerilen durum:

*System\CurrentControlSet\Control\Print\Printers System\CurrentControlSet\Services\Eventlog*

*Software\Microsoft\OLAP Server Software\Microsoft\Windows NT\CurrentVersion\Print Software\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex System\CurrentControlSet\Control\Terminal Server System\CurrentControlSet\Control\Terminal Server\UserConfig System\CurrentControlSet\Control\Terminal Server\DefaultUserConfiguration Software\Microsoft\Windows NT\CurrentVersion\Perflib System\CursControlSet \SysmonLog*

**Gerekçe:**

Kayıt defteri, bir saldırgan tarafından yetkisiz etkinlikleri kolaylaştırmak için kullanılabilecek hassas bilgisayar yapılandırma bilgilerini içerir. Kayıt defteri boyunca atanan varsayılan ACL'lerin oldukça kısıtlayıcı olması ve kayıt defterinin yetkisiz kullanıcıların erişimine karşı korunmasına yardımcı olması, bu tür bir saldırı riskini azaltır. Etki: Yok - bu varsayılan davranıştır. Ancak, erişilebilir olanlar listesinden varsayılan kayıt defteri yollarını kaldırırsanız, bilgisayarları düzgün bir şekilde izlemek ve yönetmek için kayıt defterine uzaktan erişim gerektirdiklerinden Microsoft Baseline Security Analyzer ve Microsoft Systems Management Server gibi uzaktan yönetim araçları başarısız olabilir. Not: Uzaktan erişime izin vermek istiyorsanız, Uzak Kayıt hizmetini de etkinleştirmeniz gerekir. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurePipeServers\Winreg\ AllowedPaths:Machine*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın:

*System\CurrentControlSet\Control\ Print\Printers System\CurrentControlSet\Services\Eventlog*

*YAZILIM\Microsoft\OLAP Server*

*YAZILIM\Microsoft\Windows NT\CurrentVersion\Print*

*YAZILIM\Microsoft\Windows NT\CurrentVersion\Windows System\CurrentControlSet\Control\ContentIndex*

*System\Control\TControlerSet Server System\CurrentControlSet\Control\TerminalServer\UserConfig System\CurrentControlSet\Control\TerminalServer\DefaultUserConfiguration*

*SOFTWARE\Microsoft\Windows NT\CurrentVersion\Perflib System\CurrentControlSet\Services\SysmonLog*

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Log İlkeler\Güvenlik Seçenekleri\Ağ erişimi: Uzaktan erişilebilir kayıt defteri yolları ve alt yolları*

**2.3.10.9 (L1) 'Ağ erişimi: Adlandırılmış Kanallar ve Paylaşımlara anonim erişimi kısıtla' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı etkinleştirildiğinde, anonim erişimi yalnızca Ağ erişimi: Anonim olarak erişilebilen adlandırılmış kanallar ve Ağ erişimi: Anonim olarak erişilebilen paylaşımlar ayarlarında belirtilen paylaşımlara ve kanallara kısıtlar. Bu ilke ayarı, *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters* kayıt defteri anahtarına 1 değeriyle *RestrictNullSessAccess* ekleyerek bilgisayarlarınızdaki paylaşımlara boş oturum erişimini denetler. Bu kayıt defteri değeri, sunucu hizmetinin kimliği doğrulanmamış istemcilerin adlandırılmış kaynaklara erişimini kısıtlayıp kısıtlamadığını denetlemek için boş oturum paylaşımlarını açar veya kapatır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Boş oturumlar, ortamınızdaki bilgisayarlardaki paylaşımlar (varsayılan paylaşımlar dahil) aracılığıyla kullanılabilecek bir zayıflıktır.

**Etki:**

Yok - bu varsayılan davranıştır. Bu ayarı etkinleştirmeyi seçerseniz ve Windows NT 4.0 etki alanlarını destekliyorsanız, etki alanları arasındaki güven ilişkilerini sürdürmek için adlandırılmış kanallardan herhangi birinin gerekli olup olmadığını kontrol etmeli ve ardından kanalı Ağ erişimine: Erişilebilen adlandırılmış kanallara eklemelisiniz. anonim olarak listeleme:

* COMNAP: SNA oturum erişimi
* COMNODE: SNA oturum erişimi
* SQL\QUERY: SQL örnek erişimi
* SPOOLSS: Biriktirici hizmeti
* LLSRPC: Lisans Günlüğü hizmeti
* NETLOGON: Net Logon hizmeti
* LSARPC: LSA erişimi
* SAMR: Uzaktan erişim SAM nesnelerine
* TARAYICI: Bilgisayar Tarayıcısı hizmeti

Windows Server 2003 Service Pack 1 (SP1) yayımlanmadan önce, bu adlandırılmış yönlendirmelere varsayılan olarak anonim erişime izin veriliyordu, ancak Windows Server 2003 SP1'de artırılmış sertleştirme ile bu yönlendirmeler açık bir şekilde olmalıdır. gerekirse eklenir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters: RestrictNullSessAccess*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları \Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Ağ erişimi: Adlandırılmış Kanallara ve Paylaşımlara anonim erişimi kısıtlayın*

**2.3.10.10 (L1) 'Ağ erişimi: İstemcilerin SAM'a uzaktan arama yapmasına izin verilmesini kısıtla' seçeneği 'Yöneticiler: Uzaktan Erişim: İzin Ver' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, SAM ile uzak RPC bağlantılarını kısıtlamanıza olanak tanır. Bu ayar için önerilen durum: Yöneticiler: Uzaktan Erişim: İzin Ver.

**Not:** Grup İlkesi'nde bu değere erişmek ve bu değeri ayarlamak için Windows 10 R1607, Server 2016 veya daha yeni bir işletim sistemi gereklidir.

**Not #2:** Kuruluşunuz Azure Gelişmiş Tehdit Koruması (APT) kullanıyorsa, "AATP Hizmeti" hizmet hesabının öneri yapılandırmasına eklenmesi gerekir. [“AATP Hizmeti” hesabı ekleme hakkında daha fazla bilgi için lütfen Microsoft Defender for Identity | Microsoft Belgeleri.](https://docs.microsoft.com/en-us/defender-for-identity/install-step8-samr)

**Gerekçe:**

Yetkisiz bir kullanıcının yerel hesap adlarını veya gruplarını anonim olarak listelememesini ve bu bilgileri parolaları tahmin etmeye veya sosyal mühendislik saldırıları gerçekleştirmeye çalışmak için kullanmamasını sağlamak. (Sosyal mühendislik saldırıları, parolaları veya bir tür güvenlik bilgisi elde etmek için kullanıcıları bir şekilde aldatmaya çalışır.) Etki: Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:restrictremotesam*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Yöneticiler olarak ayarlayın: Uzaktan Erişim: İzin Ver:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Ağ erişimi: İstemcilerin yapmasına izin verilenleri kısıtlayın SAM'a uzaktan aramalar*

**2.3.10.11 (L1) 'Ağ erişimi: Paylaşımlar anonim olarak erişilebilir' seçeneği 'Hiçbiri' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, anonim kullanıcılar tarafından hangi ağ paylaşımlarına erişilebileceğini belirler. Bu ilke ayarının varsayılan yapılandırmasının çok az etkisi vardır çünkü tüm kullanıcıların sunucudaki paylaşılan kaynaklara erişebilmeleri için kimliklerinin doğrulanması gerekir. Bu ayar için önerilen durum: (yani Yok).

**Gerekçe:**

Bu ayarda herhangi bir değere izin vermek çok tehlikelidir. Listelenen paylaşımlara herhangi bir ağ kullanıcısı tarafından erişilebilir, bu da hassas verilerin açığa çıkmasına veya bozulmasına neden olabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanManServer\Parameters: NullSessionShares*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu (yani Yok):

*Bilgisayar Yapılandırması\İlkeler olarak ayarlayın. \Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Ağ erişimi: Anonim olarak erişilebilen paylaşımlar*

**2.3.10.12 (L1) 'Ağ erişimi: Yerel hesaplar için paylaşım ve güvenlik modeli' seçeneği 'Klasik - yerel kullanıcılar kendileri gibi kimlik doğrulaması yapar' olarak ayarlanmalıdır. (Otomatik)**

**Açıklama:**

Bu ilke ayarı, yerel hesapları kullanan ağ oturum açma işlemlerinin nasıl doğrulanacağını belirler. Klasik seçeneği, aynı kaynak için farklı kullanıcılara farklı erişim türleri atama yeteneği de dahil olmak üzere, kaynaklara erişim üzerinde kesin kontrol sağlar. Yalnızca misafir seçeneği, tüm kullanıcılara eşit davranmanıza olanak tanır. Bu bağlamda, tüm kullanıcılar yalnızca belirli bir kaynağa aynı erişim düzeyini almak için Misafir olarak kimlik doğrulaması yapar. Bu ayar için önerilen durum şudur: Klasik - yerel kullanıcılar kimliklerini kendileri olarak doğrular.

**Not:** Bu ayar, Telnet veya Uzak Masaüstü Hizmetleri (eski adıyla Terminal Hizmetleri) gibi hizmetler kullanılarak uzaktan gerçekleştirilen etkileşimli oturum açmaları etkilemez.

**Gerekçe:**

Yalnızca konuk modelinde, ağ üzerinden bilgisayarınızda kimlik doğrulaması yapabilen herhangi bir kullanıcı bunu konuk ayrıcalıklarıyla yapar; bu, muhtemelen o bilgisayardaki paylaşılan kaynaklara yazma erişimine sahip olmayacakları anlamına gelir. Bu kısıtlama güvenliği artırsa da, bu kaynaklardaki ACL'lerin Konuk hesabı için erişim denetimi girişlerini (ACE'ler) içermesi gerektiğinden, yetkili kullanıcıların bu bilgisayarlardaki paylaşılan kaynaklara erişmesini zorlaştırır. Klasik model ile yerel hesaplar parola korumalı olmalıdır. Aksi takdirde, Konuk erişimi etkinleştirilirse, herkes paylaşılan sistem kaynaklarına erişmek için bu kullanıcı hesaplarını kullanabilir.

**Etki:**

Yok - bu, etki alanına katılmış bilgisayarlar için varsayılan yapılandırmadır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:ForceGuest*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Klasik olarak ayarlayın - yerel kullanıcılar kendilerinin kimliğini doğrular:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Ağ erişimi: Paylaşım ve güvenlik modeli yerel hesaplar için*

**2.3.11 Ağ güvenliği**

**2.3.11.1 (L1) 'Ağ güvenliği: Yerel Sistemin NTLM için bilgisayar kimliğini kullanmasına izin ver' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, NTLM kimlik doğrulamasına geri dönerken Anlaşma kullanan Yerel Sistem hizmetlerinin bilgisayar kimliğini kullanıp kullanamayacağını belirler. Bu ilke, en az Windows 7 veya Windows Server 2008 R2'de desteklenir. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Windows'un Windows Vista veya Windows Server 2008'den (R2 olmayan) önceki sürümlerini çalıştıran bilgisayarlara bağlanırken, Yerel Sistem olarak çalışan ve NTLM'ye dönen SPNEGO (Anlaşma) kullanan hizmetler bilgisayar kimliğini kullanır. Windows 7'de, Windows Server 2008 veya Windows Vista çalıştıran bir bilgisayara bağlanıyorsanız, bir sistem hizmeti bilgisayar kimliğini veya NULL oturumunu kullanır. NULL oturumuyla bağlanırken, koruma sağlamayan ancak uygulamaların verileri hatasız olarak imzalamasına ve şifrelemesine izin veren, sistem tarafından oluşturulan bir oturum anahtarı oluşturulur. Bilgisayar kimliğine bağlanırken, veri koruması sağlamak için hem imzalama hem de şifreleme desteklenir.

**Etki:**

NTLM kimlik doğrulamasına geri dönerken Anlaşmayı kullanan Yerel Sistem olarak çalışan hizmetler, bilgisayar kimliğini kullanır. Bu, Windows işletim sistemleri arasındaki bazı kimlik doğrulama isteklerinin başarısız olmasına ve bir hata kaydetmesine neden olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:UseMachineId*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Ağ güvenliği: Yerel Sistemin NTLM için bilgisayar kimliğini kullanmasına izin verin*

**2.3.11.2 (L1) 'Ağ güvenliği: Yerel sistemin NULL oturum geri dönüşüne izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, LocalSystem ile kullanıldığında NTLM'nin NULL oturumuna geri dönmesine izin verilip verilmeyeceğini belirler. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

NULL oturumları, tanım gereği kimlik doğrulaması yapılmadığından daha az güvenlidir. Etki: Yok - bu varsayılan davranıştır. LocalSystem için NULL oturum gerektiren uygulamalar tasarlandığı gibi çalışmayacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1\_0:AllowNullSessi onFallback*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarlar\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Ağ güvenliği: LocalSystem NULL oturum geri dönüşüne izin ver*

**2.3.11.3 (L1) 'Ağ Güvenliği: Bu bilgisayara yapılan PKU2U kimlik doğrulama isteklerinin çevrimiçi kimlikleri kullanmasına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, çevrimiçi kimliklerin bu bilgisayarda kimlik doğrulaması yapıp yapamayacağını belirler. Windows 7 ve Windows Server 2008 R2'de tanıtılan Ortak Anahtar Şifreleme Tabanlı Kullanıcıdan Kullanıcıya (PKU2U) protokolü, bir güvenlik destek sağlayıcısı (SSP) olarak uygulanır. SSP, özellikle bir etki alanının üyesi olmayan bilgisayarlar arasında paylaşıma izin veren HomeGroup adlı Windows 7 medya ve dosya paylaşım özelliği aracılığıyla eşler arası kimlik doğrulamayı mümkün kılar. PKU2U ile, Negotiate kimlik doğrulama paketi Spnego.dll'ye yeni bir uzantı eklendi. Windows'un önceki sürümlerinde, Negotiate, kimlik doğrulama için Kerberos'un mu yoksa NTLM'nin mi kullanılacağına karar verirdi. Windows tarafından bir kimlik doğrulama protokolü olarak kabul edilen Negotiate için SSP uzantısı Negoexts.dll, PKU2U dahil Microsoft SSP'lerini destekler. Bilgisayarlar, çevrimiçi kimlikleri kullanarak kimlik doğrulama isteklerini kabul edecek şekilde yapılandırıldığında, Negoexts.dll, oturum açmak için kullanılan bilgisayarda PKU2U SSP'yi çağırır. PKU2U SSP, yerel bir sertifika alır ve politikayı eş bilgisayarlar arasında değiştirir. Eş bilgisayarda doğrulandığında, meta veriler içindeki sertifika, doğrulama için oturum açma eşine gönderilir ve kullanıcının sertifikasını bir güvenlik belirteciyle ilişkilendirir ve oturum açma işlemi tamamlanır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

PKU2U protokolü, eşler arası bir kimlik doğrulama protokolüdür - kimlik doğrulama, yönetilen ağların çoğunda merkezi olarak yönetilmelidir. Etki: Yok - bu, etki alanına katılmış bilgisayarlar için varsayılan yapılandırmadır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\pku2u:AllowOnlineID*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları \Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Ağ Güvenliği: Bu bilgisayara PKU2U kimlik doğrulama isteklerinin çevrimiçi kimlikleri kullanmasına izin verin*

**2.3.11.4 (L1) 'Ağ güvenliği: Kerberos için izin verilen şifreleme türlerini yapılandır' seçeneği 'AES128\_HMAC\_SHA1, AES256\_HMAC\_SHA1, Gelecekteki şifreleme türleri' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Kerberos'un kullanmasına izin verilen şifreleme türlerini ayarlamanıza olanak tanır. Bu ayar için önerilen durum: AES128\_HMAC\_SHA1, AES256\_HMAC\_SHA1, Gelecekteki şifreleme türleri.

**Not:** Bazı eski uygulamalar ve işletim sistemleri hala RC4\_HMAC\_MD5 gerektirebilir - ortamınızda test etmenizi ve güvenli bir şekilde kaldırıp kaldıramayacağınızı doğrulamanızı öneririz.

**Gerekçe:**

Her şifreleme algoritmasının gücü birinden diğerine değişir, daha güçlü algoritmalar seçmek, uzlaşma riskini azaltır, ancak bunu yapmak, bilgisayar bunları desteklemeyen sistemlerle kimlik doğrulaması yapmaya çalıştığında sorunlara neden olabilir.

**Etki:**

Seçilmezse şifreleme türüne izin verilmeyecektir. Bu ayar, istemci bilgisayarlar veya hizmetler ve uygulamalarla uyumluluğu etkileyebilir. Çoklu seçime izin verilir.

**Not:** Bazı eski uygulamalar ve işletim sistemleri hala RC4\_HMAC\_MD5 gerektirebilir - ortamınızda test etmenizi ve güvenli bir şekilde kaldırıp kaldıramayacağınızı doğrulamanızı öneririz.

**Not 2:** Windows Vista ve altı, varsayılan olarak Kerberos için DES'ye izin verir, ancak sonraki işletim sistemi sürümleri buna izin vermez.

**Not 3:** Bu önerinin çalışması için Kerberos AES 128 ve 256 bit şifreleme türlerini desteklemenin yanı sıra kullanıcı hesaplarında (hesap seçeneklerinde) Kerberos AES 128 ve 256 bit desteğinin etkinleştirilmesi için Etki Alanı Denetleyicilerinde bazı ön koşulların karşılanması gerekebilir. doğru şekilde.

**Not 4:** Kuruluşunuz Azure Dosyalarını kullanıyorsa, Microsoft'un AD DS kimlik doğrulama modülü v0.2.2'ye kadar AES 256 Kerberos şifreleme desteği sağlamadığını lütfen unutmayın. Daha fazla bilgi için lütfen bu bağlantıya bakın: [AES 256 Kerberos şifrelemesi için şirket içi Azure Dosyaları AD DS Kimlik Doğrulaması desteği | Microsoft Docs](https://docs.microsoft.com/en-us/azure/storage/files/storage-troubleshoot-windows-file-connection-problems#azure-files-on-premises-ad-ds-authentication-support-for-aes-256-kerberos-encryption)

**Denetim:**

Düzeltme bölümünde belirtilen Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ Kerberos\Parameters:SupportedEncryptionTypes*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu AES128\_HMAC25\_SHAAC1, AES\_ olarak ayarlayın. , Gelecekteki şifreleme türleri:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Ağ güvenliği: Kerberos için izin verilen şifreleme türlerini yapılandırın*

**2.3.11.5 (L1) 'Ağ güvenliği: Bir sonraki parola değişikliğinde LAN Manager karma değerini saklamayın' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, parola değiştirildiğinde yeni parola için LAN Manager (LM) karma değerinin saklanıp saklanmayacağını belirler. LM karması, kriptografik olarak daha güçlü Microsoft Windows NT karmasına kıyasla nispeten zayıf ve saldırıya açık. LM karmaları yerel bilgisayarda güvenlik veritabanında depolandığından, veritabanı saldırıya uğrarsa parolalar kolayca tehlikeye girebilir.

**Not:** Bu ilke ayarı etkinleştirildiğinde daha eski işletim sistemleri ve bazı üçüncü taraf uygulamaları başarısız olabilir. Ayrıca, doğru faydayı elde etmek için bu ayarı etkinleştirdikten sonra parolanın tüm hesaplarda değiştirilmesi gerekeceğini unutmayın. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

SAM dosyası, kullanıcı adı ve parola karmalarına erişim arayan saldırganlar tarafından hedeflenebilir. Bu tür saldırılar, daha sonra kullanıcıları taklit etmek ve ağınızdaki kaynaklara erişim sağlamak için kullanılabilecek parolaları kırmak için özel araçlar kullanır. Bu ilke ayarını etkinleştirirseniz bu tür saldırılar engellenmeyecektir, ancak bu tür saldırıların başarılı olması çok daha zor olacaktır.

**Etki:**

Yok - bu varsayılan davranıştır. Windows 95, Windows 98 ve Windows ME gibi önceki işletim sistemleri ve bazı üçüncü taraf uygulamalar başarısız olacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:NoLMHash*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Ağ güvenliği: LAN Yöneticisi karma değerini sonraki parolada saklama değiştirmek*

**2.3.11.6 (L1) 'Ağ güvenliği: Oturum açma saatleri sona erdiğinde oturumu kapatmaya zorla' seçeneği 'Etkin' olarak ayarlandığından emin olun (Manuel)**

**Açıklama:**

Bu ilke ayarı, yerel bilgisayara kendi kullanıcı hesaplarının geçerli oturum açma saatleri dışında bağlanan kullanıcıların bağlantısının kesilip kesilmeyeceğini belirler. Bu ayar, Sunucu İleti Bloğu (SMB) bileşenini etkiler. Bu ilke ayarını etkinleştirirseniz, Microsoft ağ sunucusunu da etkinleştirmelisiniz: Oturum açma saatleri sona erdiğinde istemcilerin bağlantısını kesin (Kural 2.3.9.4). Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bu ayar devre dışı bırakılırsa, kullanıcı kendilerine ayrılan oturum açma saatleri dışında bilgisayara bağlı kalabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Ağ güvenliği: Oturum açma saatleri sona erdiğinde oturumu kapatmaya zorla*

**2.3.11.7 (L1) 'Ağ güvenliği: LAN Manager kimlik doğrulama düzeyi' seçeneği 'Yalnızca NTLMv2 yanıtı gönder. LM & NTLM’i reddet' olarak ayarlanmalıdır. (Otomatik)**

**Açıklama:**

LAN Manager (LM), kullanıcıların kişisel bilgisayarları tek bir ağ üzerinde birbirine bağlamasına izin veren, eski bir Microsoft istemci/sunucu yazılımı ailesiydi (Windows NT'den önce). LM ağ yetenekleri arasında şeffaf dosya ve baskı paylaşımı, kullanıcı güvenliği özellikleri ve ağ yönetim araçları yer alır. Active Directory etki alanlarında, Kerberos protokolü varsayılan kimlik doğrulama protokolüdür. Ancak, herhangi bir nedenle Kerberos protokolü üzerinde anlaşma sağlanmazsa, Active Directory LM, NTLM veya NTLMv2'yi kullanır. LAN Manager kimlik doğrulaması, LM, NTLM ve NTLM sürüm 2 (NTLMv2) türevlerini içerir ve aşağıdaki işlemleri gerçekleştirirken tüm Windows istemcilerinin kimliğini doğrulamak için kullanılan protokoldür:

* Bir etki alanına katılın
* Active Directory ormanları arasında kimlik doğrulaması
* Alt düzey etki alanları
* Windows 2000, Windows Server 2003 veya Windows XP çalıştırmayan bilgisayarlarda kimlik doğrulaması
* Etki alanında olmayan bilgisayarlarda kimlik doğrulaması

Ağ güvenliği: LAN Yöneticisi kimlik doğrulama düzeyi ayarı, hangi sorgulama/yanıt kimlik doğrulama protokolünün kullanıldığını belirler ağ oturumları için. Bu seçim, istemciler tarafından kullanılan kimlik doğrulama protokolünün düzeyini, üzerinde anlaşılan oturum güvenliği düzeyini ve sunucular tarafından kabul edilen kimlik doğrulama düzeyini etkiler. Bu ayar için önerilen durum şudur: Yalnızca NTLMv2 yanıtını gönder. LM ve NTLM'yi reddet.

**Gerekçe:**

Windows 2000 ve Windows XP istemcileri, varsayılan olarak LM ve NTLM kimlik doğrulama yanıtları gönderecek şekilde yapılandırılmıştır (Windows 95 tabanlı ve Windows 98 tabanlı istemciler yalnızca LM gönderir). Windows Vista / Windows Server 2008'den (R2 olmayan) önceki işletim sistemlerindeki varsayılan ayarlar, tüm istemcilerin sunucularla kimlik doğrulaması yapmasına ve kaynaklarını kullanmasına izin verdi. Ancak bu, kimlik doğrulama yanıtının en zayıf biçimi olan LM yanıtlarının ağ üzerinden gönderildiği ve saldırganların kullanıcının parolasını daha kolay yeniden üretmek için bu trafiği koklamasının olası olduğu anlamına geliyordu. Windows 95, Windows 98 ve Windows NT işletim sistemleri, kimlik doğrulama için Kerberos sürüm 5 protokolünü kullanamaz. Bu nedenle, bir Windows Server 2003 etki alanında, bu bilgisayarlar varsayılan olarak ağ kimlik doğrulaması için hem LM hem de NTLM protokolleriyle kimlik doğrulaması yapar. NTLMv2 kullanarak Windows 95, Windows 98 ve Windows NT için daha güvenli bir kimlik doğrulama protokolü uygulayabilirsiniz. Oturum açma işlemi için NTLMv2, kimlik doğrulama sürecini korumak için güvenli bir kanal kullanır. NTLMv2'yi daha eski istemciler ve sunucular için kullansanız bile, etki alanının üyesi olan Windows tabanlı istemciler ve sunucular, Windows Server 2003 veya daha yeni Etki Alanı Denetleyicileri ile kimlik doğrulaması yapmak için Kerberos kimlik doğrulama protokolünü kullanır. Bu nedenlerle, LM & NTLM (v2 olmayan) kullanımının mümkün olduğunca sınırlandırılması şiddetle tercih edilir.

**Etki:**

İstemciler yalnızca NTLMv2 kimlik doğrulamasını kullanır ve sunucu destekliyorsa NTLMv2 oturum güvenliğini kullanır; Etki Alanı Denetleyicileri LM ve NTLM'yi reddeder (yalnızca NTLMv2 kimlik doğrulamasını kabul eder). NTLMv2 kimlik doğrulamasını desteklemeyen istemciler, LM ve NTLM kullanarak etki alanında kimlik doğrulaması yapamaz ve etki alanı kaynaklarına erişemez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa:LmCompatibilityLevel*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki UI yolunu şu şekilde ayarlayın: Yalnızca NTLMv2 yanıtı gönder. LM ve NTLM'yi Reddet:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Ağ güvenliği: LAN Yöneticisi kimlik doğrulama düzeyi*

**2.3.11.8 (L1) 'Ağ güvenliği: LDAP istemcisi imzalama gereksinimleri' seçeneği 'İmzalama anlaşması yap veya üstü '(Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, LDAP BIND istekleri yayınlayan istemciler adına istenen veri imzalama düzeyini belirler.

**Not:** Bu ilke ayarının, LDAP basit bağlama (ldap\_simple\_bind) veya SSL aracılığıyla LDAP basit bağlama (ldap\_simple\_bind\_s) üzerinde herhangi bir etkisi yoktur. Windows XP Professional'da bulunan hiçbir Microsoft LDAP istemcisi, Etki Alanı Denetleyicisi ile iletişim kurmak için ldap\_simple\_bind veya ldap\_simple\_bind\_s kullanmaz. Bu ayar için önerilen durum şudur: İmzalama anlaşması. Bu ayarın İmza iste olarak yapılandırılması da kıyaslamayla uyumludur.

**Gerekçe:**

İmzasız ağ trafiği, davetsiz misafirin istemci ile sunucu arasındaki paketleri yakaladığı, değiştirdiği ve ardından sunucuya ilettiği ortadaki adam saldırılarına açıktır. Bir LDAP sunucusu için bu duyarlılık, bir saldırganın bir sunucunun LDAP sorgularından alınan yanlış veya değiştirilmiş verilere dayalı kararlar almasına neden olabileceği anlamına gelir. Ağınızdaki bu riski azaltmak için ağ altyapısını korumak için güçlü fiziksel güvenlik önlemleri uygulayabilirsiniz. Ayrıca, IPsec kimlik doğrulama başlıkları aracılığıyla tüm ağ paketlerinde dijital imzalara ihtiyacınız varsa, her tür ortadaki adam saldırısını son derece zor hale getirebilirsiniz.

**Etki:**

Yok - bu varsayılan davranıştır. Ancak bunun yerine sunucuyu LDAP imzaları gerektirecek şekilde yapılandırmayı seçerseniz, istemciyi de yapılandırmanız gerekir. İstemciyi yapılandırmazsanız, sunucuyla iletişim kuramaz; bu, kullanıcı kimlik doğrulaması, Grup İlkesi ve oturum açma komut dosyaları dahil olmak üzere birçok özelliğin başarısız olmasına neden olabilir, çünkü arayana LDAP BIND komut isteğinin başarısız olduğu söylenecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LDAP:LDAPClientIntegrity*

**Düzeltme**:

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu İmzalamayı iste olarak ayarlayın (İmza iste olarak yapılandırma, kıyaslama):

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Ağ güvenliği: LDAP istemci imzalama gereksinimleri*

**2.3.11.9 (L1) 'Ağ güvenliği: NTLM SSP tabanlı (güvenli RPC dahil) istemciler için minimum oturum güvenliği' seçeneği 'NTLMv2 oturum güvenliği gerektir, 128 bit şifreleme gerektir' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, NTLM Güvenlik Destek Sağlayıcısı (SSP) kullanan uygulamalar için istemciler tarafından hangi davranışlara izin verildiğini belirler. SSP Arayüzü (SSPI), kimlik doğrulama hizmetlerine ihtiyaç duyan uygulamalar tarafından kullanılır. Ayar, kimlik doğrulama sırasının nasıl çalıştığını değiştirmez, bunun yerine SSPI kullanan uygulamalarda belirli davranışları gerektirir. Bu ayar için önerilen durum şudur: NTLMv2 oturum güvenliği gerektir, 128 bit şifreleme gerektir.

**Not:** Bu değerler Ağ güvenliğine bağlıdır: LAN Manager Kimlik Doğrulama Düzeyi (Kural 2.3.11.7) güvenlik ayarı değeri.

**Gerekçe:**

NTLM Güvenlik Destek Sağlayıcısı'nı (NTLM SSP) kullanan ağ trafiğini, aynı ağa erişim kazanmış bir saldırganın açığa çıkmasına veya kurcalanmasına karşı korumaya yardımcı olmak için bu ilke ayarı için her iki seçeneği de etkinleştirebilirsiniz. Başka bir deyişle, bu seçenekler ortadaki adam saldırılarına karşı korunmaya yardımcı olur.

**Etki:**

NTLMv2 protokolü ve güçlü şifreleme (128 bit) üzerinde anlaşma sağlanmazsa NTLM bağlantıları başarısız olur. Bu ayarları zorunlu kılan istemci uygulamaları, onları desteklemeyen eski sunucularla iletişim kuramaz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1\_0:NTLMMinClientS ec*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu NTLMv2 oturum güvenliği gerektir, 128 bit şifreleme gerektir olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Ağ güvenliği: Minimum NTLM SSP tabanlı (güvenli RPC dahil) istemciler için oturum güvenliği*

**2.3.11.10 (L1) 'Ağ güvenliği: NTLM SSP tabanlı (güvenli RPC dahil) sunucular için minimum oturum güvenliği' seçeneği 'NTLMv2 oturum güvenliği gerektir, 128 bit şifreleme gerektir' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, NTLM Güvenlik Destek Sağlayıcısı (SSP) kullanan uygulamalar için sunucular tarafından hangi davranışlara izin verildiğini belirler. SSP Arayüzü (SSPI), kimlik doğrulama hizmetlerine ihtiyaç duyan uygulamalar tarafından kullanılır. Ayar, kimlik doğrulama sırasının nasıl çalıştığını değiştirmez, bunun yerine SSPI kullanan uygulamalarda belirli davranışları gerektirir. Bu ayar için önerilen durum şudur: NTLMv2 oturum güvenliği gerektir, 128 bit şifreleme gerektir.

**Not:** Bu değerler Ağ güvenliğine bağlıdır: LAN Manager Kimlik Doğrulama Düzeyi (Kural 2.3.11.7) güvenlik ayarı değeri.

**Gerekçe:**

NTLM Güvenlik Destek Sağlayıcısı'nı (NTLM SSP) kullanan ağ trafiğini, aynı ağa erişim kazanmış bir saldırganın açığa çıkmasına veya kurcalanmasına karşı korumaya yardımcı olmak için bu ilke ayarının tüm seçeneklerini etkinleştirebilirsiniz. Yani, bu seçenekler ortadaki adam saldırılarına karşı korunmaya yardımcı olur.

**Etki:**

NTLMv2 protokolü ve güçlü şifreleme (128 bit) üzerinde anlaşma sağlanmazsa NTLM bağlantıları başarısız olur. Bu ayarları zorunlu kılan sunucu uygulamaları, onları desteklemeyen eski sunucularla iletişim kuramaz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa\MSV1\_0:NTLMMinServerS ec*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu NTLMv2 oturum güvenliği gerektir, 128 bit şifreleme gerektir olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Ağ güvenliği: Minimum NTLM SSP tabanlı (güvenli RPC dahil) sunucular için oturum güvenliği*

**2.3.14 Kriptografik sistemler**

**2.3.14.1 (L2) 'Sistem şifrelemesi: Bilgisayarda depolanan kullanıcı anahtarları için güçlü anahtar korumasını zorla' seçeneği 'Anahtar ilk kullanıldığında kullanıcıya sorulur veya üstü’ (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların özel anahtarlarının (S-MIME anahtarları gibi) kullanılması için bir parola gerektirip gerektirmediğini belirler. Bu ayar için önerilen durum şudur: Anahtar ilk kullanıldığında kullanıcıya sorulur. Bu ayarı Kullanıcı olarak yapılandırmak, her anahtar kullandıklarında bir parola girmelidir, ayrıca kıyaslamayla da uyumludur.

**Gerekçe:**

Bir kullanıcının hesabının güvenliği ihlal edilirse veya bilgisayarı yanlışlıkla güvensiz bırakılırsa, kötü niyetli kullanıcı, korunan kaynaklara erişmek için kullanıcının depoladığı anahtarları kullanabilir. Bu ilke ayarını, kullanıcıların her anahtar kullandıklarında etki alanı parolalarından farklı bir parola sağlamaları gerektiği şekilde yapılandırabilirsiniz. Bu yapılandırma, saldırganın kullanıcının bilgisayarının denetimini ele geçirip oturum açma parolasını belirlemesine rağmen, yerel olarak depolanan kullanıcı anahtarlarına erişmesini zorlaştırır.

**Etki:**

Kullanıcılar, bilgisayarlarında depolanan bir anahtara ilk kez eriştiklerinde parolalarını girmek zorunda kalacaklardır. Örneğin, kullanıcılar e-postalarını dijital olarak imzalamak için bir S-MIME sertifikası kullanırlarsa, imzalı bir e-posta iletisini ilk kez gönderdiklerinde bu sertifikanın parolasını girmek zorunda kalacaklardır. Daha da güçlü güvenlik için, Kullanıcının her anahtar kullandığında bir parola girmesi gerektiği değeri ayarlanabilir, ancak bu yapılandırmanın kullanılmasıyla ilgili ek yük bazı kuruluşlar için çok yüksek olabilir. Microsoft, yönetilebilirlik üzerindeki önemli etkisi nedeniyle bu ayarın sunucularda uygulanmasını önermez. Örneğin, Uzak Masaüstü Hizmetlerini SSL sertifikalarını kullanacak şekilde yapılandıramayabilirsiniz. Windows PKI TechNet Blogunda daha fazla bilgi bulabilirsiniz: [Windows'ta güçlü bir anahtar koruması nedir?](https://blogs.technet.microsoft.com/pki/2009/06/16/what-is-a-strong-key-protection-in-windows/)

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Cryptography:ForceKeyProtection*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki UI yolunu, anahtar ilk kullanıldığında sorulacak Kullanıcı olarak ayarlayın ( Kullanıcının bir anahtarı her kullandıklarında bir parola girmesi gerektiğini yapılandırmak, aynı zamanda kıyaslama ile de uyumludur):

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Sistem şifrelemesi: Sistemde depolanan kullanıcı anahtarları için güçlü anahtar korumasını zorla bilgisayar*

**2.3.15 Sistem nesneleri**

**2.3.15.1 (L1) 'Sistem nesneleri: Windows dışı alt sistemler için büyük/küçük harf duyarsızlığı gerektir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, tüm alt sistemler için büyük/küçük harf duyarsızlığının uygulanıp uygulanmayacağını belirler. Microsoft Win32 alt sistemi büyük/küçük harfe duyarlı değildir. Ancak çekirdek, UNIX için Taşınabilir İşletim Sistemi Arayüzü (POSIX) gibi diğer alt sistemler için büyük/küçük harf duyarlılığını destekler. Windows büyük/küçük harf duyarlı olmadığından (ancak POSIX alt sistemi büyük/küçük harf duyarlılığını destekleyecektir), bu ilke ayarının uygulanmaması, POSIX alt sisteminin bir kullanıcısının, karışık büyük/küçük harf kullanarak etiketlemek için başka bir dosyayla aynı ada sahip bir dosya oluşturmasını mümkün kılar. Böyle bir durum, dosyalardan yalnızca biri kullanılabilir olacağından, tipik Win32 araçlarını kullanan başka bir kullanıcının bu dosyalara erişimini engelleyebilir. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Windows büyük/küçük harfe duyarlı olmadığından, ancak POSIX alt sistemi büyük/küçük harf duyarlılığını destekleyeceğinden, bu ilke ayarının etkinleştirilmemesi, o alt sistemin bir kullanıcısının başka bir dosyayla aynı ada sahip ancak farklı bir dosya karışımına sahip bir dosya oluşturmasını mümkün kılacaktır. büyük ve küçük harfler. Böyle bir durum, dosyalardan yalnızca biri kullanılabilir olacağından, normal Win32 araçlarından bu tür dosyalara erişmeye çalıştıklarında kullanıcıların kafasını karıştırabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager\Kernel:ObCaseInSense*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Sistem nesneleri: Windows olmayan alt sistemler için büyük/küçük harf duyarlılığı gerektir*

**2.3.15.2 (L1) 'Sistem nesneleri: Dahili sistem nesnelerinin (ör. Sembolik Bağlantılar) varsayılan izinlerini güçlendir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, nesneler için varsayılan isteğe bağlı erişim denetim listesinin (DACL) gücünü belirler. Active Directory, DOS aygıt adları, muteksler ve semaforlar gibi paylaşılan sistem kaynaklarının genel bir listesini tutar. Bu şekilde nesneler süreçler arasında bulunabilir ve paylaşılabilir. Her nesne türü, nesnelere kimlerin erişebileceğini ve hangi izinlerin verildiğini belirten varsayılan bir DACL ile oluşturulur. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bu ayar, nesneler için varsayılan DACL'nin gücünü belirler. Windows, nesnelerin bulunabilmesi ve işlemler arasında paylaşılabilmesi için paylaşılan bilgisayar kaynaklarının genel bir listesini tutar. Her nesne türü, nesnelere kimlerin ve hangi izinlerle erişebileceğini belirten varsayılan bir DACL ile oluşturulur.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager:ProtectionMode*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\ Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Sistem nesneleri: Dahili sistem nesnelerinin varsayılan izinlerini güçlendirin (ör. Sembolik Bağlantılar)*

**2.3.17 Kullanıcı Hesabı Kontrolü**

**2.3.17.1 (L1) 'Kullanıcı Hesabı Denetimi: Yerleşik Yönetici hesabı için Yönetici Onay Modu' seçeneği ‘Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, yerleşik Yönetici hesabı için Yönetici Onay Modu'nun davranışını kontrol eder. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Windows Vista ile sunulan Kullanıcı Hesabı Denetimi özelliğinin azaltmaya çalıştığı risklerden biri, kötü amaçlı yazılımların, kullanıcı veya yöneticinin etkinliğinin farkında olmadan yüksek kimlik bilgileri altında çalışmasıdır. Bu programlar için bir saldırı vektörü, "Yönetici" adlı hesabın parolasını keşfetmekti çünkü bu kullanıcı hesabı tüm Windows yüklemeleri için oluşturuldu. Bu riski gidermek için Windows Vista ve daha yeni sürümlerde, yerleşik Yönetici hesabı artık varsayılan olarak devre dışı bırakılmıştır. Yeni bir bilgisayarın varsayılan yüklemesinde, bilgisayar üzerinde yönetici denetimine sahip hesaplar başlangıçta iki yoldan biriyle kurulur:

* Bilgisayar bir etki alanına katılmamışsa, oluşturduğunuz ilk kullanıcı hesabı yerel olarak eşdeğer izinlere sahiptir. Yönetici.
* Bilgisayar bir etki alanına katılmışsa, yerel yönetici hesabı oluşturulmaz. Kuruluş veya Etki Alanı Yöneticisi bilgisayarda oturum açmalı ve yerel yönetici hesabı garanti ediliyorsa bir tane oluşturmalıdır.

Windows yüklendikten sonra, yerleşik Yönetici hesabı manuel olarak etkinleştirilebilir, ancak bu hesabın devre dışı kalmasını kesinlikle öneririz.

**Etki:**

Yerleşik Yönetici hesabı, Yönetici Onay Modunu kullanır. Yerel Yönetici hesabını kullanarak oturum açan kullanıcılardan, diğer herhangi bir kullanıcının yapacağı gibi, bir program ayrıcalık yükseltmesi istediğinde onay istenir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: FilterAdministratorToken*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\ Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Kullanıcı Hesabı Denetimi: Yerleşik Yönetici hesabı için Yönetici Onay Modu*

**2.3.17.2(L1) 'Kullanıcı Hesabı Denetimi: Yönetici Onay Modu'nda yöneticiler için yükseltme isteminin davranışı’ seçeneği 'Güvenli masaüstünde onay istemi' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, yöneticiler için yükseltme isteminin davranışını kontrol eder. Bu ayar için önerilen durum şudur: Güvenli masaüstünde onay iste.

**Gerekçe:**

Windows Vista ile sunulan UAC özelliğinin azaltmaya çalıştığı risklerden biri, kullanıcı veya yöneticinin faaliyetinin farkında olmadan yüksek kimlik bilgileri altında çalışan kötü amaçlı yazılımlardır. Bu ayar, yöneticinin yükseltilmiş ayrıcalık işlemleri konusunda farkındalığını artırır ve yöneticinin, program bunu yapmaya çalıştığında kötü amaçlı bir programın ayrıcalığını yükseltmesini engellemesine izin verir.

**Etki:**

Bir işlem (bir Windows ikili dosyasının yürütülmesi dahil) ayrıcalık yükseltmesi gerektirdiğinde, kullanıcıdan güvenli masaüstünde İzin Ver veya Reddet'i seçmesi istenir. Kullanıcı İzin Ver'i seçerse işlem, kullanıcının mevcut en yüksek ayrıcalığı ile devam eder.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: ConsentPromptBehaviorAdmin*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Güvenli masaüstünde onay iste olarak ayarlayın :

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Kullanıcı Hesabı Denetimi: Yönetici Onay Modunda yöneticiler için yükseltme isteminin davranışı*

**2.3.17.3 (L1) 'Kullanıcı Hesabı Denetimi: Standart kullanıcılar için yükseltme isteminin davranışı' seçeneği 'Yükseltme isteklerini otomatik olarak reddet' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, standart kullanıcılar için yükseltme isteminin davranışını kontrol eder. Bu ayar için önerilen durum: Yükseltme isteklerini otomatik olarak reddet.

**Gerekçe:**

Windows Vista ile sunulan Kullanıcı Hesabı Denetimi özelliğinin azaltmaya çalıştığı risklerden biri, kötü amaçlı programların, kullanıcı veya yöneticinin etkinliklerinden haberdar olmadan yüksek kimlik bilgileri altında çalışmasıdır. Bu ayar, bir programın yükseltilmiş ayrıcalık işlemlerinin kullanılmasını gerektirdiği konusunda kullanıcıyı bilinçlendirir ve programın çalışması için kullanıcının yönetici kimlik bilgilerini sağlayabilmesini gerektirir.

**Etki:**

Bir işlem ayrıcalık yükselmesi gerektirdiğinde, yapılandırılabilir bir erişim reddedildi hata mesajı görüntülenir. Standart kullanıcı olarak masaüstlerini çalıştıran bir kuruluş, yardım masası çağrılarını azaltmak için bu ayarı seçebilir.

**Not:** Bu ayar önerildiği şekilde yapılandırıldığında, bir kullanıcı bir işlemi gerçekleştirmeye veya ayrıcalık yükseltmesi gerektiren bir programı (Yönetici hakları olmadan) çalıştırmaya çalıştığında görüntülenen varsayılan hata mesajı "Bu program çalışmayacak. Bu program grup ilkesi tarafından engellendi. Daha fazla bilgi için sistem yöneticinize başvurun." Bu mesajı görmeye alışkın olmayan bazı kullanıcılar, çalıştırmaya çalıştıkları işlemin veya programın, mesajın ima ettiği gibi göründüğü için, özellikle grup ilkesi tarafından engellendiğine inanabilirler. Bu mesaj, bu nedenle, bu belirli işlemin/programın neden engellendiğine ilişkin kullanıcı sorularına neden olabilir, ancak aslında sorun, işlemi gerçekleştirmeleri veya programı bir Yönetici hesabıyla çalıştırmaları gerektiğidir (veya "Yönetici Olarak Çalıştır"). zaten bir Yönetici hesabıdır) ve bunu yapmıyorlar.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: ConsentPromptBehaviorUser*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Yükseltme isteklerini otomatik olarak reddet olarak ayarlayın:

*Bilgisayar Yapılandırması \İlkeler\Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Kullanıcı Hesabı Denetimi: Standart kullanıcılar için yükseltme isteminin davranışı*

**2.3.17.4 (L1) 'Kullanıcı Hesabı Denetimi: Uygulama yüklemelerini algıla ve yükseltme istemi' seçeneği 'Etkin' (Otomatik) olarak ayarlandığından emin olun**

**Açıklama:**

Bu ilke ayarı, bilgisayar için uygulama yükleme algılama davranışını denetler. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bazı kötü amaçlı yazılımlar, çalıştırma izni verildikten sonra kendini yüklemeye çalışır. Örneğin, güvenilir bir uygulama kabuğuna sahip kötü amaçlı yazılım. Kullanıcı, program güvenilir olduğu için programın çalışmasına izin vermiş olabilir, ancak daha sonra bilinmeyen bir bileşenin yüklenmesi istenirse, bu, yazılımı zarar vermeden önce yakalamanın başka bir yolunu sağlar

**Etki:**

Bir uygulama yükleme paketi ayrıcalık yükselmesi gerektirdiği tespit edildiğinde, kullanıcıdan bir yönetici kullanıcı adı ve parolası girmesi istenir. Kullanıcı geçerli kimlik bilgilerini girerse, işlem geçerli ayrıcalıkla devam eder.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: EnableInstallerDetection*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\ Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Kullanıcı Hesabı Denetimi: Uygulama yüklemelerini algılayın ve yükseltme isteyin*

**2.3.17.5 (L1) 'Kullanıcı Hesabı Denetimi: Yalnızca güvenli konumlara yüklenen UIAccess uygulamalarını yükselt' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Kullanıcı Arabirimi Erişilebilirlik (UIAccess) bütünlük düzeyiyle çalışmayı isteyen uygulamaların dosya sisteminde güvenli bir konumda bulunması gerekip gerekmediğini denetler. Güvenli konumlar aşağıdakilerle sınırlıdır:

* …\Program Files\, alt klasörler dahil
* …\Windows\System32\
* …\Program Files (x86)\, alt klasörler dahil (Windows'un 64-bit sürümleri için)

**Not:** Windows, bir Bu güvenlik ayarının durumundan bağımsız olarak bir UIAccess bütünlük düzeyiyle çalıştırmayı talep eden herhangi bir etkileşimli uygulamada ortak anahtar altyapısı (PKI) imza kontrolü. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

UIAccess Bütünlüğü, bir uygulamanın ayrıcalığı standart bir kullanıcıdan bir yöneticiye yükseltildiğinde, bir uygulamanın Kullanıcı Arayüzü Ayrıcalığı Yalıtımı (UIPI) kısıtlamalarını atlamasına izin verir. Bu, kullanıcı arabirimlerini alternatif formlara aktaran ekran okuyucular gibi erişilebilirlik özelliklerini desteklemek için gereklidir. UIAccess haklarıyla başlatılan bir işlem aşağıdaki yeteneklere sahiptir:

* Ön plan penceresini ayarlamak için.
* SendInput işlevini kullanarak herhangi bir uygulama penceresini sürmek için.
* Düşük seviyeli kancalar, ham giriş, GetKeyState, GetAsyncKeyState ve GetKeyboardInput kullanarak tüm bütünlük seviyeleri için okuma girişi kullanmak.
* Günlük kancalarını ayarlamak için.
* Daha yüksek bir bütünlük girdi kuyruğuna bir iş parçacığı eklemek için AttachThreadInput'u kullanmak.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: EnableSecureUIAPaths*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\ Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Kullanıcı Hesabı Denetimi: Yalnızca güvenli konumlara yüklenen UIAccess uygulamalarını yükseltin*

**2.3.17.6 (L1) 'Kullanıcı Hesabı Denetimi: Tüm yöneticileri Yönetici Onay Modunda çalıştır' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bilgisayar için tüm Kullanıcı Hesabı Denetimi (UAC) ilkesi ayarlarının davranışını denetler. Bu ilke ayarını değiştirirseniz, bilgisayarınızı yeniden başlatmanız gerekir. Bu ayar için önerilen durum: Etkin.

**Not:** Bu ilke ayarı devre dışı bırakılırsa Güvenlik Merkezi, işletim sisteminin genel güvenliğinin azaltıldığını size bildirir.

**Gerekçe:**

Bu, UAC'yi açan veya kapatan ayardır. Bu ayar devre dışı bırakılırsa, UAC kullanılmaz ve sistemde UAC'ye bağlı herhangi bir güvenlik avantajı ve risk azaltma özelliği bulunmaz.

**Etki:**

Yok - bu varsayılan davranıştır. Kullanıcıların ve yöneticilerin, UAC istemleriyle çalışmayı öğrenmesi ve çalışma alışkanlıklarını en az ayrıcalık işlemlerini kullanacak şekilde ayarlaması gerekecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: EnableLUA*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\ Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Kullanıcı Hesabı Denetimi: Tüm yöneticileri Yönetici Onay Modunda çalıştırın*

**2.3.17.7 (L1) 'Kullanıcı Hesabı Denetimi: Yükseltme istendiğinde güvenli masaüstüne geç' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, yükseltme isteği isteminin etkileşimli kullanıcının masaüstünde mi yoksa güvenli masaüstünde mi görüntülendiğini denetler. Bu ayar için önerilen durum: Etkin. **Gerekçe:**

Standart yükseltme istemi iletişim kutuları, kullanıcıların parolalarını kötü amaçlı yazılımlara ifşa etmesine neden olabilecek şekilde sahte olabilir. Güvenli masaüstü, kullanıcı masaüstünün karardığı ve yükseltme istemi kullanıcı arayüzünün daha belirgin olduğu yükseltme istenirken çok farklı bir görünüm sunar. Bu, güvenli masaüstüne alışan kullanıcıların sahte bir yükseltme istemi iletişim kutusunu tanıma ve bu oyuna gelmeme olasılığını artırır.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: PromptOnSecureDesktop*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\ Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Kullanıcı Hesabı Denetimi: Yükseltme istenirken güvenli masaüstüne geçin*

**2.3.17.8 (L1) 'Kullanıcı Hesabı Denetimi: Dosya ve kayıt defteri yazma hatalarını kullanıcı başına konumlara sanallaştır' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, uygulama yazma hatalarının tanımlanan kayıt defteri ve dosya sistemi konumlarına yönlendirilip yönlendirilmeyeceğini denetler. Bu ilke ayarı, yönetici olarak çalışan ve çalışma zamanı uygulama verilerini şunlara yazan uygulamaları azaltır:

* %ProgramFiles%
* %windir%
* %windir%\System32
* HKEY\_LOCAL\_MACHINE\SOFTWARE

Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bu ayar, eski uygulamaların yalnızca izin verilen konumlara veri yazmasını sağlayarak güvenlik açıklarını azaltır.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: EnableVirtualization*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\ Windows Ayarları\Güvenlik Ayarları\Yerel İlkeler\Güvenlik Seçenekleri\Kullanıcı Hesabı Denetimi: Dosya ve kayıt defteri yazma hatalarını kullanıcı başına konumlara sanallaştırın*

**5 Sistem Hizmetleri**

**5.1 (L2) 'Bluetooth Ses Ağ Geçidi Hizmeti (BTAGService)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bluetooth Eller Serbest Profilinin ses ağ geçidi rolünü destekleyen hizmet. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bluetooth teknolojisinin kendine özgü güvenlik riskleri vardır - özellikle v2.1 standardından önce. Kablosuz Bluetooth trafiği (hiç değilse) iyi bir şekilde şifrelenmemiştir, bu nedenle yüksek güvenlikli bir ortamda, Bluetooth cihazlarını kullanamama gibi ek rahatsızlığa rağmen buna izin verilmemelidir.

**Etki:**

Bluetooth eller serbest aygıtları bilgisayarla düzgün çalışmayacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\BTAGService:Start*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\ Güvenlik Ayarları\Sistem Hizmetleri\Bluetooth Ses Ağ Geçidi Hizmeti*

**Not:** Bu hizmet ilk olarak Windows 10 Sürüm 1803'te tanıtıldı. Bu sürümde Windows'tan kaldırılan eski Bluetooth Eller Serbest Hizmetinin (BthHFSrv) yerini almış gibi görünüyor (yalnızca bir yeniden adlandırma, ancak farklı bir hizmet).

**5.2 (L2) 'Bluetooth Destek Hizmeti (bthserv)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bluetooth hizmeti, uzak Bluetooth cihazlarının keşfedilmesini ve ilişkilendirilmesini destekler. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bluetooth teknolojisinin kendine özgü güvenlik riskleri vardır - özellikle v2.1 standardından önce. Kablosuz Bluetooth trafiği (hiç değilse) iyi bir şekilde şifrelenmemiştir, bu nedenle yüksek güvenlikli bir ortamda, Bluetooth cihazlarını kullanamama gibi ek rahatsızlığa rağmen buna izin verilmemelidir.

**Etki:**

Halihazırda kurulmuş Bluetooth cihazları düzgün çalışmayabilir ve yeni cihazların keşfedilmesi veya ilişkilendirilmesi engellenebilir. Bluetooth aygıtları kurulmuşsa, Aygıtlar ve Yazıcılar gibi bazı Windows bileşenleri doğru şekilde çalışmayabilir - açıldığında askıda kalma/donma dahil. Çözüm, bu hizmeti yeniden etkinleştirmenin yanı sıra, Aygıt Yöneticisi'nde sorunlu Bluetooth aygıtlarını devre dışı bırakmak veya silmek veya aygıtı sistem BIOS'u (yerleşik bir Bluetooth aygıtıysa) aracılığıyla tamamen devre dışı bırakmaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\bthserv: Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Bluetooth Destek Hizmeti*

**5.3 (L1) 'Bilgisayar Tarayıcısı (Browser)' seçeneği 'Devre Dışı' veya 'Yüklü Değil' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Ağdaki bilgisayarların güncel bir listesini tutar ve bu listeyi tarayıcı olarak belirlenmiş bilgisayarlara sağlar. Bu ayar için önerilen durum şudur: Devre Dışı veya Yüklenmedi.

**Not:** Windows 8.1 ve Windows 10'da bu hizmet, isteğe bağlı SMB 1.0/CIFS Dosya Paylaşım Desteği özelliği ile birlikte gelir. Sonuç olarak, bu özelliğin kaldırılması (XP/2003 ve daha eski Windows işletim sistemlerinde geriye dönük uyumluluk gerekmedikçe şiddetle tavsiye edilir - bkz. Bu özellik, Windows 10 R1709'dan başlayarak varsayılan olarak yüklenmez.

**Gerekçe:**

Bu eski bir hizmettir - tek amacı bilgisayarların ve ortamdaki ağ paylaşımlarının bir listesini tutmaktır (yani "Ağ Komşuları"). Etkinleştirilirse, kimin "ana tarayıcı" olacağını görmek için "seçimler" de dahil olmak üzere birçok gereksiz trafik oluşturur. Bu gürültülü trafik, kötü niyetli saldırganların çevrimiçi makineleri keşfetmesine de yardımcı olabilir, çünkü hizmet aynı zamanda herkesin herhangi bir kimlik doğrulaması olmadan paylaşılan kaynaklara "göz atmasına" izin verir. Bu hizmet, eski Windows sürümlerinde (örn. Windows XP) varsayılan olarak çalışırdı, ancak bugün yalnızca bunu gerektiren çok eski yazılımlar için geriye dönük uyumluluk için kalır.

**Etki:**

Bilgisayarların listesi ve ağdaki paylaşımları güncellenmeyecek veya korunmayacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Browser:Start*

**Düzeltme:** GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı veya hizmetin kurulu olmadığından emin olun.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Bilgisayar Tarayıcısı*

**5.4 (L2) 'İndirilen Haritalar Yöneticisi (MapsBroker)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

İndirilen haritalara uygulama erişimi için Windows hizmeti. Bu hizmet, indirilen haritalara erişen uygulama tarafından talep üzerine başlatılır.

**Gerekçe:**

Haritalama teknolojileri, saldırganlara ve bilgileri alan diğer yazılımlara isteksizce konumunuzu gösterebilir. Ayrıca, gerekli olmadığında 3. taraf kaynaklardan gelen verilerin otomatik olarak indirilmesi en aza indirilmelidir. Bu nedenle yüksek güvenlikli ortamlarda bu hizmete ihtiyaç duyulmamalıdır.

**Etki:**

Uygulamaların harita verilerine erişmesi engellenecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\MapsBroker:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\İndirilen Haritalar Yöneticisi*

**5.5 (L2) 'Coğrafi Konum Hizmeti (lfsvc)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu hizmet, sistemin geçerli konumunu izler ve coğrafi sınırları yönetir (ilişkili olaylarla birlikte bir coğrafi konum). Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bu ayar, konum özelliğini etkiler (ör. GPS veya diğer konum izleme). Güvenlik açısından, çoğu durumda yazılıma konumunuzu açıklamak iyi bir fikir değildir, ancak haritalama yazılımı gibi meşru kullanımlar vardır. Ancak, yüksek güvenlikli ortamlarda kullanılmamalıdırlar.

**Etki:**

Uygulamalar, coğrafi konum veya coğrafi sınırlar için bildirimleri kullanamayacak veya alamayacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\lfsvc:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Coğrafi Konum Hizmeti*

**5.6 (L1) 'IIS Yönetim Hizmeti (IISADMIN)' seçeneği 'Devre Dışı' veya 'Yüklenmemiş' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Sunucunun IIS metatabanını yönetmesini sağlar. IIS metatabanı, SMTP ve FTP hizmetleri için yapılandırmayı depolar. Bu ayar için önerilen durum şudur: Devre Dışı veya Yüklenmedi.

**Not:** Bu hizmet varsayılan olarak yüklenmez. Windows ile birlikte sağlanır, ancak isteğe bağlı bir Windows özelliği (İnternet Bilgi Hizmetleri) etkinleştirilerek yüklenir.

**Not 2:** Bir kuruluş, web sayfalarını yerel olarak test etmeleri ve geliştirmeleri için iş istasyonlarında IIS'ye (veya başka bir web sunucusuna) izin vermeleri için web geliştiricilerine seçici olarak istisnalar vermeyi seçebilir. Ancak, kuruluş bu makineleri izlemeli ve uzlaşma riskini azaltmak için güvenlik kontrollerinin ve azaltmaların güncel tutulmasını sağlamalıdır.

**Gerekçe:**

Bir iş istasyonundan bir web sitesi barındırmak, bu iş istasyonunun saldırı yüzeyi büyük ölçüde arttığından, artan bir güvenlik riskidir. Uygun güvenlik azaltma önlemleri izlenmezse, başarılı saldırı şansı önemli ölçüde artar.

**Not:** Bu güvenlik sorunu, yalnızca IIS için değil, bir iş istasyonuna yüklenen herhangi bir web sunucusu uygulaması için geçerlidir.

**Etki:**

Web, SMTP veya FTP hizmetleri dahil olmak üzere IIS çalışmayacaktır. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\IISADMIN:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı veya hizmetin kurulu olmadığından emin olun.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\IIS Yönetici Hizmeti*

**5.7 (L1) 'Kızılötesi monitör hizmeti (irmon)' seçeneği 'Devre Dışı' veya 'Yüklü Değil' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Menzildeki diğer Kızılötesi cihazları algılar ve dosya aktarım uygulamasını başlatır. Bu ayar için önerilen durum şudur: Devre Dışı veya Yüklü Değil.

**Gerekçe:**

Kızılötesi bağlantılar, özellikle otomatik "dosya aktarım uygulaması" işlevi aracılığıyla, potansiyel olarak bir veri güvenliği ihlali kaynağı olabilir. Kurumsal yönetilen sistemler, kızılötesinden daha güvenli bir bağlantı yöntemi kullanmalıdır.

**Etki:**

Kızılötesi dosya aktarımlarının çalışması engellenecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\irmon:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu şu şekilde ayarlayın: Devre dışı bırakıldı veya hizmetin kurulu olmadığından emin olun.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Kızılötesi monitör hizmeti*

**5.8 (L1)** **'İnternet Bağlantısı Paylaşımı (ICS) (SharedAccess)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bir ev veya küçük ofis ağı için ağ erişim çevirisi, adresleme, ad çözümleme ve/veya izinsiz giriş önleme hizmetleri sağlar. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

İnternet Bağlantı Paylaşımı (ICS), birinin İnternet bağlantısını ağdaki diğer makinelerle "paylaşmasını" sağlayan bir özelliktir - yalnızca bir makinenin İnternet erişimine sahip olduğu ev veya küçük ofis ortamları için tasarlanmıştır - bu makineyi etkin bir şekilde döndürür bir İnternet yönlendiricisine. Bu özellik, ağların köprülenmesine ve muhtemelen diğer, daha güvenli yolların atlanmasına neden olur. Herhangi bir kuruluş tarafından yönetilen sistemde kullanılmamalıdır.

**Etki:**

İnternet Bağlantı Paylaşımı (ICS) kullanılamayacak. Miracast kullanan kablosuz bağlantılar da engellenecektir.

**Not:** Bu hizmet, Windows 10'daki Microsoft Defender Uygulama Koruması özelliği için bir ön koşuldur, bu nedenle Microsoft Defender Uygulama Koruması'nı kullanmayı planlıyorsanız bu öneriye bir istisna yapılmalıdır.

**Not #2**: Kuruluşunuz Linux için Windows Alt Sistemini (WSL) kullanıyorsa, WSL'nin çalışması için bu hizmet gereklidir, bu nedenle bu öneriye bir istisna yapılmalıdır. Daha fazla bilgi için lütfen aşağıdaki Microsoft Blogunu ziyaret edin: [Linux için Windows Alt Sisteminde Sorun Giderme | Microsoft Belgeleri](https://docs.microsoft.com/en-us/windows/wsl/troubleshooting#wsl-2-errors-when-ics-is-disabled)

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SharedAccess:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\İnternet Bağlantı Paylaşımı (ICS)*

**5.9 (L2) 'Bağlantı Katmanı Topolojisi Keşif Eşleştiricisi' (lltdsvc)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bilgisayar ve cihaz topolojisi (bağlantı) bilgilerinden ve her bir bilgisayarı ve cihazı açıklayan meta verilerden oluşan bir Ağ Haritası oluşturur. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bu hizmetin etkinleştirdiği özellik, yetkisiz keşif ve ağ cihazlarına bağlantı için potansiyel olarak kullanılabilir. Hizmetin devre dışı bırakılması, yüksek güvenlikli ortamlarda ağ topolojisi keşfi isteklerine yanıt verilmesini önlemeye yardımcı olur.

**Etki**:

Ağ Haritası düzgün çalışmayacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\lltdsvc:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Bağlantı Katmanı Topolojisi Bulma Eşleyicisi*

**5.10 (L1) 'LxssManager (LxssManager)' seçeneği 'Devre Dışı' veya 'Yüklenmedi' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

LXSS Manager hizmeti, yerel ELF ikili dosyalarının çalıştırılmasını destekler. Hizmet, ELF ikili dosyalarının Windows üzerinde çalışması için gerekli altyapıyı sağlar. Bu ayar için önerilen durum şudur: Devre Dışı veya Yüklü Değil.

**Not:** Bu hizmet varsayılan olarak yüklenmez. Windows ile birlikte sağlanır, ancak isteğe bağlı bir Windows özelliği etkinleştirilerek yüklenir (Linux için Windows Alt Sistemi).

**Gerekçe:**

Linux Alt Sistemi (LXSS) Yöneticisi, dosya sistemi de dahil olmak üzere Windows'taki Linux uygulamalarına tam sistem erişimi sağlar. Bu, bu uygulamaları çalıştırmak için kesinlikle bazı işlevsellik ve performans avantajlarına sahip olsa da, bir bilgisayar korsanının bir Linux uygulamasına kötü amaçlı kod eklemesi durumunda yeni güvenlik riskleri de oluşturur. En iyi güvenlik için Linux üzerinde Linux uygulamalarının, Windows üzerinde Windows uygulamalarının çalıştırılması tercih edilir.

**Etki:**

Linux Alt Sistemi kullanılamayacak ve yerel ELF ikili dosyaları artık çalışmayacak. Not: Kuruluşunuz bu öneriye bir istisna yaptıysa ve Linux için Windows Alt Sistemini (WSL) kullanıyorsa, WSL'nin çalışması için İnternet Bağlantı Paylaşımı (ICS) (SharedAccess) hizmetinin Etkinleştirilmesi gerekir. Daha fazla bilgi için lütfen aşağıdaki Microsoft Blogunu ziyaret edin: [Linux için Windows Alt Sisteminde Sorun Giderme | Microsoft Docs](https://docs.microsoft.com/en-us/windows/wsl/troubleshooting#wsl-2-errors-when-ics-is-disabled)

**Denetim:**

Düzeltme bölümünde belirtilen Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LxssManager:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı veya hizmetin kurulu olmadığından emin olun.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\LxssManager*

**5.11 (L1) 'Microsoft FTP Hizmeti (FTPSVC)' seçeneği 'Devre Dışı' veya 'Yüklü Değil' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Sunucunun bir Dosya Aktarım Protokolü (FTP) sunucusu olmasını sağlar. Bu ayar için önerilen durum şudur: Devre Dışı veya Yüklü Değil.

**Not:** Bu hizmet varsayılan olarak yüklenmez. Windows ile birlikte sağlanır, ancak isteğe bağlı bir Windows özelliği etkinleştirilerek yüklenir (İnternet Bilgi Hizmetleri - FTP Sunucusu).

**Gerekçe:**

Bir iş istasyonundan bir FTP sunucusunun (özellikle güvenli olmayan bir FTP sunucusunun) barındırılması, bu iş istasyonunun saldırı yüzeyi büyük ölçüde arttığından, artan bir güvenlik riskidir.

**Not:** Bu güvenlik sorunu, yalnızca IIS için değil, bir iş istasyonuna yüklenen tüm FTP sunucu uygulamaları için geçerlidir.

**Etki:**

Bilgisayar bir FTP sunucusu olarak çalışmayacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\FTPSVC:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı veya hizmetin kurulu olmadığından emin olun.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Microsoft FTP Hizmeti*

**5.12 (L2) 'Microsoft iSCSI Başlatıcı Hizmeti (MSiSCSI)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu bilgisayardan uzak hedef cihazlara İnternet SCSI (iSCSI) oturumlarını yönetir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bu hizmet, bir iSCSI aygıtına doğrudan bağlanmak için kritik derecede gereklidir. Bununla birlikte, iSCSI'nin kendisi çok zayıf bir kimlik doğrulama protokolü (CHAP) kullanır; bu, tüm trafik yalıtılmadıkça ve/veya IPsec gibi başka bir teknoloji kullanılarak şifrelenmedikçe, iSCSI iletişimi için parolaların kolayca açığa çıkarılacağı anlamına gelir. Bu hizmet genellikle kontrollü bir ortamdaki sunucular için yüksek güvenlik gerektiren iş istasyonlarına göre daha uygundur.

**Etki:**

Bilgisayar, iSCSI hedeflerine doğrudan giriş yapamayacak veya bu hedeflere erişemeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\MSiSCSI:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Microsoft iSCSI Başlatıcı Hizmeti*

**5.13 (L1) 'OpenSSH SSH Sunucusu (sshd)' seçeneği 'Devre Dışı' veya 'Yüklü Değil' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Güvenli olmayan bir ağ üzerinden güvenilmeyen iki ana bilgisayar arasında güvenli şifreli iletişim sağlamak için SSH protokolü tabanlı hizmet. Bu ayar için önerilen durum şudur: Devre Dışı veya Yüklü Değil.

**Not:** Bu hizmet varsayılan olarak yüklenmez. Windows ile birlikte sağlanır, ancak isteğe bağlı bir Windows özelliği (OpenSSH Sunucusu) etkinleştirilerek yüklenir.

**Gerekçe:**

Bir iş istasyonundan bir SSH sunucusu barındırmak, bu iş istasyonunun saldırı yüzeyi büyük ölçüde arttığından, artan bir güvenlik riskidir.

**Not:** Bu güvenlik sorunu, yalnızca Windows ile sağlananlar için değil, bir iş istasyonuna yüklenen tüm SSH sunucu uygulamaları için geçerlidir.

**Etki:**

İş istasyonunun bir SSH ana bilgisayar sunucusu olmasına izin verilmeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\sshd:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre dışı veya hizmetin kurulu olmadığından emin olun.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\OpenSSH SSH Sunucusu*

**5.14 (L2) 'Eş Adı Çözümleme Protokolü (PNRPsvc)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Eş Adı Çözümleme Protokolü'nü (PNRP) kullanarak İnternet üzerinden sunucusuz eş adı çözümlemesini etkinleştirir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Eş Adı Çözümleme Protokolü, istemcilerin birbirleriyle ad çözümlemesini gerçekleştirmenin dağıtılmış ve (çoğunlukla) sunucusuz bir yoludur. Yüksek güvenlikli bir ortamda, yetkili personel tarafından yürütülen merkezi ad çözümleme yöntemlerine güvenmek daha güvenlidir.

**Etki:**

Uzaktan Yardım gibi bazı eşler arası ve işbirliğine dayalı uygulamalar çalışmayabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\PNRPsvc:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Eş Adı Çözümleme Protokolü*

**5.15 (L2) 'Eş Ağ Gruplaması (p2psvc)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Eşler Arası Gruplama kullanarak çok taraflı iletişimi etkinleştirir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Eş Adı Çözümleme Protokolü, istemcilerin birbirleriyle ad çözümlemesini gerçekleştirmenin dağıtılmış ve (çoğunlukla) sunucusuz bir yoludur. Yüksek güvenlikli bir ortamda, yetkili personel tarafından yürütülen merkezi ad çözümleme yöntemlerine güvenmek daha güvenlidir.

**Etki:**

Ev Grubu gibi bazı uygulamalar çalışmayabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\p2psvc:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Eş Ağ Gruplaması*

**5.16 (L2) 'Peer Networking Identity Manager (p2pimsvc)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Eş Adı Çözümleme Protokolü (PNRP) ve Eşler Arası Gruplama hizmetleri için kimlik hizmetleri sağlar. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Eş Adı Çözümleme Protokolü, istemcilerin birbirleriyle ad çözümlemesini gerçekleştirmenin dağıtılmış ve (çoğunlukla) sunucusuz bir yoludur. Yüksek güvenlikli bir ortamda, yetkili personel tarafından yürütülen merkezi ad çözümleme yöntemlerine güvenmek daha güvenlidir.

**Etki:**

Eş Adı Çözümleme Protokolü (PNRP) ve Eşler Arası Gruplandırma hizmetleri çalışmayabilir ve Ev Grubu ve Uzaktan Yardım gibi bazı uygulamalar düzgün çalışmayabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\p2pimsvc:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Eş Ağ Kimliği Yöneticisi*

**5.17 (L2) 'PNRP Machine Name Publication Service (PNRPAutoReg)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:** Bu hizmet, Eş Adı Çözümleme Protokolünü kullanarak bir makine adı yayınlar. Yapılandırma, netsh bağlamı "p2p pnrp eş" aracılığıyla yönetilir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Eş Adı Çözümleme Protokolü, istemcilerin birbirleriyle ad çözümlemesini gerçekleştirmenin dağıtılmış ve (çoğunlukla) sunucusuz bir yoludur. Yüksek güvenlikli bir ortamda, yetkili personel tarafından yürütülen merkezi ad çözümleme yöntemlerine güvenmek daha güvenlidir.

**Etki:**

Uzaktan Yardım gibi bazı eşler arası ve işbirliğine dayalı uygulamalar çalışmayabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\PNRPAutoReg:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\PNRP Makine Adı Yayın Hizmeti*

**5,18 (L2) 'Yazdırma Biriktiricisi (Spooler)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu hizmet, yazdırma işlerini biriktirir ve yazıcılarla etkileşimi yönetir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Yüksek güvenlikli bir ortamda, özellikle zafiyetleri bilinen gereksiz servisler devre dışı bırakılmalıdır. Yazdırma Biriktiricisi (Biriktirici) hizmetini devre dışı bırakmak, PrintNightmare güvenlik açığını (CVE-2021-34527) ve hizmete yönelik diğer saldırıları azaltır.

**Etki:**

Kullanıcılar, Yazdırma Biriktiricisi hizmetini kullanan dosyalara (Adobe Portable Document Format (PDF) gibi) yazdırma da dahil olmak üzere yazdıramaz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Spooler:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki kullanıcı arabirimi yolunu şu şekilde ayarlayın: Devre Dışı:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Yazdırma Biriktiricisi*

**5.19 (L2) 'Sorun Raporları ve Çözümleri Denetim Masası Desteği (wercplsupport)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu hizmet, Sorun Raporları ve Çözümleri kontrol paneli için sistem düzeyinde sorun raporlarının görüntülenmesi, gönderilmesi ve silinmesi için destek sağlar. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bu hizmet, sorunları ve Microsoft'a/ Microsoft'tan gelen çözümleri görüntüleme/bildirme sürecinde yer alır. Yüksek güvenlikli bir ortamda, bu bilgilerin gönderilmesini engellemek, hassas kurumsal bilgiler için gizlilik endişelerini azaltmaya yardımcı olabilir.

**Etki:**

Microsoft'a ve Microsoft'tan sistem düzeyinde sorun raporları ve çözümleri gönderme ve görüntüleme artık çalışmayabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\wercplsupport:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Sorun Raporları ve Çözümleri Denetim Masası Desteği*

**5.20 (L2) 'Uzaktan Erişim Otomatik Bağlantı Yöneticisi (RasAuto)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bir program uzak bir DNS veya NetBIOS adına veya adresine başvurduğunda uzak bir ağa bağlantı oluşturur. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bu hizmetin işlevi, "isteğe bağlı arama" türünde bir işlevsellik sağlamaktır. Yüksek güvenlikli bir ortamda, herhangi bir uzak "çevirme" bağlantısının (ister eski çevirmeli POTS ister VPN olsun) sistem tarafından otomatik olarak değil, kullanıcı tarafından başlatılması tercih edilir.

**Etki:**

"İstek üzerine arama" işlevi artık çalışmayacak - uzaktan arama (POTS) ve VPN bağlantıları kullanıcı tarafından manuel olarak başlatılmalıdır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\RasAuto:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Uzaktan Erişim Otomatik Bağlantı Yöneticisi*

**5.21 (L2) 'Uzak Masaüstü Yapılandırması (SessionEnv)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Uzak Masaüstü Yapılandırma hizmeti (RDCS), SYSTEM bağlamı gerektiren Uzak Masaüstü ile ilgili tüm yapılandırma ve oturum bakım etkinliklerinden sorumludur. Bunlar, oturum başına geçici klasörleri, RD temalarını ve RD sertifikalarını içerir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Yüksek güvenlikli bir ortamda Uzak Masaüstü erişimi, artan bir güvenlik riskidir. Bu ortamlar için yalnızca yerel konsol erişimine izin verilmelidir.

**Etki:**

Kullanıcılar Uzaktan Yardım'ı kullanamayacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SessionEnv:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Uzak Masaüstü Yapılandırması*

**5.22 (L2) 'Uzak Masaüstü Hizmetleri (TermService)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Kullanıcıların uzak bir bilgisayara etkileşimli olarak bağlanmasına izin verir. Uzak Masaüstü ve Uzak Masaüstü Oturum Ana Sunucusu bu hizmete bağlıdır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Yüksek güvenlikli bir ortamda Uzak Masaüstü erişimi, artan bir güvenlik riskidir. Bu ortamlar için yalnızca yerel konsol erişimine izin verilmelidir.

**Etki:**

Uzak Masaüstü Hizmetleri bilgisayarda kullanılamayacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\TermService:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Uzak Masaüstü Hizmetleri*

**5.23 (L2) 'Uzak Masaüstü Hizmetleri Kullanıcı Modu Bağlantı Noktası Yeniden Yönlendiricisi (UmRdpService)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Yazıcıların/Sürücülerin/Bağlantı Noktalarının RDP bağlantıları için yeniden yönlendirilmesine izin verir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Güvenlik açısından hassas bir ortamda, olası saldırı yüzeyinin azaltılması arzu edilir - COM, LPT ve PnP bağlantı noktalarının yeniden yönlendirilmesini önlemek, bir RDP oturumu içinde veri hırsızlığı ve/veya kötü amaçlı kod aktarımı için beklenmeyen yolların sayısını azaltacaktır.

**Etki:**

Yazıcıların, sürücülerin ve bağlantı noktalarının (COM, LPT, PnP vb.) RDP oturumları içinde yeniden yönlendirilmesine izin verilmeyecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\UmRdpService:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Uzak Masaüstü Hizmetleri Kullanıcı Modu Bağlantı Noktası Yönlendiricisi*

**5.24 (L1) 'Uzaktan Yordam Çağrısı (RPC) Konum Belirleyicisi (RpcLocator)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Windows 2003 ve Windows'un daha eski sürümlerinde, Uzaktan Yordam Çağrısı (RPC) Bulucu hizmeti, RPC ad hizmeti veritabanını yönetir. Windows Vista ve Windows'un daha yeni sürümlerinde, bu hizmet herhangi bir işlevsellik sağlamaz ve uygulama uyumluluğu için mevcuttur. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bu, çok eski yazılımlar için uygulama uyumluluğu dışında hiçbir değeri veya amacı olmayan eski bir hizmettir. Sistemde hala kullanımda olan belirli bir eski uygulama olmadığı sürece devre dışı bırakılmalıdır.

**Etki:**

Eski, eski bir uygulama gerektirmediği sürece etkisi yoktur.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\RpcLocator:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Uzaktan Yordam Çağrısı (RPC) Bulucu*

**5.25 (L2) 'Uzak Kayıt Defteri (RemoteRegistry)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Uzak kullanıcıların bu bilgisayardaki kayıt defteri ayarlarını görüntülemesine ve değiştirmesine olanak tanır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Yüksek güvenlikli bir ortamda, kayıt defterini uzaktan erişime açmak, artan bir güvenlik riskidir.

**Etki:**

Kayıt defteri yalnızca bilgisayardaki kullanıcılar tarafından görüntülenebilir ve değiştirilebilir.

**Not:** System Center Configuration Manager (SCCM) gibi birçok uzaktan yönetim aracı, uzaktan yönetim için Remote Registry hizmetinin çalışır durumda olmasını gerektirir. Ayrıca birçok güvenlik açığı tarayıcısı, kayıt defterine uzaktan erişmek için bu hizmeti kullanır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteRegistry:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Uzak Kayıt Defteri*

**5.26 (L1) 'Yönlendirme ve Uzaktan Erişim (RemoteAccess)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Yerel alan ve geniş alan ağı ortamlarında işletmelere yönlendirme hizmetleri sunar. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bu hizmetin ana amacı, Windows yönlendirici işlevselliği sağlamaktır - bu, kurumsal yönetilen bir ortamda iş istasyonlarının uygun kullanımı değildir.

**Etki:**

Bilgisayar, farklı bağlantılar arasında bir Windows yönlendiricisi olarak yapılandırılamayacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\RemoteAccess:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Yönlendirme ve Uzaktan Erişim*

**5.27 (L2) 'Sunucu (LanmanServer)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu bilgisayar için ağ üzerinden dosya, yazdırma ve adlandırılmış boru paylaşımını destekler. Bu hizmet durdurulursa, bu işlevler kullanılamayacaktır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Yüksek güvenlikli bir ortamda, güvenli bir iş istasyonu bir sunucu değil, yalnızca bir istemci olmalıdır. İş istasyonu kaynaklarını uzaktan erişim için paylaşmak, saldırı yüzeyi önemli ölçüde daha yüksek olduğundan güvenlik riskini artırır.

**Etki**:

Dosya, yazdırma ve adlandırılmış boru paylaşım işlevleri bu makineden ağ üzerinden kullanılamayacak. Not: System Center Configuration Manager (SCCM) gibi birçok uzaktan yönetim aracı, uzaktan yönetim için Sunucu hizmetinin çalışır durumda olmasını gerektirir. Ayrıca birçok güvenlik açığı tarayıcısı, dosya sistemini uzaktan taramak için bu hizmeti kullanır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Sunucu*

**5.28 (L1) 'Basit TCP/IP Hizmetleri (simptcp)' seçeneği 'Devre Dışı' veya 'Yüklenmemiş' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu bilgisayar için ağ üzerinden dosya, yazdırma ve adlandırılmış boru paylaşımını destekler. Bu hizmet durdurulursa, bu işlevler kullanılamayacaktır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Yüksek güvenlikli bir ortamda, güvenli bir iş istasyonu bir sunucu değil, yalnızca bir istemci olmalıdır. İş istasyonu kaynaklarını uzaktan erişim için paylaşmak, saldırı yüzeyi önemli ölçüde daha yüksek olduğundan güvenlik riskini artırır.

**Etki:**

Dosya, yazdırma ve adlandırılmış boru paylaşım işlevleri bu makineden ağ üzerinden kullanılamayacak.

**Not:** System Center Configuration Manager (SCCM) gibi birçok uzaktan yönetim aracı, uzaktan yönetim için Sunucu hizmetinin çalışır durumda olmasını gerektirir. Ayrıca birçok güvenlik açığı tarayıcısı, dosya sistemini uzaktan taramak için bu hizmeti kullanır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Sunucu*

**5.29 (L2) 'SNMP Hizmeti (SNMP)' seçeneği 'Devre Dışı' veya 'Yüklenmemiş' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Basit Ağ Yönetimi Protokolü (SNMP) isteklerinin bu bilgisayar tarafından işlenmesini sağlar. Bu ayar için önerilen durum şudur: Devre Dışı veya Yüklenmedi.

**Not:** Bu hizmet varsayılan olarak yüklenmez. Windows ile birlikte sağlanır, ancak isteğe bağlı bir Windows özelliği (Basit Ağ Yönetimi Protokolü (SNMP)) etkinleştirilerek yüklenir.

**Gerekçe**:

Gelen ağ bağlantılarını etkinleştiren özellikler saldırı yüzeyini artırır. Yüksek güvenlikli bir ortamda, güvenli iş istasyonlarının yönetimi yerel olarak ele alınmalıdır.

**Etki:**

Bilgisayar SNMP isteklerini işleyemeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SNMP:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre dışı veya hizmetin kurulu olmadığından emin olun.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\SNMP Hizmeti*

**5.30 (L1) 'Özel Yönetim Konsol Yardımcısı (sacsvr)' seçeneği 'Devre Dışı' veya 'Yüklenmemiş' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu hizmet, yöneticilerin Acil Durum Yönetim Hizmetlerini kullanarak bir komut istemine uzaktan erişmesine olanak tanır. Bu ayar için önerilen durum şudur: Devre Dışı veya Yüklenmedi.

**Not:** Bu hizmet varsayılan olarak yüklenmez. Windows ile birlikte sağlanır, ancak isteğe bağlı bir Windows özelliği etkinleştirilerek yüklenir (Windows Acil Durum Yönetim Hizmetleri ve Seri Konsol).

**Gerekçe:**

Bir bilgisayarda uzaktan yönetim görevlerini gerçekleştirme yeteneği sağlayan uzaktan erişilebilir bir komut isteminin kullanımına izin vermek bir güvenlik riskidir.

**Etki:**

Kullanıcılar, Acil Durum Yönetim Hizmetlerini kullanarak uzaktan komut istemine erişemeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\sacsvr:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre dışı veya hizmetin kurulu olmadığından emin olun.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Özel Yönetim Konsolu Yardımcısı*

**5,31 (L1) 'SSDP Bulma (SSDPSRV)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

UPnP cihazları gibi SSDP keşif protokolünü kullanan ağ bağlantılı cihazları ve hizmetleri keşfeder. Ayrıca yerel bilgisayarda çalışan SSDP cihazlarını ve hizmetlerini duyurur. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Evrensel Tak ve Çalıştır (UPnP) gerçek bir güvenlik riskidir - otomatik keşif ve ağ cihazlarının bağlanmasına izin verir. UPnP'nin normal Tak ve Çalıştır'dan (PnP) farklı olduğunu unutmayın. İş istasyonları, güvenlik bilincine sahip bir kurumsal yönetilen ortamda hizmetlerinin reklamını yapmamalı (veya ağ bağlantılı hizmetleri otomatik olarak keşfetme ve bunlara bağlanma).

**Etki:**

SSDP tabanlı cihazlar keşfedilmeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\SSDPSRV:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\SSDP Keşfi*

**5,32 (L1) 'UPnP Device Host (upnphost)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

UPnP cihazlarının bu bilgisayarda barındırılmasına izin verir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Evrensel Tak ve Çalıştır (UPnP) gerçek bir güvenlik riskidir - otomatik keşif ve ağ cihazlarının bağlanmasına izin verir. UPnP'nin normal Tak ve Çalıştır'dan (PnP) farklı olduğunu not eder. İş istasyonları, güvenlik bilincine sahip kurumsal yönetilen bir ortamda hizmetlerinin reklamını yapmamalı (veya ağ bağlantılı hizmetleri otomatik olarak keşfetme ve bunlara bağlanma).

**Etki:**

Barındırılan tüm UPnP cihazları çalışmayı durduracak ve barındırılan başka cihazlar eklenemez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\upnphost:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\UPnP Aygıt Ana Bilgisayarı*

**5.33 (L1) 'Web Yönetim Hizmeti (WMSvc)' seçeneği 'Devre Dışı' veya 'Yüklü Değil' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Web Yönetim Hizmeti, yöneticilerin makinede bulunan Web sunucusu, siteler ve uygulamaları yönetmeleri için uzaktan ve yetki verilmiş yönetim yetenekleri sağlar. Bu ayar için önerilen durum şudur: Devre Dışı veya Yüklü Değil.

**Not:** Bu hizmet varsayılan olarak yüklenmez. Windows ile birlikte sağlanır, ancak isteğe bağlı bir Windows özelliği etkinleştirilerek yüklenir (İnternet Bilgi Hizmetleri - Web Yönetim Araçları - IIS Yönetim Hizmeti).

**Gerekçe:**

Bir iş istasyonunda IIS'nin uzaktan web yönetimi, bu iş istasyonunun saldırı yüzeyi büyük ölçüde arttığından, artan bir güvenlik riskidir. Uygun güvenlik azaltma önlemleri izlenmezse, başarılı saldırı şansı önemli ölçüde artar.

**Etki:**

IIS'nin uzaktan web tabanlı yönetimi kullanılamayacak. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\WMSvc:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre dışı veya hizmetin kurulu olmadığından emin olun.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Web Yönetim Hizmeti*

**5.34 (L2) 'Windows Hata Raporlama Hizmeti (WerSvc)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Programlar çalışmayı veya yanıt vermeyi durdurduğunda hataların bildirilmesine ve mevcut çözümlerin teslim edilmesine olanak tanır. Ayrıca tanılama ve onarım hizmetleri için günlüklerin oluşturulmasına izin verir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Güvenli, kurumsal olarak yönetilen bir ortamda bir Windows Hatası oluşursa, sorun giderme ve düzeltme için hata doğrudan BT personeline bildirilmelidir. Bu hataları doğrudan Microsoft'a bildirmenin şirkete hiçbir faydası yoktur ve hatanın bir parçası olarak hassas verilerin bilmeden açığa çıkma riski vardır.

**Etki:**

Bu hizmet durdurulursa, hata raporlama düzgün çalışmayabilir ve tanılama hizmetleri ve onarımların sonuçları görüntülenmeyebilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\WerSvc:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Windows Hata Raporlama Hizmeti*

**5,35 (L2) 'Windows Olay Toplayıcısı (Wecsvc)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Programlar çalışmayı veya yanıt vermeyi durdurduğunda hataların bildirilmesine ve mevcut çözümlerin teslim edilmesine olanak tanır. Ayrıca tanılama ve onarım hizmetleri için günlüklerin oluşturulmasına izin verir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Güvenli, kurumsal olarak yönetilen bir ortamda bir Windows Hatası oluşursa, sorun giderme ve düzeltme için hata doğrudan BT personeline bildirilmelidir. Bu hataları doğrudan Microsoft'a bildirmenin şirkete hiçbir faydası yoktur ve hatanın bir parçası olarak hassas verilerin bilmeden açığa çıkma riski vardır.

**Etki:**

Bu hizmet durdurulursa, hata raporlama düzgün çalışmayabilir ve tanılama hizmetleri ve onarımların sonuçları görüntülenmeyebilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\WerSvc:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Windows Hata Raporlama Hizmeti*

**5.36 (L1) 'Windows Media Player Ağ Paylaşım Hizmeti (WMPNetworkSvc)' seçeneği 'Devre Dışı' veya 'Yüklü Değil' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Evrensel Tak ve Kullan özelliğini kullanarak Windows Media Player kitaplıklarını diğer ağa bağlı oynatıcılar ve medya cihazlarıyla paylaşır. Bu ayar için önerilen durum şudur: Devre Dışı veya Yüklü Değil.

**Gerekçe**:

Media Player'dan medyanın ağ paylaşımının kurumsal yönetilen bir ortamda yeri yoktur.

**Etki:**

Windows Media Player kitaplıkları ağ üzerinden diğer cihazlar ve sistemlerle paylaşılmayacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\WMPNetworkSvc:Star*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre dışı veya hizmetin kurulu olmadığından emin olun.

Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem *Hizmetleri\Windows Media Player Ağ Paylaşımı Hizmeti*

**5.37 (L1) 'Windows Mobile Etkin Nokta Hizmeti (icssvc)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Hücresel veri bağlantısını başka bir cihazla paylaşma yeteneği sağlar. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Etki alanına bağlı bir bilgisayardan bir mobil erişim noktası çalıştırma yeteneği, dahili ağı kolayca savaş sürücülerine veya diğer bilgisayar korsanlarına maruz bırakabilir.

**Etki:**

Windows Mobile Hotspot özelliği kullanılamayacak. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\icssvc:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Windows Mobile Erişim Noktası Hizmeti*

**5.38 (L2) 'Windows Bildirim Gönderme Sistemleri Servisi (WpnService)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu hizmet, oturum 0'da çalışır ve aygıt ile WNS sunucusu arasındaki bağlantıyı yöneten bildirim platformunu ve bağlantı sağlayıcısını barındırır. Bu ayar için önerilen durum: Devre Dışı.

**Not:** Windows 10'un ilk iki sürümünde (R1507 ve R1511), bu hizmetin görünen adı başlangıçta Windows Anında Bildirimler Hizmeti olarak adlandırıldı - ancak Windows 10 R1607'den başlayarak Windows Anında İlet Bildirimleri Sistem Hizmeti olarak yeniden adlandırıldı.

**Gerekçe:**

Windows Anında Bildirim Hizmetleri (WNS), buluttan/İnternet'ten üçüncü taraf bildirimlerini ve güncellemelerini almak için bir mekanizmadır. Yüksek güvenlikli bir ortamda, özellikle kurum dışında barındırılan harici sistemlerin güvenli iş istasyonlarını etkilemesi engellenmelidir.

**Etki:**

Canlı Kutucuklar ve diğer özellikler canlı güncellemeleri almayacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\WpnService:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Windows Anında Bildirimler Sistem Hizmeti*

**5,39 (L2) 'Windows PushToInstall Hizmeti (PushToInstall)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu hizmet, diğer cihazlarda veya web'de çalışan Microsoft Store Uygulamasından cihaza aktarılan Uygulamaları yönetir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Yüksek güvenlikli yönetilen bir ortamda, uygulama kurulumları son kullanıcılar tarafından değil, BT personeli tarafından merkezi olarak yönetilmelidir.

**Etki:**

Kullanıcılar, diğer cihazlarda veya web'de çalışan Microsoft Store'dan Uygulamaları bu cihaza aktaramayacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\PushToInstall:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Windows PushToInstall Hizmeti (PushToInstall)*

**5,40 (L2) 'Windows Uzaktan Yönetim (WSManagement) (WinRM)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Windows Uzaktan Yönetim (WinRM) hizmeti, uzaktan yönetim için WS-Management protokolünü uygular. WS-Management, uzaktan yazılım ve donanım yönetimi için kullanılan standart bir web hizmetleri protokolüdür. WinRM hizmeti, ağda WS-Management isteklerini dinler ve bunları işler. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Gelen ağ bağlantılarını etkinleştiren özellikler saldırı yüzeyini artırır. Yüksek güvenlikli bir ortamda, güvenli iş istasyonlarının yönetimi yerel olarak ele alınmalıdır.

**Etki:**

Sistemi WinRM ile uzaktan yönetme yeteneği kaybolacak. Not: System Center Configuration Manager (SCCM) gibi birçok uzaktan yönetim aracı, uzaktan yönetim için WinRM hizmetinin çalışır durumda olmasını gerektirebilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\WinRM:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Windows Uzaktan Yönetimi (WS-Management)*

**5.41 (L1) 'World Wide Web Yayımlama Servisi (W3SVC)' seçeneği 'Devre Dışı' veya 'Yüklü Değil' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

İnternet Bilgi Hizmetleri Yöneticisi aracılığıyla Web bağlantısı ve yönetim sağlar. Bu ayar için önerilen durum şudur: Devre Dışı veya Yüklü Değil.

**Not:** Bu hizmet varsayılan olarak yüklenmez. Windows ile birlikte sağlanır, ancak isteğe bağlı bir Windows özelliği etkinleştirilerek yüklenir (Internet Information Services - World Wide Web Services).

**Not 2:** Bir kuruluş, web sayfalarını yerel olarak test etmeleri ve geliştirmeleri için web geliştiricilerine iş istasyonlarında IIS'ye (veya başka bir web sunucusuna) izin vermeleri için seçici olarak istisnalar vermeyi seçebilir. Ancak, kuruluş bu makineleri izlemeli ve uzlaşma riskini azaltmak için güvenlik kontrollerinin ve azaltmaların güncel tutulmasını sağlamalıdır.

**Gerekçe:**

Bir iş istasyonundan bir web sitesi barındırmak, bu iş istasyonunun saldırı yüzeyi büyük ölçüde arttığından, artan bir güvenlik riskidir. Uygun güvenlik azaltma önlemleri izlenmezse, başarılı saldırı şansı önemli ölçüde artar.

**Not:** Bu güvenlik sorunu, yalnızca IIS için değil, bir iş istasyonuna yüklenen herhangi bir web sunucusu uygulaması için geçerlidir.

**Etki:**

IIS Web Hizmetleri çalışmayacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\W3SVC:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı veya hizmetin kurulu olmadığından emin olun.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\World Wide Web Publishing Service*

**5.42 (L1) 'Xbox Aksesuar Yönetim Hizmeti (XboxGipSvc)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu hizmet, bağlı Xbox Aksesuarlarını yönetir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Xbox Live bir oyun hizmetidir ve kurumsal olarak yönetilen bir ortamda (belki bir oyun şirketi olmadığı sürece) yeri yoktur.

**Etki:**

Bağlı Xbox aksesuarları çalışmayabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\XboxGipSvc:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Xbox Aksesuar Yönetim Hizmeti*

**5.43 (L1) 'Xbox Live Kimlik Doğrulama Yöneticisi (XblAuthManager)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Xbox Live ile etkileşim için kimlik doğrulama ve yetkilendirme hizmetleri sağlar. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Xbox Live bir oyun hizmetidir ve kurumsal olarak yönetilen bir ortamda (belki bir oyun şirketi olmadığı sürece) yeri yoktur.

**Etki:**

Xbox Live bağlantıları başarısız olabilir ve bu hizmetle etkileşime giren uygulamalar da başarısız olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\XblAuthManager:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Xbox Live Auth Manager*

**5.44 (L1) 'Xbox Live Oyun Kaydetme (XblGameSave)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu hizmet, Xbox Live kaydetme özellikli oyunlar için kaydetme verilerini eşitler. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Xbox Live bir oyun hizmetidir ve kurumsal olarak yönetilen bir ortamda (belki bir oyun şirketi olmadığı sürece) yeri yoktur.

**Etki:**

Oyun kaydetme verileri Xbox Live'a yüklenmeyecek veya Xbox Live'dan indirilmeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\XblGameSave:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Xbox Canlı Oyun Kaydetme*

**5,45 (L1) 'Xbox Live Ağ Hizmeti (XboxNetApiSvc)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu hizmet, Windows.Networking.XboxLive uygulama programlama arabirimini destekler. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Xbox Live bir oyun hizmetidir ve kurumsal olarak yönetilen bir ortamda (belki bir oyun şirketi olmadığı sürece) yeri yoktur.

**Etki:**

Xbox Live bağlantıları başarısız olabilir ve bu hizmetle etkileşime giren uygulamalar da başarısız olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\XboxNetApiSvc:Start*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu şu şekilde ayarlayın: Devre Dışı.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Sistem Hizmetleri\Xbox Canlı Ağ Hizmeti*

**9 Gelişmiş Güvenlik Özellikli Windows Defender Güvenlik Duvarı (eski adıyla Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı)**

**9.1 Domain Profili**

**9.1.1 (L1) ‘Windows Güvenlik Duvarı: Etki Alanı: Güvenlik duvarı durumu' seçeneği 'Açık (önerilen)' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı'nın ağ trafiğini filtrelemek üzere bu profilin ayarlarını kullanması için Açık (önerilir) öğesini seçin. Kapalı'yı seçerseniz, Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı, bu profil için güvenlik duvarı kurallarının veya bağlantı güvenlik kurallarının hiçbirini kullanmaz. Bu ayar için önerilen durum: Açık (önerilir).

**Gerekçe:**

Güvenlik duvarı kapatılırsa, tüm trafik sisteme erişebilir ve bir saldırgan, bir ağ hizmetindeki bir zayıflıktan uzaktan daha kolay yararlanabilir. Etki: Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile: EnableFirewall*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Açık (önerilir):

*Bilgisayar Yapılandırması\İlkeler \Windows Ayarları\Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Etki Alanı Profili\Güvenlik Duvarı durumu*

**9.1.2 (L1) ‘Windows Güvenlik Duvarı: Etki Alanı: Gelen bağlantılar' seçeneği 'Engelle (varsayılan)' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:** Bu ayar, gelen güvenlik duvarı kuralıyla eşleşmeyen gelen bağlantıların davranışını belirler. Bu ayar için önerilen durum: Engelle (varsayılan).

**Gerekçe:**

Güvenlik duvarı tüm trafiğin sisteme erişmesine izin veriyorsa, saldırgan bir ağ hizmetindeki bir zayıflıktan uzaktan daha kolay yararlanabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile: DefaultInboundAction*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Engelle (varsayılan):

*Bilgisayar Yapılandırması\İlkeler \Windows Ayarları\Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Etki Alanı Profili\Gelen bağlantılar*

**9.1.3 (L1) ‘Windows Güvenlik Duvarı: Etki Alanı: Giden bağlantılar' seçeneği 'İzin Ver (varsayılan)' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, giden güvenlik duvarı kuralıyla eşleşmeyen giden bağlantıların davranışını belirler. Bu ayar için önerilen durum şudur: İzin ver (varsayılan).

**Gerekçe:**

Bazı kişiler, kullanıcı veya yönetici tarafından özel olarak onaylananlar dışındaki tüm giden bağlantıları engellemenin ihtiyatlı olduğuna inanmaktadır. Microsoft bu görüşe katılmamaktadır, varsayılan olarak giden bağlantıları engellemek, kullanıcıları web tarayıcıları veya anlık mesajlaşma yazılımları gibi uygulamaları yetkilendirmelerini veya engellemelerini isteyen çok sayıda iletişim kutusuyla uğraşmaya zorlayacaktır. Ek olarak, giden trafiği engellemenin çok az değeri vardır çünkü bir saldırgan sistemin güvenliğini ihlal etmişse güvenlik duvarını yine de yeniden yapılandırabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile: DefaultOutboundAction*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki kullanıcı arabirimi yolunu İzin Ver (varsayılan):

*Bilgisayar Yapılandırması\İlkeler \Windows Ayarları\Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Etki Alanı Profili\Giden bağlantılar*

**9.1.4 (L1) ‘Windows Güvenlik Duvarı: Etki Alanı: Ayarlar: Bildirim görüntüle' seçeneği 'Hayır' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bir programın gelen bağlantıları alması engellendiğinde, Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı'nın kullanıcıya bildirimler göstermesi için bu seçeneği belirleyin. Bu ayar için önerilen durum: Hayır.

**Not:** Yerel güvenlik duvarı kurallarını uygula ayarı Hayır olarak yapılandırıldığında, ayrıca Bildirim görüntüle ayarını Hayır olarak yapılandırmanız önerilir. Aksi takdirde, kullanıcılar isteyip istemediklerini soran iletileri almaya devam eder. kısıtlanmış bir gelen bağlantının engellemesini kaldırmak için, ancak kullanıcının yanıtı yok sayılacaktır.

**Gerekçe**:

Güvenlik duvarı bildirimleri karmaşık olabilir ve uyarıyı ele alamayan son kullanıcıların kafasını karıştırabilir.

**Etki:**

Windows Güvenlik Duvarı, bir programın gelen bağlantıları alması engellendiğinde bir bildirim görüntülemeyecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile: DisableNotifications*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Hayır olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları \Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Etki Alanı Profili\Ayarlar Özelleştirme\Bir bildirim görüntüle*

**9.1.5 (L1) ‘Windows Güvenlik Duvarı: Etki Alanı: Günlüğe Kaydetme: Ad' seçeneği '%SystemRoot%\System32\logfiles\firewall\domainfw.log' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Windows Güvenlik Duvarı'nın günlük bilgilerini yazacağı dosyanın yolunu ve adını belirtmek için bu seçeneği kullanın. Bu ayar için önerilen durum: *%SystemRoot%\System32\logfiles\firewall\domainfw.log.*

**Gerekçe:**

Olaylar kaydedilmezse, sistem sorunlarının veya kötü niyetli kullanıcıların yetkisiz faaliyetlerinin temel nedenini belirlemek zor veya imkansız olabilir.

**Etki:**

Günlük dosyası belirtilen dosyada depolanacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\ Logging:LogFilePath*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu *%SystemRoot%\System32\logfiles olarak ayarlayın \firewall\domainfw.log:*

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Etki Alanı Profili\Logging Özelleştirme\Ad*

**9.1.6 (L1) 'Windows Güvenlik Duvarı: Etki Alanı: Günlüğe Kaydetme: Boyut sınırı (KB)' ifadesi '16.384 KB veya üzeri' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Windows Güvenlik Duvarı'nın günlük bilgilerini yazacağı dosyanın boyut sınırını belirtmek için bu seçeneği kullanın. Bu ayar için önerilen durum: 16.384 KB veya üstü.

**Gerekçe:**

Olaylar kaydedilmezse, sistem sorunlarının veya kötü niyetli kullanıcıların yetkisiz faaliyetlerinin temel nedenini belirlemek zor veya imkansız olabilir.

**Etki:**

Günlük dosyası boyutu belirtilen boyutla sınırlandırılacak, sınıra ulaşıldığında eski olayların üzerine yenileri yazılacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\ Logging:LogFileSize*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu 16.384 KB veya daha büyük olarak ayarlayın:

*Bilgisayar Yapılandırması \İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Etki Alanı Profili\Günlük Özelleştirme\Boyut sınırı (KB)*

**9.1.7 (L1) 'Windows Güvenlik Duvarı: Etki Alanı: Günlük bırakılan paketler' seçeneği 'Evet' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı herhangi bir nedenle gelen paketi attığında günlüğe kaydetmek için bu seçeneği kullanın. Günlük, paketin neden ve ne zaman bırakıldığını kaydeder. Günlüğün eylem sütununda DROP kelimesini içeren girişleri arayın. Bu ayar için önerilen durum: Evet.

**Gerekçe:**

Olaylar kaydedilmezse, sistem sorunlarının veya kötü niyetli kullanıcıların yetkisiz faaliyetlerinin temel nedenini belirlemek zor veya imkansız olabilir.

**Etki:**

Bırakılan paketlerle ilgili bilgiler güvenlik duvarı günlük dosyasına kaydedilecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\ Logging:LogDroppedPackets*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Evet olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\ Windows Ayarları\Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Etki Alanı Profili\Günlük Özelleştirme\Düşen paketleri günlüğe kaydet*

**9.1.8 (L1) 'Windows Güvenlik Duvarı: Etki Alanı: Günlük başarılı bağlantılar' seçeneği 'Evet' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı gelen bağlantıya izin verdiğinde günlüğe kaydetmek için bu seçeneği kullanın. Günlük, bağlantının neden ve ne zaman kurulduğunu kaydeder. Günlüğün eylem sütununda İZİN VERİN kelimesini içeren girişleri arayın. Bu ayar için önerilen durum: Evet.

**Gerekçe:**

Olaylar kaydedilmezse, sistem sorunlarının veya kötü niyetli kullanıcıların yetkisiz faaliyetlerinin temel nedenini belirlemek zor veya imkansız olabilir.

**Etki:**

Başarılı bağlantılarla ilgili bilgiler güvenlik duvarı günlük dosyasına kaydedilecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\DomainProfile\ Logging:LogSuccessfulConnections*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Evet olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\ Windows Ayarları\Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Etki Alanı Profili\Logging Özelleştir\Başarılı bağlantıları günlüğe kaydet*

**9.2 Özel Profil**

**9.2.1 (L1) 'Windows Güvenlik Duvarı: Özel: Güvenlik duvarı durumu' seçeneği 'Açık (önerilen)' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı'nın ağ trafiğini filtrelemek üzere bu profilin ayarlarını kullanması için Açık (önerilir) öğesini seçin. Kapalı'yı seçerseniz, Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı, bu profil için güvenlik duvarı kurallarının veya bağlantı güvenlik kurallarının hiçbirini kullanmaz. Bu ayar için önerilen durum: Açık (önerilir).

**Gerekçe**:

Güvenlik duvarı kapatılırsa, tüm trafik sisteme erişebilir ve bir saldırgan, bir ağ hizmetindeki bir zayıflıktan uzaktan daha kolay yararlanabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile :EnableFirewall*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için aşağıdaki UI yolunu Açık (önerilir):

*Bilgisayar Yapılandırması\İlkeler \Windows Ayarları\Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Özel Profil\Güvenlik Duvarı durumu*

**9.2.2 (L1) 'Windows Güvenlik Duvarı: Özel: Gelen bağlantılar' seçeneği 'Engelle (varsayılan)' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, gelen güvenlik duvarı kuralıyla eşleşmeyen gelen bağlantıların davranışını belirler. Bu ayar için önerilen durum: Engelle (varsayılan).

**Gerekçe:**

Güvenlik duvarı tüm trafiğin sisteme erişmesine izin veriyorsa, saldırgan bir ağ hizmetindeki bir zayıflıktan uzaktan daha kolay yararlanabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile :DefaultInboundAction*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Engelle (varsayılan):

*Bilgisayar Yapılandırması\İlkeler \Windows Ayarları\Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Özel Profil\Gelen bağlantılar*

**9.2.3 (L1) 'Windows Güvenlik Duvarı: Özel: Giden bağlantılar' seçeneği 'İzin Ver (varsayılan)' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, giden güvenlik duvarı kuralıyla eşleşmeyen giden bağlantıların davranışını belirler. Bu ayar için önerilen durum şudur: İzin ver (varsayılan).

**Not:** Giden bağlantıları Engelle olarak ayarlar ve ardından bir GPO kullanarak güvenlik duvarı ilkesini dağıtırsanız, Grup İlkesi'nin çalışmasını sağlayan bir giden kuralı oluşturup dağıtmadığınız sürece, GPO ayarlarını alan bilgisayarlar sonraki Grup İlkesi güncellemelerini alamaz. Çekirdek Ağ Oluşturma için önceden tanımlanmış kurallar, Grup İlkesinin çalışmasını sağlayan giden kuralları içerir. Bu giden kurallarının etkin olduğundan emin olun ve dağıtmadan önce güvenlik duvarı profillerini kapsamlı bir şekilde test edin.

**Gerekçe:**

Bazı kişiler, kullanıcı veya yönetici tarafından özel olarak onaylananlar dışındaki tüm giden bağlantıları engellemenin ihtiyatlı olduğuna inanmaktadır. Microsoft bu görüşe katılmamaktadır, varsayılan olarak giden bağlantıları engellemek, kullanıcıları web tarayıcıları veya anlık mesajlaşma yazılımları gibi uygulamaları yetkilendirmelerini veya engellemelerini isteyen çok sayıda iletişim kutusuyla uğraşmaya zorlayacaktır. Ek olarak, giden trafiği engellemenin çok az değeri vardır çünkü bir saldırgan sistemin güvenliğini ihlal etmişse güvenlik duvarını yine de yeniden yapılandırabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim**:

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile :DefaultOutboundAction*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu İzin Ver (varsayılan) olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\ Özel Profil\Giden bağlantılar*

**9.2.4 (L1) 'Windows Güvenlik Duvarı: Özel: Ayarlar: Bildirim görüntüle' seçeneği 'Hayır' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bir programın gelen bağlantıları alması engellendiğinde, Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı'nın kullanıcıya bildirimler göstermesi için bu seçeneği belirleyin. Bu ayar için önerilen durum: Hayır.

**Not:** Yerel güvenlik duvarı kurallarını uygula ayarı Hayır olarak yapılandırıldığında, ayrıca Bildirim görüntüle ayarını Hayır olarak yapılandırmanız önerilir. Aksi takdirde, kullanıcılar isteyip istemediklerini soran iletileri almaya devam eder. kısıtlanmış bir gelen bağlantının engellemesini kaldırmak için, ancak kullanıcının yanıtı yok sayılacaktır.

**Gerekçe:**

Güvenlik duvarı bildirimleri karmaşık olabilir ve uyarıyı ele alamayan son kullanıcıların kafasını karıştırabilir.

**Etki:**

Windows Güvenlik Duvarı, bir programın gelen bağlantıları alması engellendiğinde bir bildirim görüntülemeyecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile :DisableNotifications*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Hayır olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları \Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Özel Profil\Ayarlar Özelleştirme\Bir bildirim görüntüle*

**9.2.5 (L1) 'Windows Güvenlik Duvarı: Özel: Günlüğe Kaydetme: Ad' seçeneği '%SystemRoot%\System32\logfiles\firewall\privatefw.log' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Windows Güvenlik Duvarı'nın günlük bilgilerini yazacağı dosyanın yolunu ve adını belirtmek için bu seçeneği kullanın. Bu ayar için önerilen durum: *%SystemRoot%\System32\logfiles\firewall\privatefw.log.*

**Gerekçe:**

Olaylar kaydedilmezse, sistem sorunlarının veya kötü niyetli kullanıcıların yetkisiz faaliyetlerinin temel nedenini belirlemek zor veya imkansız olabilir.

**Etki:**

Günlük dosyası belirtilen dosyada depolanacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile \Logging:LogFilePath*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu *%SystemRoot%\System32\logfiles olarak ayarlayın \firewall\privatefw.log:*

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Özel Profil\Logging Özelleştirme\Ad*

**9.2.6 (L1) 'Windows Güvenlik Duvarı: Özel: Günlüğe kaydetme: Boyut sınırı (KB)' ifadesi '16.384 KB veya üzeri' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Windows Güvenlik Duvarı'nın günlük bilgilerini yazacağı dosyanın boyut sınırını belirtmek için bu seçeneği kullanın. Bu ayar için önerilen durum: 16.384 KB veya üstü.

**Gerekçe:**

Olaylar kaydedilmezse, sistem sorunlarının veya kötü niyetli kullanıcıların yetkisiz faaliyetlerinin temel nedenini belirlemek zor veya imkansız olabilir.

**Etki:**

Günlük dosyası boyutu belirtilen boyutla sınırlandırılacak, sınıra ulaşıldığında eski olayların üzerine yenileri yazılacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging:LogFileSize*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu 16.384 KB veya daha büyük olarak ayarlayın:

*Bilgisayar Yapılandırması \İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Özel Profil\Günlük Özelleştirme\Boyut sınırı (KB)*

**9.2.7 (L1) 'Windows Güvenlik Duvarı: Özel: Günlüğe bırakılan paketler' seçeneği 'Evet' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı herhangi bir nedenle gelen paketi attığında günlüğe kaydetmek için bu seçeneği kullanın. Günlük, paketin neden ve ne zaman bırakıldığını kaydeder. Günlüğün eylem sütununda DROP kelimesini içeren girişleri arayın. Bu ayar için önerilen durum: Evet.

**Gerekçe:**

Olaylar kaydedilmezse, sistem sorunlarının veya kötü niyetli kullanıcıların yetkisiz faaliyetlerinin temel nedenini belirlemek zor veya imkansız olabilir.

**Etki:**

Bırakılan paketlerle ilgili bilgiler güvenlik duvarı günlük dosyasına kaydedilecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging:LogDroppedPackets*

Düzeltme: Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Evet olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\ Windows Ayarları\Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Özel Profil\Günlük Özelleştirme\Düşen paketleri günlüğe kaydet*

**9.2.8 (L1) 'Windows Güvenlik Duvarı: Özel: Günlüğe kaydetme: Başarılı bağlantılar' seçeneği 'Evet' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı gelen bağlantıya izin verdiğinde günlüğe kaydetmek için bu seçeneği kullanın. Günlük, bağlantının neden ve ne zaman kurulduğunu kaydeder. Günlüğün eylem sütununda İZİN VERİN kelimesini içeren girişleri arayın. Bu ayar için önerilen durum: Evet.

**Gerekçe:**

Olaylar kaydedilmezse, sistem sorunlarının veya kötü niyetli kullanıcıların yetkisiz faaliyetlerinin temel nedenini belirlemek zor veya imkansız olabilir.

**Etki:**

Başarılı bağlantılarla ilgili bilgiler güvenlik duvarı günlük dosyasına kaydedilecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PrivateProfile\Logging:LogSuccessfulConnections*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Evet olarak ayarlayın:

**9.3 Genel Profil**

**9.3.1 (L1) 'Windows Güvenlik Duvarı: Genel: Güvenlik duvarı durumu' seçeneği 'Açık (önerilen)' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı'nın ağ trafiğini filtrelemek üzere bu profilin ayarlarını kullanması için Açık (önerilir) öğesini seçin. Kapalı'yı seçerseniz, Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı, bu profil için güvenlik duvarı kurallarının veya bağlantı güvenlik kurallarının hiçbirini kullanmaz. Bu ayar için önerilen durum: Açık (önerilir).

**Gerekçe:**

Güvenlik duvarı kapatılırsa, tüm trafik sisteme erişebilir ve bir saldırgan, bir ağ hizmetindeki bir zayıflıktan uzaktan daha kolay yararlanabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile: EnableFirewall*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Açık (önerilir):

*Bilgisayar Yapılandırması\İlkeler \Windows Ayarları\Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Genel Profil\Güvenlik Duvarı durumu*

**9.3.2 (L1) 'Windows Güvenlik Duvarı: Genel: Gelen bağlantılar' seçeneği 'Engelle (varsayılan)' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, gelen güvenlik duvarı kuralıyla eşleşmeyen gelen bağlantıların davranışını belirler. Bu ayar için önerilen durum: Engelle (varsayılan).

**Gerekçe:**

Güvenlik duvarı tüm trafiğin sisteme erişmesine izin veriyorsa, saldırgan bir ağ hizmetindeki bir zayıflıktan uzaktan daha kolay yararlanabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile: DefaultInboundAction*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Engelle (varsayılan):

*Bilgisayar Yapılandırması\İlkeler \Windows Ayarları\Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Genel Profil\Gelen bağlantılar*

**9.3.3 (L1) 'Windows Güvenlik Duvarı: Genel: Giden bağlantılar' seçeneği 'İzin Ver (varsayılan)' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:** Bu ayar, giden güvenlik duvarı kuralıyla eşleşmeyen giden bağlantıların davranışını belirler. Bu ayar için önerilen durum şudur: İzin ver (varsayılan).

**Not:**

Giden bağlantıları Engelle olarak ayarlar ve ardından bir GPO kullanarak güvenlik duvarı ilkesini dağıtırsanız, Grup İlkesi'nin çalışmasını sağlayan bir giden kuralı oluşturup dağıtmadığınız sürece, GPO ayarlarını alan bilgisayarlar sonraki Grup İlkesi güncellemelerini alamaz. Çekirdek Ağ Oluşturma için önceden tanımlanmış kurallar, Grup İlkesinin çalışmasını sağlayan giden kuralları içerir. Bu giden kurallarının etkin olduğundan emin olun ve dağıtmadan önce güvenlik duvarı profillerini kapsamlı bir şekilde test edin.

**Gerekçe:**

Bazı kişiler, kullanıcı veya yönetici tarafından özel olarak onaylananlar dışındaki tüm giden bağlantıları engellemenin ihtiyatlı olduğuna inanmaktadır. Microsoft bu görüşe katılmamaktadır, varsayılan olarak giden bağlantıları engellemek, kullanıcıları web tarayıcıları veya anlık mesajlaşma yazılımları gibi uygulamaları yetkilendirmelerini veya engellemelerini isteyen çok sayıda iletişim kutusuyla uğraşmaya zorlayacaktır. Ek olarak, giden trafiği engellemenin çok az değeri vardır çünkü bir saldırgan sistemin güvenliğini ihlal etmişse güvenlik duvarını yine de yeniden yapılandırabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile: DefaultOutboundAction*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu İzin Ver (varsayılan) olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\ Genel Profil\Giden bağlantılar*

**9.3.4 (L1) 'Windows Güvenlik Duvarı: Genel: Ayarlar: Bildirim görüntüle' seçeneği 'Hayır' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bir programın gelen bağlantıları alması engellendiğinde, Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı'nın kullanıcıya bildirimler göstermesi için bu seçeneği belirleyin. Bu ayar için önerilen durum: Hayır.

**Gerekçe**:

Bazı kuruluşlar, güvenlik duvarı kuralları belirli ağ etkinliği türlerini engellediğinde kullanıcıları alarma geçirmekten kaçınmayı tercih edebilir. Ancak, güvenlik duvarını içeren ağ sorunlarını giderirken bildirimler yardımcı olabilir.

**Etki:**

Windows Güvenlik Duvarı, bir programın gelen bağlantıları alması engellendiğinde bir bildirim görüntülemeyecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile: DisableNotifications*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu 'Hayır' olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\ Windows Ayarları\Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Genel Profil\Ayarlar Özelleştirme\Bir bildirim görüntüle*

**9.3.5 (L1) 'Windows Güvenlik Duvarı: Genel: Ayarlar: Yerel güvenlik duvarı kurallarını uygula' seçeneği 'Hayır' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, yerel yöneticilerin Grup İlkesi tarafından yapılandırılan güvenlik duvarı kurallarıyla birlikte uygulanan yerel güvenlik duvarı kuralları oluşturmasına izin verilip verilmediğini denetler. Bu ayar için önerilen durum: Hayır.

**Not:** Yerel güvenlik duvarı kurallarını uygula ayarı Hayır olarak yapılandırıldığında, ayrıca Bildirim görüntüle ayarını Hayır olarak yapılandırmanız önerilir. Aksi takdirde, kullanıcılar isteyip istemediklerini soran iletileri almaya devam eder. kısıtlanmış bir gelen bağlantının engellemesini kaldırmak için, ancak kullanıcının yanıtı yok sayılacaktır.

**Gerekçe:**

Genel profildeyken, bilgisayar başına özel bir yerel güvenlik duvarı istisnası olmamalıdır. Bu ayarlar, merkezi bir ilke tarafından yönetilmelidir.

**Etki:**

Yöneticiler yine de güvenlik duvarı kuralları oluşturabilir, ancak kurallar uygulanmaz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile: AllowLocalPolicyMerge*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Hayır olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları \Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Genel Profil\Ayarlar Özelleştirme\Yerel güvenlik duvarı kurallarını uygula*

**9.3.6 (L1) 'Windows Güvenlik Duvarı: Genel: Ayarlar: Yerel bağlantı güvenliği kurallarını uygula' seçeneği 'Hayır' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, yerel yöneticilerin Grup İlkesi tarafından yapılandırılan bağlantı güvenlik kurallarıyla birlikte uygulanan bağlantı güvenlik kuralları oluşturmasına izin verilip verilmediğini denetler. Bu ayar için önerilen durum: Hayır.

**Gerekçe:**

Yönetici ayrıcalıklarına sahip kullanıcılar, sistemi uzaktan saldırıya maruz bırakan güvenlik duvarı kuralları oluşturabilir.

**Etki:**

Yöneticiler yerel bağlantı güvenlik kuralları oluşturmaya devam edebilir, ancak kurallar uygulanmaz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile: AllowLocalIPsecPolicyMerge*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Hayır olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları \Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Genel Profil\Ayarlar Özelleştirme\Yerel bağlantı güvenlik kurallarını uygula*

**9.3.7 (L1) 'Windows Güvenlik Duvarı: Ortak: Günlüğe Kaydetme: Ad' seçeneği '%SystemRoot%\System32\logfiles\firewall\publicfw.log' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Windows Güvenlik Duvarı'nın günlük bilgilerini yazacağı dosyanın yolunu ve adını belirtmek için bu seçeneği kullanın. Bu ayar için önerilen durum: *%SystemRoot%\System32\logfiles\firewall\publicfw.log.*

**Gerekçe**:

Olaylar kaydedilmezse, sistem sorunlarının veya kötü niyetli kullanıcıların yetkisiz faaliyetlerinin temel nedenini belirlemek zor veya imkansız olabilir.

**Etki:**

Günlük dosyası belirtilen dosyada depolanacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\ Logging:LogFilePath*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu *%SystemRoot%\System32\logfiles\firewall\publicfw.log olarak ayarlayın :*

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Genel Profil\Günlük Özelleştirme\Ad*

**9.3.8 (L1) 'Windows Güvenlik Duvarı: Genel: Günlüğe kaydetme: Boyut sınırı (KB)' seçeneği '16.384 KB veya daha büyük' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Windows Güvenlik Duvarı'nın günlük bilgilerini yazacağı dosyanın boyut sınırını belirtmek için bu seçeneği kullanın. Bu ayar için önerilen durum: 16.384 KB veya üstü.

**Gerekçe:**

Olaylar kaydedilmezse, sistem sorunlarının veya kötü niyetli kullanıcıların yetkisiz faaliyetlerinin temel nedenini belirlemek zor veya imkansız olabilir.

**Etki:**

Günlük dosyası boyutu belirtilen boyutla sınırlandırılacak, sınıra ulaşıldığında eski olayların üzerine yenileri yazılacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\ Logging:LogFileSize*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu 16.384 KB veya daha büyük olarak ayarlayın:

*Bilgisayar Yapılandırması \İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Genel Profil\Günlük Özelleştirme\Boyut sınırı (KB)*

**9.3.9 (L1) 'Windows Güvenlik Duvarı: Genel: Günlük bırakılan paketler' seçeneği 'Evet' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı herhangi bir nedenle gelen paketi attığında günlüğe kaydetmek için bu seçeneği kullanın. Günlük, paketin neden ve ne zaman bırakıldığını kaydeder. Günlüğün eylem sütununda DROP kelimesini içeren girişleri arayın. Bu ayar için önerilen durum: Evet.

**Gerekçe:**

Olaylar kaydedilmezse, sistem sorunlarının veya kötü niyetli kullanıcıların yetkisiz faaliyetlerinin temel nedenini belirlemek zor veya imkansız olabilir.

**Etki:**

Bırakılan paketlerle ilgili bilgiler güvenlik duvarı günlük dosyasına kaydedilecektir. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\ Logging:LogDroppedPackets*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Evet olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\ Windows Ayarları\Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Genel Profil\Günlük Özelleştirme\Düşen paketleri günlüğe kaydet*

**9.3.10 (L1) 'Windows Güvenlik Duvarı: Genel: Günlüğe kaydetme: Başarılı bağlantılar' seçeneği 'Evet' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı gelen bağlantıya izin verdiğinde günlüğe kaydetmek için bu seçeneği kullanın. Günlük, bağlantının neden ve ne zaman kurulduğunu kaydeder. Günlüğün eylem sütununda İZİN VERİN kelimesini içeren girişleri arayın. Bu ayar için önerilen durum: Evet.

**Gerekçe:**

Olaylar kaydedilmezse, sistem sorunlarının veya kötü niyetli kullanıcıların yetkisiz faaliyetlerinin temel nedenini belirlemek zor veya imkansız olabilir.

**Etki:**

Başarılı bağlantılarla ilgili bilgiler güvenlik duvarı günlük dosyasına kaydedilecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsFirewall\PublicProfile\ Logging:LogSuccessfulConnections*

**Düzeltme**:

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Evet olarak ayarlayın.

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Gelişmiş Güvenlik Özellikli Windows Güvenlik Duvarı\Windows Güvenlik Duvarı Özellikleri\Genel Profil\Günlük Tutma Özelleştirme\Başarılı bağlantıları günlüğe kaydet*

**17 Gelişmiş Denetim İlkesi Yapılandırması**

**17.1 Hesapta Oturum Açma**

**17.1.1 (L1) 'Kimlik Bilgileri Doğrulamasını Denetle' seçeneği 'Başarılı ve Başarısız' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

* Bu alt kategori, bir kullanıcı hesabı oturum açma isteği için gönderilen kimlik bilgilerine ilişkin doğrulama testlerinin sonuçlarını bildirir. Bu olaylar, kimlik bilgileri için yetkili olan bilgisayarda gerçekleşir. Etki alanı hesapları için Etki Alanı Denetleyicisi yetkilidir, oysa yerel hesaplar için yerel bilgisayar yetkilidir. Etki alanı ortamlarında, Hesap Oturum Açma olaylarının çoğu, etki alanı hesapları için yetkili Etki Alanı Denetleyicilerinin Güvenlik günlüğünde gerçekleşir. Ancak, bu olaylar, oturum açmak için yerel hesaplar kullanıldığında kuruluştaki diğer bilgisayarlarda meydana gelebilir. Bu alt kategori için olaylar şunları içerir:
* 4774: Oturum açmak için bir hesap eşlendi.
* 4775: Bir hesap, oturum açmak için eşlenemedi.
* 4776: Etki Alanı Denetleyicisi, bir hesabın kimlik bilgilerini doğrulamaya çalıştı.
* 4777: Etki Alanı Denetleyicisi bir hesabın kimlik bilgilerini doğrulayamadı.
* Bu ayar için önerilen durum: Başarılı ve Başarısız.

**Gerekçe:**

Bir güvenlik olayı araştırılırken bu olayların denetlenmesi yararlı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki kullanıcı arabirimi yolunu Başarı ve Hata olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\Hesap Oturum Açma\Denetim Kimlik Bilgileri Doğrulaması*

**17.2 Hesap Yönetimi**

**17.2.1 (L1) 'Uygulama Grubu Yönetimini Denetle' seçeneği 'Başarı ve Başarısızlık' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:** Bu ilke ayarı, aşağıdakiler gibi uygulama gruplarında yapılan değişiklikler tarafından oluşturulan olayları denetlemenize olanak tanır:

* Uygulama grubu oluşturulur, değiştirilir veya silinir.
* Bir uygulama grubuna üye eklenir veya gruptan çıkarılır.

Uygulama grupları, rol tabanlı erişim denetimini (RBAC) uygulamalara entegre etmek için Microsoft tarafından oluşturulan esnek bir çerçeve olan Windows Yetkilendirme Yöneticisi tarafından kullanılır. Windows Yetkilendirme Yöneticisi hakkında daha fazla bilgi [MSDN - Windows Yetkilendirme Yöneticisi'nde mevcuttur.](https://msdn.microsoft.com/en-us/library/bb897401.aspx)

Bu ayar için önerilen durum: Başarılı ve Başarısız.

**Gerekçe:**

Bu kategorideki olayları denetlemek, bir olayı araştırırken faydalı olabilir. Etki: Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki kullanıcı arabirimi yolunu Başarı ve Hata olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\Hesap Yönetimi\Denetim Uygulama Grubu Yönetimi*

**17.2.2 (L1) 'Güvenlik Grubu Yönetimini Denetle' seçeneği 'Başarılı' (Otomatik) içerecek şekilde ayarlanmalıdır.**

**Açıklama:**

Bu alt kategori, bir güvenlik grubu oluşturulduğunda, değiştirildiğinde veya silindiğinde veya bir güvenlik grubuna bir üye eklendiğinde veya bir güvenlik grubuna bir üyenin kaldırıldığında olduğu gibi, güvenlik grubu yönetiminin her olayını raporlar. Bu Denetim ilkesi ayarını etkinleştirirseniz, yöneticiler, güvenlik grubu hesaplarının kötü amaçlı, yanlışlıkla ve yetkili oluşturulmasını algılamak için olayları izleyebilir. Bu alt kategori için olaylar şunları içerir:

* 4727: Güvenliği etkinleştirilmiş bir genel grup oluşturuldu.
* 4728: Güvenliği etkinleştirilmiş bir küresel gruba bir üye eklendi.
* 4729: Güvenliğin etkin olduğu bir genel gruptan bir üye çıkarıldı.
* 4730: Güvenliği etkinleştirilmiş bir genel grup silindi.
* 4731: Güvenliği etkinleştirilmiş bir yerel grup oluşturuldu.
* 4732: Güvenliğin etkin olduğu bir yerel gruba bir üye eklendi.
* 4733: Güvenliğin etkin olduğu bir yerel gruptan bir üye çıkarıldı.
* 4734: Güvenliği etkinleştirilmiş bir yerel grup silindi.
* 4735: Güvenliği etkinleştirilmiş bir yerel grup değiştirildi.
* 4737: Güvenliği etkinleştirilmiş bir genel grup değiştirildi.
* 4754: Güvenliği etkinleştirilmiş bir evrensel grup oluşturuldu.
* 4755: Güvenliği etkinleştirilmiş bir evrensel grup değiştirildi.
* 4756: Güvenliği etkinleştirilmiş bir evrensel gruba bir üye eklendi.
* 4757: Güvenliğin etkin olduğu evrensel bir gruptan bir üye çıkarıldı.
* 4758: Güvenliği etkinleştirilmiş bir evrensel grup silindi.
* 4764: Bir grubun türü değiştirildi.

Bu ayar için önerilen durum şunları içerir: Başarılı.

**Gerekçe:**

Bir güvenlik olayı araştırılırken bu olayların denetlenmesi yararlı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, Başarı'yı içerecek şekilde şu kullanıcı arabirimi yolunu ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\Hesap Yönetimi\Denetim Güvenlik Grup Yönetimi*

**17.2.3 (L1) 'Kullanıcı Hesabı Yönetimini Denetle' seçeneği 'Başarı ve Başarısızlık' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu alt kategori, bir kullanıcı hesabı oluşturulduğunda, değiştirildiğinde veya silindiğinde; bir kullanıcı hesabının yeniden adlandırılması, devre dışı bırakılması veya etkinleştirilmesi; veya bir parola ayarlanmış veya değiştirilmiş. Bu Denetim ilkesi ayarını etkinleştirirseniz, yöneticiler kötü amaçlı, yanlışlıkla ve yetkili kullanıcı hesapları oluşturmayı algılamak için olayları izleyebilir. Bu alt kategori için olaylar şunları içerir:

* 4720: Bir kullanıcı hesabı oluşturuldu.
* 4722: Bir kullanıcı hesabı etkinleştirildi.
* 4723: Bir hesabın şifresi değiştirilmeye çalışıldı.
* 4724: Bir hesabın parolasını sıfırlama girişiminde bulunuldu.
* 4725: Bir kullanıcı hesabı devre dışı bırakıldı.
* 4726: Bir kullanıcı hesabı silindi.
* 4738: Bir kullanıcı hesabı değiştirildi.
* 4740: Bir kullanıcı hesabı kilitlendi.
* 4765: Bir hesaba SID Geçmişi eklendi.
* 4766: Bir hesaba SID Geçmişi ekleme denemesi başarısız oldu.
* 4767: Bir kullanıcı hesabının kilidi açıldı.
* 4780: ACL, yönetici gruplarının üyesi olan hesaplarda ayarlandı.
* 4781: Bir hesabın adı değiştirildi.
* 4794: Dizin Hizmetleri Geri Yükleme Modu ayarlanmaya çalışıldı.
* 5376: Credential Manager kimlik bilgileri yedeklendi.
* 5377: Kimlik Bilgileri Yöneticisi kimlik bilgileri bir yedekten geri yüklendi.

Bu ayar için önerilen durum: Başarılı ve Başarısız.

**Gerekçe:**

Bir güvenlik olayı araştırılırken bu olayların denetlenmesi yararlı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki kullanıcı arabirimi yolunu Başarı ve Hata olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\Hesap Yönetimi\Denetim Kullanıcı Hesabı Yönetimi*

**17.3 Ayrıntılı İzleme**

**17.3.1 (L1) 'PNP Etkinliğini Denetle' seçeneği 'Başarı' (Otomatik) içerecek şekilde ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, tak ve çalıştır harici bir cihaz algıladığında denetlemenize olanak tanır. Bu ayar için önerilen durum şunları içerir: Başarılı.

**Not:** Grup İlkesi'nde bu değere erişmek ve bu değeri ayarlamak için Windows 10, Server 2016 veya daha yeni bir işletim sistemi gereklidir.

**Gerekçe:**

Bu ayarın etkinleştirilmesi, bir cihaz bir sisteme takıldığında kullanıcının olayları denetlemesine olanak tanır. Bu, onaylanmamış cihazlar takılıysa BT personelini uyarmaya yardımcı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları algılanamayabilir veya bunlar için yeterli kanıt bulunamayabilir. güvenlik olayları meydana geldikten sonra ağ adli analizi. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, Başarı'yı içerecek şekilde aşağıdaki UI yolunu ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\Ayrıntılı İzleme\Denetim PNP Etkinliği*

**17.3.2 (L1) 'Süreç Oluşturmayı Denetle' seçeneği 'Başarılı' (Otomatik) içerecek şekilde ayarlanmalıdır.**

**Açıklama:**

Bu alt kategori, bir işlemin oluşturulmasını ve onu oluşturan programın veya kullanıcının adını bildirir. Bu alt kategori için olaylar şunları içerir:

* 4688: Yeni bir süreç oluşturuldu.
* 4696: İşleme için bir birincil belirteç atandı. Bu ayar hakkında en son bilgiler için 947226 numaralı Microsoft Bilgi Bankası makalesine bakın: Windows Vista ve Windows Server 2008'deki güvenlik olaylarının açıklaması.

Bu ayar için önerilen durum şunları içerir: Başarılı.

**Gerekçe:**

Bir güvenlik olayı araştırılırken bu olayların denetlenmesi yararlı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, Başarı'yı içerecek şekilde şu kullanıcı arabirimi yolunu ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\Ayrıntılı İzleme\Denetim Süreci Oluşturma*

**17.4 DS Access**

**17.5 Oturum Açma/Oturumu Kapatma**

**17.5.1 (L1) 'Hesap Oturumu Kapatmayı Denetle' seçeneği 'Hata' (Otomatik) içerecek şekilde ayarlanmalıdır.**

**Açıklama:**

Bu alt kategori, çok sayıda başarısız oturum açma girişimi nedeniyle bir kullanıcının hesabının kilitlendiğini bildirir. Bu alt kategori için olaylar şunları içerir:

* 4625: Bir hesapta oturum açılamadı.

Bu ayar için önerilen durum şunları içerir: Hata.

**Gerekçe:**

Bir güvenlik olayı araştırılırken bu olayların denetlenmesi yararlı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Hata içerecek şekilde ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\Oturum Açma/Oturum Kapatma\Denetim Hesabı Kilitleme*

**17.5.2 (L1) 'Grup Üyeliğini Denetle' seçeneği 'Başarılı' (Otomatik) içerecek şekilde ayarlanmalıdır.**

**Açıklama:**

Bu ilke, kullanıcının oturum açma belirtecindeki grup üyelik bilgilerini denetlemenize olanak tanır. Bu alt kategorideki olaylar, oturum açma oturumunun oluşturulduğu bilgisayarda oluşturulur. Etkileşimli oturum açma için, kullanıcının oturum açtığı bilgisayarda güvenlik denetimi olayı oluşturulur. Ağdaki paylaşılan bir klasöre erişim gibi bir ağ oturum açma işlemi için, kaynağı barındıran bilgisayarda güvenlik denetimi olayı oluşturulur. Bu ayar için önerilen durum şunları içerir: Başarılı.

**Not:** Grup İlkesi'nde bu değere erişmek ve bu değeri ayarlamak için Windows 10, Server 2016 veya daha yeni bir işletim sistemi gereklidir.

**Gerekçe**:

Bir güvenlik olayı araştırılırken bu olayların denetlenmesi yararlı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, Başarı'yı içerecek şekilde şu kullanıcı arabirimi yolunu ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\Oturum Açma/Oturum Kapatma\Denetim Grubu Üyeliği*

**17.5.3 (L1) 'Oturum Kapatmayı Denetle' seçeneği 'Başarılı' (Otomatik) içerecek şekilde ayarlanmalıdır.**

**Açıklama:**

Bu alt kategori, bir kullanıcı sistemden çıkış yaptığında rapor verir. Bu olaylar, erişilen bilgisayarda gerçekleşir. Etkileşimli oturum açmalar için, bu olayların oluşturulması, oturumun açıldığı bilgisayarda gerçekleşir. Bir paylaşıma erişmek için bir ağ oturumu açılırsa, bu olaylar, erişilen kaynağı barındıran bilgisayarda oluşturulur. Bu ayarı Denetim yok olarak yapılandırırsanız, hangi kullanıcının kuruluş bilgisayarlarına eriştiğini veya erişmeye çalıştığını belirlemek zor veya imkansızdır. Bu alt kategori için olaylar şunları içerir:

* 4634: Bir hesabın oturumu kapatıldı.
* 4647: Kullanıcı tarafından başlatılan oturum kapatma.

Bu ayar için önerilen durum şunları içerir: Başarılı.

**Gerekçe:**

Bir güvenlik olayı araştırılırken bu olayların denetlenmesi yararlı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, Başarı'yı içerecek şekilde şu kullanıcı arabirimi yolunu ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\Oturum Açma/Oturum Kapatma\Denetim Oturumu Kapatma*

**17.5.4 (L1) 'Oturum Açmayı Denetle' seçeneği 'Başarılı ve Başarısız' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu alt kategori, bir kullanıcı sistemde oturum açmaya çalıştığında bildirir. Bu olaylar, erişilen bilgisayarda gerçekleşir. Etkileşimli oturum açmalar için, bu olayların oluşturulması, oturumun açıldığı bilgisayarda gerçekleşir. Bir paylaşıma erişmek için bir ağ oturumu açılırsa, bu olaylar, erişilen kaynağı barındıran bilgisayarda oluşturulur. Bu ayarı Denetim yok olarak yapılandırırsanız, hangi kullanıcının kuruluş bilgisayarlarına eriştiğini veya erişmeye çalıştığını belirlemek zor veya imkansızdır. Bu alt kategori için olaylar şunları içerir:

* 4624: Bir hesapta başarıyla oturum açıldı.
* 4625: Bir hesapta oturum açılamadı.
* 4648: Açık kimlik bilgileri kullanılarak oturum açılmaya çalışıldı.
* 4675: SID'ler filtrelendi.

Bu ayar için önerilen durum: Başarılı ve Başarısız.

**Gerekçe:**

Bir güvenlik olayı araştırılırken bu olayların denetlenmesi yararlı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Başarı ve Hata olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\Oturum Açma/Oturum Kapatma\Denetim Oturum Açma*

**17.5.5 (L1) 'Diğer Oturum Açma/Oturum Kapatma Olaylarını Denetle' seçeneği 'Başarılı ve Hatalı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:** Bu alt kategori, Uzak Masaüstü Hizmetleri oturumunun bağlantısının kesilmesi ve yeniden bağlanması, işlemleri farklı bir hesap altında çalıştırmak için RunAs'ın kullanılması ve bir iş istasyonunun kilitlenmesi ve kilidinin açılması gibi oturum açma/oturum kapatmayla ilgili diğer olayları bildirir. Bu alt kategori için olaylar şunları içerir:

* 4649: Bir tekrar saldırısı algılandı.
* 4778: Bir oturum, bir Pencere İstasyonuna yeniden bağlandı.
* 4779: Bir Pencere İstasyonundan bir oturumun bağlantısı kesildi.
* 4800: İş istasyonu kilitlendi.
* 4801: İş istasyonunun kilidi açıldı.
* 4802: Ekran koruyucu çağrıldı.
* 4803: Ekran koruyucu kapatıldı.
* 5378: İstenen kimlik bilgileri delegasyonuna ilke tarafından izin verilmedi.
* 5632: Bir kablosuz ağda kimlik doğrulaması yapmak için bir istekte bulunuldu.
* 5633: Kablolu bir ağda kimlik doğrulaması için bir istekte bulunuldu.

Bu ayar için önerilen durum: Başarılı ve Başarısız.

**Gerekçe:**

Bir güvenlik olayı araştırılırken bu olayların denetlenmesi yararlı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki kullanıcı arabirimi yolunu Başarı ve Hata olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\Oturum Açma/Oturum Kapatma\Denetim Diğer Oturum Açma/Oturum Kapatma Olayları*

**17.5.6 (L1) 'Özel Oturum Açmayı Denetle' seçeneği 'Başarılı' (Otomatik) içerecek şekilde ayarlanmalıdır.**

**Açıklama:**

Bu alt kategori, özel bir oturum açma kullanıldığında bildirir. Özel oturum açma, yöneticiye eşdeğer ayrıcalıklara sahip olan ve bir işlemi daha yüksek bir düzeye yükseltmek için kullanılabilen bir oturum açmadır. Bu alt kategori için olaylar şunları içerir:

* 4964 : Yeni bir oturum açmaya özel gruplar atanmıştır.

Bu ayar için önerilen durum şunları içerir: Başarılı.

**Gerekçe:**

Bir güvenlik olayı araştırılırken bu olayların denetlenmesi yararlı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, Başarı'yı içerecek şekilde aşağıdaki kullanıcı arabirimi yolunu ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\Oturum Açma/Oturum Kapatma\Denetim Özel Oturum Açma*

**17.6 Nesne Erişimi**

**17.6.1 (L1) 'Ayrıntılı Dosya Paylaşımını Denetle' seçeneği 'Hata' (Otomatik) içerecek şekilde ayarlanmalıdır.**

**Açıklama:**

Bu alt kategori, paylaşılan bir klasördeki dosya ve klasörlere erişim girişimlerini denetlemenize olanak tanır. Bu alt kategori için olaylar şunları içerir:

* 5145: istemciye istenen erişimin verilip verilmediğini görmek için ağ paylaşım nesnesi kontrol edildi.

Bu ayar için önerilen durum şunları içerir: Hata

**Gerekçe:**

Hataların denetlenmesi, hangi yetkisiz kullanıcıların bu bilgisayardaki bir ağ paylaşımındaki bir dosyaya veya klasöre erişmeye çalıştığını (ve başarısız olduğunu) günlüğe kaydeder; bu, muhtemelen kötü amaçlı yazılımın bir göstergesi olabilir. niyet.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Hata içerecek şekilde ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\Nesne Erişimi\Denetim Ayrıntılı Dosya Paylaşımı*

**17.6.2 (L1) 'Dosya Paylaşımını Denetle' seçeneği 'Başarılı ve Başarısız' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, paylaşılan bir klasöre erişme girişimlerini denetlemenize olanak tanır. Bu ayar için önerilen durum: Başarılı ve Başarısız.

**Not:**

Paylaşılan klasörler için sistem erişim kontrol listesi (SACL'ler) yoktur. Bu ilke ayarı etkinleştirilirse, sistemdeki tüm paylaşılan klasörlere erişim denetlenir.

**Gerekçe:**

Bir kuruluş tarafından yönetilen ortamda, dosya sunucuları normalde dosya paylaşım etkinliklerinin genel yükünü üstleneceğinden, iş istasyonlarının sınırlı dosya paylaşım etkinliği olmalıdır. Bu nedenle, iş istasyonlarındaki herhangi bir olağandışı dosya paylaşım etkinliği, potansiyel olarak kötü amaçlı etkinliğin araştırılmasında yararlı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Başarı ve Hata olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\Nesne Erişimi\Denetim Dosya Paylaşımı*

**17.6.3 (L1) 'Diğer Nesne Erişim Olaylarını Denetle' seçeneği 'Başarı ve Başarısızlık' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, görev zamanlayıcı işlerinin veya COM+ nesnelerinin yönetimi tarafından oluşturulan olayları denetlemenize olanak tanır.

Zamanlayıcı işleri için aşağıdakiler denetlenir:

* İş oluşturuldu.
* İş silindi.
* İş etkinleştirildi.
* İş devre dışı bırakıldı.
* İş güncellendi.

COM+ nesneleri için aşağıdakiler denetlenir:

* Katalog nesnesi eklendi.
* Katalog nesnesi güncellendi.
* Katalog nesnesi silindi.

Bu ayar için önerilen durum: Başarılı ve Başarısız.

**Gerekçe:**

Zamanlanmış görevlerin ve COM+ nesnelerinin beklenmedik şekilde oluşturulması, potansiyel olarak kötü niyetli etkinliğin bir göstergesi olabilir. Bu tür eylemler genellikle düşük hacimli olduğundan, bunları bir araştırma sırasında kullanmak üzere denetim günlüklerinde yakalamak yararlı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki kullanıcı arabirimi yolunu Başarı ve Hata olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\Nesne Erişimi\Denetim Diğer Nesne Erişim Olayları*

**17.6.4 (L1) 'Çıkarılabilir Depolamayı Denetle' seçeneği 'Başarılı ve Hatalı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcının çıkarılabilir bir depolama aygıtındaki dosya sistemi nesnelerine erişme girişimlerini denetlemenize olanak tanır. İstenen tüm erişim türleri için yalnızca tüm nesneler için bir güvenlik denetimi olayı oluşturulur. Bu ilke ayarını yapılandırırsanız, bir hesap çıkarılabilir depolama birimindeki bir dosya sistemi nesnesine her eriştiğinde bir denetim olayı oluşturulur. Başarı denetimleri başarılı girişimleri kaydeder ve Başarısızlık denetimleri başarısız girişimleri kaydeder. Bu ilke ayarını yapılandırmazsanız, bir hesap çıkarılabilir depolama birimindeki bir dosya sistemi nesnesine eriştiğinde hiçbir denetim olayı oluşturulmaz. Bu ayar için önerilen durum: Başarılı ve Başarısız.

**Not:** Grup İlkesi'nde bu değere erişmek ve bu değeri ayarlamak için Windows 8.0, Server 2012 (R2 olmayan) veya daha yeni bir işletim sistemi gerekir.

**Gerekçe:**

Bir olayı araştırırken çıkarılabilir depolamayı denetlemek yararlı olabilir. Örneğin, bir kişinin hassas bilgileri bir USB sürücüsüne kopyaladığından şüpheleniliyorsa.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Başarı ve Hata olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\Nesne Erişimi\Denetim Çıkarılabilir Depolama Birimi*

**17.7 İlke Değişikliği**

**17.7.1 (L1) 'Denetim İlkesi Değişikliğini Denetle' seçeneği 'Başarı' (Otomatik) içerecek şekilde ayarlanmalıdır.**

**Açıklama:**

Bu alt kategori, SACL değişiklikleri de dahil olmak üzere denetim politikasındaki değişiklikleri bildirir. Bu alt kategori için olaylar şunları içerir:

* 4715: Bir nesne üzerindeki denetim ilkesi (SACL) değiştirildi.
* 4719: Sistem denetim politikası değiştirildi.  4902: Kullanıcı başına denetim ilkesi tablosu oluşturuldu.
* 4904: Bir güvenlik olayı kaynağı kaydedilmeye çalışıldı.
* 4905: Bir güvenlik olayı kaynağının kaydını silme girişiminde bulunuldu.
* 4906: CrashOnAuditFail değeri değişti.
* 4907: Nesne üzerindeki denetim ayarları değiştirildi.
* 4908: Özel Gruplar Oturum açma tablosu değiştirildi.
* 4912: Kullanıcı Başına Denetim Politikası değiştirildi.
* Bu ayar için önerilen durum şunları içerir: Başarılı.

**Gerekçe:**

Bir güvenlik olayı araştırılırken bu olayların denetlenmesi yararlı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, Başarı'yı içerecek şekilde aşağıdaki kullanıcı arabirimi yolunu ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\İlke Değişikliği\Denetim Denetim İlkesi Değişikliği*

**17.7.2 (L1) 'Kimlik Doğrulama İlkesi Değişikliğini Denetle' seçeneği 'Başarılı' (Otomatik) içerecek şekilde ayarlanmalıdır.**

**Açıklama:**

Bu alt kategori, kimlik doğrulama ilkesindeki değişiklikleri bildirir. Bu alt kategori için olaylar şunları içerir:

* 4706: Bir etki alanına yeni bir güven oluşturuldu.
* 4707: Bir etki alanına güven kaldırıldı.
* 4713: Kerberos politikası değiştirildi.
* 4716: Güvenilir alan bilgisi değiştirildi.
* 4717: Bir hesaba sistem güvenlik erişimi verildi.
* 4718: Bir hesaptan sistem güvenlik erişimi kaldırıldı.
* 4739: Etki Alanı Politikası değiştirildi.
* 4864: Bir ad alanı çakışması algılandı.
* 4865: Güvenilir bir orman bilgi girişi eklendi.
* 4866: Güvenilir bir orman bilgi girişi kaldırıldı.
* 4867: Güvenilir bir orman bilgi girişi değiştirildi.

Bu ayar için önerilen durum şunları içerir: Başarılı.

**Gerekçe:**

Bir güvenlik olayı araştırılırken bu olayların denetlenmesi yararlı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, Başarı'yı içerecek şekilde aşağıdaki UI yolunu ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\İlke Değişikliği\Denetim Kimlik Doğrulama İlkesi Değişikliği*

**17.7.3 (L1) 'Yetkilendirme İlkesi Değişikliğini Denetle' seçeneği 'Başarılı' (Otomatik) içerecek şekilde ayarlanmalıdır.**

**Açıklama:**

Bu alt kategori, yetkilendirme politikasındaki değişiklikleri bildirir. Bu alt kategori için olaylar şunları içerir:

* 4704: Bir kullanıcı hakkı atandı.
* 4705: Bir kullanıcı hakkı kaldırıldı.
* 4706: Bir etki alanına yeni bir güven oluşturuldu.
* 4707: Bir etki alanına güven kaldırıldı.
* 4714: Şifreli veri kurtarma ilkesi değiştirildi.

Bu ayar için önerilen durum şunları içerir: Başarılı.

**Gerekçe:**

Bir güvenlik olayı araştırılırken bu olayların denetlenmesi yararlı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, Başarı'yı içerecek şekilde aşağıdaki UI yolunu ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\İlke Değişikliği\Denetim Yetkilendirme İlkesi Değişikliğ*

**17.7.4 (L1) 'MPSSVC Kural Düzeyinde İlke Değişikliğini Denetle' seçeneği 'Başarılı ve Başarısız' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu alt kategori, Microsoft Koruma Hizmeti (MPSSVC.exe) için ilke kurallarında değişiklik yapıldığında işletim sisteminin denetim olayları oluşturup oluşturmadığını belirler. Bu alt kategori için olaylar şunları içerir:

* 4944: Windows Güvenlik Duvarı başlatıldığında aşağıdaki ilke etkindi.
* 4945: Windows Güvenlik Duvarı başladığında bir kural listelendi.
* 4946: Windows Güvenlik Duvarı istisna listesinde bir değişiklik yapıldı. Bir kural eklendi.
* 4947: Windows Güvenlik Duvarı istisna listesinde bir değişiklik yapıldı. Bir kural değiştirildi.
* 4948: Windows Güvenlik Duvarı istisna listesinde bir değişiklik yapıldı. Bir kural silindi.
* 4949: Windows Güvenlik Duvarı ayarları varsayılan değerlere geri yüklendi.  4950: Bir Windows Güvenlik Duvarı ayarı değişti.
* 4951: Ana sürüm numarası Windows Güvenlik Duvarı tarafından tanınmadığı için bir kural yok sayıldı.
* 4952: Alt sürüm numarası Windows Güvenlik Duvarı tarafından tanınmadığı için bir kuralın bazı bölümleri yok sayıldı. Kuralın diğer kısımları uygulanacaktır.
* 4953: Bir kural, kuralı ayrıştıramadığı için Windows Güvenlik Duvarı tarafından yok sayıldı.
* 4954: Windows Güvenlik Duvarı Grup İlkesi ayarları değişti. Yeni ayarlar uygulandı.
* 4956: Windows Güvenlik Duvarı etkin profili değiştirdi.
* 4957: Windows Güvenlik Duvarı aşağıdaki kuralı uygulamadı.
* 4958: Kural, bu bilgisayarda yapılandırılmamış öğelere atıfta bulunduğundan, Windows Güvenlik Duvarı aşağıdaki kuralı uygulamadı.

Bu ayar için önerilen durum şudur: Başarı ve Başarısızlık

**Gerekçe:**

Güvenlik duvarı kurallarındaki değişiklikler, bilgisayarın güvenlik durumunu ve ağ saldırılarına karşı ne kadar iyi korunduğunu anlamak için önemlidir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki kullanıcı arabirimi yolunu Başarı ve Hata olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\İlke Değişikliği\Audit MPSSVC Kural Düzeyi İlke Değişikliği*

**17.7.5 (L1) 'Diğer İlke Değişikliği Olaylarını Denetle' seçeneği 'Hata' (Otomatik) içerecek şekilde ayarlanmalıdır.**

**Açıklama:**

Bu alt kategori, EFS Data Recovery Agent ilke değişiklikleri, Windows Filtreleme Platformu filtresindeki değişiklikler, yerel Grup İlkesi ayarları için Güvenlik ilkesi ayarları güncellemelerindeki durum, Merkezi Erişim İlkesi değişiklikleri ve Kriptografik Yeni Nesil (CNG) işlemleri için ayrıntılı sorun giderme olaylarıyla ilgili olayları içerir:

* 5063: Bir kriptografik sağlayıcı işlemi denendi.
* 5064: Bir kriptografik bağlam işlemi denendi.
* 5065: Bir kriptografik bağlam değişikliği denendi.
* 5066: Bir şifreleme işlevi işlemi denendi.
* 5067: Bir şifreleme işlevi değişikliği denendi.
* 5068: Bir şifreleme işlevi sağlayıcı işlemi denendi.
* 5069: Bir şifreleme işlevi özelliği işlemi denendi.
* 5070: Bir şifreleme işlevi özelliği değişikliği denendi.
* 6145: Grup ilkesi nesnelerinde güvenlik ilkesi işlenirken bir veya daha fazla hata oluştu.

Bu ayar için önerilen durum şunları içerir: Hata.

**Gerekçe:**

Bu ayar, Grup İlkesi'nden gelen uygulanan Güvenlik ayarlarındaki hataların ve Şifreli Yeni Nesil (CNG) işlevleriyle ilgili hata olaylarının algılanmasına yardımcı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Hata içerecek şekilde ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\İlke Değişikliği\Denetim Diğer İlke Değişikliği Olayları*

**17.8 Ayrıcalık Kullanımı**

**17.8.1 (L1) 'Hassas Ayrıcalık Kullanımını Denetle' seçeneği 'Başarılı ve Başarısız' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu alt kategori, EFS Data Recovery Agent ilke değişiklikleri, Windows Filtreleme Platformu filtresindeki değişiklikler, yerel Grup İlkesi ayarları için Güvenlik ilkesi ayarları güncellemelerindeki durum, Merkezi Erişim İlkesi değişiklikleri ve Kriptografik Yeni Nesil (CNG) işlemleri için ayrıntılı sorun giderme olaylarıyla ilgili olayları içerir:

* 5063: Bir kriptografik sağlayıcı işlemi denendi.
* 5064: Bir kriptografik bağlam işlemi denendi.
* 5065: Bir kriptografik bağlam değişikliği denendi.
* 5066: Bir şifreleme işlevi işlemi denendi.
* 5067: Bir şifreleme işlevi değişikliği denendi.
* 5068: Bir şifreleme işlevi sağlayıcı işlemi denendi.
* 5069: Bir şifreleme işlevi özelliği işlemi denendi.
* 5070: Bir şifreleme işlevi özelliği değişikliği denendi.
* 6145: Grup ilkesi nesnelerinde güvenlik ilkesi işlenirken bir veya daha fazla hata oluştu.

Bu ayar için önerilen durum şunları içerir: Hata.

**Gerekçe:**

Bu ayar, Grup İlkesi'nden gelen uygulanan Güvenlik ayarlarındaki hataların ve Şifreli Yeni Nesil (CNG) işlevleriyle ilgili hata olaylarının algılanmasına yardımcı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Hata içerecek şekilde ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\İlke Değişikliği\Denetim Diğer İlke Değişikliği Olayları*

**17.9 Sistem**

**17.9.1 (L1) 'IPsec Sürücüsünü Denetle' seçeneği 'Başarılı ve Hatalı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:** Bu alt kategori, İnternet Protokolü güvenlik (IPsec) sürücüsünün etkinlikleri hakkında raporlar. Bu alt kategori için olaylar şunları içerir:

* 4960: IPsec, bütünlük denetiminde başarısız olan bir gelen paketi bıraktı. Bu sorun devam ederse, bir ağ sorununu veya bu bilgisayara geçiş sırasında paketlerin değiştirildiğini gösterebilir. Uzak bilgisayardan gönderilen paketlerin bu bilgisayar tarafından alınan paketlerle aynı olduğunu doğrulayın. Bu hata, diğer IPsec uygulamalarıyla birlikte çalışabilirlik sorunlarını da gösterebilir.
* 4961: IPsec, tekrar denetiminde başarısız olan bir gelen paketi bıraktı. Bu sorun devam ederse, bu bilgisayara karşı bir tekrar saldırısı olduğunu gösterebilir.
* 4962: IPsec, tekrar denetiminde başarısız olan bir gelen paketi bıraktı. Gelen paketin bir tekrar olmadığından emin olmak için çok düşük bir sıra numarası vardı.
* 4963: IPsec, güvence altına alınması gereken bir gelen düz metin paketi bıraktı. Bunun nedeni genellikle uzak bilgisayarın IPsec ilkesini bu bilgisayarı bilgilendirmeden değiştirmesidir. Bu aynı zamanda bir sızdırma saldırısı girişimi olabilir.
* 4965: IPsec, uzak bir bilgisayardan yanlış Güvenlik Parametre Dizini (SPI) içeren bir paket aldı. Bu genellikle paketleri bozan hatalı çalışan donanımdan kaynaklanır. Bu hatalar devam ederse, uzak bilgisayardan gönderilen paketlerin bu bilgisayar tarafından alınan paketlerle aynı olduğunu doğrulayın. Bu hata, diğer IPsec uygulamalarıyla birlikte çalışabilirlik sorunlarını da gösterebilir. Bu durumda, bağlantı engellenmezse, bu olaylar göz ardı edilebilir.
* 5478: IPsec Hizmetleri başarıyla başlatıldı.
* 5479: IPsec Hizmetleri başarıyla kapatıldı. IPsec Hizmetlerinin kapatılması, bilgisayarı daha fazla ağ saldırısı riskine sokabilir veya bilgisayarı potansiyel güvenlik risklerine maruz bırakabilir.
* 5480: IPsec Hizmetleri bilgisayardaki ağ arabirimlerinin tam listesini alamadı. Bazı ağ arayüzleri, uygulanan IPsec filtreleri tarafından sağlanan korumayı alamayabileceğinden, bu potansiyel bir güvenlik riski oluşturur. Sorunu tanılamak için IP Güvenlik İzleyicisi ek bileşenini kullanın.
* 5483: IPsec Hizmetleri, RPC sunucusunu başlatamadı. IPsec Hizmetleri başlatılamadı.
* 5484: IPsec Hizmetleri kritik bir hata yaşadı ve kapatıldı. IPsec Hizmetlerinin kapatılması, bilgisayarı daha fazla ağ saldırısı riskine sokabilir veya bilgisayarı potansiyel güvenlik risklerine maruz bırakabilir.
* 5485: IPsec Hizmetleri, ağ arabirimleri için bir tak ve çalıştır olayında bazı IPsec filtrelerini işleyemedi. Bazı ağ arayüzleri, uygulanan IPsec filtreleri tarafından sağlanan korumayı alamayabileceğinden, bu potansiyel bir güvenlik riski oluşturur. Sorunu tanılamak için IP Güvenlik İzleyicisi ek bileşenini kullanın.

Bu ayar için önerilen durum: Başarılı ve Başarısız.

**Gerekçe:**

Bir güvenlik olayı araştırılırken bu olayların denetlenmesi yararlı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki kullanıcı arabirimi yolunu Başarı ve Hata olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\Sistem\Audit IPsec Sürücüsü*

**17.9.2 (L1) 'Diğer Sistem Olaylarını Denetle' seçeneği 'Başarı ve Başarısızlık' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu alt kategori, diğer sistem olaylarını raporlar. Bu alt kategori için olaylar şunları içerir:

* 5024 : Windows Güvenlik Duvarı Hizmeti başarıyla başlatıldı.
* 5025 : Windows Güvenlik Duvarı Hizmeti durduruldu.
* 5027: Windows Güvenlik Duvarı Hizmeti, güvenlik ilkesini yerel depolamadan alamadı. Hizmet, mevcut politikayı uygulamaya devam edecek.
* 5028: Windows Güvenlik Duvarı Hizmeti, yeni güvenlik ilkesini ayrıştıramadı. Hizmet, şu anda uygulanan politikayla devam edecek.
* 5029: Windows Güvenlik Duvarı Hizmeti, sürücüyü başlatamadı. Hizmet, geçerli politikayı uygulamaya devam edecek.
* 5030: Windows Güvenlik Duvarı Hizmeti başlatılamadı.
* 5032: Windows Güvenlik Duvarı, bir uygulamanın ağ üzerinden gelen bağlantıları kabul etmesini engellediğini kullanıcıya bildiremedi.
* 5033 : Windows Güvenlik Duvarı Sürücüsü başarıyla başlatıldı.
* 5034 : Windows Güvenlik Duvarı Sürücüsü durduruldu.
* 5035: Windows Güvenlik Duvarı Sürücüsü başlatılamadı.
* 5037: Windows Güvenlik Duvarı Sürücüsü kritik çalışma zamanı hatası algıladı. sonlandırılıyor.
* 5058: Anahtar dosya işlemi.
* 5059: Anahtar taşıma işlemi.

Bu ayar için önerilen durum: Başarılı ve Başarısız.

**Gerekçe:**

Bu denetim olaylarını yakalamak, Windows Güvenlik Duvarı'nın ne zaman beklendiği gibi çalışmadığını belirlemek için yararlı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki kullanıcı arabirimi yolunu Başarı ve Hata olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\Sistem\Denetim Diğer Sistem Olayları*

**17.9.3 (L1) 'Güvenlik Durumu Değişikliğini Denetle' seçeneği 'Başarılı' (Otomatik) içerecek şekilde ayarlanmalıdır.**

**Açıklama:**

Bu alt kategori, güvenlik alt sisteminin ne zaman başlayıp ne zaman durduğu gibi, sistemin güvenlik durumundaki değişiklikleri bildirir. Bu alt kategori için olaylar şunları içerir:

* 4608: Windows başlatılıyor.
* 4609: Windows kapanıyor.
* 4616: Sistem saati değiştirildi.
* 4621: Yönetici, CrashOnAuditFail'den sistemi kurtardı. Yönetici olmayan kullanıcıların artık oturum açmasına izin verilecek. Denetlenebilir bazı etkinlikler kaydedilmemiş olabilir.

Bu ayar için önerilen durum şunları içerir: Başarılı.

**Gerekçe:**

Bir güvenlik olayı araştırılırken bu olayların denetlenmesi yararlı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, Başarı'yı içerecek şekilde aşağıdaki UI yolunu ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\Sistem\Denetim Güvenlik Durumu Değişikliği*

**17.9.4 (L1) 'Güvenlik Sistemi Uzantısını Denetle' seçeneği 'Başarılı' (Otomatik) içerecek şekilde ayarlanmalıdır.**

**Açıklama:**

Bu alt kategori, güvenlik alt sistemi tarafından kimlik doğrulama paketleri gibi uzantı kodunun yüklenmesini bildirir. Bu alt kategori için olaylar şunları içerir:

* 4610: Yerel Güvenlik Yetkilisi tarafından bir kimlik doğrulama paketi yüklendi.
* 4611: Yerel Güvenlik Yetkilisi'ne güvenilir bir oturum açma işlemi kaydedildi.
* 4614: Güvenlik Hesabı Yöneticisi tarafından bir bildirim paketi yüklendi.
* 4622: Yerel Güvenlik Yetkilisi tarafından bir güvenlik paketi yüklendi.
* 4697: Sisteme bir servis kuruldu.

Bu ayar için önerilen durum şunları içerir: Başarılı.

**Gerekçe:**

Bir güvenlik olayı araştırılırken bu olayların denetlenmesi yararlı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Başarı içerecek şekilde ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\Sistem\Denetim Güvenlik Sistem Uzantısı*

**17.9.5 (L1) 'Sistem Bütünlüğünü Denetle' seçeneği 'Başarı ve Başarısızlık' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu alt kategori, güvenlik alt sisteminin bütünlüğünün ihlallerini bildirir. Bu alt kategori için olaylar şunları içerir:

* 4612 : Denetim mesajlarının sıralanması için ayrılan dahili kaynaklar tükendi ve bazı denetimlerin kaybedilmesine neden oldu.
* 4615: LPC bağlantı noktasının geçersiz kullanımı.
* 4618: İzlenen bir güvenlik olayı paterni oluştu.
* 4816: RPC, gelen bir mesajın şifresini çözerken bir bütünlük ihlali tespit etti.
* 5038 : Kod bütünlüğü, bir dosyanın görüntü karmasının geçerli olmadığını belirledi. Dosya, yetkisiz değişiklik nedeniyle bozulmuş olabilir veya geçersiz karma, olası bir disk aygıtı hatasını gösterebilir.
* 5056: Bir kriptografik kendi kendine test yapıldı.
* 5057: Bir şifreleme ilkel işlemi başarısız oldu.
* 5060: Doğrulama işlemi başarısız oldu.
* 5061: Şifreleme işlemi.
* 5062: Bir çekirdek modu kriptografik kendi kendine test yapıldı.

Bu ayar için önerilen durum: Başarılı ve Başarısız.

**Gerekçe:**

Bir güvenlik olayı araştırılırken bu olayların denetlenmesi yararlı olabilir.

**Etki:**

Hiçbir denetim ayarı yapılandırılmamışsa veya kuruluşunuzdaki bilgisayarlarda denetim ayarları çok gevşekse, güvenlik olayları tespit edilemeyebilir veya güvenlik olayları meydana geldikten sonra ağ adli analizi için yeterli kanıt bulunamayabilir. Ancak, denetim ayarları çok ciddiyse, Güvenlik günlüğündeki kritik öneme sahip girişler, tüm anlamsız girişler ve bilgisayar performansı tarafından gizlenebilir ve kullanılabilir veri depolama miktarı ciddi şekilde etkilenebilir. Düzenlenmiş belirli sektörlerde faaliyet gösteren şirketlerin, belirli olayları veya faaliyetleri kaydetme konusunda yasal yükümlülükleri olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki kullanıcı arabirimi yolunu Başarı ve Hata olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Windows Ayarları\Güvenlik Ayarları\Gelişmiş Denetim İlkesi Yapılandırması\Denetim İlkeleri\Sistem\Denetim Sistem Bütünlüğü*

**18 Yönetim Şablonları (Bilgisayar)**

**18.1 Kontrol Paneli**

Bu bölüm, Kontrol Paneli ayarları için öneriler içerir.

Bu Grup İlkesi bölümü, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu *Windows.admx/adml* tarafından sağlanır.

**18.1.1 Kişiselleştirme**

**18.1.1.1 (L1) 'Kilit ekranı kamerasının etkinleştirilmesini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bilgisayar Ayarlarında kilit ekranı kamera geçiş anahtarını devre dışı bırakır ve kilit ekranında bir kameranın çağrılmasını engeller. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Kilit ekranı kamerasının devre dışı bırakılması, kilit ekranının sağladığı korumayı kamera özelliklerine kadar genişletir.

**Etki:**

Bu ayarı etkinleştirirseniz, kullanıcılar artık PC Ayarları'nda kilit ekranı kamera erişimini etkinleştiremez veya devre dışı bırakamaz ve kamera kilit ekranında çağrılamaz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Personalization:NoLock ScreenCamera*

**Düzeltme**:

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonlar\Denetim Masası\Kişiselleştirme\Kilit ekranı kamerasının etkinleştirilmesini engelle*

**18.1.1.2 (L1) 'Kilit ekranı slayt gösterisinin etkinleştirilmesini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

PC Ayarları'nda kilit ekranı slayt gösterisi ayarlarını devre dışı bırakır ve bir slayt gösterisinin kilit ekranında oynatılmasını engeller. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Kilit ekranı slayt gösterisini devre dışı bırakmak, kilit ekranının sağladığı korumayı slayt gösterisi içeriğine genişletir.

**Etki:**

Bu ayarı etkinleştirirseniz, kullanıcılar artık Bilgisayar Ayarları'ndaki slayt gösterisi ayarlarını değiştiremez ve hiçbir slayt gösterisi başlamaz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Personalization:NoLock ScreenSlideshow*

**Düzeltme**:

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonlar\Denetim Masası\Kişiselleştirme\Kilit ekranı slayt gösterisini etkinleştirmeyi engelle*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.1 ve 2012 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu ControlPanelDisplay.admx/adml tarafından sağlanır.

**18.1.2 Bölge ve Dil Seçenekleri**

**18.1.2.1 El yazısı kişiselleştirme**

**18.1.2.2 (L1) 'Kullanıcıların çevrimiçi konuşma tanıma hizmetlerini etkinleştirmesine izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu politika, konuşma, mürekkep oluşturma ve yazmayı içeren girdi kişiselleştirmenin otomatik öğrenme bileşenini etkinleştirir. Otomatik öğrenme, konuşma ve el yazısı kalıplarının, yazma geçmişinin, kişilerin ve son takvim bilgilerinin toplanmasını sağlar. Cortana kullanımı için gereklidir. Bu toplanan bilgilerin bir kısmı, mürekkep oluşturma ve yazma durumunda kullanıcının OneDrive'ında depolanabilir; bazı bilgiler konuşmayı kişiselleştirmek için Microsoft'a yüklenecektir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bu ayar Etkin ise, hassas bilgiler bulutta saklanabilir veya Microsoft'a gönderilebilir.

**Etki:**

Konuşma, mürekkep oluşturma ve yazmanın otomatik olarak öğrenilmesi durur ve kullanıcılar PC Ayarları aracılığıyla değerini değiştiremez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\InputPersonalization:AllowInpu tPersonalization*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\ Denetim Masası\Bölge ve Dil Seçenekleri\Kullanıcıların çevrimiçi konuşma tanıma hizmetlerini etkinleştirmesine izin ver*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 RTM (Sürüm 1507) Yönetim Şablonları (veya daha yenisi) ile birlikte verilen Grup İlkesi şablonu Globalization.admx/adml tarafından sağlanır.

**Not #2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Giriş kişiselleştirmeye izin ver olarak adlandırıldı, ancak Windows 10 R1809 ve Server 2019 Yönetim Şablonlarından başlayarak kullanıcıların çevrimiçi konuşma tanıma hizmetlerini etkinleştirmesine izin ver olarak yeniden adlandırıldı.

**18.1.3 (L2) 'Çevrimiçi İpuçlarına İzin Ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Ayarlar uygulaması için çevrimiçi ipuçlarının ve yardımın alınmasını yapılandırır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Gizlilik endişeleri nedeniyle, bu veriler hassas bilgiler içerebileceğinden, veriler hiçbir zaman 3. şahıslara gönderilmemelidir.

**Etki:**

Ayarlar, ipuçlarını ve yardım içeriğini almak için Microsoft içerik hizmetleriyle iletişim kurmayacak. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore r:AllowOnlineTips*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Denetim Masası\Çevrimiçi İpuçlarına İzin Ver*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1709 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu ControlPanel.admx/adml tarafından sağlanır.

**18.2 LAPS ( Yerel Yöneticiler içim Parola Çözümleyici)**

**18.2.1 (L1) LAPS AdmPwd GPO Uzantısı / CSE'nin yüklü olmalıdır. (Otomatik)**

**Açıklama:**

Mayıs 2015'te Microsoft, bir kuruluşun etki alanına bağlı iş istasyonlarında ve Üye Sunucularda rastgele ve benzersiz yerel Yönetici hesabı parolalarını otomatik olarak ayarlamasına olanak tanıyan ücretsiz ve desteklenen bir yazılım olan Yerel Yönetici Parola Çözümü (LAPS) aracını yayımladı. Parolalar, etki alanı bilgisayar hesabının gizli bir özniteliğinde saklanır ve gerektiğinde onaylı Sistem Yöneticileri tarafından Active Directory'den alınabilir. LAPS aracı, hedeflenen bilgisayarlarda bir Grup İlkesi İstemci Tarafı Uzantısının (CSE) kurulmasının yanı sıra uygulamak için küçük bir Active Directory Şeması güncellemesi gerektirir. Ayrıntılar için lütfen LAPS belgelerine bakın. LAPS, Windows Vista veya daha yeni iş istasyonu işletim sistemlerini ve Server 2003 veya daha yeni sunucu işletim sistemlerini destekler. LAPS, bağımsız bilgisayarları desteklemez - bir etki alanına katılmaları gerekir.

**Not:** Etki alanı üyelerindeki benzersiz ve karmaşık yerel Yönetici parolalarını yönetmek için üçüncü taraf ticari yazılım kullanan kuruluşlar, bu LAPS önerilerini göz ardı etmeyi seçebilir.

**Not #2:** LAPS, yalnızca yerel Yönetici parolalarını yönetmek için tasarlanmıştır ve bu nedenle, geleneksel bir yerel Yönetici hesabına sahip olmayan Etki Alanı Denetleyicilerinde doğrudan kullanılması önerilmez (veya desteklenmez). Yalnızca LAPS CSE ve LAPS GPO ayarlarını üye sunuculara ve iş istasyonlarına dağıtmanızı şiddetle tavsiye ederiz.

**Gerekçe:**

Yerel Yönetici parolalarını yönetmenin zorluğu nedeniyle, birçok kuruluş bunları dağıtırken tüm iş istasyonlarında ve/veya Üye Sunucularda aynı parolayı kullanmayı tercih eder. Bu, ciddi bir saldırı yüzeyi güvenlik riski oluşturur, çünkü bir saldırgan bir sistemin güvenliğini aşmayı başarır ve yerel Yönetici hesabının parolasını öğrenirse, yerel Yöneticileri için bu parolayı kullanan diğer tüm bilgisayarlara anında erişim sağlamak için bu hesaptan yararlanabilir. hesap.

**Etki:**

Etki yok. AdmPwd.dll düzgün yüklendiğinde ve kaydedildiğinde, Grup İlkesi yenilemesi sırasında uygun GPO komutları verilmedikçe hiçbir işlem yapmaz. Bellekte yerleşik bir aracı veya hizmet değildir. Active Directory'nin kullanılamadığı bir olağanüstü durum kurtarma senaryosunda, yerel Yönetici parolası alınamaz ve bir araç (Microsoft'un Felaket ve Kurtarma Araç Seti (DaRT) Kurtarma Görüntüsü gibi) kullanılarak yerel bir parola sıfırlaması gerekli olabilir.

**Denetim:**

LAPS AdmPwd GPO Uzantısı / CSE'nin yüklendiği, aşağıdaki kayıt defteri değerinin varlığıyla doğrulanabilir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon\GPExtensions\{D76B9641-3288-4f75-942D 087DE603E3EA} :DllName*

**Düzeltme:**

LAPS'i kullanmak için küçük bir Active Directory Şeması güncellemesi gerekir ve yönetilen her bilgisayara bir Grup İlkesi İstemci Tarafı Uzantısı (CSE) yüklenmelidir. LAPS kurulduğunda, AdmPwd.dll dosyasının aşağıdaki konumda bulunması ve Windows'ta kayıtlı olması gerekir (LAPS AdmPwd GPO Uzantısı / CSE kurulumu bunu sizin için yapar):

*C:\Program Files\LAPS\CSE\AdmPwd.dll*

**18.2.2 (L1) 'Politikanın gerektirdiğinden daha uzun parola süre sonlarına izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Mayıs 2015'te Microsoft, bir kuruluşun etki alanına bağlı iş istasyonlarında ve Üye Sunucularda rastgele ve benzersiz yerel Yönetici hesabı parolalarını otomatik olarak ayarlamasına olanak tanıyan ücretsiz ve desteklenen bir yazılım olan Yerel Yönetici Parola Çözümü (LAPS) aracını yayımladı. Parolalar, etki alanı bilgisayar hesabının gizli bir özniteliğinde saklanır ve gerektiğinde onaylı Sistem Yöneticileri tarafından Active Directory'den alınabilir. LAPS aracı, hedeflenen bilgisayarlarda bir Grup İlkesi İstemci Tarafı Uzantısının (CSE) kurulmasının yanı sıra uygulamak için küçük bir Active Directory Şeması güncellemesi gerektirir. Ayrıntılar için lütfen LAPS belgelerine bakın. LAPS, Windows Vista veya daha yeni iş istasyonu işletim sistemlerini ve Server 2003 veya daha yeni sunucu işletim sistemlerini destekler. LAPS, bağımsız bilgisayarları desteklemez - bir etki alanına katılmaları gerekir. Bu ayar için önerilen durum: Etkin.

**Not:** Etki alanı üyelerindeki benzersiz ve karmaşık yerel Yönetici parolalarını yönetmek için üçüncü taraf ticari yazılım kullanan kuruluşlar, bu LAPS önerilerini göz ardı etmeyi seçebilir.

**Not #2:** LAPS, yalnızca yerel Yönetici parolalarını yönetmek için tasarlanmıştır ve bu nedenle, geleneksel bir yerel Yönetici hesabına sahip olmayan Etki Alanı Denetleyicilerinde doğrudan kullanılması önerilmez (veya desteklenmez). Yalnızca LAPS CSE ve LAPS GPO ayarlarını üye sunuculara ve iş istasyonlarına dağıtmanızı şiddetle tavsiye ederiz.

**Gerekçe:**

Yerel Yönetici parolalarını yönetmenin zorluğu nedeniyle, birçok kuruluş bunları dağıtırken tüm iş istasyonlarında ve/veya Üye Sunucularda aynı parolayı kullanmayı tercih eder. Bu, ciddi bir saldırı yüzeyi güvenlik riski oluşturur, çünkü bir saldırgan bir sistemin güvenliğini aşmayı başarır ve yerel Yönetici hesabının parolasını öğrenirse, yerel Yöneticileri için bu parolayı kullanan diğer tüm bilgisayarlara anında erişim sağlamak için bu hesaptan yararlanabilir.

**Etki:**

"Parola Ayarları" ilkesi tarafından belirlenen parola yaşından daha uzun planlanan parola kullanım süresinin dolmasına izin VERİLMEZ. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\MicrosoftServices\AdmPwd:PwdExpirationProtectionEnabled*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\ LAPS\Don't allow password sona erme süresi ilkenin gerektirdiğinden daha uzun*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Ek bir Grup İlkesi şablonu (AdmPwd.admx/adml) gereklidir - Microsoft Yerel Yönetici Parola Çözümü'ne (LAPS) dahildir.

**18.2.3 (L1) 'Yerel Yönetici Şifre Yönetimini Etkinleştir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Mayıs 2015'te Microsoft, bir kuruluşun etki alanına bağlı iş istasyonlarında ve Üye Sunucularda rastgele ve benzersiz yerel Yönetici hesabı parolalarını otomatik olarak ayarlamasına olanak tanıyan ücretsiz ve desteklenen bir yazılım olan Yerel Yönetici Parola Çözümü (LAPS) aracını yayımladı. Parolalar, etki alanı bilgisayar hesabının gizli bir özniteliğinde saklanır ve gerektiğinde onaylı Sistem Yöneticileri tarafından Active Directory'den alınabilir. LAPS aracı, hedeflenen bilgisayarlarda bir Grup İlkesi İstemci Tarafı Uzantısının (CSE) kurulmasının yanı sıra uygulamak için küçük bir Active Directory Şeması güncellemesi gerektirir. Ayrıntılar için lütfen LAPS belgelerine bakın. LAPS, Windows Vista veya daha yeni iş istasyonu işletim sistemlerini ve Server 2003 veya daha yeni sunucu işletim sistemlerini destekler. LAPS, bağımsız bilgisayarları desteklemez - bir etki alanına katılmaları gerekir. Bu ayar için önerilen durum: Etkin.

**Not:** Etki alanı üyelerindeki benzersiz ve karmaşık yerel Yönetici parolalarını yönetmek için üçüncü taraf ticari yazılım kullanan kuruluşlar, bu LAPS önerilerini göz ardı etmeyi seçebilir.

**Not #2:** LAPS, yalnızca yerel Yönetici parolalarını yönetmek için tasarlanmıştır ve bu nedenle, geleneksel bir yerel Yönetici hesabına sahip olmayan Etki Alanı Denetleyicilerinde doğrudan kullanılması önerilmez (veya desteklenmez). Yalnızca LAPS CSE ve LAPS GPO ayarlarını üye sunuculara ve iş istasyonlarına dağıtmanızı şiddetle tavsiye ederiz.

**Gerekçe:**

Yerel Yönetici parolalarını yönetmenin zorluğu nedeniyle, birçok kuruluş bunları dağıtırken tüm iş istasyonlarında ve/veya Üye Sunucularda aynı parolayı kullanmayı tercih eder. Bu, ciddi bir saldırı yüzeyi güvenlik riski oluşturur, çünkü bir saldırgan bir sistemin güvenliğini aşmayı başarır ve yerel Yönetici hesabının parolasını öğrenirse, yerel Yöneticileri için bu parolayı kullanan diğer tüm bilgisayarlara anında erişim sağlamak için bu hesaptan yararlanabilir.

**Etki:**

Yerel yönetici parolası yönetilir (hedef bilgisayarda LAPS AdmPwd GPO Uzantısının / CSE'nin kurulu olması şartıyla (bkz. etki alanında). Active Directory'nin kullanılamadığı bir olağanüstü durum kurtarma senaryosunda, yerel Yönetici parolası alınamaz ve bir araç (Microsoft'un Felaket ve Kurtarma Araç Seti (DaRT) Kurtarma Görüntüsü gibi) kullanılarak yerel bir parola sıfırlaması gerekli olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft Services\AdmPwd:AdmPwdEnabled*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\ LAPS\Enable Local Admin Password Management*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Ek bir Grup İlkesi şablonu (AdmPwd.admx/adml) gereklidir - Microsoft Yerel Yönetici Parola Çözümü'ne (LAPS) dahildir.

**18.2.4 (L1) 'Parola Ayarları: Parola Karmaşıklığı' seçeneği 'Etkin: Büyük harfler + küçük harfler + sayılar + özel karakterler' olarak ayarlanmalıdır. (Otomatik)**

**Açıklama:**

Mayıs 2015'te Microsoft, bir kuruluşun etki alanına bağlı iş istasyonlarında ve Üye Sunucularda rastgele ve benzersiz yerel Yönetici hesabı parolalarını otomatik olarak ayarlamasına olanak tanıyan ücretsiz ve desteklenen bir yazılım olan Yerel Yönetici Parola Çözümü (LAPS) aracını yayımladı. Parolalar, etki alanı bilgisayar hesabının gizli bir özniteliğinde saklanır ve gerektiğinde onaylı Sistem Yöneticileri tarafından Active Directory'den alınabilir. LAPS aracı, hedeflenen bilgisayarlarda bir Grup İlkesi İstemci Tarafı Uzantısının (CSE) kurulmasının yanı sıra uygulamak için küçük bir Active Directory Şeması güncellemesi gerektirir. Ayrıntılar için lütfen LAPS belgelerine bakın. LAPS, Windows Vista veya daha yeni iş istasyonu işletim sistemlerini ve Server 2003 veya daha yeni sunucu işletim sistemlerini destekler. LAPS, bağımsız bilgisayarları desteklemez - bir etki alanına katılmaları gerekir. Bu ayar için önerilen durum: Etkin: Büyük harfler + küçük harfler + sayılar + özel karakterler.

**Not:** Etki alanı üyelerindeki benzersiz ve karmaşık yerel Yönetici parolalarını yönetmek için üçüncü taraf ticari yazılım kullanan kuruluşlar, bu LAPS önerilerini göz ardı etmeyi seçebilir.

**Not #2:** LAPS, yalnızca yerel Yönetici parolalarını yönetmek için tasarlanmıştır ve bu nedenle, geleneksel bir yerel Yönetici hesabına sahip olmayan Etki Alanı Denetleyicilerinde doğrudan kullanılması önerilmez (veya desteklenmez). Yalnızca LAPS CSE ve LAPS GPO ayarlarını üye sunuculara ve iş istasyonlarına dağıtmanızı şiddetle tavsiye ederiz.

**Gerekçe:**

Yerel Yönetici parolalarını yönetmenin zorluğu nedeniyle, birçok kuruluş bunları dağıtırken tüm iş istasyonlarında ve/veya Üye Sunucularda aynı parolayı kullanmayı tercih eder. Bu, ciddi bir saldırı yüzeyi güvenlik riski oluşturur, çünkü bir saldırgan bir sistemin güvenliğini aşmayı başarır ve yerel Yönetici hesabının parolasını öğrenirse, yerel Yöneticileri için bu parolayı kullanan diğer tüm bilgisayarlara anında erişim sağlamak için bu hesaptan yararlanabilir. hesap.

**Etki:**

LAPS tarafından oluşturulan parolaların büyük harfler + küçük harfler + sayılar + özel karakterler içermesi gerekecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\MicrosoftServices\AdmPwd:PasswordComplexity*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın ve Parola Karmaşıklığı seçeneğini Büyük olarak yapılandırın harfler + küçük harfler + sayılar + özel karakterler:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\LAPS\Parola Ayarları*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Ek bir Grup İlkesi şablonu (AdmPwd.admx/adml) gereklidir - Microsoft Yerel Yönetici Parola Çözümü'ne (LAPS) dahildir.

**18.2.5 (L1) 'Şifre Ayarları: Şifre Uzunluğu' seçeneği 'Etkin: 15 veya daha fazla' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Mayıs 2015'te Microsoft, bir kuruluşun etki alanına bağlı iş istasyonlarında ve Üye Sunucularda rastgele ve benzersiz yerel Yönetici hesabı parolalarını otomatik olarak ayarlamasına olanak tanıyan ücretsiz ve desteklenen bir yazılım olan Yerel Yönetici Parola Çözümü (LAPS) aracını yayımladı. Parolalar, etki alanı bilgisayar hesabının gizli bir özniteliğinde saklanır ve gerektiğinde onaylı Sistem Yöneticileri tarafından Active Directory'den alınabilir. LAPS aracı, hedeflenen bilgisayarlarda bir Grup İlkesi İstemci Tarafı Uzantısının (CSE) kurulmasının yanı sıra uygulamak için küçük bir Active Directory Şeması güncellemesi gerektirir. Ayrıntılar için lütfen LAPS belgelerine bakın. LAPS, Windows Vista veya daha yeni iş istasyonu işletim sistemlerini ve Server 2003 veya daha yeni sunucu işletim sistemlerini destekler. LAPS, bağımsız bilgisayarları desteklemez - bir etki alanına katılmaları gerekir. Bu ayar için önerilen durum: Etkin: 15 veya daha fazla.

**Not:**Etki alanı üyelerindeki benzersiz ve karmaşık yerel Yönetici parolalarını yönetmek için üçüncü taraf ticari yazılım kullanan kuruluşlar, bu LAPS önerilerini göz ardı etmeyi seçebilir.

**Not #2:** LAPS, yalnızca yerel Yönetici parolalarını yönetmek için tasarlanmıştır ve bu nedenle, geleneksel bir yerel Yönetici hesabına sahip olmayan Etki Alanı Denetleyicilerinde doğrudan kullanılması önerilmez (veya desteklenmez). Yalnızca LAPS CSE ve LAPS GPO ayarlarını üye sunuculara ve iş istasyonlarına dağıtmanızı şiddetle tavsiye ederiz.

**Gerekçe:**

Yerel Yönetici parolalarını yönetmenin zorluğu nedeniyle, birçok kuruluş bunları dağıtırken tüm iş istasyonlarında ve/veya Üye Sunucularda aynı parolayı kullanmayı tercih eder. Bu, ciddi bir saldırı yüzeyi güvenlik riski oluşturur, çünkü bir saldırgan bir sistemin güvenliğini aşmayı başarır ve yerel Yönetici hesabının parolasını öğrenirse, yerel Yöneticileri için bu parolayı kullanan diğer tüm bilgisayarlara anında erişim sağlamak için bu hesaptan yararlanabilir.

**Etki:**

LAPS tarafından oluşturulan parolaların 15 karakter uzunluğunda (veya seçilirse daha fazla) olması gerekir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft Services\AdmPwd:PasswordLength*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın ve Parola Uzunluğu seçeneğini 15 olarak yapılandırın. veya daha fazlası:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\LAPS\Parola Ayarları*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Ek bir Grup İlkesi şablonu (AdmPwd.admx/adml) gereklidir - Microsoft Yerel Yönetici Parola Çözümü'ne (LAPS) dahildir.

**18.2.6 (L1) 'Şifre Ayarları: Şifre Yaşı (Gün)' seçeneği 'Etkin: 30 veya daha az' (Otomatik) olarak ayarlandığından emin olun**

**Açıklama:**

Mayıs 2015'te Microsoft, bir kuruluşun etki alanına bağlı iş istasyonlarında ve Üye Sunucularda rastgele ve benzersiz yerel Yönetici hesabı parolalarını otomatik olarak ayarlamasına olanak tanıyan ücretsiz ve desteklenen bir yazılım olan Yerel Yönetici Parola Çözümü (LAPS) aracını yayımladı. Parolalar, etki alanı bilgisayar hesabının gizli bir özniteliğinde saklanır ve gerektiğinde onaylı Sistem Yöneticileri tarafından Active Directory'den alınabilir. LAPS aracı, hedeflenen bilgisayarlarda bir Grup İlkesi İstemci Tarafı Uzantısının (CSE) kurulmasının yanı sıra uygulamak için küçük bir Active Directory Şeması güncellemesi gerektirir. Ayrıntılar için lütfen LAPS belgelerine bakın. LAPS, Windows Vista veya daha yeni iş istasyonu işletim sistemlerini ve Server 2003 veya daha yeni sunucu işletim sistemlerini destekler. LAPS, bağımsız bilgisayarları desteklemez - bir etki alanına katılmaları gerekir. Bu ayar için önerilen durum: Etkin: 30 veya daha az.

**Not:** Etki alanı üyelerindeki benzersiz ve karmaşık yerel Yönetici parolalarını yönetmek için üçüncü taraf ticari yazılım kullanan kuruluşlar, bu LAPS önerilerini göz ardı etmeyi seçebilir.

**Not #2:** LAPS, yalnızca yerel Yönetici parolalarını yönetmek için tasarlanmıştır ve bu nedenle, geleneksel bir yerel Yönetici hesabına sahip olmayan Etki Alanı Denetleyicilerinde doğrudan kullanılması önerilmez (veya desteklenmez). Yalnızca LAPS CSE ve LAPS GPO ayarlarını üye sunuculara ve iş istasyonlarına dağıtmanızı şiddetle tavsiye ederiz.

**Gerekçe:**

Yerel Yönetici parolalarını yönetmenin zorluğu nedeniyle, birçok kuruluş bunları dağıtırken tüm iş istasyonlarında ve/veya Üye Sunucularda aynı parolayı kullanmayı tercih eder. Bu, ciddi bir saldırı yüzeyi güvenlik riski oluşturur, çünkü bir saldırgan bir sistemin güvenliğini aşmayı başarır ve yerel Yönetici hesabının parolasını öğrenirse, yerel Yöneticileri için bu parolayı kullanan diğer tüm bilgisayarlara anında erişim sağlamak için bu hesaptan yararlanabilir.

**Etki:**

LAPS tarafından oluşturulan parolaların maksimum 30 günlük (veya seçilirse daha az) olması gerekir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\MicrosoftServices\AdmPwd:PasswordAgeDays*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın ve Parola Yaşını (Gün) yapılandırın. 30 veya daha az seçenek:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\LAPS\Parola Ayarları*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Ek bir Grup İlkesi şablonu (AdmPwd.admx/adml) gereklidir - Microsoft Yerel Yönetici Parola Çözümü'ne (LAPS) dahildir

**18.3 MS Güvenlik Kılavuzu**

**18.3.1 (L1) 'Ağda oturum açarken yerel hesaplara UAC (Kullanıcı Hesap Denetimi) kısıtlamaları uygula' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, yerel hesapların ağda oturum açma (örneğin, NET USE, C$'a bağlanma vb.) aracılığıyla uzaktan yönetim için kullanılıp kullanılamayacağını kontrol eder. Aynı hesap ve parola birden fazla sistemde yapılandırıldığında, yerel hesaplar yüksek kimlik bilgisi hırsızlığı riski altındadır. Bu politikanın etkinleştirilmesi, bu riski önemli ölçüde azaltır.

**Etkin**: Ağ oturum açmalarında yerel hesaplara UAC belirteç filtrelemesi uygular. Yöneticiler gibi güçlü bir gruba üyelik devre dışı bırakılır ve sonuçta ortaya çıkan erişim belirtecinden güçlü ayrıcalıklar kaldırılır. Bu, LocalAccountTokenFilterPolicy kayıt defteri değerini 0 olarak yapılandırır. Bu, Windows için varsayılan davranıştır.

**Devre Dışı:** LocalAccountTokenFilterPolicy kayıt defteri değerini 1 olarak yapılandırarak, ağda oturum açma yoluyla kimlik doğrulaması yaparken yerel hesapların tam yönetici haklarına sahip olmasına izin verir.

Yerel hesaplar ve kimlik bilgisi hırsızlığı hakkında daha fazla bilgi için, "[Pass-the-Hash (PtH) Saldırılarını ve Diğer Kimlik Hırsızlığı Teknikleri](http://www.microsoft.com/en-us/download/details.aspx?id=36036)" belgeleri. LocalAccountTokenFilterPolicy hakkında daha fazla bilgi için, 951016 numaralı Microsoft Bilgi Bankası makalesine bakın: [Windows Vista'da Kullanıcı Hesabı Denetimi ve uzaktan kısıtlamaların açıklaması.](https://support.microsoft.com/en-us/kb/951016)

Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Aynı hesap ve parola birden fazla sistemde yapılandırıldığında, yerel hesaplar kimlik bilgilerinin çalınması açısından yüksek risk altındadır. Bu politikanın Etkin olduğundan emin olmak, bu riski önemli ölçüde azaltır.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: LocalAccountTokenFilterPolicy*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\ Yönetim Şablonları\MS Güvenlik Kılavuzu\Ağ oturum açmalarında yerel hesaplara UAC kısıtlamaları uygula*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Ek bir Grup İlkesi şablonu (SecGuide.admx/adml) gereklidir - Microsoft'tan [bu bağlantı](https://www.microsoft.com/en-us/download/details.aspx?id=55319)dan edinilebilir

**18.3.2 (L1) 'SMB v1 istemci sürücüsünü yapılandır' seçeneği 'Etkin: Sürücüyü devre dışı bırak (önerilen)' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, devre dışı bırakılması önerilen Sunucu İleti Bloğu sürüm 1 (SMBv1) istemci sürücü hizmeti (MRxSmb10) için başlatma türünü yapılandırır. Bu ayar için önerilen durum: Etkin: Sürücüyü devre dışı bırak (önerilir).

**Not:** Hiçbir koşulda bu genel ayarı Devre Dışı olarak yapılandırmayın, aksi takdirde temel kayıt defteri girdisi tamamen silinecek ve bu da ciddi sorunlara neden olacaktır.

**Gerekçe:**

Eylül 2016'dan bu yana Microsoft, SMBv1'in devre dışı bırakılmasını ve artık modern ağlarda kullanılmamasını şiddetle teşvik etmektedir, çünkü bu 30 yıllık bir tasarımdır ve saldırılara karşı SMBv2 ve SMBv3 gibi çok daha yeni tasarımlardan çok daha savunmasızdır. Bununla ilgili daha fazla bilgiyi aşağıdaki bağlantılarda bulabilirsiniz:

[SMB1'i kullanmayı bırakın | Microsoft'ta Depolama](https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/)

[Grup İlkesi ile Yönetilen Ortamlarda SMB v1'i Devre Dışı Bırak "Güvenli Kal" Siber Güvenlik Blogu](https://blogs.technet.microsoft.com/staysafe/2017/05/17/disable-smb-v1-in-managed-environments-with-ad-group-policy/)

[Grup İlkesi aracılığıyla SMBv1'i Devre Dışı Bırakma – Microsoft Güvenlik Rehberi blogu](https://blogs.technet.microsoft.com/secguide/2017/06/15/disabling-smbv1-through-group-policy/)

**Etki:**

Bazı eski işletim sistemleri (ör. Windows XP, Server 2003 veya daha eski), uygulamalar ve cihazlar SMBv1 devre dışı bırakıldığında artık sistemle iletişim kuramaz. Bunu yaygın bir kontrol olarak yapılandırmadan önce etkiyi belirlemek için dikkatli testler yapılmasını ve mümkünse, uyumsuz sistemin satıcısıyla bulunan uyumsuzlukları gidermenizi öneririz. Microsoft ayrıca şu bağlantıda bilinen SMBv1 uyumsuzluklarının (kapsamlı olmasa da) eksiksiz bir listesini tutmaktadır: [SMB1 Ürün Takas Merkezi | Microsoft’da Depolama](https://blogs.technet.microsoft.com/filecab/2017/06/01/smb1-product-clearinghouse/)

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\mrxsmb10:Start*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın: Sürücüyü devre dışı bırak (önerilir):

*Bilgisayar Yapılandırması\ İlkeler\Yönetim Şablonları\MS Güvenlik Kılavuzu\SMB v1 istemci sürücüsünü yapılandır*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Ek bir Grup İlkesi şablonu (SecGuide.admx/adml) gereklidir - Microsoft'tan bu bağlantıdan edinilebilir.

**18.3.3 (L1) 'SMB v1 sunucusunu yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, Sunucu İleti Bloğu sürüm 1 (SMBv1) protokolünün sunucu tarafı işlemesini yapılandırır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Eylül 2016'dan bu yana Microsoft, SMBv1'in devre dışı bırakılmasını ve artık modern ağlarda kullanılmamasını şiddetle teşvik etmektedir, çünkü bu 30 yıllık bir tasarımdır ve saldırılara karşı SMBv2 ve SMBv3 gibi çok daha yeni tasarımlardan çok daha savunmasızdır. Bununla ilgili daha fazla bilgiyi aşağıdaki bağlantılarda bulabilirsiniz:

[SMB1'i kullanmayı bırakın | Microsoft'ta Depolama](https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/)

[Grup İlkesi ile Yönetilen Ortamlarda SMB v1'i Devre Dışı Bırak – "Güvenli Kal" Siber Güvenlik Blogu](https://blogs.technet.microsoft.com/staysafe/2017/05/17/disable-smb-v1-in-managed-environments-with-ad-group-policy/)

[Grup İlkesi aracılığıyla SMBv1'i Devre Dışı Bırakma – Microsoft Güvenlik Rehberi blogu](https://blogs.technet.microsoft.com/secguide/2017/06/15/disabling-smbv1-through-group-policy/)

**Etki:**

Bazı eski işletim sistemleri (ör. Windows XP, Server 2003 veya daha eski), uygulamalar ve cihazlar SMBv1 devre dışı bırakıldığında artık sistemle iletişim kuramaz. Bunu yaygın bir kontrol olarak yapılandırmadan önce etkiyi belirlemek için dikkatli testler yapılmasını ve mümkünse, uyumsuz sistemin satıcısıyla bulunan uyumsuzlukları gidermenizi öneririz. Microsoft ayrıca şu bağlantıda bilinen SMBv1 uyumsuzluklarının (kapsamlı olmasa da) eksiksiz bir listesini tutmaktadır: [SMB1 Ürün Takas Merkezi | Microsoft’da Depolama](https://blogs.technet.microsoft.com/filecab/2017/06/01/smb1-product-clearinghouse/)

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\LanmanServer\Parameters: SMB1*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları \MS Security Guide\Configure SMB v1 server*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Ek bir Grup İlkesi şablonu (SecGuide.admx/adml) gereklidir - Microsoft'tan [bu bağlantı](https://techcommunity.microsoft.com/t5/Microsoft-Security-Baselines/Security-baseline-FINAL-for-Windows-10-v1903-and-Windows-Server/ba-p/701084)dan edinilebilir

**18.3.4 (L1) 'Yapılandırılmış İstisna İşleme Üzerine Yazma Korumasını (SEHOP) Etkinleştir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Windows, Yapılandırılmış İstisna İşleme Üzerine Yazma Koruması (SEHOP) için destek içerir. Bilgisayarın güvenlik profilini iyileştirmek için bu özelliği etkinleştirmenizi öneririz. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bu özellik, Structured Exception Handler (SEH) üzerine yazma tekniğini kullanan istismarları engellemek için tasarlanmıştır. Bu koruma mekanizması çalışma zamanında sağlanır. Bu nedenle, /SAFESEH seçeneği gibi en son geliştirmelerle derlenip derlenmediklerine bakılmaksızın uygulamaların korunmasına yardımcı olur.

**Etki:**

SEHOP'u etkinleştirdikten sonra Cygwin, Skype ve Armadillo korumalı uygulamaların mevcut sürümleri düzgün çalışmayabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SessionManager\kernel:DisableExceptionChainValidation*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\MS Güvenlik Kılavuzu\Yapılandırılmış İstisna İşleme Üzerine Yazma Korumasını Etkinleştir (SEHOP)*

**Not:** Bu Grup İlkesi yolu mevcut değil varsayılan olarak. Ek bir Grup İlkesi şablonu (SecGuide.admx/adml) gereklidir - Microsoft'tan [bu bağlantı](https://techcommunity.microsoft.com/t5/Microsoft-Security-Baselines/Security-baseline-FINAL-for-Windows-10-v1903-and-Windows-Server/ba-p/701084)dan edinilebilir. Daha fazla bilgi MSKB 956607'de bulunabilir: [Windows işletim sistemlerinde Yapılandırılmış İstisna İşleme Üzerine Yazma Koruması (SEHOP) nasıl etkinleştirilir](https://support.microsoft.com/en-us/help/956607/how-to-enable-structured-exception-handling-overwrite-protection-sehop)

**18.3.5 (L1) 'Yazıcı sürücüsü yüklemesini Yöneticilerle sınırlar' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Yönetici olmayan kullanıcıların sisteme yazdırma sürücülerini yükleyip yükleyemeyeceğini denetler. Bu ayar için önerilen durum: Etkin.

**Not:** 10 Ağustos 2021'de Microsoft, varsayılan İşaretle ve Yazdır sürücü yüklemesini ve güncelleme davranışını Yönetici ayrıcalıkları gerektirecek şekilde değiştiren bir İşaretle ve Yazdır Varsayılan Davranış Değişikliği duyurdu. Bu, KB5005652—Yeni İşaretle ve Yazdır varsayılan sürücü yükleme davranışını yönet (CVE-2021-34481) belgesinde belgelenmiştir.

**Gerekçe:**

Yazdırma sürücülerinin yüklenmesinin Yöneticilerle sınırlandırılması, PrintNightmare güvenlik açığının (CVE-2021-34527) ve diğer Yazdırma Biriktiricisi saldırılarının azaltılmasına yardımcı olabilir. Etki: Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsNT\Printers\PointAndPrint:RestrictDriverInstallationToAdministrators*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın.

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\MS Güvenlik Kılavuzu\Yazdırma sürücüsü yüklemesini Yöneticilerle sınırlar*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Ek bir Grup İlkesi şablonu SecGuide.admx/adml gereklidir - Microsoft'tan [bu bağlantı](https://www.microsoft.com/en-us/download/details.aspx?id=55319)dan edinilebilir.

**18.3.6 (L1) 'NetBT NodeType yapılandırması' seçeneği 'Etkin: P-düğümü (önerilen)' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, adları kaydetmek ve çözmek için TCP/IP üzerinden NetBIOS'un (NetBT) hangi yöntemi kullanacağını belirler. Kullanılabilir yöntemler şunlardır:

* B düğümü (yayın) yöntemi yalnızca yayınları kullanır.
* P-node (noktadan noktaya) yöntemi yalnızca bir ad sunucusuna (WINS) yönelik ad sorgularını kullanır.
* M-düğüm (karma) yöntemi önce yayın yapar, ardından yayın başarısız olursa bir ad sunucusunu (WINS) sorgular.
* H düğümü (karma) yöntemi önce bir ad sunucusunu (WINS) sorgular, ardından sorgu başarısız olursa yayın yapar.

Bu ayar için önerilen durum: Etkin: P-node (önerilen) (noktadan noktaya).

**Not:** LMHOSTS veya DNS aracılığıyla çözümleme bu yöntemleri izler. NodeType kayıt defteri değeri varsa, herhangi bir DhcpNodeType kayıt defteri değerini geçersiz kılar. NodeType veya DhcpNodeType yoksa, ağ için yapılandırılmış WINS sunucusu yoksa bilgisayar B düğümünü (yayın) veya yapılandırılmış en az bir WINS sunucusu varsa H düğümünü (karma) kullanır.

**Gerekçe:**

NetBIOS Ad Hizmeti (NBT-NS) zehirlenmesi saldırıları riskini azaltmaya yardımcı olmak için, düğüm türünü P-node (noktadan noktaya) olarak ayarlamak sistemin NetBIOS yayınları göndermesini engeller. Etki: NetBIOS ad çözümleme sorguları, harici NetBIOS ad çözümlemesi için tanımlı ve kullanılabilir bir WINS sunucusu gerektirecektir. Bir WINS sunucusu tanımlanmadıysa veya erişilemiyorsa ve istenen ana bilgisayar adı yerel önbellekte, yerel LMHOSTS veya HOSTS dosyalarında tanımlanmadıysa, NetBIOS ad çözümlemesi başarısız olur.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters:NodeType*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın: P-node (önerilir) :

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\MS Güvenlik Kılavuzu\NetBT NodeType yapılandırması*

**Not:** Bu değişiklik bilgisayar yeniden başlatılıncaya kadar geçerli olmaz.

**Not #2:** Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Ek bir Grup İlkesi şablonu (SecGuide.admx/adml) gereklidir - Microsoft'tan [bu bağlantı](https://techcommunity.microsoft.com/t5/Microsoft-Security-Baselines/Security-baseline-FINAL-for-Windows-10-v1903-and-Windows-Server/ba-p/701084)dan edinilebilir. Lütfen bu ayarın yalnızca SecGuide.admx/adml'nin Windows 10 v1903 ve Windows Server v1903 (veya daha yeni) sürümü için Güvenlik temel çizgisinde (FINAL) mevcut olduğunu unutmayın; bu nedenle, bu şablonu daha önce indirdiyseniz, güncellemeniz gerekebilir. bu yeni NetBT NodeType yapılandırma ayarını elde etmek için daha yeni bir Microsoft temeli.

**18.3.7 (L1) 'WDigest Kimlik Doğrulaması' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

WDigest kimlik doğrulaması etkinleştirildiğinde, Lsass.exe, kullanıcının düz metin parolasının bir kopyasını hırsızlık riski altında olabileceği bellekte tutar. Bu ayar yapılandırılmazsa, Windows 8.1 ve Windows Server 2012 R2'de WDigest kimlik doğrulaması devre dışı bırakılır; Windows ve Windows Server'ın önceki sürümlerinde varsayılan olarak etkindir. Yerel hesaplar ve kimlik bilgisi hırsızlığı hakkında daha fazla bilgi için, "[Karma Geçiş (PtH) Saldırılarını ve Diğer Kimlik Bilgisi Hırsızlığı Tekniklerini Azaltma](http://www.microsoft.com/en-us/download/details.aspx?id=3603)" belgelerini inceleyin. UseLogonCredential hakkında daha fazla bilgi için, bkz. Microsoft Bilgi Bankası makalesi 2871997: [Kimlik bilgilerinin korunmasını ve yönetimini iyileştirmek için Microsoft Güvenlik Danışma Güncelleştirmesi 13 Mayıs 2014.](https://support.microsoft.com/en-us/kb/2871997) Bu ayar için önerilen durum: Devre dışı.

**Gerekçe:**

Kimlik bilgilerinin bellekte düz metin olarak saklanmasını önlemek, kimlik bilgisi hırsızlığı olasılığını azaltabilir.

**Etki:**

Yok - bu aynı zamanda Windows 8.1 ve daha yeni sürümler için varsayılan yapılandırmadır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\SecurityProviders\WDigest :UseLogonCredential*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\MS Güvenlik Kılavuzu\WDigest Kimlik Doğrulaması (devre dışı bırakmak KB2871997)*

**Not:** Bu Grup İlkesi yolu, varsayılan. Ek bir Grup İlkesi şablonu (SecGuide.admx/adml) gereklidir - Microsoft'tan [bu bağlantı](https://blogs.technet.microsoft.com/secguide/2018/11/20/security-baseline-final-for-windows-10-v1809-and-windows-server-2019/)dan edinilebilir

**18.4 MSS (Eski)**

**18.4.1 (L1) 'MSS: Otomatik Oturum Açmayı Etkinleştir (önerilmez)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, Windows XP ve Windows Vista'daki Karşılama ekranı özelliğinden ayrıdır; bu özellik devre dışı bırakılırsa, bu ayar devre dışı bırakılmaz. Bir bilgisayarı otomatik oturum açma için yapılandırırsanız, bilgisayara fiziksel olarak erişebilen herkes, bilgisayarın bağlı olduğu herhangi bir ağ veya ağlar da dahil olmak üzere bilgisayardaki her şeye erişim sağlayabilir. Ayrıca, otomatik oturum açmayı etkinleştirirseniz parola, kayıt defterinde düz metin olarak saklanır ve bu değeri depolayan belirli kayıt defteri anahtarı, Authenticated Users grubu tarafından uzaktan okunabilir. Ek bilgi için, 324737 numaralı Microsoft Bilgi Bankası makalesine bakın: [Windows'ta otomatik oturum açma nasıl açılır.](https://support.microsoft.com/en-us/kb/324737)

Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bir bilgisayarı otomatik oturum açma için yapılandırırsanız, bilgisayara fiziksel olarak erişebilen herkes, bilgisayarın bağlı olduğu ağ veya ağlar da dahil olmak üzere bilgisayardaki her şeye erişim sağlayabilir. Ayrıca, otomatik oturum açmayı etkinleştirirseniz, parola kayıt defterinde düz metin olarak saklanır. Bu ayarı depolayan belirli kayıt defteri anahtarı, Authenticated Users grubu tarafından uzaktan okunabilir. Sonuç olarak, bu girdi yalnızca bilgisayar fiziksel olarak güvenliyse ve güvenilmeyen kullanıcıların kayıt defterini uzaktan görememesini sağlarsanız uygundur.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon:AutoAdminLogon*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki kullanıcı arabirimi yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\MSS (Eski)\MSS: (AutoAdminLogon) Otomatik Oturum Açmayı Etkinleştir (önerilmez)*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Ek bir Grup İlkesi şablonu (MSS-legacy.admx/adml) gereklidir - bu TechNet blog gönderisinden edinilebilir: [MSS ayarları – Microsoft Güvenlik Kılavuzu blogu](https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/)

**18.4.2 (L1) 'MSS: IP kaynak yönlendirme koruma düzeyi (paket sahteciliğine karşı korur)' seçeneği 'Etkin: En yüksek koruma, kaynak yönlendirme tamamen devre dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

IP kaynak yönlendirmesi, göndericinin bir datagramın ağ üzerinden izlemesi gereken IP yolunu belirlemesine izin veren bir mekanizmadır. Bu ayar için önerilen durum: Etkin: En yüksek koruma, kaynak yönlendirme tamamen devre dışı.

**Gerekçe:**

Bir saldırgan, kimliklerini ve konumlarını gizlemek için kaynak yönlendirilmiş paketleri kullanabilir. Kaynak yönlendirme, paket gönderen bir bilgisayarın, paketin izlediği yolu belirlemesine olanak tanır.

**Etki:**

Gelen tüm kaynak yönlendirilmiş paketler bırakılacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip6\Parameters:Disable eIPSourceRouting*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın: En yüksek koruma, kaynak yönlendirme tamamen devre dışı:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\MSS (Eski)\MSS: (DisableIPSourceRouting IPv6) IP kaynağı yönlendirme koruma düzeyi (paket sahtekarlığına karşı korur)*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Ek bir Grup İlkesi şablonu (MSS-legacy.admx/adml) gereklidir - bu TechNet blog gönderisinden edinilebilir: MSS ayarları – Microsoft Güvenlik Kılavuzu blogu

**18.4.3 (L1) 'MSS: IP kaynak yönlendirme koruma düzeyi (paket sahteciliğine karşı korur)' seçeneği 'Etkin: En yüksek koruma, kaynak yönlendirme tamamen devre dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

IP kaynak yönlendirmesi, göndericinin bir datagramın ağ üzerinden izlemesi gereken IP yolunu belirlemesine izin veren bir mekanizmadır. Kaynak yönlendirmeyi tamamen devre dışı bırakmak için bu ayarın kurumsal ortamlar için Tanımlanmadı ve yüksek güvenlikli ortamlar için En Yüksek Koruma olarak yapılandırılması önerilir. Bu ayar için önerilen durum: Etkin: En yüksek koruma, kaynak yönlendirme tamamen d

evre dışı.

**Gerekçe:**

Bir saldırgan, kimliklerini ve konumlarını gizlemek için kaynak yönlendirilmiş paketleri kullanabilir. Kaynak yönlendirme, paket gönderen bir bilgisayarın, paketin izlediği yolu belirlemesine olanak tanır.

**Etki:**

Gelen tüm kaynak yönlendirilmiş paketler bırakılacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:Disable IPSourceRouting*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın: En yüksek koruma, kaynak yönlendirme tamamen devre dışı:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\MSS (Eski)\MSS: (DisableIPSourceRouting) IP kaynak yönlendirmesi koruma düzeyi (paket sahtekarlığına karşı koruma sağlar)*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Ek bir Grup İlkesi şablonu (MSS-legacy.admx/adml) gereklidir - bu TechNet blog gönderisinden edinilebilir: [MSS ayarları – Microsoft Güvenlik Kılavuzu blogu](https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/)

**18.4.4 (L2) 'MSS: Çevirmeli ağ şifresinin kaydedilmesini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Çevirmeli Ağda bir telefon defteri veya VPN girişi çevirdiğinizde, Çevirmeli Ağ parolanızın önbelleğe alınması ve art arda yapılan arama denemelerinde parolayı girmeniz gerekmemesi için "Parolayı Kaydet" seçeneğini kullanabilirsiniz. Güvenlik için yöneticiler, kullanıcıların parolaları önbelleğe almasını engellemek isteyebilir. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bir mobil kullanıcının bilgisayarını çalan bir saldırgan, kuruluşunuzun ağına bağlanmak için kullanılan çevirmeli bağlantı veya VPN ağ girişi için Bu Parolayı Kaydet onay kutusu seçilirse, kuruluşun ağına otomatik olarak bağlanabilir.

**Etki:**

Kullanıcılar, çevirmeli ağ ve VPN bağlantıları için oturum açma kimlik bilgilerini otomatik olarak depolayamaz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\RasMan\Parameters:Disable eSavePassword*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\MSS (Eski)\MSS:(DisableSavePassword) Çevirmeli ağ parolasının kaydedilmesini engelle*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değil. Ek bir Grup İlkesi şablonu (MSS-legacy.admx/adml) gereklidir - bu TechNet blog gönderisinden edinilebilir: [MSS ayarları – Microsoft Güvenlik Kılavuzu blogu](https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/)

**18.4.5 (L1) 'MSS: ICMP yönlendirmelerinin OSPF tarafından oluşturulan yolları geçersiz kılmasına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

İnternet Denetim İletisi Protokolü (ICMP) yeniden yönlendirmeleri, IPv4 yığınının ana bilgisayar yollarını belirlemesine neden olur. Bu yollar, Önce En Kısa Yolu Aç (OSPF) tarafından oluşturulan yolları geçersiz kılar. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bu davranış bekleniyor. Sorun şu ki, ICMP yeniden yönlendirme tesisatlı rotalar için 10 dakikalık zaman aşımı süresi, geçici olarak, trafiğin etkilenen ana bilgisayar için artık doğru şekilde yönlendirilmeyeceği bir ağ durumu yaratır. Bu tür ICMP yönlendirmelerini yok saymak, sistemin ağa katılma yeteneğini etkileyecek saldırılara maruz kalmasını sınırlayacaktır.

**Etki:**

Yönlendirme ve Uzaktan Erişim Hizmeti (RRAS), bağımsız bir sistem sınır yönlendiricisi (ASBR) olarak yapılandırıldığında, bağlı arabirim alt ağ yollarını doğru şekilde içe aktarmaz. Bunun yerine, bu yönlendirici ana bilgisayar yollarını OSPF yollarına enjekte eder. Ancak, OSPF yönlendiricisi bir ASBR yönlendiricisi olarak kullanılamaz ve bağlı arabirim alt ağ yolları OSPF'ye aktarıldığında, sonuç, yönlendirme tablolarını garip yönlendirme yollarıyla karıştırır.

**Denetim:**

Düzeltme bölümünde belirtilen Kullanıcı Arayüzü Yoluna gidin ve kuruluşunuz için öngörülen şekilde ayarlandığını onaylayın. Bu grup ilkesi nesnesi aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:EnableI CMPRedirect*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\MSS (Eski)\MSS: (EnableICMPRedirect) ICMP yönlendirmelerinin OSPF tarafından oluşturulan yolları geçersiz kılmasına izin verin*

**Not:** Bu Grup İlke yolu varsayılan olarak mevcut değil. Ek bir Grup İlkesi şablonu (MSS-legacy.admx/adml) gereklidir - bu TechNet blog gönderisinden edinilebilir: [MSS ayarları – Microsoft Güvenlik Kılavuzu blogu](https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/)

**18.4.6 (L2) 'MSS: Canlı tutma paketlerinin milisaniye cinsinden ne sıklıkta gönderildiği' seçeneği 'Etkin: 300.000 veya 5 dakika (önerilen)' olarak ayarlanmalıdır. (Otomatik)**

**Açıklama:**

Bu değer, TCP'nin bir canlı tutma paketi göndererek boş bir bağlantının hala bozulmamış olduğunu doğrulamaya ne sıklıkta çalışacağını kontrol eder. Uzak bilgisayar hala erişilebilir durumdaysa, canlı tutma paketini kabul eder. Bu ayar için önerilen durum: Etkin: 300.000 veya 5 dakika (önerilir).

**Gerekçe:**

Ağ uygulamalarına bağlanabilen bir saldırgan, bir DoS durumuna neden olmak için çok sayıda bağlantı kurabilir.

**Etki:**

Canlı tutma paketleri varsayılan olarak Windows tarafından gönderilmez. Ancak bazı uygulamalar, canlı tutma paketleri isteyen TCP yığın bayrağını yapılandırabilir. Bu tür yapılandırmalarda, etkin olmayan oturumların bağlantısını daha hızlı bir şekilde kesmek için bu değeri varsayılan ayar olan iki saatten beş dakikaya düşürebilirsiniz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:KeepAli veTime*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın: 300.000 veya 5 dakika (önerilen):

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\MSS (Eski)\MSS: (KeepAliveTime) canlı paketler milisaniye cinsinden gönderilir*

Not: Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Ek bir Grup İlkesi şablonu (MSS-legacy.admx/adml) gereklidir - bu TechNet blog gönderisinden edinilebilir: [MSS ayarları – Microsoft Güvenlik Kılavuzu blogu](https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/)

**18.4.7 (L1) 'MSS: Bilgisayarın WINS sunucuları dışındaki NetBIOS ad bırakma isteklerini yok saymasına izin ver' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

TCP/IP üzerinden NetBIOS, Windows tabanlı sistemlerde kayıtlı NetBIOS adlarını bu sistemlerde yapılandırılan IP adreslerine kolayca çözümlemenin bir yolunu sağlayan bir ağ protokolüdür. Bu ayar, bir ad bırakma isteği aldığında bilgisayarın NetBIOS adını yayınlayıp yayınlamayacağını belirler. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

NetBT protokolü, kimlik doğrulaması kullanmayacak şekilde tasarlanmıştır ve bu nedenle, kimlik sahtekarlığına karşı savunmasızdır. Sahtekarlık, iletimin eylemi gerçekleştiren kullanıcı dışındaki bir kullanıcıdan geldiğini gösterir. Kötü niyetli bir kullanıcı, hedef bilgisayara bir ad çakışması datagramı göndermek için protokolün kimliği doğrulanmamış yapısından yararlanabilir, bu da bilgisayarın adından vazgeçmesine ve sorgulara yanıt vermemesine neden olabilir. Saldırgan, ağ üzerinden bir istek gönderebilir ve bir bilgisayarı NetBIOS adını serbest bırakması için sorgulayabilir. Uygulamaları etkileyebilecek herhangi bir değişiklikte olduğu gibi, üretim ortamını değiştirmeden önce bu değişikliği üretim dışı bir ortamda test etmeniz önerilir. Bu tür bir saldırının sonucu, hedef bilgisayarda kesintili bağlantı sorunlarına neden olmak veya hatta Ağ Komşuları, etki alanı oturum açmaları, NET SEND komutunu veya ek NetBIOS ad çözümlemesi kullanımını engellemek olabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\NetBT\Parameters:NoNameR eleaseOnDemand*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki kullanıcı arabirimi yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\MSS (Legacy)\MSS: (NoNameReleaseOnDemand) Bilgisayarın, WINS sunucuları dışında NetBIOS ad bırakma isteklerini yok saymasına izin verin*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Ek bir Grup İlkesi şablonu (MSS-legacy.admx/adml) gereklidir - bu TechNet blog gönderisinden edinilebilir: [MSS ayarları – Microsoft Güvenlik Kılavuzu blogu](https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/)

**18.4.8 (L2) 'MSS: IRDP'nin Varsayılan Ağ Geçidi adreslerini algılamasına ve yapılandırmasına izin ver (DoS'a yol açabilir)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, sistemin varsayılan ağ geçidi adreslerini her arabirim temelinde RFC 1256'da açıklandığı gibi otomatik olarak algılamasını ve yapılandırmasını sağlayan İnternet Yönlendirici Keşif Protokolünü (IRDP) etkinleştirmek veya devre dışı bırakmak için kullanılır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Aynı ağ kesimindeki bir bilgisayarın kontrolünü ele geçiren bir saldırgan, ağdaki bir bilgisayarı bir yönlendiricinin kimliğine bürünecek şekilde yapılandırabilir. IRDP'nin etkin olduğu diğer bilgisayarlar, trafiğini zaten güvenliği ihlal edilmiş bilgisayar üzerinden yönlendirmeye çalışır.

**Etki:**

Windows, bilgisayardaki varsayılan ağ geçidi adreslerini otomatik olarak algılamaz ve yapılandırmaz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:Perform RouterDiscovery*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\MSS (Eski)\MSS: (PerformRouterDiscovery) IRDP'nin Varsayılan Ağ Geçidi adreslerini algılamasına ve yapılandırmasına izin verin (bu DoS'a)*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Ek bir Grup İlkesi şablonu (MSS-legacy.admx/adml) gereklidir - bu TechNet blog gönderisinden edinilebilir: [MSS ayarları – Microsoft Güvenlik Kılavuzu blogu](https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/)

**18.4.9 (L1) 'MSS: Güvenli DLL arama modunu etkinleştir (önerilen)' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

DLL arama sırası, işlemler çalıştırılarak istenen DLL'leri aramak için iki yoldan biriyle yapılandırılabilir:

* Önce sistem yolunda belirtilen klasörleri arayın ve ardından geçerli çalışma klasörünü arayın.
* Önce mevcut çalışma klasörünü arayın ve ardından sistem yolunda belirtilen klasörleri arayın.

Etkinleştirildiğinde, kayıt defteri değeri 1'e ayarlanır. 1 ayarıyla, sistem önce sistem yolunda belirtilen klasörleri arar ve ardından geçerli çalışma klasörünü arar. Devre dışı bırakıldığında, kayıt defteri değeri 0'a ayarlanır ve sistem önce mevcut çalışma klasörünü arar ve ardından sistem yolunda belirtilen klasörleri arar. Uygulamalar önce sistem yolunda DLL'leri aramaya zorlanacak. Uygulamada bulunan bu DLL'lerin benzersiz sürümlerini gerektiren uygulamalar için bu girdi, performans veya kararlılık sorunlarına neden olabilir. Bu ayar için önerilen durum: Etkin.

**Not:** Güvenli DLL arama modunun nasıl çalıştığı hakkında daha fazla bilgi bu bağlantıda mevcuttur: [Dinamik Bağlantı Kitaplığı Arama Sırası - Windows uygulamaları | Microsoft Belgeler](https://docs.microsoft.com/en-us/windows/win32/dlls/dynamic-link-library-search-order)

**Gerekçe:**

Bir kullanıcı, sistem DLL'lerinin değiştirilmiş sürümlerini içeren ek dosyalarla paketlenmiş düşmanca kodu bilmeden yürütürse, düşmanca kod, bu DLL'lerin kendi sürümlerini yükleyebilir ve potansiyel olarak kodun verebileceği hasarın türünü ve derecesini artırabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetimi:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Control\Session Manager:SafeDllSearchMode*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\ MSS (Eski)\MSS: (SafeDllSearchMode) Güvenli DLL arama modunu etkinleştir (önerilir)*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Ek bir Grup İlkesi şablonu (MSS-legacy.admx/adml) gereklidir - bu TechNet blog gönderisinden edinilebilir: [MSS ayarları – Microsoft Güvenlik Kılavuzu blogu](https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/)

**18.4.10 (L1) 'MSS: Ekran koruyucu yetkisiz kullanım süresinin sona ermesinden önceki saniye cinsinden süre (0 önerilir)' seçeneği 'Etkin: 5 veya daha az saniye' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Windows, ekran koruyucunun başlatıldığı zaman ile ekran koruyucu kilitleme etkinleştirildiğinde konsolun gerçekten otomatik olarak kilitlendiği zaman arasında bir yetkisiz kullanım süresi içerir. Bu ayar için önerilen durum: Etkin: 5 veya daha az saniye.

**Gerekçe:**

Ekran koruyucu kilidi devreye girmeden önce kullanıcı hareketi için izin verilen varsayılan ek süre beş saniyedir. Varsayılan yetkisiz kullanım süresi yapılandırmasını bırakırsanız, bilgisayarınız, konsola yaklaşabilecek ve kilit devreye girmeden önce bilgisayarda oturum açmaya çalışabilecek birinden gelebilecek olası bir saldırıya açık hale gelir. Ödemesiz sürenin uzunluğunu ayarlamak için kayıt defterine bir giriş yapılabilir.

**Etki:**

Kullanıcıların, ekran koruyucu etkinleştirmesinden sonra ek süre sona erer ermez konsol oturumlarına devam etmek için parolalarını girmeleri gerekecek. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\WindowsNT\CurrentVersion\Winlogon:ScreenSaverGracePeriod*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: 5 veya daha az saniye:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\MSS (Eski)\MSS: (ScreenSaverGracePeriod) Ekrandan önceki saniye cinsinden süre saver yetkisiz kullanım süresi sona eriyor (0 önerilir)*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Ek bir Grup İlkesi şablonu (MSS-legacy.admx/adml) gereklidir - bu TechNet blog gönderisinden edinilebilir: [MSS ayarları – Microsoft Güvenlik Kılavuzu blogu](https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/)

**18.4.11 (L2) 'MSS : Onaylanmamış verilerin kaç kez yeniden iletildiği' seçeneği 'Etkin: 3' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, bağlantı iptal edilmeden önce TCP'nin tek bir veri kesimini (bağlı olmayan kesim) kaç kez yeniden ileteceğini kontrol eder. Yeniden iletim zaman aşımı, bir bağlantıdaki her ardışık yeniden iletimde ikiye katlanır. Yanıtlar devam ettiğinde sıfırlanır. Temel zaman aşımı değeri, bağlantıda ölçülen gidiş-dönüş süresi tarafından dinamik olarak belirlenir. Bu ayar için önerilen durum şudur: Etkin: 3.

**Gerekçe:**

Kötü niyetli bir kullanıcı, hedef bilgisayar tarafından iletilen veriler için hiçbir bildirim mesajı göndermediyse, hedef bilgisayarın kaynaklarını tüketebilir.

**Etki:**

Her giden segment IP'ye iletildiğinde, TCP bir yeniden iletim zamanlayıcısı başlatır. Zamanlayıcı sona ermeden önce belirli bir segmentteki veriler için herhangi bir onay alınmazsa, segment üç defaya kadar yeniden iletilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters:TcpMax DataRetransmissions*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: 3:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\MSS (Eski)\MSS:(TcpMaxDataRetransmissions IPv6) Onaylanmayan veri kaç kez yeniden iletilir*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Ek bir Grup İlkesi şablonu (MSS-legacy.admx/adml) gereklidir - bu TechNet blog gönderisinden edinilebilir: [MSS ayarları – Microsoft Güvenlik Kılavuzu blogu](https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/)

**18.4.12 (L2) 'MSS: Onaylanmamış verilerin kaç kez yeniden iletildiği' seçeneği 'Etkin: 3' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, bağlantı iptal edilmeden önce TCP'nin tek bir veri kesimini (bağlı olmayan kesim) kaç kez yeniden ileteceğini kontrol eder. Yeniden iletim zaman aşımı, bir bağlantıdaki her ardışık yeniden iletimde ikiye katlanır. Yanıtlar devam ettiğinde sıfırlanır. Temel zaman aşımı değeri, bağlantıda ölçülen gidiş-dönüş süresi tarafından dinamik olarak belirlenir. Bu ayar için önerilen durum şudur: Etkin: 3.

**Gerekçe:**

Kötü niyetli bir kullanıcı, hedef bilgisayar tarafından iletilen veriler için hiçbir bildirim mesajı göndermediyse, hedef bilgisayarın kaynaklarını tüketebilir.

**Etki:**

Her giden segment IP'ye iletildiğinde, TCP bir yeniden iletim zamanlayıcısı başlatır. Zamanlayıcı sona ermeden önce belirli bir segmentteki veriler için herhangi bir onay alınmazsa, segment üç defaya kadar yeniden iletilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters:TcpMaxD ataRetransmissions*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: 3:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\MSS (Eski)\MSS:(TcpMaxDataRetransmissions) Onaylanmamış veri kaç kez yeniden iletilir*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değil. Ek bir Grup İlkesi şablonu (MSS-legacy.admx/adml) gereklidir - bu TechNet blog gönderisinden edinilebilir: [MSS ayarları – Microsoft Güvenlik Kılavuzu blogu](https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/)

**18.4.13 (L1) 'MSS: Sistemin uyarı oluşturacağı güvenlik olay günlüğü için yüzde eşiği' seçeneği 'Etkin: %90 veya daha az' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, günlük kullanıcı tanımlı bir eşiğe ulaştığında Güvenlik olay günlüğünde bir güvenlik denetimi oluşturabilir. Bu ayar için önerilen durum: Etkin: %90 veya daha az. Not: Günlük ayarları, gerektiğinde Olayların üzerine yaz veya x günden eski olayların üzerine yaz olarak yapılandırılırsa, bu olay oluşturulmaz.

**Gerekçe:**

Güvenlik günlüğü kapasitesinin yüzde 90'ına ulaşırsa ve bilgisayar gerektiği gibi olayların üzerine yazacak şekilde yapılandırılmamışsa, günlüğe daha yeni olaylar yazılmaz. Günlük kapasitesine ulaşırsa ve bilgisayar, olayları artık Güvenlik günlüğüne kaydedemediğinde kapanacak şekilde yapılandırılmışsa, bilgisayar kapanır ve artık ağ hizmetleri sağlayamaz.

**Etki:**

Günlük, gerektiğinde olayların üzerine yazmak üzere yapılandırılmadığı sürece, Güvenlik günlüğü yüzde 90 tam eşiğe ulaştığında (veya daha düşük değer ne olursa olsun) ulaştığında bir denetim olayı oluşturulur.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\Eventlog\Security:Warnin gLevel*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın: %90 veya daha az:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\MSS (Eski)\MSS: (Uyarı Düzeyi) Güvenlik olay günlüğü için yüzde eşiği sistemin bir uyarı oluşturacağı*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Ek bir Grup İlkesi şablonu (MSS-legacy.admx/adml) gereklidir - bu TechNet blog gönderisinden edinilebilir: [MSS ayarları – Microsoft Güvenlik Kılavuzu blogu](https://blogs.technet.microsoft.com/secguide/2016/10/02/the-mss-settings/)

**18.5 Ağ**

**18.5.1 Arka Plan Akıllı Aktarım Hizmeti (BITS)**

**18.5.2 BranchCache**

**18.5.3 DirectAccess İstemci Deneyimi Ayarları**

**18.5.4 DNS İstemcisi**

**18.5.4.1 (L1) 'HTTPS üzerinden DNS yapılandırma (DoH) ad çözümlemesi' seçeneği 'Etkin: DoH'ye İzin Ver' veya üstü (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, sistem tarafından HTTPS üzerinden DNS (DoH) kullanılıp kullanılmadığını belirler. HTTPS üzerinden DNS (DoH), Güvenli Köprü Metni Aktarım Protokolü (HTTPS) üzerinden uzak Etki Alanı Adı Sistemi (DNS) çözümlemesi gerçekleştirmek için bir protokoldür. HTTPS üzerinden DNS (DoH) hakkında ek bilgi için şu adresi ziyaret edin: [Windows Server 2022'de HTTPS üzerinden Güvenli DNS İstemcisi (DoH) | Microsoft Belgeleri](https://docs.microsoft.com/en-us/windows-server/networking/dns/doh-client-support).

Bu ayar için önerilen durum: Etkin: DoH'ye İzin Ver. Bu ayarın Etkin olarak yapılandırılması: DoH Gerektirmesi de kıyaslama ile uyumludur.

**Gerekçe:**

HTTPS üzerinden DNS (DoH), DNS sahtekarlığına karşı korunmaya yardımcı olur. Sahtekarlık, iletimin eylemi gerçekleştiren kullanıcı dışındaki bir kullanıcıdan geldiğini gösterir. Aradaki oturum şifreli olduğu için ortadaki adam (MitM) saldırılarını önlemeye de yardımcı olabilir.

**Etki:**

Etkin: DoH gerektir seçeneği seçilirse, trafik geçiş sırasında şifreleneceğinden bu, 3. taraf ürünlerin DNS trafiğini (aktarma sırasında) kaydetmesini sınırlayabilir. DoH Gerektir seçeneği, etki alanına katılmış sistemlerin ortam içinde düzgün çalışmamasına da yol açabilir. Etkin: DoH'a İzin Ver seçeneği, yapılandırılmış DNS sunucuları destekliyorsa DoH sorguları gerçekleştirir. Desteklemiyorlarsa klasik isim çözümlemesi kullanılacaktır. Bu en güvenli seçenektir.

**Not:** Microsoft uyarınca, Windows Server DNS Sunucusu hizmeti DoH sorgularını desteklemediğinden, Active Directory Etki Alanı Hizmetleri DNS'ye büyük ölçüde bağımlı olduğundan, etki alanına katılmış bilgisayarlar için Etkin: DoH Gerektir seçeneğini etkinleştirmeyin.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\DNSClient:DoHPolicy*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: DoH'a İzin Ver (yapılandırmayı Etkinleştir) : DoH gerektirsin ayrıca kıyaslama ile uyumludur):

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Ağ\DNS İstemcisi\HTTPS üzerinden DNS'yi Yapılandır (DoH) ad çözümlemesi*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 21H2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu DnsClient.admx/adml tarafından sağlanır.

**18.5.4.2 (L1) 'Çok noktaya yayın adı çözünürlüğünü kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

LLMNR, ikincil bir ad çözümleme protokolüdür. LLMNR ile sorgular, tek bir alt ağdaki yerel ağ bağlantısı üzerinden çok noktaya yayın kullanılarak bir istemci bilgisayardan aynı alt ağdaki aynı zamanda LLMNR'nin etkinleştirilmiş olduğu başka bir istemci bilgisayara gönderilir. LLMNR, bir DNS sunucusu veya DNS istemcisi yapılandırması gerektirmez ve geleneksel DNS ad çözümlemesinin mümkün olmadığı senaryolarda ad çözümlemesi sağlar. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bir saldırgan, bu LLMNR (UDP/5355) veya NBT-NS (UDP/137) yayınlarını bir ağda dinleyebilir ve bunlara yanıt vererek, ana bilgisayarı istenen sistemin konumunu bildiğini düşünmesi için kandırabilir.

**Not:** Yerel ad çözümlemesi zehirlenmesini tamamen azaltmak için, bu ayara ek olarak, yüklü her NIC'nin özellikleri de TCP/IP üzerinden NetBIOS'u Devre Dışı Bırak olarak ayarlanmalıdır (NIC özelliklerindeki WINS sekmesinde). Ne yazık ki, bunu başarmak için tüm NIC'ler için otomatik olarak geçerli olan global bir ayar yoktur - bu, farklı NIC donanım kurulumlarına göre değişen NIC başına bir ayardır.

**Etki:**

DNS'nin kullanılamaması durumunda, sistem aynı alt ağdaki diğer sistemlerden bunu talep edemez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsNT\DNSClient:EnableMulticast*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Ağ\DNS İstemcisi\Çok noktaya yayın ad çözümlemesini kapat*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu DnsClient.admx/adml tarafından sağlanır.

**18.5.5 Fontlar**

**18.5.5.1 (L2) 'Font Sağlayıcılarını Etkinleştir' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows'un çevrimiçi bir yazı tipi sağlayıcısından yazı tiplerini ve yazı tipi kataloğu verilerini indirmesine izin verilip verilmeyeceğini belirler. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Kurumsal olarak yönetilen bir ortamda BT departmanı, tüm değişikliklerin test edildiğinden ve onaylandığından emin olmak için sistem yapılandırmasındaki değişiklikleri yönetmelidir.

**Etki:**

Windows çevrimiçi bir yazı tipi sağlayıcısına bağlanmayacak ve yalnızca yerel olarak yüklenen yazı tiplerini sıralayacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:EnableFontProviders*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Ağ\Fonts\Yazı Tipi Sağlayıcılarını Etkinleştir*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1607 ve Server 2016 Yönetim Şablonlarında (veya daha yenisinde) bulunan GroupPolicy.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.5.6 Hotspot Kimlik Doğrulaması**

**18.5.7 Lanman Sunucusu**

**18.5.8 Lanman İş İstasyonu**

**18.5.8.1 (L1) 'Güvenli olmayan misafir oturum açmalarını etkinleştir' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, SMB istemcisinin bir SMB sunucusunda güvenli olmayan konuk oturum açmalarına izin verip vermeyeceğini belirler. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Güvenli olmayan konuk oturum açma işlemleri, dosya sunucuları tarafından paylaşılan klasörlere kimliği doğrulanmamış erişime izin vermek için kullanılır.

**Etki:**

SMB istemcisi, güvenli olmayan konuk oturum açma işlemlerini reddedecektir. Bu, orijinal olarak Windows'un eski sürümlerinde varsayılan davranış değildi, ancak Microsoft, Windows 10 R1709'dan başlayarak varsayılan davranışı değiştirdi: SMB2'de konuk erişimi, Windows 10 ve Windows Server 2016'da varsayılan olarak devre dışı bırakıldı

**Denetim:**

Düzeltme bölümünde belirtilen UI Yoluna gidin bölümüne gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LanmanWorkstation:Allo wInsecureGuestAuth*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Ağ\Lanman İş İstasyonu\Güvenli olmayan konuk oturum açmalarını etkinleştir*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1511 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu LanmanWorkstation.admx/adml tarafından sağlanır.

**18.5.9 Bağlantı Katmanı Topolojisi Keşfi**

**18.5.9.1 (L2) 'Eşleyici G/Ç (LLTDIO) sürücüsünü aç' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Eşleştirici G/Ç ağ protokolü sürücüsünün çalışma davranışını değiştirir. LLTDIO, bir bilgisayarın bağlı olduğu bir ağın topolojisini keşfetmesini sağlar. Ayrıca bir bilgisayarın bant genişliği tahmini ve ağ sağlığı analizi gibi Hizmet Kalitesi isteklerini başlatmasına da izin verir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Potansiyel olarak yetkisiz cihazların keşfedilmesine ve bunlara bağlanmaya karşı korunmaya yardımcı olmak için, ağ topolojisi keşfi için ağ trafiğine yanıt verilmesini önlemek için bu ayar devre dışı bırakılmalıdır.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumları tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowLLTDIOOnDomain*

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowLLTDIOOnPubl\SOALNet\_ HKEY\_LOCARE LLTD:EnableLLTDIO*

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:ProhibitLLTDIOOnP rivateNet*

**Düzeltme:** GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki kullanıcı arabirimi yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Ağ\Bağlantı Katmanı \ Eşleştirici G/Ç (LLTDIO) sürücüsünü aç*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu LinkLayerTopologyDiscovery.admx/adml tarafından sağlanır.

**18.5.9.2 (L2) 'Yanıtlayıcı Aç (RSPNDR) sürücüsünü aç' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Yanıtlayıcı ağ protokolü sürücüsünün çalışma davranışını değiştirir. Yanıtlayıcı, bir bilgisayarın ağda bulunabilmesi ve bulunabilmesi için Bağlantı Katmanı Topolojisi Keşfi isteklerine katılmasına izin verir. Ayrıca, bir bilgisayarın bant genişliği tahmini ve ağ sağlığı analizi gibi Hizmet Kalitesi etkinliklerine katılmasına da izin verir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Potansiyel olarak yetkisiz cihazların keşfedilmesine ve bunlara bağlanmaya karşı korunmaya yardımcı olmak için, ağ topolojisi keşfi için ağ trafiğine yanıt verilmesini önlemek için bu ayar devre dışı bırakılmalıdır.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumları tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowRspndrOnDomain*

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:AllowRspndrOnPubl\ic\_Policies\WKEYMACHLOCALNet HKEY\_ LLTD:EnableRspndr*

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LLTD:ProhibitRspndrOnP rivateNet*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Ağ\Bağlantı Katmanı Topolojisi Keşfi\Yanıtlayıcıyı Aç (RSPNDR) sürücüsü*

**Not:** Bu Grup İlkesi yolu Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu LinkLayerTopologyDiscovery.admx/adml tarafından sağlanır.

**18.5.10 Microsoft Eşler Arası Ağ Hizmetleri**

**18.5.10.1 Eş Adı Çözümleme Protokolü**

**18.5.10.2 (L2) 'Microsoft Eşler Arası Ağ Hizmetlerini Kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Eş Adı Çözümleme Protokolü (PNRP), bir adın bir IPv6 adresine ve bağlantı noktası numarasına dağıtılmış olarak çözülmesine izin verir. Protokol, bulutlar bağlamında çalışır. Bulut, aynı IPv6 kapsamını kullanarak birbirleriyle iletişim kurabilen bir dizi eş bilgisayardır. Eşler Arası protokoller, RTC, işbirliği, içerik dağıtımı ve dağıtılmış işleme alanlarındaki uygulamalara izin verir. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bu ayar, ortamın güvenliğini artırır ve eşler arası ağ iletişimi ile ilgili genel risk maruziyetini azaltır.

**Etki:**

Microsoft Eşler Arası Ağ Hizmetleri bütünüyle kapatılır ve bunlara bağlı tüm uygulamalar çalışmayı durdurur.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Peernet:Disabled*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki kullanıcı arabirimi yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Ağ \Microsoft Eşler Arası Ağ Hizmetleri\Microsoft Eşler Arası Ağ Hizmetlerini Kapat*

**Not**: Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonları'nın tüm sürümlerinde bulunan Grup İlkesi şablonu P2P pnrp.admx/adml tarafından sağlanır.

**18.5.11 Ağ Bağlantıları**

**18.5.11.1 Windows Defender Güvenlik Duvarı (eski adıyla Windows Güvenlik Duvarı)**

**18.5.11.2 (L1) 'DNS etki alanı ağınızda Ağ Köprüsü'nün yüklenmesini ve yapılandırılmasını yasakla' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bir kullanıcının bir Ağ Köprüsü kurma ve yapılandırma yeteneğini kontrol etmek için bu prosedürü kullanabilirsiniz. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Ağ Köprüsü ayarı, etkinleştirilirse, kullanıcıların bir Katman 2 Medya Erişim Kontrolü (MAC) köprüsü oluşturmasına ve iki veya daha fazla fiziksel ağ kesimini birbirine bağlamasına olanak tanır. Böylece bir Ağ Köprüsü, iki farklı ağa bağlantısı olan bir bilgisayarın bu ağlar arasında veri paylaşmasına izin verir. Yalnızca yetkili yollara giden ağ trafiğini kontrol etme ihtiyacının olduğu kurumsal olarak yönetilen bir ortamda, kullanıcıların bir Ağ Köprüsü oluşturmasına izin vermek, köprülü ağdan riski ve saldırı yüzeyini artırır.

**Etki:**

Kullanıcılar bir Ağ Köprüsü oluşturamaz veya yapılandıramaz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Network Connections:NC\_AllowNetBridge\_NLA*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Ağ\Ağ Bağlantıları\DNS etki alanı ağınızda Ağ Köprüsü kurulumunu ve yapılandırmasını yasaklayın*

**Not:** Bu Grup İlkesi yol, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu NetworkConnections.admx/adml tarafından sağlanır.

**18.5.11.3 (L1) 'DNS alan adı ağınızda İnternet Bağlantısı Paylaşımının kullanımını yasakla' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu "eski" ayar geleneksel olarak Windows 2000, Windows XP ve Server 2003'te İnternet Bağlantı Paylaşımı (ICS) kullanımına uygulanmış olsa da, bu ayar şimdi Windows 10 ve Server 2016'daki Mobile Hotspot özelliği için yeni geçerlidir. Önerilen durum bu ayar için: Etkin.

**Gerekçe:**

Yönetici olmayanlar, Mobil Erişim Noktası özelliğini açamaz ve İnternet bağlantılarını yakındaki mobil cihazlara açamaz.

**Etki:**

Mobil Erişim Noktası, Yöneticiler ve Yönetici olmayanlar tarafından etkinleştirilemez veya yapılandırılamaz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Network Connections:NC\_ShowSharedAccessUI*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonlar\Ağ\Ağ Bağlantıları\DNS etki alanı ağınızda İnternet Bağlantısı Paylaşımı kullanımını yasaklayın*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu NetworkConnections.admx/adml tarafından sağlanır.

**18.5.11.4 (L1) 'Bir ağın konumunu ayarlarken alan adı kullanıcılarının yükselmesini iste' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir ağın konumunu ayarlarken etki alanı kullanıcılarının yükseltme yapmasının gerekip gerekmediğini belirler. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Normal kullanıcıların bir ağ konumu belirlemesine izin vermek, riski ve saldırı yüzeyini artırır.

**Etki:**

Etki alanı kullanıcıları, bir ağın konumunu ayarlarken yükseltmelidir. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Network Connections:NC\_StdDomainUserSetLocation*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\Network\Network Connections\Bir ağın konumunu ayarlarken etki alanı kullanıcılarının yükseltmesini gerektir*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu NetworkConnections.admx/adml tarafından sağlanır.

**18.5.12 Ağ Bağlantısı Durum Göstergesi**

**18.5.13 Ağ** **İzolasyonu**

**18.5.14 Ağ Sağlayıcı**

**18.5.14.1 (L1) Tüm NETLOGON ve SYSVOL paylaşımları için 'Sağlamlaştırılmış UNC Yolları' seçeneği 'Etkin, 'Karşılıklı Kimlik Doğrulaması İste' ve 'Bütünlük İste' olarak ayarlanmalıdır. (Otomatik)**

**Açıklama:**

Bu ilke ayarı, UNC yollarına güvenli erişimi yapılandırır. Bu ayar için önerilen durum: Etkin, tüm NETLOGON ve SYSVOL paylaşımları için "Karşılıklı Kimlik Doğrulama İste" ve "Bütünlük İste" ayarlanmış olarak. Not: Ortam yalnızca Windows 8.0 / Server 2012 (R2 olmayan) veya daha yeni sistemler içeriyorsa, "Gizlilik" ayarı da (isteğe bağlı olarak) SMB şifrelemesini etkinleştirecek şekilde ayarlanabilir. Ancak, SMB şifrelemesinin kullanılması, hedeflenen paylaşım yollarının eski işletim sistemleri tarafından tamamen erişilemez hale gelmesine neden olacaktır, bu nedenle bu ek seçeneği yalnızca dikkatli ve kapsamlı testlerle kullanın.

**Gerekçe:**

Şubat 2015'te Microsoft, [MS15-011](https://technet.microsoft.com/library/security/MS15-011) / [MSKB 3000483](https://support.microsoft.com/en-us/kb/3000483) güvenlik güncelleştirmesinin bir parçası olarak Grup İlkesi'ndeki bir güvenlik riskini azaltmak için yeni bir denetim mekanizması yayımladı. Bu mekanizma, hem yeni güvenlik güncelleştirmesinin yüklenmesini hem de Windows Vista / Server 2008 (R2 olmayan) veya daha yeni sürümlerden etki alanındaki tüm bilgisayarlara belirli grup ilkesi ayarlarının dağıtılmasını gerektirir (bu özelliği etkinleştirmek için ilişkili güvenlik yaması Sunucu 2003 için yayınlandı). Güvenlik güncellemesiyle birlikte yeni bir grup ilkesi şablonu da (NetworkProvider.admx/adml) sağlandı. Yeni GPO şablonu yerleştirildikten sonra, Grup İlkesi güvenlik riskini düzeltmek için minimum gereksinimler şunlardır:

*\\\*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1*

*\\\*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1*

**Not:** Yukarıdaki yollara erişmek için ayar bir istemci makineye uygulandıktan sonra yeniden başlatma gerekebilir. Bu güvenlik ayarının dağıtımına ilişkin ek kılavuz, Microsoft Premier Saha Mühendisliği (PFE) Platformları TechNet Blog'unda şu adresten edinilebilir: [MS15-011 ve MS15-014 Dağıtımına İlişkin Kılavuz.](http://blogs.technet.com/b/askpfeplat/archive/2015/02/23/guidance-on-deployment-of-ms15-011-and-ms15-014.aspx)

Etki: Windows, yalnızca ek güvenlik gereksinimleri karşılandıktan sonra belirtilen UNC yollarına erişime izin verir. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumları tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\Harden edPaths:\\\*\NETLOGON*

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\NetworkProvider\Harden\ed \SYSVOL*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki yollar yapılandırılarak en az olarak aşağıdaki UI yolunu Etkin olarak ayarlayın:

*\\\*\NETLOGON RequireMutualAuthentication=1, RequireIntegrity=1*

*\\\*\SYSVOL RequireMutualAuthentication=1, RequireIntegrity=1*

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Ağ\Ağ Sağlayıcı\Sertleştirilmiş UNC Yolları*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Ek bir Grup İlkesi şablonu (NetworkProvider.admx/adml) gereklidir - MS15-011 / MSKB 3000483 güvenlik güncelleştirmesine veya Microsoft Windows 10 RTM (Sürüm 1507) Yönetim Şablonlarına (veya daha yenisine) dahildir.

**18.5.15 Çevrimdışı Dosyalar**

**18.5.16 QoS Paket Zamanlayıcı**

**18.5.17 SNMP**

**18.5.18 SSL Yapılandırma Ayarları**

**18.5.19 TCPIP Ayarları**

**18.5.19.1 IPv6 Geçiş Teknolojileri**

**18.5.19.2 Parametreler**

**18.5.19.2.1 (L2) IPv6'yı devre dışı bırak (TCPIP6 Parametresi 'Disabled Components') seçeneği '0xff (255)' olarak ayarlanmalıdır. (Otomatik)**

**Açıklama:**

İnternet Protokolü sürüm 6 (IPv6), bilgisayarların İnternet üzerinden ve ev ve iş ağları üzerinden bilgi alışverişi yapmak için kullandığı bir dizi protokoldür. IPv6, IPv4'ten çok daha fazla IP adresinin atanmasına izin verir. Daha eski ağ iletişimi, ana bilgisayarlar ve işletim sistemleri yerel olarak IPv6'yı desteklemeyebilir. Bu ayar için önerilen durum şudur: DisabledComponents - 0xff (255)

**Gerekçe:**

Özel kurumsal yönetilen ağların büyük çoğunluğunun IPv6'yı kullanması gerekmediğinden (çünkü özel IPv4 adreslemeye erişimleri vardır), IPv6 bileşenlerinin devre dışı bırakılması olası bir saldırı yüzeyini ortadan kaldırır. bu da trafiği izlemek daha zordur. Sonuç olarak, gerekli olmadığında IPv6'yı Devre Dışı durumuna yapılandırmanızı öneririz.

**Etki:**

IPv6 kullanan diğer sistemlerle bağlantı artık çalışmayacak ve IPv6'ya bağlı yazılımlar çalışmayı durduracak. IPv6 kullanabilen Microsoft uygulamalarına örnekler: Uzaktan Yardım, HomeGroup, DirectAccess, Windows Mail. Bu kayıt defteri değişikliği, Microsoft Bilgi Bankası makalesi 929852'de belgelenmiştir: [Windows'ta IPv6 veya bileşenleri nasıl devre dışı bırakılır.](https://support.microsoft.com/en-us/kb/929852)

**Not:** Bu kayıt defteri değişikliği, bir sonraki yeniden başlatmaya kadar etkili olmaz.

**Denetim:**

Düzeltme bölümünde belirtilen Kayıt yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın.

**Düzeltme:**

Önerilen yapılandırmayı oluşturmak için aşağıdaki Kayıt Defteri değerini 0xff (255) (DWORD) olarak ayarlayın:

*HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Services\TCPIP6\Parameters:Disable edComponents*

**Not:** Bu değişiklik, bilgisayar yeniden başlatılıncaya kadar geçerli olmaz .

**Not #2:** Microsoft, bu kayıt defteri değerini yapılandırmak için bir ADMX şablonu sağlamasa da, yapılandırmasını kolaylaştırmak için CIS Benchmark Remediation Kit'te özel bir .ADM şablonu (Disable-IPv6-Components-KB929852.adm) sağlanmıştır. .ADM şablonundaki grup ilkesi ayarını kapatmanın, uygulandıktan sonra değişikliği "geri almayacağını" unutmayın. Bunun yerine, kayıt defteri değerini ters duruma değiştirmek için karşıt ayar uygulanmalıdır.

**18.5.20 Windows Şimdi Bağlan**

**18.5.20.1 (L2) 'Windows Şimdi Bağlan kullanarak kablosuz ayarların yapılandırılması' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows Connect Now (WCN) kullanılarak kablosuz ayarların yapılandırılmasına izin verir. WCN Registrar, Windows Portable Device API (WPD) ve USB Flash sürücüler aracılığıyla bant içi 802.11 Wi-Fi üzerinden Ethernet (UPnP) üzerinden aygıtların bulunmasını ve yapılandırılmasını sağlar. Belirli bir ortam üzerinden keşif ve yapılandırmaya izin vermek için ek seçenekler mevcuttur. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bu ayar, ortamın güvenliğini artırır ve kablosuz ayarların kullanıcı yapılandırmasıyla ilgili genel risk maruziyetini azaltır.

**Etki:**

WCN işlemleri tüm ortamlarda devre dışı bırakıldı.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumları tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars:EnableR egistrars HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars:Disable UPnPRegistrar HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars:Disable InBand802DOT11Registrar HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars:Disable FlashConfigRegistrar HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\Registrars:Disable WPDRegistrar*

**Düzeltme:**

Önerilen yapılandırmayı devre dışı bırakın: GP, aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Ağ\Windows Şimdi Bağlan\Windows Şimdi Bağlan kullanılarak kablosuz ayarların yapılandırılması*

**Not:** Bu Grup İlkesi yolu, Grup İlkesi şablonu WindowsConnectNow.admx/adml tarafından sağlanır Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunur.

**18.5.20.2 (L2) 'Windows Şimdi Bağlan sihirbazlarının erişimini yasakla' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows Şimdi Bağlan (WCN) sihirbazlarına erişimi yasaklar. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Standart kullanıcıların Windows Connect Now sihirbazına erişmesine izin vermek, riski ve saldırı yüzeyini artırır.

**Etki:**

WCN sihirbazları kapatılır ve kullanıcıların hiçbir sihirbaz görevine erişimi yoktur. "Kablosuz yönlendirici veya erişim noktası kur" ve "Kablosuz cihaz ekle" dahil olmak üzere yapılandırmayla ilgili tüm görevler devre dışı bırakılır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WCN\UI:DisableWcnUi*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\ Yönetim Şablonları\Ağ\Windows Şimdi Bağlan\Windows Şimdi Bağlan sihirbazlarının erişimini yasakla*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu WindowsConnectNow.admx/adml tarafından sağlanır.

**18.5.21 Windows Bağlantı Yöneticisi**

**18.5.21.1 (L1) 'İnternete veya Windows Etki Alanı'na eşzamanlı bağlantı sayısını en aza indir' seçeneği 'Etkin: 3 = Ethernet üzerindeyken Wi-Fi engelle' olarak ayarlanmalıdır. (Otomatik)**

**Açıklama:**

Bu ilke ayarı, bilgisayarların İnternet'e veya bir Windows etki alanına aynı anda birden çok bağlantı kurmasını engeller. Bu ayar için önerilen durum: Etkin: 3 = Ethernet üzerindeyken Wi-Fi'yi engelle.

**Gerekçe:**

Köprülü ağ bağlantılarının önlenmesi, bir kullanıcının farkında olmadan trafiğin dahili ve harici ağlar arasında yönlendirilmesine izin vererek hassas dahili verilere maruz kalma riskini ortadan kaldırmaya yardımcı olabilir.

**Etki:**

Bir Ethernet bağlantısına bağlıyken, Windows, Ethernet bağlantısı kesilene kadar WLAN kullanımına (otomatik veya manuel olarak) izin vermez. Bununla birlikte, bir hücresel veri bağlantısı mevcutsa, bunu gerektiren hizmetler için her zaman bağlı kalacaktır, ancak bir Ethernet veya WLAN bağlantısı mevcutsa hiçbir İnternet trafiği hücresel ağ üzerinden yönlendirilmeyecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WcmSvc\GroupPolicy:fMi nimizeConnections*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın: 3 = Wi'yi Engelle -Fi Ethernet üzerindeyken:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Ağ\Windows Bağlantı Yöneticisi\İnternet'e veya Windows Etki Alanına eşzamanlı bağlantı sayısını en aza indirin*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonlarında bulunan Grup İlkesi şablonu WCM.admx/adml tarafından sağlanır. Windows 10 Sürüm 1903 Yönetim Şablonlarından başlayarak yeni bir İlke Seçeneklerini Küçült alt ayarıyla güncellendi.

**18.5.21.2 (L1) 'Alan kimliği doğrulanmış ağa bağlanıldığında alan adı olmayan ağlara bağlantıyı yasakla' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bilgisayarların aynı anda hem etki alanı tabanlı bir ağa hem de etki alanı tabanlı olmayan bir ağa bağlanmasını engeller. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Olası endişe, bir kullanıcının bilmeden ağ trafiğinin güvenli olmayan genel ağ ile kurumsal yönetilen ağ arasında akmasına izin vermesidir.

**Etki:**

Bilgisayar, otomatik ve manuel ağ bağlantısı girişimlerine aşağıdaki koşullara göre yanıt verir: Otomatik bağlantı girişimleri - Bilgisayar zaten etki alanı tabanlı bir ağa bağlı olduğunda, etki alanı dışındaki ağlara yapılan tüm otomatik bağlantı girişimleri engellenir. - Bilgisayar etki alanı tabanlı olmayan bir ağa zaten bağlı olduğunda, etki alanı tabanlı ağlara otomatik bağlantı girişimleri engellenir. El ile bağlantı girişimleri - Bilgisayar Ethernet dışında bir ortam üzerinden etki alanı tabanlı olmayan bir ağa veya etki alanı tabanlı bir ağa zaten bağlıysa ve bir kullanıcı bu ilke ayarını ihlal ederek ek bir ağa manuel bağlantı oluşturmaya çalıştığında, mevcut ağ bağlantısı kesilir ve manuel bağlantıya izin verilir. - Bilgisayar zaten etki alanı tabanlı olmayan bir ağa veya Ethernet üzerinden etki alanı tabanlı bir ağa bağlıysa ve kullanıcı bu ilke ayarını ihlal ederek ek bir ağa manuel bağlantı oluşturmaya çalıştığında, mevcut Ethernet bağlantısı korunur ve manuel bağlantı girişimi engellendi.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WcmSvc\GroupPolicy:fBl ockDomain*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Ağ\Windows Bağlantı Yöneticisi\Etki alanı kimliği doğrulanmış ağa bağlanıldığında etki alanı dışındaki ağlara bağlantıyı yasakla*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu WCM.admx/adml tarafından sağlanır.

**18.5.22 Kablosuz Ekran**

**18.5.23** **WLAN Hizmeti**

**18.5.23.1 WLAN Medya Maliyeti**

**18.5.23.2 WLAN Ayarları**

**18.5.23.2.1 (L1) 'Windows'un önerilen açık etkin noktalara, kişiler tarafından paylaşılan ağlara ve ücretli hizmetler sunan etkin noktalara otomatik olarak bağlanmasına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların şu WLAN ayarlarını etkinleştirip etkinleştiremeyeceğini belirler: "Önerilen açık erişim noktalarına bağlan", "Kişilerim tarafından paylaşılan ağlara bağlan" ve "Ücretli hizmetleri etkinleştir".

* "Önerilen açık erişim noktalarına bağlan", Windows'un, Windows kullanan diğer kişilerin bağlandığı ağları kitle kaynaklı kullanarak bildiği açık erişim noktalarına kullanıcıları otomatik olarak bağlamasını sağlar.
* "Kişilerim tarafından paylaşılan ağlara bağlan", Windows'un kullanıcının kişilerinin kendileriyle paylaştığı ağlara otomatik olarak bağlanmasına ve bu cihazdaki kullanıcıların kendi kişileriyle ağları paylaşmasına olanak tanır.
* "Ücretli hizmetleri etkinleştir", Windows'un ücretli hizmetlerin mevcut olup olmadığını belirlemek için geçici olarak açık erişim noktalarına bağlanmasını sağlar.

Bu ayar için önerilen durum: Devre Dışı.

**Not:** Bu özellikler aynı zamanda "Wi-Fi Sense" adıyla da bilinir.

**Gerekçe:**

Açık bir etkin noktaya veya ağa otomatik olarak bağlanmak, sistemi kötü niyetli bir hileli ağa tanıtabilir.

**Etki:**

Önerilen açık erişim noktalarına bağlanın, Kişilerim tarafından paylaşılan ağlara bağlanın ve Ücretli hizmetleri etkinleştir seçeneklerinin her biri kapatılacak ve cihazdaki kullanıcıların bunları etkinleştirmesi engellenecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\WcmSvc\wifinetworkmanager\config:AutoCo nnectAllowedOEM*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\Network\WLAN Service\WLAN Settings\Windows'un önerilen açık erişim noktalarına, kişiler tarafından paylaşılan ağlara ve ücretli hizmetler sunan erişim noktalarına otomatik olarak bağlanmasına izin ver*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1511 Yönetim Şablonlarında (veya daha yenisinde) bulunan wlansvc.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.6 Yazıcılar**

**18.6.1 (L1) 'Yazdırma Biriktiricisinin istemci bağlantılarını kabul etmesine izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Yazdırma Biriktiricisi hizmetinin istemci bağlantılarını kabul edip etmeyeceğini denetler. Bu ayar için önerilen durum: Devre Dışı.

**Not:** Bu ilkede yapılan değişikliklerin geçerli olması için Yazdırma Biriktiricisi hizmetinin yeniden başlatılması gerekir.

**Gerekçe:**

Yazdırma Biriktiricisi hizmetinin istemci bağlantılarını kabul etme yeteneğinin devre dışı bırakılması, PrintNightmare güvenlik açığına ([CVE-2021-34527](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527)) ve diğer uzaktan Yazdırma Biriktiricisi saldırılarına yönelik uzaktan saldırıları azaltır. Ancak bu öneri, Yazdırma Biriktiricisi hizmetine yapılan yerel saldırılara karşı bir etki yaratmaz.

**Etki:**

Yazdırma Biriktiricisi hizmetinin devre dışı bırakılmaması koşuluyla, kullanıcılar iş istasyonlarından yazdırmaya devam edebilir. Ancak, iş istasyonunun Yazdırma Biriktiricisi hizmeti, istemci bağlantılarını kabul etmeyecek veya kullanıcıların yazıcıları paylaşmasına izin vermeyecektir. Halihazırda paylaşılmış olan tüm yazıcıların paylaşılmaya devam edeceğini unutmayın.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumları tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\WindowsNT\Printers:RegisterSpoolerRemoteRpcEndPoint*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonlar\Yazıcılar\Yazdırma Biriktiricisinin istemci bağlantılarını kabul etmesine izin ver*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Printing2.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.6.2 (L1) 'İşaretle ve Yazdır Kısıtlamaları: Yeni bir bağlantı için sürücü yüklerken' seçeneği 'Etkin: Uyarı ve yükseltme istemini göster' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcılar İşaretle ve Yazdır'ı kullanarak yeni bir yazıcı bağlantısı oluşturduğunda bilgisayarların bir uyarı ve güvenlik yükseltme istemi gösterip göstermeyeceğini kontrol eder. Bu ayar için önerilen durum: Etkin: Uyarı ve yükseltme istemini göster.

**Not:** 10 Ağustos 2021'de Microsoft, varsayılan İşaretle ve Yazdır sürücü yüklemesini ve güncelleme davranışını Yönetici ayrıcalıkları gerektirecek şekilde değiştiren bir İ[şaretle ve Yazdır Varsayılan Davranış Değişikliği](https://msrc-blog.microsoft.com/2021/08/10/point-and-print-default-behavior-change/) duyurdu. Bu, [KB5005652—Yeni İşaretle ve Yazdır varsayılan sürücü yükleme davranışını yönet (CVE-2021-34481)](https://support.microsoft.com/en-gb/topic/kb5005652-manage-new-point-and-print-default-driver-installation-behavior-cve-2021-34481-873642bf-2634-49c5-a23b-6d8e9a302872) belgesinde belgelenmiştir. Bu değişiklik, tüm İşaretle ve Yazdır Grup İlkesi ayarlarını geçersiz kılar ve İşaretle ve Yazdır'ı kullanarak yalnızca Yöneticilerin yazıcı sürücülerini bir yazdırma sunucusundan yükleyebilmesini sağlar.

**Gerekçe:**

Yeni yazdırma sürücülerinin yüklenmesi için Windows Kullanıcı Hesabı Denetimi'nin (UAC) etkinleştirilmesi, PrintNightmare güvenlik açığının [(CVE-2021-34527)](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527) ve diğer Yazdırma Biriktiricisi saldırılarının azaltılmasına yardımcı olabilir. İşaretle ve Yazdır varsayılan sürücü yükleme davranışı bu ayarı geçersiz kılsa da, davranışın tersine çevrilmesi durumunda bunu bir geri dönüş noktası olarak yapılandırmak önemlidir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\WindowsNT\Printers\PointAndPrint:NoWarningNoElevationOnInstall*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Uyarı ve yükseltme istemini göster:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Yazıcılar\Nokta ve Yazdırma Kısıtlamaları: Yeni bir bağlantı için sürücüleri yüklerken*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Printing.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.6.3 (L1) 'İşaretle ve Yazdır Kısıtlamaları: Mevcut bir bağlantı için sürücüleri güncellerken' seçeneği 'Etkin: Uyarı ve yükseltme istemi göster' olarak ayarlanmalıdır. (Otomatik)**

**Açıklama:**

Bu ilke ayarı, kullanıcılar İşaretle ve Yazdır'ı kullanarak mevcut bir bağlantının sürücülerini güncellerken bilgisayarların bir uyarı ve güvenlik yükseltme istemi gösterip göstermeyeceğini denetler. Bu ayar için önerilen durum: Etkin: Uyarı ve yükseltme istemini göster.

**Not:** 10 Ağustos 2021'de Microsoft, varsayılan İşaretle ve Yazdır sürücü yüklemesini ve güncelleme davranışını Yönetici ayrıcalıkları gerektirecek şekilde değiştiren bir İ[şaretle ve Yazdır Varsayılan Davranış Değişikliği](https://msrc-blog.microsoft.com/2021/08/10/point-and-print-default-behavior-change/) duyurdu. Bu, [KB5005652—Yeni İşaretle ve Yazdır varsayılan sürücü yükleme davranışını yönet (CVE-2021-34481)](https://support.microsoft.com/en-gb/topic/kb5005652-manage-new-point-and-print-default-driver-installation-behavior-cve-2021-34481-873642bf-2634-49c5-a23b-6d8e9a302872) belgesinde belgelenmiştir. Bu değişiklik, tüm İşaretle ve Yazdır Grup İlkesi ayarlarını geçersiz kılar ve İşaretle ve Yazdır'ı kullanarak yalnızca Yöneticilerin yazıcı sürücülerini bir yazdırma sunucusundan yükleyebilmesini sağlar.

**Gerekçe:**

Mevcut yazıcı sürücülerini güncellemek için Windows Kullanıcı Hesabı Denetimi'ni (UAC) etkinleştirmek, PrintNightmare güvenlik açığını [(CVE-2021-34527)](https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527) ve diğer Yazdırma Biriktiricisi saldırılarını azaltmaya yardımcı olabilir. İşaretle ve Yazdır varsayılan sürücü yükleme davranışı bu ayarı geçersiz kılsa da, davranışın tersine çevrilmesi durumunda bunu bir geri dönüş noktası olarak yapılandırmak önemlidir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\Software\Policies\Microsoft\WindowsNT\Printers\PointAndPrint:UpdatePromptSettings*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Uyarıyı ve yükseltmeyi göster komut istemi:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Yazıcılar\Nokta ve Yazdırma Kısıtlamaları: Mevcut bir bağlantı için sürücüleri güncellerken*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Printing.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.7 Başlat Menüsü ve Görev Çubuğu**

**18.7.1 Bildirimler**

**18.7.1.1 (L2) 'Ağ kullanımı bildirimlerini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, uygulamaların ağı kullanarak kutucukları, kutucuk rozetlerini, bildirimleri veya ham bildirimleri güncellemek için bildirim göndermesini engeller. Bu ilke ayarı, Windows ile Windows Anında Bildirim Hizmeti (WNS) arasındaki bağlantıyı kapatır. Bu ilke ayarı, uygulamaların kutucukları güncellemek için uygulama hizmetlerini yoklamasını da durdurur. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Windows Anında Bildirim Hizmetleri (WNS), buluttan/İnternet'ten üçüncü taraf bildirimlerini ve güncellemelerini almak için bir mekanizmadır. Yüksek güvenlikli bir ortamda, özellikle kurum dışında barındırılan harici sistemlerin güvenli iş istasyonlarını etkilemesi engellenmelidir.

**Etki:**

Uygulamalar ve sistem özellikleri, ağdan WNS'den veya bildirim yoklama API'leri aracılığıyla bildirim alamaz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\PushNot ifications:NoCloudApplicationNotification*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Başlat Menüsü ve Görev Çubuğu\Bildirimler ağ kullanımını kapat*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu WPN.admx/adml tarafından sağlanır.

**18.8 Sistem**

**18.8.1 Erişim Reddedilen Yardım**

**18.8.2 Uygulama-V**

**18.8.3 Denetim Sürecinin Oluşturulması**

**18.8.3.1 (L1) 'İşlem oluşturma olaylarına komut satırını dahil et' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, yeni bir işlem oluşturulduğunda işlem oluşturma komut satırı metninin güvenlik denetimi olaylarında günlüğe kaydedilip kaydedilmeyeceğini denetler. Bu ayar için önerilen durum: Etkin.

**Not:** Bu ayarın kontrol ettiği bu özellik, orijinal olarak Windows 8.1'den daha eski iş istasyonu işletim sistemlerinde desteklenmemektedir. Ancak, Şubat 2015'te Microsoft, bir güncelleştirme - [KB3004375](https://support.microsoft.com/en-us/help/3004375/microsoft-security-advisory-update-to-improve-windows-command-line-aud) aracılığıyla Windows 7 ve Windows 8.0'a özellik desteği ekledi. Bu nedenle, bu ayarın bu eski işletim sistemlerinde ayarlanması da önemlidir.

**Gerekçe**:

Olay günlüklerinde işlem komut satırı bilgilerinin yakalanması, saldırı olaylarının adli incelemelerini gerçekleştirirken çok değerli olabilir.

**Etki:**

İşlem komut satırı bilgileri, parolalar veya kullanıcı verileri gibi hassas veya özel bilgileri içerebilen olay günlüklerine dahil edilecektir.

**Uyarı:** Olay günlüklerine okuma erişimi olan kullanıcılara maruz kalabilecek kimlik bilgilerini ve hassas bilgileri ele geçirmenin olası riskleri vardır. Microsoft, olay günlüğü verilerini daha iyi korumak için "Korumalı Olay Günlüğü" adlı bir özellik sağlar. Olay günlüğünü korumayla ilgili yardım için şu adresi ziyaret edin: [Windows'u Günlüğe Kaydetme Hakkında - PowerShell | Microsoft Belgeleri.](https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_logging_windows?view=powershell-7.2#protected-event-logging)

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ Audit:ProcessCreationIncludeCmdLine\_Enabled*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\ İlkeler\Yönetim Şablonları\Sistem\Denetim İşlemi Oluşturma\Süreç oluşturma olaylarına komut satırını dahil et*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.1 ve Server 2012 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan AuditSettings.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.8.4 Kimlik Bilgileri Delegasyonu**

**18.8.4.1 (L1) 'Oracle Düzeltme Şifrelemesi' seçeneği 'Etkin: Güncellenen İstemcileri Zorla' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bazı uygulamalar (Uzak Masaüstü Bağlantısı gibi) tarafından kullanılan CredSSP protokolünün bazı sürümleri, istemciye yönelik bir şifreleme oracle saldırısına karşı savunmasızdır. Bu ilke, savunmasız istemciler ve sunucularla uyumluluğu kontrol eder ve şifreleme kehaneti güvenlik açığı için istenen koruma düzeyini ayarlamanıza olanak tanır. Bu ayar için önerilen durum: Etkin: Güncellenen İstemcileri Zorla.

**Gerekçe:**

Bu ayar, Microsoft tarafından 13/03/2018 tarihinde [CVE-2018-0886 | CredSSP Uzaktan Kod Yürütme Güvenlik Açığı](https://portal.msrc.microsoft.com/en-us/security-guidance/advisory/CVE-2018-0886) Windows Vista'dan sonraki tüm Windows sürümleri bu güvenlik açığından etkilenir ve en azından Mayıs 2018'e (veya daha sonra) kadar yama uygulanmış olmaları koşuluyla bu öneriyle uyumlu olacaktır.

**Etki:**

CredSSP kullanan istemci uygulamaları, güvenli olmayan sürümlere geri dönemez ve CredSSP kullanan hizmetler yama uygulanmamış istemcileri kabul etmez. Bu ayar, tüm uzak ana bilgisayarlar, en az Mayıs 2018'e kadar tüm Microsoft güvenlik güncelleştirmelerinin yüklenmesini sağlayarak elde edilen en yeni sürümü destekleyene kadar dağıtılmamalıdır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ CredSSP\Parameters:AllowEncryptionOracle*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın: Zorla Güncellenen İstemciler:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Kimlik Bilgileri Temsilcisi\Şifreleme Oracle Düzeltme*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1803 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu CredSsp.admx/adml tarafından sağlanır.

**18.8.4.2 (L1) 'Uzak ana bilgisayar, dışa aktarılamayan kimlik bilgilerinin devredilmesine izin veriyor' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Uzak ana bilgisayar, dışa aktarılamayan kimlik bilgilerinin yetkilendirilmesine izin verir. Kimlik bilgisi yetkisini kullanırken, cihazlar uzak ana bilgisayara dışa aktarılabilir bir kimlik bilgisi sürümü sağlar. Bu, kullanıcıları uzak ana bilgisayardaki saldırganlardan kimlik bilgilerinin çalınması riskine maruz bırakır. Kısıtlı Yönetici Modu ve Windows Defender Uzaktan Kimlik Bilgisi Koruması özellikleri, bu riske karşı korunmaya yardımcı olacak iki seçenektir. Bu ayar için önerilen durum: Etkin.

**Not:** Windows Defender Uzaktan Kimlik Bilgisi Koruması ve Kısıtlı Yönetici Modu ile karşılaştırması hakkında daha ayrıntılı bilgi bu bağlantıda bulunabilir: Uzak Masaüstü kimlik bilgilerini [Windows Defender Uzaktan Kimlik Bilgisi Koruması ile koruyun (Windows 10) | Microsoft Docs](https://docs.microsoft.com/en-us/windows/access-protection/remote-credential-guard)

**Gerekçe:**

Kısıtlı Yönetici Modu, yeniden kullanılabilir kimlik bilgilerinin güvenliği ihlal edilebilecek uzak cihazlarda bellekte saklanmamasını sağlayarak yönetici hesaplarının korunmasına yardımcı olmak için tasarlanmıştır. Windows Defender Remote Credential Guard, Kerberos isteklerini bağlantıyı isteyen cihaza yeniden yönlendirerek bir Uzak Masaüstü bağlantısı üzerinden kimlik bilgilerinizi korumanıza yardımcı olur. Kimlik bilgileri hırsızlığı olasılığını azalttığı için her iki özellik de etkinleştirilmeli ve desteklenmelidir.

**Etki:**

Ana bilgisayar, Kısıtlı Yönetici Modu ve Windows Defender Uzaktan Kimlik Bilgisi Koruması özelliklerini destekleyecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CredentialsDelegation: AllowProtectedCreds*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Kimlik Bilgileri Temsilciliği\Uzak ana bilgisayar, dışa aktarılamayan kimlik bilgilerinin yetkilendirilmesine izin verir*

**Not:** Bu Grup İlkesi yolu, varsayılan olarak var. Microsoft Windows 10 Sürüm 1703 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu CredSsp.admx/adml tarafından sağlanır.

**18.8.5 Cihaz Koruması**

**18.8.5.1 (NG) 'Sanallaştırma Tabanlı Güvenliği Aç' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Sanallaştırma Tabanlı Güvenliğin etkinleştirilip etkinleştirilmediğini belirtir. Sanallaştırma Tabanlı Güvenlik, güvenlik hizmetlerine destek sağlamak için Windows Hiper Yöneticiyi kullanır. Bu ayar için önerilen durum: Etkin.

**Not:** Sanallaştırma Tabanlı Güvenlik, Windows'un Güvenli Önyükleme etkinleştirilmiş 64 bit sürümünü gerektirir; bu da Windows'un Eski BIOS yapılandırmasıyla değil UEFI BIOS yapılandırmasıyla yüklenmesini gerektirir. Ayrıca, Windows bir sanal makinede çalıştırılıyorsa, donanım destekli CPU sanallaştırma özelliği (Intel VT-x veya AMD-V) ana bilgisayar tarafından konuk VM'ye gösterilmelidir. Bu özellik için sistem gereksinimleri hakkında daha fazla bilgi için: [Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs](https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-requirements)

**Not #2:** Azure IaaS VM'leri kullanılırken Credential Guard ve Device Guard şu anda desteklenmemektedir.

**Gerekçe:**

Kerberos, NTLM ve Credential manager sanallaştırma tabanlı güvenlik kullanarak gizli dizileri yalıtır. Windows'un önceki sürümleri, sırları Yerel Güvenlik Yetkilisi'nde (LSA) saklıyordu. Windows 10'dan önce, LSA, işletim sistemi tarafından kullanılan sırları işlem belleğinde depolardı. Windows Defender Kimlik Bilgisi Koruması etkinleştirildiğinde, işletim sistemindeki LSA işlemi, bu sırları saklayan ve koruyan yalıtılmış LSA işlemi adı verilen yeni bir bileşenle iletişim kurar. Yalıtılmış LSA işlemi tarafından depolanan veriler, sanallaştırma tabanlı güvenlik kullanılarak korunur ve işletim sisteminin geri kalanına erişilemez.

**Etki:**

**Uyarı:** Sistemdeki tüm sürücüler bu özellikle uyumlu olmalıdır, aksi takdirde sistem çökebilir. Bu ilke ayarının yalnızca uyumlu olduğu bilinen bilgisayarlara dağıtıldığından emin olun.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:EnableVirt ualizationBasedSecurity*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\System\Device Guard\Sanallaştırma Tabanlı Güvenliği Aç*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 RTM (Sürüm 1507) Yönetim Şablonları (veya daha yenisi) ile birlikte verilen Grup İlkesi şablonu DeviceGuard.admx/adml tarafından sağlanır.

**18.8.5.2 (NG) 'Sanallaştırma Tabanlı Güvenliği Aç: Platform Güvenlik Düzeyini Seç' seçeneği 'Güvenli Önyükleme ve DMA Koruması' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Sanallaştırma Tabanlı Güvenliğin etkinleştirilip etkinleştirilmediğini belirtir. Sanallaştırma Tabanlı Güvenlik, güvenlik hizmetlerine destek sağlamak için Windows Hiper Yöneticiyi kullanır. Bu ayar için önerilen durum: Güvenli Önyükleme ve DMA Koruması.

**Not:** Sanallaştırma Tabanlı Güvenlik, Windows'un Güvenli Önyükleme etkinleştirilmiş 64 bit sürümünü gerektirir; bu da Windows'un Eski BIOS yapılandırmasıyla değil UEFI BIOS yapılandırmasıyla yüklenmesini gerektirir. Ayrıca, Windows bir sanal makinede çalıştırılıyorsa, donanım destekli CPU sanallaştırma özelliği (Intel VT-x veya AMD-V) ana bilgisayar tarafından konuk VM'ye gösterilmelidir. Bu özellik için sistem gereksinimleri hakkında daha fazla bilgi, [Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs](https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-requirements)

**Not #2:**

Azure IaaS VM'leri kullanılırken Credential Guard ve Device Guard şu anda desteklenmemektedir.

**Gerekçe:**

Güvenli Önyükleme, önyükleyici saldırıları riskini azaltmaya yardımcı olabilir ve verilerin bellekten silinmesini önlemeye yardımcı olmak için DMA korumalarıyla birlikte.

**Etki:**

**Uyarı:** Sistemdeki tüm sürücüler bu özellikle uyumlu olmalıdır, aksi takdirde sistem çökebilir. Bu ilke ayarının yalnızca uyumlu olduğu bilinen bilgisayarlara dağıtıldığından emin olun.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:RequirePla tformSecurityFeatures*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki UI yolunu Güvenli Önyükleme ve DMA Koruması olarak ayarlayın:

*Bilgisayar Yapılandırması \Policies\Administrative Templates\System\Device Guard\Sanallaştırma Tabanlı Güvenliği Açın: Platform Güvenlik Düzeyini Seçin*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 RTM (Sürüm 1507) Yönetim Şablonları (veya daha yenisi) ile birlikte verilen Grup İlkesi şablonu DeviceGuard.admx/adml tarafından sağlanır.

**18.8.5.3 (NG) 'Sanallaştırma Tabanlı Güvenliği Aç: Kod Bütünlüğünün Sanallaştırma Tabanlı Koruması' seçeneği 'UEFI kilidi ile etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, Çekirdek Modu Kod Bütünlüğünün sanallaştırma tabanlı korunmasını sağlar. Bu etkinleştirildiğinde, çekirdek modu bellek korumaları uygulanır ve Kod Bütünlüğü doğrulama yolu, Sanallaştırma Tabanlı Güvenlik özelliği tarafından korunur. Bu ayar için önerilen durum: UEFI kilidi ile etkinleştirildi.

**Not:** Sanallaştırma Tabanlı Güvenlik, Windows'un Güvenli Önyükleme etkinleştirilmiş 64 bit sürümünü gerektirir; bu da Windows'un Eski BIOS yapılandırmasıyla değil UEFI BIOS yapılandırmasıyla yüklenmesini gerektirir. Ayrıca, Windows bir sanal makinede çalıştırılıyorsa, donanım destekli CPU sanallaştırma özelliği (Intel VT-x veya AMD-V) ana bilgisayar tarafından konuk VM'ye gösterilmelidir. Bu özellik için sistem gereksinimleri hakkında daha fazla bilgi, [Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs](https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-requirements)

**Not #2:** Azure IaaS VM'leri kullanılırken Credential Guard ve Device Guard şu anda desteklenmemektedir.

**Gerekçe:**

Enabled with UEFI kilidi seçeneği, Sanallaştırma Tabanlı Kod Bütünlüğü Korumasının uzaktan devre dışı bırakılamayacağını garanti eder.

**Etki:**

**Uyarı:** Sistemdeki tüm sürücüler bu özellikle uyumlu olmalıdır, aksi takdirde sistem çökebilir. Bu ilke ayarının yalnızca uyumlu olduğu bilinen bilgisayarlara dağıtıldığından emin olun.

**Uyarı #2:** Bu ayar açıldığında ve etkinleştirildiğinde, Sanallaştırma Tabanlı Güvenlik yalnızca GPO veya başka herhangi bir uzak yöntemle devre dışı bırakılamaz. Ayarı GPO'dan kaldırdıktan sonra, bu bağlantıda sağlanan adımlar kullanılarak özellikler makinede yerel olarak manuel olarak devre dışı bırakılmalıdır: [Windows Defender Kimlik Bilgisi Korumasını Yönetin (Windows 10) | Microsoft Docs](https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage#disable-windows-defender-credential-guard)

**Denetim:**

Düzeltme bölümünde belirtilen Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:Hypervisor EnforcedCodeIntegrity*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki UI yolunu UEFI kilidi ile Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\ İlkeler\Yönetim Şablonları\Sistem\Aygıt Koruması\Sanallaştırma Tabanlı Güvenliği Aç: Kod Bütünlüğünün Sanallaştırma Tabanlı Koruması*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 RTM (Sürüm 1507) Yönetim Şablonları (veya daha yenisi) ile birlikte verilen Grup İlkesi şablonu DeviceGuard.admx/adml tarafından sağlanır.

**18.8.5.4 (NG) 'Sanallaştırma Tabanlı Güvenliği Aç: UEFI Bellek Öznitelikleri Tablosunu Gerektir' seçeneği 'Doğru (işaretli)' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu seçenek, Bellek Öznitelikleri Tablosu için UEFI ürün yazılımı desteğine sahip cihazlarda yalnızca Sanallaştırma Tabanlı Kod Bütünlüğünü Korumasını etkinleştirir. UEFI Bellek Öznitelikleri Tablosu olmayan aygıtlarda, bazı durumlarda çökmelere, veri kaybına veya belirli eklenti kartlarıyla uyumsuzluğa neden olabilecek Sanallaştırma Tabanlı Kod Bütünlüğü Koruması ile uyumlu olmayan bellenim bulunabilir. Bu seçenek ayarlanmazsa, uyumluluğun sağlanması için hedeflenen cihazlar test edilmelidir. Bu ayar için önerilen durum: Doğru (işaretli).

**Not:** Sanallaştırma Tabanlı Güvenlik, Windows'un Güvenli Önyükleme etkinleştirilmiş 64 bit sürümünü gerektirir; bu da Windows'un Eski BIOS yapılandırmasıyla değil UEFI BIOS yapılandırmasıyla yüklenmesini gerektirir. Ayrıca, Windows bir sanal makinede çalıştırılıyorsa, donanım destekli CPU sanallaştırma özelliği (Intel VT-x veya AMD-V) ana bilgisayar tarafından konuk VM'ye gösterilmelidir. Bu özellik için sistem gereksinimleri hakkında daha fazla bilgi, [Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs](https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-requirements)

**Not #2:** Azure IaaS VM'leri kullanılırken Credential Guard ve Device Guard şu anda desteklenmemektedir.

**Gerekçe:**

Bu ayar, bu kontrolün uyumlu olmayan bir sistemde kilitlenmeye veya veri kaybına neden olabilecek şekilde etkinleştirilmesini önlemeye yardımcı olur.

**Etki:**

**Uyarı:** Sistemdeki tüm sürücüler bu özellikle uyumlu olmalıdır, aksi takdirde sistem çökebilir. Bu ilke ayarının yalnızca uyumlu olduğu bilinen bilgisayarlara dağıtıldığından emin olun.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:HVCIMATRequired*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu DOĞRU olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\System\Device Guard\Sanallaştırma Tabanlı Güvenliği Aç: UEFI Bellek Öznitelikleri Tablosu Gerektir*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1703 Yönetim Şablonlarında (veya daha yenisinde) bulunan DeviceGuard.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.8.5.5 (NG) 'Sanallaştırma Tabanlı Güvenliği Aç: Kimlik Bilgileri Koruma Yapılandırması' seçeneği 'UEFI kilidi ile etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, kullanıcıların kimlik bilgilerini korumaya yardımcı olmak için sanallaştırma tabanlı güvenlikle Credential Guard'ı açmasına olanak tanır. "UEFI kilidi ile etkinleştirildi" seçeneği, Credential Guard'ın uzaktan devre dışı bırakılamayacağını garanti eder. Özelliği devre dışı bırakmak için, Grup İlkesi'ni "Devre Dışı" olarak ayarlamanız ve ayrıca UEFI'de kalıcı olan yapılandırmayı temizlemek için fiziksel olarak mevcut bir kullanıcıyla her bilgisayardan güvenlik işlevini kaldırmanız gerekir. Bu ayar için önerilen durum: UEFI kilidi ile etkinleştirildi.

**Not:** Sanallaştırma Tabanlı Güvenlik, Windows'un Güvenli Önyükleme etkinleştirilmiş 64 bit sürümünü gerektirir; bu da Windows'un Eski BIOS yapılandırmasıyla değil UEFI BIOS yapılandırmasıyla yüklenmesini gerektirir. Ayrıca, Windows bir sanal makinede çalıştırılıyorsa, donanım destekli CPU sanallaştırma özelliği (Intel VT-x veya AMD-V) ana bilgisayar tarafından konuk VM'ye gösterilmelidir. Bu özellik için sistem gereksinimleri hakkında daha fazla bilgi, [Windows Defender Credential Guard Requirements (Windows 10) | Microsoft Docs](https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-requirements)

**Not #2:** Azure IaaS VM'leri kullanılırken Credential Guard ve Device Guard şu anda desteklenmemektedir.

**Gerekçe:**

Enabled with UEFI kilidi seçeneği, Credential Guard'ın uzaktan devre dışı bırakılamayacağını garanti eder.

**Etki:**

**Uyarı:** Sistemdeki tüm sürücüler bu özellikle uyumlu olmalıdır, aksi takdirde sistem çökebilir. Bu ilke ayarının yalnızca uyumlu olduğu bilinen bilgisayarlara dağıtıldığından emin olun.

**Uyarı #2:** Bu ayar açıldığında ve etkinleştirildiğinde, Credential Guard yalnızca GPO veya başka bir uzak yöntemle devre dışı bırakılamaz. Ayarı GPO'dan kaldırdıktan sonra, bu bağlantıda sağlanan adımlar kullanılarak özellikler makinede yerel olarak manuel olarak devre dışı bırakılmalıdır: [Windows Defender Kimlik Bilgisi Korumasını Yönetin (Windows 10) | Microsoft Docs](https://docs.microsoft.com/en-us/windows/security/identity-protection/credential-guard/credential-guard-manage#disable-windows-defender-credential-guard)

**Denetim:**

Düzeltme bölümünde belirtilen Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:LsaCfgFlags*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu UEFI kilidiyle Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\ İlkeler\Yönetim Şablonları\Sistem\Aygıt Koruması\Sanallaştırma Tabanlı Güvenliği Aç: Kimlik Bilgisi Koruması Yapılandırması*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1511 Yönetim Şablonlarında (veya daha yenisinde) bulunan DeviceGuard.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.8.5.6 (NG) 'Sanallaştırma Tabanlı Güvenliği Aç: Güvenli Başlatma Yapılandırması' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Güvenli Başlatma, Sanallaştırma Tabanlı Güvenlik ortamını aygıt bellenimindeki istismar edilen güvenlik açıklarından korur. Bu ayar için önerilen durum: Etkin.

**Not:** Credential Guard ve Device Guard, şu anda Azure IaaS VM'leri kullanılırken desteklenmemektedir.

**Gerekçe:**

Güvenli Başlatma, bellenim açıklarının Windows Sanallaştırma Tabanlı Güvenlik ortamının güvenliğini etkilemesini önlemek için Windows'un Intel Güvenilir Yürütme Teknolojisi (TXT) ve Çalışma Zamanı BIOS Esnekliği özelliklerini kullanacak şekilde önyükleme şeklini değiştirir.

**Etki:**

**Uyarı:** Sistemdeki tüm sürücüler bu özellikle uyumlu olmalıdır, aksi takdirde sistem çökebilir. Bu ilke ayarının yalnızca uyumlu olduğu bilinen bilgisayarlara dağıtıldığından emin olun.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceGuard:ConfigureS ystemGuardLaunch*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Aygıt Koruması\Sanallaştırma Tabanlı Güvenliği Açın: Güvenli Başlatma Yapılandırması*

**Not:** Bu Grup İlkesi yolu, varsayılan olarak var. Microsoft Windows 10 Sürüm 1809 ve Sunucu 2019 Yönetim Şablonlarında (veya daha yenisinde) bulunan DeviceGuard.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.8.6 Cihaz Sağlığı Tasdik Hizmeti**

**18.8.7 Cihaz Kurulumu**

**18.8.7.1 Cihaz Yükleme Kısıtlamaları**

**18.8.7.1.1 (BL) 'Bu cihaz kimliklerinden herhangi biriyle eşleşen cihazların yüklenmesini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows'un yüklemesi engellenen aygıtlar için bir Tak ve Kullan donanım kimlikleri ve uyumlu kimlikler listesi belirtmenize olanak tanır. Bu ilke ayarı, Windows'un bir aygıt yüklemesine izin veren diğer tüm ilke ayarlarından önceliklidir. Bu ilke ayarını etkinleştirirseniz, Windows'un, oluşturduğunuz listede donanım kimliği veya uyumlu kimliği görünen bir aygıtı yüklemesi engellenir. Bu ilke ayarını bir uzak masaüstü sunucusunda etkinleştirirseniz, ilke ayarı, belirtilen cihazların bir uzak masaüstü istemcisinden uzak masaüstü sunucusuna yeniden yönlendirilmesini etkiler. Bu ilke ayarını devre dışı bırakırsanız veya yapılandırmazsanız, cihazlar diğer ilke ayarları tarafından izin verildiği veya engellendiği şekilde yüklenebilir ve güncellenebilir. Bu ayar için önerilen durum: Etkin.

**Not:** Windows 10 Sürüm 1803 (ve daha yenisi) sürümlerinde, Doğrudan Bellek Erişimi (DMA) saldırıları gerçekleştirebilecek kötü amaçlı cihazlar için riskin çoğunu azaltan, Çekirdek DMA Koruması ile uyumlu olmayan harici cihazlar için Numaralandırma ilkesi adlı yeni bir denetim vardır. . Daha yeni kontrol, artık 18.8.26 bölümündeki Windows 10 CIS karşılaştırmasının bir parçasıdır. Ancak ortamınız hala Windows 10 Sürüm 1709 (veya daha eski) iş istasyonları içeriyorsa, yeni denetim çalışmayacaktır, bu nedenle bu sistemlerde Thunderbolt aygıtlarını devre dışı bırakmak için bu ayar önemli olmaya devam eder.

**Gerekçe:**

BitLocker ile korunan bir bilgisayar, bilgisayar açıldığında veya Bekleme güç durumundayken Doğrudan Bellek Erişimi (DMA) saldırılarına karşı savunmasız olabilir - buna iş istasyonu kilitliyken de dahildir. Yalnızca TPM kimlik doğrulamalı BitLocker, bilgisayarın herhangi bir önyükleme öncesi kimlik doğrulaması olmadan açılış durumuna girmesine izin verir. Bu nedenle, bir saldırgan DMA saldırıları gerçekleştirebilir. Bu sorun 2516445 numaralı Microsoft Bilgi Bankası makalesinde belgelenmiştir: BitLocker'a yönelik 1394 DMA ve Thunderbolt DMA tehditlerini azaltmak için SBP-2 sürücüsünü ve Thunderbolt denetleyicilerini engelleme.

**Etki:**

Belirtilen cihaz kimlikleriyle eşleşen cihazların yüklenmesi engellenecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrict ions:DenyDeviceIDs*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Sistem\Aygıt Kurulumu\Aygıt Yükleme Kısıtlamaları\Bu aygıt kimliklerinden herhangi biriyle eşleşen aygıtların yüklenmesini engelle*

Not: Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan DeviceInstallation.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.8.7.1.2 (BL) 'Bu cihaz kimliklerinden herhangi biriyle eşleşen cihazların yüklenmesini engelle: Bu cihaz kimliklerinden herhangi biriyle eşleşen cihazların yüklenmesini engelle' seçeneği 'PCI\CC\_0C0A' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows'un yüklemesi engellenen aygıtlar için bir Tak ve Kullan donanım kimlikleri ve uyumlu kimlikler listesi belirtmenize olanak tanır. Bu ilke ayarı, Windows'un bir aygıt yüklemesine izin veren diğer tüm ilke ayarlarından önceliklidir. Bu ilke ayarını etkinleştirirseniz, Windows'un, oluşturduğunuz listede donanım kimliği veya uyumlu kimliği görünen bir aygıtı yüklemesi engellenir. Bu ilke ayarını bir uzak masaüstü sunucusunda etkinleştirirseniz, ilke ayarı, belirtilen cihazların bir uzak masaüstü istemcisinden uzak masaüstü sunucusuna yeniden yönlendirilmesini etkiler. Bu ilke ayarını devre dışı bırakırsanız veya yapılandırmazsanız, cihazlar diğer ilke ayarları tarafından izin verildiği veya engellendiği şekilde yüklenebilir ve güncellenebilir. Bu ayar için önerilen durum: PCI\CC\_0C0A

**Not:** Bu aygıt kimliği Thunderbolt denetleyicileri içindir. Artık birçok bilgisayarda, özellikle dizüstü bilgisayarlarda yaygın olan USB Type-C (USB-C) bağlantı noktası standardı Thunderbolt teknolojisini kullanır ve bu nedenle bu kısıtlamadan etkilenebilir. Kuruluşunuzun USB-C'yi kapsamlı bir şekilde kullanması gerekiyorsa, kendinize bu öneriye bir istisna tanımak için dahili olarak karar vermeniz gerekebilir. Ancak, lütfen gerekli tüm karar vericilerin, kötü niyetli Thunderbolt cihazları (gözetimsiz bırakıldığında) yoluyla artan BitLocker şifreleme anahtarı hırsızlığı (ve dolayısıyla veri hırsızlığı) riskini kabul ettiğinden emin olun.

**Not 2:** Windows 10 Sürüm 1803 (ve daha yenisi) sürümlerinde, Doğrudan Bellek Erişimi gerçekleştirebilecek kötü amaçlı aygıtlar için riskin çoğunu azaltan, Çekirdek DMA Koruması ile uyumlu olmayan harici aygıtlar için Numaralandırma ilkesi adlı yeni bir denetim vardır. (DMA) saldırıları. Daha yeni kontrol, artık 18.8.26 bölümündeki Windows 10 CIS karşılaştırmasının bir parçasıdır. Ancak ortamınız hala Windows 10 Sürüm 1709 (veya daha eski) iş istasyonları içeriyorsa, yeni denetim çalışmayacaktır, bu nedenle bu sistemlerde Thunderbolt aygıtlarını devre dışı bırakmak için bu ayar önemli olmaya devam eder.

**Gerekçe:**

BitLocker ile korunan bir bilgisayar, bilgisayar açıldığında veya Bekleme güç durumundayken Doğrudan Bellek Erişimi (DMA) saldırılarına karşı savunmasız olabilir - buna iş istasyonu kilitliyken de dahildir. Yalnızca TPM kimlik doğrulamalı BitLocker, bilgisayarın herhangi bir önyükleme öncesi kimlik doğrulaması olmadan açılış durumuna girmesine izin verir. Bu nedenle, bir saldırgan DMA saldırıları gerçekleştirebilir. Bu sorun 2516445 numaralı Microsoft Bilgi Bankası makalesinde belgelenmiştir: [BitLocker'a yönelik 1394 DMA ve Thunderbolt DMA tehditlerini azaltmak için SBP-2 sürücüsünü ve Thunderbolt denetleyicilerini engelleme.](https://support.microsoft.com/en-us/kb/2516445)

**Etki:**

Thunderbolt denetleyicilerinin Windows'a yüklenmesi engellenecek. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrict ions\DenyDeviceIDs:1*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın ve Aygıt Kimlikleri listesine PCI\CC\_0C0A ekleyin:

*Bilgisayar Yapılandırması\ İlkeler\Yönetim Şablonları\Sistem\Aygıt Kurulumu\Aygıt Yükleme Kısıtlamaları\Bu aygıt kimliklerinden herhangi biriyle eşleşen aygıtların yüklenmesini engelle*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan DeviceInstallation.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.8.7.1.3 (BL) 'Bu cihaz kimliklerinden herhangi biriyle eşleşen cihazların yüklenmesini engelle: Zaten yüklü olan eşleşen cihazlara da uygulanır.' seçeneği 'Doğru' (işaretli) (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows'un yüklemesi engellenen aygıtlar için bir Tak ve Kullan donanım kimlikleri ve uyumlu kimlikler listesi belirtmenize olanak tanır. Bu ilke ayarı, Windows'un bir aygıt yüklemesine izin veren diğer tüm ilke ayarlarından önceliklidir. Bu ilke ayarını etkinleştirirseniz, Windows'un, oluşturduğunuz listede donanım kimliği veya uyumlu kimliği görünen bir aygıtı yüklemesi engellenir. Bu ilke ayarını bir uzak masaüstü sunucusunda etkinleştirirseniz, ilke ayarı, belirtilen cihazların bir uzak masaüstü istemcisinden uzak masaüstü sunucusuna yeniden yönlendirilmesini etkiler. Bu ilke ayarını devre dışı bırakırsanız veya yapılandırmazsanız, cihazlar diğer ilke ayarları tarafından izin verildiği veya engellendiği şekilde yüklenebilir ve güncellenebilir. Bu ayar için önerilen durum: Doğru (işaretli).

**Not:** Windows 10 Sürüm 1803 (ve daha yenisi) sürümlerinde, Doğrudan Bellek Erişimi (DMA) saldırıları gerçekleştirebilecek kötü amaçlı cihazlar için riskin çoğunu azaltan, Çekirdek DMA Koruması ile uyumlu olmayan harici cihazlar için Numaralandırma ilkesi adlı yeni bir denetim vardır. Daha yeni kontrol, artık 18.8.26 bölümündeki Windows 10 CIS karşılaştırmasının bir parçasıdır. Ancak ortamınız hala Windows 10 Sürüm 1709 (veya daha eski) iş istasyonları içeriyorsa, yeni denetim çalışmayacaktır, bu nedenle bu sistemlerde Thunderbolt aygıtlarını devre dışı bırakmak için bu ayar önemli olmaya devam eder.

**Gerekçe:**

BitLocker ile korunan bir bilgisayar, bilgisayar açıldığında veya Bekleme güç durumundayken Doğrudan Bellek Erişimi (DMA) saldırılarına karşı savunmasız olabilir - buna iş istasyonu kilitliyken de dahildir. Yalnızca TPM kimlik doğrulamalı BitLocker, bilgisayarın herhangi bir önyükleme öncesi kimlik doğrulaması olmadan açılış durumuna girmesine izin verir. Bu nedenle, bir saldırgan DMA saldırıları gerçekleştirebilir. Bu sorun 2516445 numaralı Microsoft Bilgi Bankası makalesinde belgelenmiştir: [BitLocker'a yönelik 1394 DMA ve Thunderbolt DMA tehditlerini azaltmak için SBP-2 sürücüsünü ve Thunderbolt denetleyicilerini engelleme.](https://support.microsoft.com/en-us/kb/2516445)

**Etki:**

Sertleştirmeden önce önceden kurulmuş olan (belirtilen cihaz kimlikleriyle eşleşen) mevcut cihazlar devre dışı bırakılacak veya kaldırılacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrict ions:DenyDeviceIDsRetroactive*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın ve Ayrıca'yı işaretleyin. Zaten kurulu olan eşleşen cihazlara uygulanır. Onay kutusu:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Aygıt Yüklemesi\Aygıt Yükleme Kısıtlamaları\Bu aygıt kimliklerinden herhangi biriyle eşleşen aygıtların yüklenmesini engelle*

**Not:** Bu Grup İlkesi yolu, Grup İlkesi şablonu DeviceInstallation.admx/adml tarafından sağlanır. Microsoft Windows Yönetim Şablonlarının tüm sürümlerine dahildir.

**18.8.7.1.4 (BL) 'Bu aygıt kurulum sınıflarıyla eşleşen sürücüleri kullanarak aygıtların yüklenmesini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows'un yüklemesinin engellendiği aygıt sürücüleri için aygıt kurulum sınıfı genel olarak benzersiz tanımlayıcıların (GUID'ler) bir listesini belirtmenize olanak tanır. Bu ilke ayarı, Windows'un bir aygıt yüklemesine izin veren diğer tüm ilke ayarlarından önceliklidir. Bu ilke ayarını etkinleştirirseniz, Windows'un, oluşturduğunuz listede aygıt kurulum sınıfı GUID'leri görünen aygıt sürücülerini yüklemesi veya güncellemesi engellenir. Bu ilke ayarını bir uzak masaüstü sunucusunda etkinleştirirseniz, ilke ayarı, belirtilen cihazların bir uzak masaüstü istemcisinden uzak masaüstü sunucusuna yeniden yönlendirilmesini etkiler. Bu ilke ayarını devre dışı bırakırsanız veya yapılandırmazsanız, Windows diğer ilke ayarları tarafından izin verildiği veya engellendiği şekilde cihazları yükleyebilir ve güncelleyebilir. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

BitLocker ile korunan bir bilgisayar, bilgisayar açıldığında veya Bekleme güç durumundayken Doğrudan Bellek Erişimi (DMA) saldırılarına karşı savunmasız olabilir - buna iş istasyonu kilitliyken de dahildir. Yalnızca TPM kimlik doğrulamalı BitLocker, bilgisayarın herhangi bir önyükleme öncesi kimlik doğrulaması olmadan açılış durumuna girmesine izin verir. Bu nedenle, bir saldırgan DMA saldırıları gerçekleştirebilir. Bu sorun 2516445 numaralı Microsoft Bilgi Bankası makalesinde belgelenmiştir: [BitLocker'a yönelik 1394 DMA ve Thunderbolt DMA tehditlerini azaltmak için SBP-2 sürücüsünü ve Thunderbolt denetleyicilerini engelleme.](https://support.microsoft.com/en-us/kb/2516445)

**Etki:** Belirtilen cihaz kurulum sınıflarıyla eşleşen cihazların kurulumu engellenecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrict ions:DenyDeviceClasses*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Sistem\Aygıt Kurulumu\Aygıt Kurulum Kısıtlamaları\Bu aygıt kurulum sınıflarıyla eşleşen sürücüleri kullanan aygıtların yüklenmesini engelle*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan DeviceInstallation.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.8.7.1.5 (BL) 'Bu aygıt kurulum sınıflarıyla eşleşen sürücüleri kullanarak aygıtların yüklenmesini engelle: Bu aygıt kurulumu için sürücüleri kullanarak aygıtların yüklenmesini engelle' seçeneği 'IEEE 1394 aygıt kurulum sınıfları' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows'un yüklemesinin engellendiği aygıt sürücüleri için aygıt kurulum sınıfı genel olarak benzersiz tanımlayıcıların (GUID'ler) bir listesini belirtmenize olanak tanır. Bu ilke ayarı, Windows'un bir aygıt yüklemesine izin veren diğer tüm ilke ayarlarından önceliklidir. Bu ilke ayarını etkinleştirirseniz, Windows'un, oluşturduğunuz listede aygıt kurulum sınıfı GUID'leri görünen aygıt sürücülerini yüklemesi veya güncellemesi engellenir. Bu ilke ayarını bir uzak masaüstü sunucusunda etkinleştirirseniz, ilke ayarı, belirtilen cihazların bir uzak masaüstü istemcisinden uzak masaüstü sunucusuna yeniden yönlendirilmesini etkiler. Bu ilke ayarını devre dışı bırakırsanız veya yapılandırmazsanız, Windows diğer ilke ayarları tarafından izin verildiği veya engellendiği şekilde cihazları yükleyebilir ve güncelleyebilir. Önerdiğimiz dört giriş ve bunların tercümesi:

* {d48179be-ec20-11d1-b6b8-00c04fa372a7} - SBP2 Protokol Sınıfını destekleyen IEEE 1394 cihazları
* {7ebefbc0-3200-11d2-b4c2-00a0C9697d07} - IEEE 1394 IEC-61883 Protokol Sınıfını destekleyen cihazlar
* {c06ff265-ae09-48f0-812c-16753d7cba83} - AVC Protokol Sınıfını destekleyen IEEE 1394 cihazları
* {6bdd1fc1-810f-11d0-bec7-08002be2092f} - IEEE 1394 Ana Bilgisayar Veri Yolu Denetleyici Sınıfı

Windows'ta bulunan sistem tanımlı aygıt kurulum sınıflarının tam listesi burada: [Satıcıların Kullanabileceği Sistem Tanımlı Aygıt Kurulum Sınıfları | Microsoft Docs](https://docs.microsoft.com/en-us/windows-hardware/drivers/install/system-defined-device-setup-classes-available-to-vendors)

Bu ayar için önerilen durum: {d48179be-ec20-11d1-b6b8-00c04fa372a7}, {7befbc0-3200-11d2-b4c2-00a0C9697d07}, {c06ff265-ae09-48f0-812c-16753d7cbadd} ve 810f-11d0-bec7-08002be2092f}

**Not:** IEEE 1394 ayrıca FireWire (Apple), i.LINK (Sony) ve Lynx (Texas Instruments) olarak bilinir/markalandırılır.

**Gerekçe:**

BitLocker ile korunan bir bilgisayar, bilgisayar açıldığında veya Bekleme güç durumundayken Doğrudan Bellek Erişimi (DMA) saldırılarına karşı savunmasız olabilir - buna iş istasyonu kilitliyken de dahildir. Yalnızca TPM kimlik doğrulamalı BitLocker, bilgisayarın herhangi bir önyükleme öncesi kimlik doğrulaması olmadan açılış durumuna girmesine izin verir. Bu nedenle, bir saldırgan DMA saldırıları gerçekleştirebilir. Bu sorun 2516445 numaralı Microsoft Bilgi Bankası makalesinde belgelenmiştir: [BitLocker'a yönelik 1394 DMA ve Thunderbolt DMA tehditlerini azaltmak için SBP-2 sürücüsünü ve Thunderbolt denetleyicilerini engelleme.](https://support.microsoft.com/en-us/kb/2516445)

**Etki:**

IEEE 1394 sürücülerinin ve aygıtlarının Windows'a yüklenmesi engellenecek. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrict ions\DenyDeviceClasses<numeric value>*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın ve {d48179be-ec20-11d1-b6b8-00c04fa372a7}, {7befbc0-3200-11d2-b4c2- 00a0C9697d07}, {c06ff265-ae09-48f0 ekleyin -812c-16753d7cba83} ve {6bdd1fc1-810f-11d0- bec7-08002be2092f} aygıt kurulum sınıfları listesine:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Aygıt Kurulumu\Aygıt Kurulum Kısıtlamaları\Eşleşen sürücüleri kullanan aygıtların yüklenmesini engelle bu cihaz kurulum sınıfları*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan DeviceInstallation.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.8.7.1.6 (BL) 'Bu aygıt kurulum sınıflarıyla eşleşen sürücüleri kullanarak aygıtların yüklenmesini engelle: Zaten yüklü olan eşleşen aygıtlara da uygulanır.' seçeneği 'Doğru' (işaretli) (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows'un yüklemesinin engellendiği aygıt sürücüleri için aygıt kurulum sınıfı genel olarak benzersiz tanımlayıcıların (GUID'ler) bir listesini belirtmenize olanak tanır. Bu ilke ayarı, Windows'un bir aygıt yüklemesine izin veren diğer tüm ilke ayarlarından önceliklidir. Bu ilke ayarını etkinleştirirseniz, Windows'un, oluşturduğunuz listede aygıt kurulum sınıfı GUID'leri görünen aygıt sürücülerini yüklemesi veya güncellemesi engellenir. Bu ilke ayarını bir uzak masaüstü sunucusunda etkinleştirirseniz, ilke ayarı, belirtilen cihazların bir uzak masaüstü istemcisinden uzak masaüstü sunucusuna yeniden yönlendirilmesini etkiler. Bu ilke ayarını devre dışı bırakırsanız veya yapılandırmazsanız, Windows diğer ilke ayarları tarafından izin verildiği veya engellendiği şekilde cihazları yükleyebilir ve güncelleyebilir. Bu ayar için önerilen durum: Doğru (işaretli).

**Gerekçe:**

BitLocker ile korunan bir bilgisayar, bilgisayar açıldığında veya Bekleme güç durumundayken Doğrudan Bellek Erişimi (DMA) saldırılarına karşı savunmasız olabilir - buna iş istasyonu kilitliyken de dahildir. Yalnızca TPM kimlik doğrulamalı BitLocker, bilgisayarın herhangi bir önyükleme öncesi kimlik doğrulaması olmadan açılış durumuna girmesine izin verir. Bu nedenle, bir saldırgan DMA saldırıları gerçekleştirebilir. Bu sorun 2516445 numaralı Microsoft Bilgi Bankası makalesinde belgelenmiştir: [BitLocker'a yönelik 1394 DMA ve Thunderbolt DMA tehditlerini azaltmak için SBP-2 sürücüsünü ve Thunderbolt denetleyicilerini engelleme.](https://support.microsoft.com/en-us/kb/2516445)

**Etki:**

Sertleştirmeden önce önceden kurulmuş olan (belirtilen cihaz kurulum sınıflarıyla eşleşen) mevcut cihazlar devre dışı bırakılır veya kaldırılır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeviceInstall\Restrict ions:DenyDeviceClassesRetroactive*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın ve Ayrıca'yı işaretleyin. zaten kurulu olan eşleşen cihazlara uygulanır. onay kutusu:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Aygıt Kurulumu\Aygıt Yükleme Kısıtlamaları\Bu aygıt kurulum sınıflarıyla eşleşen sürücüleri kullanan aygıtların yüklenmesini engelle*

**Not:** Bu Grup İlkesi yolu, Grup İlkesi şablonu DeviceInstallation.admx/adml tarafından sağlanır. Microsoft Windows Yönetim Şablonlarının tüm sürümlerine dahildir.

**18.8.7.2 (L1) 'İnternetten cihaz meta verilerinin alınmasını engelle' seçeneği 'Etkin'**  **(Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows'un İnternet'ten cihaz meta verilerini almasını engellemenize olanak tanır. Bu ayar için önerilen durum: Etkin. Not: Bu, temel donanım sürücülerinin yüklenmesini engellemez, ancak ilişkili 3. taraf yardımcı program yazılımının SYSTEM hesabı bağlamında otomatik olarak yüklenmesini engeller.

**Gerekçe:**

Yazılımın kurulumu, standart bir kullanıcı tarafından değil, yetkili bir sistem yöneticisi tarafından gerçekleştirilmelidir. SYSTEM hesabı bağlamında otomatik üçüncü taraf yazılım kurulumlarına izin vermek, arka kapılar veya kurulum yazılımı hataları aracılığıyla yetkisiz erişime izin verme potansiyeline sahiptir.

**Etki:**

Yönetici ayrıcalıklarına sahip olmayan standart kullanıcılar, çevrebirim aygıtları için ilişkili 3. taraf yardımcı program yazılımını yükleyemez. Bu, bir yönetici cihaz için ilişkili yardımcı yazılım yazılımını yüklemedikçe/tana kadar bu cihazların gelişmiş özelliklerinin kullanımını sınırlayabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Device Metadata:PreventDeviceMetadataFromNetwork*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Aygıt Kurulumu\İnternet'ten cihaz meta verilerinin alınmasını engelle*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında bulunan Grup İlkesi şablonu DeviceInstallation.admx/adml veya Microsoft Windows 8.0 ve Server 2012'de bulunan Grup İlkesi şablonu DeviceSetup.admx/adml (R2 olmayan) Yönetim Şablonları (veya daha yenisi).

**18.8.8 Cihaz Yeniden Yönlendirme**

**18.8.9 Disk NV Önbelleği**

**18.8.10 Disk Kotaları**

**18.8.11 Ekran**

**18.8.12** **Dağıtılmış COM**

**18.8.13 Sürücü Kurulumu**

**18.8.14 Erken Başlatma Kötü Amaçlı Yazılımdan Koruma**

**18.8.14.1 (L1) 'Boot-Start Driver Initialization Policy' (Önyükleme-Başlat Sürücüsü Başlatma İlkesi) seçeneği 'Etkin: İyi, bilinmeyen ve kötü ama kritik' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir Erken Başlatma Kötü Amaçlı Yazılım Önyükleme başlatma sürücüsü tarafından belirlenen bir sınıflandırmaya göre hangi önyükleme başlatma sürücülerinin başlatılacağını belirtmenize olanak tanır. Erken Başlatma Kötü Amaçlı Yazılım Önyükleme başlatma sürücüsü, her önyükleme başlatma sürücüsü için aşağıdaki sınıflandırmaları döndürebilir:

* İyi: Sürücü imzalanmıştır ve üzerinde değişiklik yapılmamıştır.
* Kötü: Sürücünün kötü amaçlı yazılım olduğu belirlendi. Bilinen hatalı sürücülerin başlatılmasına izin vermemeniz önerilir.
* Kötü, ancak önyükleme için gerekli: Sürücü kötü amaçlı yazılım olarak tanımlandı, ancak bilgisayar bu sürücü yüklenmeden başarıyla önyüklenemiyor.
* Bilinmeyen: Bu sürücü, kötü amaçlı yazılım algılama uygulamanız tarafından onaylanmamıştır ve Early Launch Antimalware önyükleme başlatma sürücüsü tarafından sınıflandırılmamıştır.

Bu ilke ayarını etkinleştirirseniz, bilgisayar bir sonraki başlatılışında hangi önyükleme başlatma sürücülerinin başlatılacağını seçebileceksiniz. Kötü amaçlı yazılım algılama uygulamanız bir Early Launch Antimalware önyükleme başlatma sürücüsü içermiyorsa veya Early Launch Antimalware önyükleme başlatma sürücünüz devre dışı bırakılmışsa, bu ayarın hiçbir etkisi olmaz ve tüm önyükleme başlatma sürücüleri başlatılır. Bu ayar için önerilen durum: Etkin: İyi, bilinmiyor ve kötü ama kritik.

**Gerekçe:**

Bu ilke ayarı, sisteminize zaten bulaşmış olan kötü amaçlı yazılımların etkisini azaltmaya yardımcı olur.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Policies\EarlyLaunch:DriverLoadPolicy*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: İyi, bilinmeyen ve kötü ancak kritik:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Erken Başlatma Kötü Amaçlı Yazılımdan Önyükleme\Önyükleme Başlatma Sürücü Başlatma İlkesi*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu EarlyLaunchAM.admx/adml tarafından sağlanır.

**18.8.15 Gelişmiş Depolama Erişimi**

**18.8.16 Dosya Sınıflandırma Altyapısı**

**18.8.17 Dosya Paylaşımı Gölge Kopya Aracısı**

**18.8.18 Dosya Paylaşımı Gölge Kopya Sağlayıcısı**

**18.8.19 Dosya Sistemi (eski adıyla NTFS Dosya Sistemi)**

**18.8.20 Klasör Yeniden Yönlendirme**

**18.8.21 Grup İlkesi**

**18.8.21.1 Günlüğe kaydetme ve izleme**

**18.8.21.2 (L1) 'Kayıt defteri ilkesi işlemeyi yapılandır: Periyodik arka plan işleme sırasında uygulamayın' seçeneği 'Etkin: YANLIŞ' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

"Periyodik arka plan işleme sırasında uygulama" seçeneği, bilgisayar kullanımdayken sistemin etkilenen ilkeleri arka planda güncellemesini engeller. Arka plan güncellemeleri devre dışı bırakıldığında, politika değişiklikleri bir sonraki kullanıcı oturum açana veya sistem yeniden başlatılıncaya kadar etkili olmaz. Bu ayar için önerilen durum: Etkin: YANLIŞ (işaretlenmemiş).

**Gerekçe:**

Bu seçeneğin false (işaretlenmemiş) olarak ayarlanması, bir sonraki kullanıcı oturum açmasına veya sistem yeniden başlatılmasına kadar beklemeye kıyasla, etki alanı politikası değişikliklerinin daha hızlı yürürlüğe girmesini sağlar.

**Etki:**

Grup İlkeleri her yenilendiğinde yeniden uygulanacaktır, bu da performans üzerinde hafif bir etkisi olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Group Policy\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}:NoBackgroundPolicy*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için UI yolunu Etkin olarak takip edin, ardından Periyodik arka plan işleme sırasında uygulama seçeneğini YANLIŞ olarak ayarlayın (işaretlenmemiş):

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Grup İlkesi\Kayıt defteri ilkesi işlemeyi yapılandır*

**Not:** Bu Grup İlkesi yolu, varsayılan. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu GroupPolicy.admx/adml tarafından sağlanır.

**18.8.21.3 (L1) 'Kayıt defteri politikası işlemeyi yapılandır: Grup İlkesi nesneleri değişmemiş olsa bile işle' seçeneği 'Etkin: DOĞRU' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

"Grup İlkesi nesneleri değişmese bile işle" seçeneği, ilkeler değişmese bile ilkeleri günceller ve yeniden uygular. Bu ayar için önerilen durum: Etkin: DOĞRU (işaretli).

**Gerekçe:**

Bu seçeneği true (işaretli) olarak ayarlamak, yerel olarak yapılandırılmış olabilecek yetkisiz değişikliklerin etki alanı tabanlı Grup İlkesi ayarlarıyla yeniden eşleşmeye zorlanmasını sağlar.

**Etki:**

Grup İlkeleri, değiştirilmemiş olsalar bile yeniden uygulanacaktır, bu da performans üzerinde hafif bir etkisi olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Group Policy\{35378EAC-683F-11D2-A89A-00C04FBBCFA2}:NoGPOListChanges*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın, ardından Grup İlkesi nesneleri değişmemiş olsa bile İşlem seçeneğini DOĞRU (işaretli) olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\ Grup İlkesi\Kayıt defteri ilkesi işlemeyi yapılandır*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu GroupPolicy.admx/adml tarafından sağlanır.

**18.8.21.4 (L1) 'Bu cihazda deneyimlere devam et' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows cihazının cihazlar arası deneyimlere (devam deneyimleri) katılmasına izin verilip verilmeyeceğini belirler. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Cihazlar arası deneyim, bir sistemin uygulamaya erişebildiği ve diğer cihazlara mesaj gönderebildiği zamandır. Kurumsal yönetilen bir ortamda, ağ içinde yalnızca güvenilir sistemler iletişim kurmalıdır. Başka herhangi bir sisteme erişim yasaklanmalıdır.

**Etki:**

Windows cihazı diğer cihazlar tarafından bulunamaz ve cihazlar arası deneyimlere katılamaz. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:EnableCdp*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları \System\Group Policy\Devam deneyimleri bu aygıtta*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1607 ve Server 2016 Yönetim Şablonlarında (veya daha yenisinde) bulunan GroupPolicy.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.8.21.5 (L1) 'Grup İlkesi arka plan yenilemesini kapat' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır**.

**Açıklama:**

Bu ilke ayarı, bilgisayar kullanımdayken Grup İlkesi'nin güncellenmesini engeller. Bu ilke ayarı, bilgisayarlar, kullanıcılar ve Etki Alanı Denetleyicileri için Grup İlkesi için geçerlidir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bu ayar, grup ilkesi değişikliklerinin bir sonraki kullanıcı oturum açmasına veya sistem yeniden başlatılmasına kadar beklemeye kıyasla daha hızlı yürürlüğe girmesini sağlar.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu mevcut olmadığında geçerlidir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: DisableBkGndGroupPolicy*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırma\İlkeler\Yönetim Şablonları\Sistem\Grup İlkesi\Grup İlkesi'nin arka plan yenilemesini kapat*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan GroupPolicy.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.8.22 İnternet İletişim Yönetimi**

**18.8.22.1 İnternet İletişimi ayarları**

**18.8.22.1.1 (L2) 'Mağazaya erişimi kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, işlenmemiş dosya türü veya protokol ilişkilendirmesi olan bir dosyayı açmak üzere bir uygulama bulmak için Mağaza hizmetinin kullanılıp kullanılmayacağını belirtir. Bir kullanıcı, bilgisayardaki herhangi bir uygulamayla ilişkili olmayan bir dosya türü veya protokolü açtığında, kullanıcıya yerel bir uygulama seçme veya bir uygulamayı bulmak için Mağaza hizmetini kullanma seçeneği sunulur. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Mağaza hizmeti, öncelikle tüketici kullanımı için Windows'ta yerleşik bir perakende satış noktasıdır. Kurumsal olarak yönetilen bir ortamda BT departmanı, güvenlik açığı bulunan yazılımların kurulum riskini azaltmak için tüm uygulamaların kurulumunu yönetmelidir.

**Etki:**

Birlikte Aç iletişim kutusundaki "Mağazada uygulama ara" öğesi kaldırıldı.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Explorer:NoUseStoreOpe nWith*

**Düzeltme**:

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\System\Internet Communication Management\Internet Communication settings\Mağazaya erişimi kapat*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu ICM.admx/adml tarafından sağlanır.

**18.8.22.1.2 (L1) 'HTTP üzerinden yazdırma sürücülerinin indirilmesini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bilgisayarın HTTP üzerinden yazıcı sürücüsü paketlerini indirip indiremeyeceğini kontrol eder. HTTP yazdırmayı ayarlamak için standart işletim sistemi kurulumunda bulunmayan yazıcı sürücülerinin HTTP üzerinden indirilmesi gerekebilir. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Kullanıcılar, kötü amaçlı kod içeren sürücüleri indirebilir.

**Etki:**

Yazdırma sürücüleri HTTP üzerinden indirilemez.

**Not:** Bu ilke ayarı, istemci bilgisayarın intranet veya Internet üzerindeki yazıcılara HTTP üzerinden yazdırma yapmasını engellemez. Yalnızca yerel olarak henüz yüklenmemiş sürücülerin indirilmesini yasaklar.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsNT\Printers:DisableWebPnPDDownload*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\Sistem\Internet Iletişim Yönetimi\İnternet İletişimi ayarları\Yazdırma sürücülerinin HTTP üzerinden indirilmesini kapat*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu ICM.admx/adml tarafından sağlanır.

**18.8.22.1.3 (L2) 'El yazısı kişiselleştirme veri paylaşımını kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, el yazısı tanıma kişiselleştirme aracından veri paylaşımını kapatır. El yazısı tanıma kişiselleştirme aracı, Tablet PC kullanıcılarının, yazı örnekleri sağlayarak el yazısı tanımayı kendi yazı stillerine uyarlamalarını sağlar. Araç, Windows'un gelecekteki sürümlerinde el yazısı tanımayı iyileştirmek için isteğe bağlı olarak kullanıcı yazma örneklerini Microsoft ile paylaşabilir. Araç, raporlar oluşturur ve bunları güvenli bir bağlantı üzerinden Microsoft'a iletir. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bir kişinin el yazısı, özellikle imzanız söz konusu olduğunda, Kişisel Tanımlanabilir Bilgilerdir (PII). Bu nedenle, birçok ortamda, kullanıcının açık onayı olmadan bir web sitesine PII'nin otomatik olarak yüklenmesi kabul edilemez.

**Etki:**

Tablet PC kullanıcıları, Microsoft ile el yazısı tanıma kişiselleştirme aracından yazı örneklerini paylaşmayı seçemezler.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\TabletPC:PreventHandwr itingDataSharing*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\İnternet İletişim Yönetimi\İnternet İletişimi ayarları\El yazısı kişiselleştirme veri paylaşımını kapat*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan ShapeCollector.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.8.22.1.4 (L2) 'El yazısı tanıma hata bildirimini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

El yazısı tanıma hatası raporlama aracını kapatır. El yazısı tanıma hatası raporlama aracı, kullanıcıların Tablet PC Giriş Panelinde karşılaşılan hataları bildirmelerini sağlar. Araç, hata raporları oluşturur ve bunları güvenli bir bağlantı üzerinden Microsoft'a iletir. Microsoft, bu hata raporlarını, Windows'un gelecekteki sürümlerinde el yazısı tanımayı geliştirmek için kullanır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bir kişinin el yazısı, özellikle imzanız söz konusu olduğunda, Kişisel Tanımlanabilir Bilgilerdir (PII). Bu nedenle, birçok ortamda, kullanıcının açık onayı olmadan bir web sitesine PII'nin otomatik olarak yüklenmesi kabul edilemez.

**Etki:**

Kullanıcılar, el yazısı tanıma hatası raporlama aracını başlatamaz veya Microsoft'a hata raporları gönderemez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\HandwritingErrorReport s:PreventHandwritingErrorReports*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\İnternet İletişim Yönetimi\İnternet İletişimi ayarları\El yazısı tanıma hatası raporlamayı kapat*

**Not:** Bu Grup İlkesi yolu Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu InkWatson.admx/adml tarafından sağlanır

**18.8.22.1.5 (L2) 'URL bağlantısı Microsoft.com atıfta bulunuyorsa İnternet Bağlantı Sihirbazını kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, İnternet Bağlantı Sihirbazı'nın İnternet Servis Sağlayıcıları (ISS'ler) listesini indirmek için Microsoft'a bağlanıp bağlanamayacağını belirtir. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Kurumsal olarak yönetilen bir ortamda, bir kullanıcının bilmeden hassas verileri ifşa etme riskini azaltmak istiyoruz.

**Etki:**

İnternet Bağlantı Sihirbazı'ndaki "İnternet Servis Sağlayıcıları listesi seçin" yolu sihirbazın çıkmasına neden olur. Bu, kullanıcıların Microsoft sunucularında bulunan ISS'lerin listesini almasını engeller.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Internet Bağlantı Sihirbazı:ExitOnMSICW*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\ Yönetim Şablonları\Sistem\İnternet İletişim Yönetimi\İnternet İletişimi ayarları\URL bağlantısı Microsoft.com'a atıfta bulunuyorsa İnternet Bağlantı Sihirbazını kapatın*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının sürümleri tüm öğelerde bulunan Grup İlkesi şablonu ICM.admx/adml tarafından sağlanır.

**18.8.22.1.6 (L1) 'Web yayıncılığı ve çevrimiçi sipariş sihirbazları için İnternet'ten indirmeyi kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows'un Web yayımlama ve çevrimiçi sipariş sihirbazları için bir sağlayıcı listesi indirip indirmeyeceğini denetler. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Risk minimum düzeyde olsa da, bu ayarın etkinleştirilmesi, kullanıcının bu özellik aracılığıyla bilmeden kötü amaçlı içerik indirme olasılığını azaltacaktır.

**Etki:**

Windows'un sağlayıcıları indirmesi engellenir; yalnızca yerel kayıt defterinde önbelleğe alınan hizmet sağlayıcılar görüntülenir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore r:NoWebServices*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Sistem\İnternet İletişim Yönetimi\İnternet İletişim ayarları\Web yayımlama ve çevrimiçi sipariş sihirbazları için İnternet indirmeyi kapat*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu ICM.admx/adml tarafından sağlanır.

**18.8.22.1.7 (L2) 'HTTP üzerinden yazdırmayı kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, istemci bilgisayarın Internet'in yanı sıra intranet üzerindeki yazıcılara yazdırmasını sağlayan HTTP üzerinden yazdırma özelliğini devre dışı bırakmanıza olanak tanır. Bu ayar için önerilen durum: Etkin.

**Not:** Bu kontrol, hem HTTP hem de HTTPS üzerinden yazdırmayı etkiler.

**Gerekçe:**

Bu yetenek aracılığıyla HTTP üzerinden iletilen bilgiler korunmaz ve kötü niyetli kullanıcılar tarafından ele geçirilebilir. Bu nedenle kurumsal yönetilen ortamlarda sıklıkla kullanılmaz.

**Etki:**

İstemci bilgisayar, HTTP veya HTTPS üzerinden İnternet yazıcılarına yazdıramayacak. Not: Bu ilke ayarı yalnızca İnternet üzerinden yazdırmanın istemci tarafını etkiler. Nasıl yapılandırıldığına bakılmaksızın, bir bilgisayar bir İnternet Yazdırma sunucusu gibi davranabilir ve paylaşılan yazıcılarını HTTP aracılığıyla kullanılabilir hale getirebilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsNT\Printers:DisableHTTPPrinting*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\İnternet İletişim Yönetimi\İnternet İletişimi ayarları\HTTP üzerinden yazdırmayı kapat*

**Not:** Bu Grup İlkesi yolu Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu ICM.admx/adml tarafından sağlanır

**18.8.22.1.8 (L2) 'URL bağlantısı Microsoft.com atıfta bulunuyorsa Kaydı kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows Kayıt Sihirbazı'nın çevrimiçi kayıt için Microsoft.com'a bağlanıp bağlanmayacağını belirtir. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Kurumsal olarak yönetilen bir ortamdaki kullanıcılar, süreçte kendi PII'lerini sağlayarak kendi Windows kopyalarını kaydetmemelidir.

**Etki:**

Kullanıcıların çevrimiçi kayıt için Microsoft.com'a bağlanması engellenir ve Windows kopyalarını çevrimiçi olarak kaydedemezler.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Registration Wizard Control:NoRegistration*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\ Yönetim Şablonları\Sistem\İnternet İletişimi Yönetimi\İnternet İletişimi ayarları\URL bağlantısı Microsoft.com'a atıfta bulunuyorsa Kaydı kapat*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu ICM.admx/adml tarafından sağlanır.

**18.8.22.1.9 (L2) 'Arama Yardımcısı içerik dosyası güncellemelerini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Search Companion'ın yerel ve İnternet aramaları sırasında içerik güncellemelerini otomatik olarak indirip indirmeyeceğini belirtir. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Kullanıcıların aradıkları konular nedeniyle bilmeden hassas bilgileri ifşa etme riski vardır. Bu risk çok düşüktür, çünkü bu ayar etkinleştirilse bile, kullanıcıların arama yapmak için yine de istenen arama motoruna arama sorguları göndermeleri gerekir.

**Etki:**

Arama Eşlikçisi, aramalar sırasında içerik güncellemelerini indirmiyor.

**Not:** İnternet aramaları, arama metnini ve aramayla ilgili bilgileri yine de Microsoft'a ve seçilen arama sağlayıcısına gönderir. Klasik Arama'yı seçerseniz, Arama Eşlikçisi özelliği kullanılamaz. Başlat, Ara, Tercihleri Değiştir ve ardından İnternet Arama Davranışını Değiştir'i tıklatarak Klasik Arama'yı seçebilirsiniz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\SearchCompanion:DisableContent FileUpdates*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\İnternet İletişim Yönetimi\İnternet İletişimi ayarları\Arama Eşlikçisi içerik dosyası güncellemelerini kapat*

**Not:** Bu Grup İlkesi yol, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu ICM.admx/adml tarafından sağlanır.

**18.8.22.1.10 (L2) ''Baskı Siparişi Ver' resim görevini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, "Çevrimiçi Baskı Siparişi Ver" görevinin Windows klasörlerindeki Resim Görevleri'nden kullanılabilir olup olmadığını belirtir. Çevrimiçi Baskı Siparişi Sihirbazı, sağlayıcıların bir listesini indirmek ve kullanıcıların çevrimiçi baskı siparişi vermesini sağlamak için kullanılır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Kurumsal olarak yönetilen bir ortamda, bir kullanıcının bilmeden hassas verileri ifşa etme riskini azaltmak istiyoruz.

**Etki:**

"Çevrimiçi Baskı Siparişi Ver" görevi, Dosya Gezgini klasörlerindeki Resim Görevleri'nden kaldırıldı.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore r:NoOnlinePrintsWizard*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Sistem\İnternet İletişim Yönetimi\İnternet İletişimi ayarları\"Baskıları Sipariş Et" resim görevini kapatın*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu ICM.admx/adml tarafından sağlanır.

**18.8.22.1.11 (L2) 'Dosya ve klasörler için 'Web'de Yayınla' görevini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Bu dosyayı Web'de Yayınla, Bu klasörü Web'de Yayınla ve Seçili öğeleri Web'de Yayımla görevlerinin Windows klasörlerindeki Dosya ve Klasör Görevleri'nden kullanılabilir olup olmadığını belirtir. Web Yayımlama sihirbazı, sağlayıcıların bir listesini indirmek ve kullanıcıların Web'de içerik yayınlamasına izin vermek için kullanılır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Kullanıcılar, kuruluşun kontrolü dışında bir kamu hizmetine gizli veya hassas bilgiler yayınlayabilir.

**Etki:**

"Web'de Yayınla" görevi, Windows klasörlerindeki Dosya ve Klasör görevlerinden kaldırıldı.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore r:NoPublishingWizard*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Sistem\İnternet İletişim Yönetimi\İnternet İletişimi ayarları\Dosyalar ve klasörler için "Web'de Yayınla" görevini kapatın*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinin öğelerde bulunan Grup İlkesi şablonu ICM.admx/adml tarafından sağlanır.

**18.8.22.1.12 (L2) 'Windows Messenger Müşteri Deneyimini Geliştirme Programı'nı kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows Müşteri Deneyimini Geliştirme Programının Windows'un nasıl kullanıldığı hakkında anonim bilgiler toplayıp toplayamayacağını belirtir. Microsoft, Windows Müşteri Deneyimini Geliştirme Programı aracılığıyla toplanan bilgileri en çok kullanılan özellikleri geliştirmek ve kusurları tespit etmek ve böylece daha hızlı düzeltilebilmelerini sağlamak için kullanır. Bu ayarın etkinleştirilmesi, Microsoft'un bu amaçla toplayabildiği veri miktarını azaltacaktır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Büyük kurumsal yönetilen ortamlar, Microsoft tarafından yönetilen istemci bilgisayarlardan toplanan bilgilere sahip olmak istemeyebilir.

**Etki:**

Windows Messenger, kullanım bilgilerini toplamaz ve kullanım bilgilerinin toplanmasını sağlayan kullanıcı ayarları gösterilmez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Messenger\Client:CEIP*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları \System\Internet Communication Management\Internet Communication settings\Windows Messenger Müşteri Deneyimi Geliştirme Programını kapatın*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu ICM.admx/adml tarafından sağlanır.

**18.8.22.1.13 (L2) 'Windows Müşteri Deneyimini Geliştirme Programını Kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows Messenger'ın Windows Messenger yazılımının ve hizmetinin nasıl kullanıldığı hakkında anonim bilgiler toplayıp toplayamayacağını belirtir. Microsoft, Windows Müşteri Deneyimini Geliştirme Programı aracılığıyla toplanan bilgileri, yazılım kusurlarını algılamak için kullanır, böylece daha hızlı düzeltilebilirler; bu ayarın etkinleştirilmesi, Microsoft'un bu amaçla toplayabildiği veri miktarını azaltacaktır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Büyük kurumsal yönetilen ortamlar, Microsoft tarafından yönetilen istemci bilgisayarlardan toplanan bilgilere sahip olmak istemeyebilir.

**Etki:**

Tüm kullanıcılar, Windows Müşteri Deneyimini Geliştirme Programından çıkarıldı.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\SQMClient\Windows:CEIPEnable*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları \System\Internet Communication Management\Internet Communication settings\Windows Müşteri Deneyimi Geliştirme Programını Kapat*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu ICM.admx/adml tarafından sağlanır.

**18.8.22.1.14 (L2) 'Windows Hata Bildirimini Kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, hataların Microsoft'a bildirilip bildirilmeyeceğini denetler. Hata Raporlama, başarısız olan veya yanıt vermeyi durduran bir sistem veya uygulama hakkındaki bilgileri bildirmek için kullanılır ve ürünün kalitesini artırmak için kullanılır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Güvenli, kurumsal yönetilen bir ortamda bir Windows Hatası oluşursa, sorun giderme ve düzeltme için hata doğrudan BT personeline bildirilmelidir. Bu hataları doğrudan Microsoft'a bildirmenin şirkete hiçbir faydası yoktur ve hatanın bir parçası olarak hassas verilerin bilmeden açığa çıkma riski vardır.

**Etki:**

Kullanıcılara hataları Microsoft'a bildirme seçeneği verilmez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Error Reporting : Disabled*

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\PCHealth\ErrorReporting:DoReport*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\İnternet İletişim Yönetimi\İnternet İletişimi ayarları\Windows Hata Bildirimini Kapat*

**Not:** Bu Grup İlkesi yolu Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu ICM.admx/adml tarafından sağlanır

**18.8.23 iSCSI**

**18.8.24** **KDC**

**18.8.25 Kerberos**

**18.8.25.1 (L2) 'Sertifika kullanarak cihaz kimlik doğrulamasını destekle' seçeneği 'Etkin: Otomatik' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Kerberos'un etki alanına yönelik cihaz sertifikasını kullanarak kimlik doğrulama girişiminde bulunma desteğini ayarlamanıza olanak tanır. Sertifika kullanarak cihaz kimlik doğrulaması desteği, bilgisayar hesapları için sertifika kimlik doğrulamasını destekleyen cihaz hesabı etki alanındaki bir DC'ye bağlantı gerektirir. Bu ayar için önerilen durum: Etkin: Otomatik.

**Gerekçe:**

Sertifikaların kullanımıyla daha güçlü cihaz kimlik doğrulamasına sahip olmak, standart kullanıcı adı ve parola doğrulaması yerine şiddetle tavsiye edilir. Bunun Otomatik olarak ayarlanması, mümkün olduğunda sertifika tabanlı kimlik doğrulamanın kullanılmasına izin verir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumları tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System\ kerberos\parameters:DevicePKInitBehavior*

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\Current\Parameters\Policies System\ kerberos\parameters:DevicePKInitEnabled*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Otomatik:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Kerberos\Support cihaz kimlik doğrulaması sertifika kullanılarak*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir . Microsoft Windows 10 RTM (Sürüm 1507) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu Kerberos.admx/adml tarafından sağlanır.

**18.8.26 Çekirdek DMA Koruması**

**18.8.26.1 (BL) 'Çekirdek DMA Koruması ile uyumlu olmayan harici cihazlar için numaralandırma politikası' seçeneği 'Etkin: Tümünü engelle' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu politika, harici DMA özellikli cihazlara karşı ek güvenlik sağlamayı amaçlamaktadır. DMA Yeniden Eşleme/cihaz bellek izolasyonu ve korumalı alan ile uyumlu olmayan harici DMA özellikli cihazların sayımı üzerinde daha fazla kontrole izin verir. Bu ayar için önerilen durum: Etkin: Tümünü Engelle.

**Not**: Bu politika 1394, PCMCIA veya ExpressCard cihazları için geçerli değildir. Koruma ayrıca yalnızca Windows 10 R1803 veya üstü için geçerlidir ve çalışması için bir UEFI BIOS gerektirir.

**Not #2:** Bu özellikle ilgili daha fazla bilgiyi şu bağlantıda bulabilirsiniz: [Thunderbolt™ 3 için Çekirdek DMA Koruması (Windows 10) | Microsoft Belgeleri](https://docs.microsoft.com/en-us/windows/security/information-protection/kernel-dma-protection-for-thunderbolt).

**Gerekçe:**

Aygıt belleği korumalı alanı, işletim sisteminin, çevre birimi tarafından izinsiz G/Ç'yi veya bellek erişimini engellemek için bir aygıtın G/Ç Bellek Yönetim Birimi'nden (IOMMU) yararlanmasına olanak tanır.

**Etki:**

DMA yeniden eşleme ile uyumlu olmayan harici cihazlar numaralandırılmayacak ve kullanıcı başarılı bir şekilde oturum açmadıkça ve kullanıcı oturumunun kilidi açılmadıkça/ana kadar çalışmayacaktır. Numaralandırıldıktan sonra, bu cihazlar, oturumun durumu ne olursa olsun çalışmaya devam edecektir. DMA yeniden eşleme ile uyumlu cihazlar, cihaz hafızası izole edilmiş olarak hemen numaralandırılacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Kernel DMA Protection:DeviceEnumerationPolicy*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Etkin: Tümünü Engelle:

*Bilgisayar Yapılandırması olarak ayarlayın Çekirdek DMA Koruması ile uyumlu olmayan harici cihazlar için \Policies\Administrative Templates\System\Kernel DMA Protection\Numaralandırma ilkesi*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1809 ve Sunucu 2019 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu DmaGuard.admx/adml tarafından sağlanır.

**18.8.27 Yerel Hizmetler**

**18.8.27.1 (L2) 'Oturum açma için kullanıcı giriş yöntemlerinin sistem hesabına kopyalanmasına izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu politika, oturum açma ekranında kullanılmak üzere kullanıcı giriş yöntemlerinin sistem hesabına otomatik olarak kopyalanmasını engeller. Kullanıcı, sistem hesabında etkinleştirilen bir dizi giriş yöntemiyle sınırlıdır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bu, sistem hesabının güvenliğini artırmanın bir yoludur.

**Etki:**

Kullanıcılar, oturum açma sayfasında sistem hesabı için etkinleştirilmiş giriş yöntemlerine sahip olacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\ControlPanel\International:BlockUserInputMethodsForSignIn*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Yerel Hizmetler\Oturum açmak için kullanıcı giriş yöntemlerinin sistem hesabına kopyalanmasına izin verme*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu Globalization.admx/adml tarafından sağlanır.

**18.8.28 Oturum açma**

**18.8.28.1 (L1) 'Kullanıcının oturum açarken hesap ayrıntılarını göstermesini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu politika, kullanıcının oturum açma ekranında hesap ayrıntılarını (e-posta adresi veya kullanıcı adı) göstermesini engeller. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Konsola erişimi olan bir saldırgan (örneğin, fiziksel erişimi olan veya iş istasyonuna Uzak Masaüstü Hizmetleri aracılığıyla bağlanabilen biri), sunucuda oturum açan son kullanıcının adını görüntüleyebilir. Saldırgan daha sonra parolayı tahmin etmeye çalışabilir, bir sözlük kullanabilir veya oturum açmayı denemek için bir kaba kuvvet saldırısı kullanabilir.

**Etki:**

Kullanıcılar, oturum açma ekranında hesap ayrıntılarını göstermeyi seçemez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:BlockUserFromSh owingAccountDetailsOnSignin*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Oturum Açma\Kullanıcının oturum açarken hesap ayrıntılarını göstermesini engelle*

**Not**: Bu Grup İlkesi yolu varsayılan olarak var. Microsoft Windows 10 Sürüm 1607 ve Server 2016 Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu Logon.admx/adml tarafından sağlanır.

**18.8.28.2 (L1) 'Ağ seçimi kullanıcı arayüzünü görüntüleme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, oturum açma ekranında herhangi birinin kullanılabilir ağ kullanıcı arabirimiyle etkileşime girip giremeyeceğini denetlemenize olanak tanır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Yetkisiz bir kullanıcı, bilgisayarın ağ bağlantısını kesebilir veya bilgisayarı Windows'ta oturum açmadan diğer kullanılabilir ağlara bağlayabilir.

**Etki:**

Bilgisayarın ağ bağlantı durumu, Windows'ta oturum açmadan değiştirilemez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:DontDisplayNetw orkSelectionUI*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\System\Logon\Ağ seçimi kullanıcı arabirimini görüntüleme*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.1 ve Server 2012 R2 Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu Logon.admx/adml tarafından sağlanır.

**18.8.28.3 (L1) 'Etki alanına katılmış bilgisayarlarda bağlı kullanıcıları numaralandırma' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bağlı kullanıcıların etki alanına katılmış bilgisayarlarda numaralandırılmasını engeller. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Kötü niyetli bir kullanıcı, diğer kullanıcıların hesap adlarını toplamak için bu özelliği kullanabilir, bu bilgiler daha sonra parola tahmin etme veya sosyal mühendislik gibi diğer saldırı türleri ile birlikte kullanılabilir. Bu önlemin değeri küçüktür, çünkü etki alanı kimlik bilgilerine sahip bir kullanıcı, diğer yöntemleri kullanarak aynı hesap bilgilerini toplayabilir.k

**Etki:**

Oturum Açma Kullanıcı Arabirimi, etki alanına katılmış bilgisayarlarda herhangi bir bağlı kullanıcıyı numaralandırmayacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:DontEnumerateCo nnectedUsers*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\System\Logon\Etki alanına katılmış bilgisayarlarda bağlı kullanıcıları numaralandırma*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu Logon.admx/adml tarafından sağlanır.

**18.8.28.4 (L1) 'Etki alanına katılmış bilgisayarlarda yerel kullanıcıları numaralandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, etki alanına katılmış bilgisayarlarda yerel kullanıcıların numaralandırılmasına olanak tanır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe**:

Kötü niyetli bir kullanıcı, diğer kullanıcıların hesap adlarını toplamak için bu özelliği kullanabilir, bu bilgiler daha sonra parola tahmin etme veya sosyal mühendislik gibi diğer saldırı türleri ile birlikte kullanılabilir. Bu önlemin değeri küçüktür, çünkü etki alanı kimlik bilgilerine sahip bir kullanıcı, diğer yöntemleri kullanarak aynı hesap bilgilerini toplayabilir.

**Etki**:

Yok - bu varsayılan davranıştır.

**Denetim**: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:EnumerateLocalU sers*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki kullanıcı arabirimi yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\System\Logon\Enumerate etki alanına katılmış bilgisayarlarda yerel kullanıcıları numaralandır*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu Logon.admx/adml tarafından sağlanır.

**18.8.28.5 (L1) 'Kilit** **ekranında uygulama bildirimlerini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, uygulama bildirimlerinin kilit ekranında görünmesini engellemenize olanak tanır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Uygulama bildirimleri, hassas iş veya kişisel verileri görüntüleyebilir.

**Etki:**

Kilit ekranında hiçbir uygulama bildirimi görüntülenmiyor.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:DisableLockScre enAppNotifications*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\System\Logon\Kilit ekranında uygulama bildirimlerini kapat*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu Logon.admx/adml tarafından sağlanır.

**18.8.28.6 (L1) 'Resimli şifre ile oturum açmayı kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir etki alanı kullanıcısının resimli parola kullanarak oturum açıp açamayacağını denetlemenize olanak tanır. Bu ayar için önerilen durum: Etkin.

**Not**: Resimli parola özelliğine izin veriliyorsa, kullanıcının etki alanı parolası, kullanım sırasında sistem kasasında önbelleğe alınır.

**Gerekçe**:

Resimli parolalar, yazılan karmaşık parola gereksinimini atlar. Paylaşılan bir çalışma ortamında, birinin ekrandaki hareketleri gözlemlediği basit bir omuz sörfü, o kişinin karmaşık şifreyi bilmesine gerek kalmadan sisteme erişmesine izin verir. Görüntülü dikey monitör ekranları, yatay tuş vuruşlarından çok daha uzaktan görülebilir, bu da fare hareketlerinin başarılı bir şekilde gözlemlenme olasılığını artırır.

**Etki**:

Kullanıcılar bir resimli parola ile kurulum yapamayacak veya oturum açamayacak.

**Denetim**:

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:BlockDomainPict urePassword*

**Düzeltme**:

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Oturum Açma\Resimli parola oturum açma*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu CredentialProviders.admx/adml tarafından sağlanır.

**18.8.28.7 (L1) 'Kolay PIN ile oturum açmayı aç' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir etki alanı kullanıcısının bir kolaylık PIN'i kullanarak oturum açıp açamayacağını denetlemenize olanak tanır. Windows 10'da kolaylık PIN'i, daha güçlü güvenlik özelliklerine sahip olan Passport ile değiştirildi. Passport'u etki alanı kullanıcıları için yapılandırmak için Bilgisayar Yapılandırması\Yönetim Şablonları\Windows Bileşenleri\Microsoft Passport for Work altındaki ilkeleri kullanın. Not: Bu özelliği kullanırken kullanıcının etki alanı parolası sistem kasasında önbelleğe alınır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe**:

Bir PIN, bir paroladan çok daha küçük bir karakter seçiminden oluşturulur, bu nedenle çoğu durumda bir PIN, bir paroladan çok daha az sağlam olacaktır.

**Etki**:

Yok - bu varsayılan davranıştır.

**Denetim**:

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:AllowDomainPINL ogon*

**Düzeltme**:

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Oturum Açma\Uygunluğu aç PIN oturum açma*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir . Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu CredentialProviders.admx/adml tarafından sağlanır.

**Not #2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta PIN ile oturum açmayı aç olarak adlandırılmıştı, ancak Windows 10 Sürüm 1511 Yönetim Şablonlarından başlayarak yeniden adlandırıldı.

**18.8.29 Azaltma Seçenekleri**

**18.8.30 Net Oturum Açma**

**18.8.31 İşletim Sistemi Politikaları**

**18.8.31.1 (L2) 'Cihazlar arasında Pano senkronizasyonuna izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, Pano içeriğinin cihazlar arasında senkronize edilip edilemeyeceğini belirler. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Yüksek güvenlikli ortamlarda, pano verileri sistemde yerel kalmalı ve yerel olarak bulunması gereken çok hassas bilgiler içerebileceğinden cihazlar arasında eşitlenmemelidir.

**Etki**:

Pano içeriği diğer cihazlarla paylaşılamaz.

**Denetim**:

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:AllowCrossDevic eClipboard*

**Düzeltme**:

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\OS Politikaları\Cihazlar arasında Pano senkronizasyonuna izin ver*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1809 ve Sunucu 2019 Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu OPolicy.admx/adml tarafından sağlanır.

**18.8.31.2 (L2) 'Kullanıcı Etkinliklerinin yüklenmesine izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, yayınlanan Kullanıcı Faaliyetlerinin buluta yüklenip yüklenemeyeceğini belirler. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe**:

Gizlilik endişeleri nedeniyle, bu veriler hassas bilgiler içerebileceğinden, veriler hiçbir zaman 3. şahıslara gönderilmemelidir.

**Etki**:

Kullanıcı Etkinliği türündeki etkinliklerin buluta yüklenmesine izin verilmez. Zaman Çizelgesi özelliği, cihazlar arasında çalışmayacaktır.

**Denetim**:

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:UploadUserActiv ities*

**Düzeltme**:

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\System\OS Policies\Kullanıcı Faaliyetlerinin yüklenmesine izin ver*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1803 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu OPolicy.admx/adml tarafından sağlanır.

**18.8.32 Performans Kontrol Paneli**

**18.8.33 PIN Karmaşıklığı**

**18.8.34 Güç Yönetimi**

**18.8.34.1 Düğme Ayarları**

**18.8.34.2 Enerji Tasarrufu Ayarları**

**18.8.34.3 Sabit Disk Ayarları**

**18.8.34.4 Bildirim Ayarları**

**18.8.34.5 Güç Azaltma Ayarları**

**18.8.34.6 Uyku Ayarları**

**18.8.34.6.1 (L1) 'Bağlı bekleme sırasında ağ bağlantısına izin ver (pilde)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, modern bekleme özellikli sistemlerde bekleme modunda ağ bağlantı durumunu denetlemenize olanak tanır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe**:

Bu ayarın devre dışı bırakılması, bilgisayarın gözetimsiz bırakıldığında, pille ve uyku durumundayken WLAN ağı üzerinden saldırganlar tarafından erişilebilir olmamasını sağlar.

**Etki**:

Bekleme modunda (pille çalışırken) ağ bağlantısı garanti edilmez. Bu bağlantı kısıtlaması şu anda yalnızca WLAN ağları için geçerlidir, ancak değişebilir (Microsoft'a göre).

**Denetim**:

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\f15576e8- 98b7-4186-b944-eafa664402d9:DCSettingIndex*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Güç Yönetimi\Uyku Ayarları\Bağlı bekleme (pille) sırasında ağ bağlantısına izin ver*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1607 ve Server 2016 Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu Power.admx/adml tarafından sağlanır.

**18.8.34.6.2 (L1) 'Bağlı bekleme sırasında ağ bağlantısına izin ver (prize takılı)' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, modern bekleme özellikli sistemlerde bekleme modunda ağ bağlantı durumunu denetlemenize olanak tanır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe**:

Bu ayarın devre dışı bırakılması, bilgisayarın gözetimsiz, takılı ve uyku durumundayken WLAN ağı üzerinden saldırganlar tarafından erişilebilir olmamasını sağlar.

**Etki**:

Bekleme modundayken (takılıyken) ağ bağlantısı garanti edilmez. Bu bağlantı kısıtlaması şu anda yalnızca WLAN ağları için geçerlidir, ancak değişebilir (Microsoft'a göre).

**Denetim**:

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\f15576e8- 98b7-4186-b944-eafa664402d9:ACSettingIndex*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu ayarlayın Devre Dışı Bırakıldı:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Güç Yönetimi\Uyku Ayarları\Bağlı bekleme sırasında ağ bağlantısına izin ver (takılı)*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1607 ve Server 2016 Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu Power.admx/adml tarafından sağlanır.

**18.8.34.6.3 (BL) 'Uyurken (pilde) bekleme durumlarına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, modern bekleme özellikli sistemlerde bekleme modunda ağ bağlantı durumunu denetlemenize olanak tanır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bu ayarın devre dışı bırakılması, bilgisayarın gözetimsiz, takılı ve uyku durumundayken WLAN ağı üzerinden saldırganlar tarafından erişilebilir olmamasını sağlar.

**Etki**: Bekleme modundayken (takılıyken) ağ bağlantısı garanti edilmez. Bu bağlantı kısıtlaması şu anda yalnızca WLAN ağları için geçerlidir, ancak değişebilir (Microsoft'a göre).

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\f15576e8- 98b7-4186-b944-eafa664402d9:ACSettingIndex*

**Düzeltme**:

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu ayarlayın Devre Dışı Bırakıldı:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Güç Yönetimi\Uyku Ayarları\Bağlı bekleme sırasında ağ bağlantısına izin ver (takılı)*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1607 ve Server 2016 Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu Power.admx/adml tarafından sağlanır.

**18.8.34.6.4 (BL) 'Uyurken bekleme durumlarına izin ver (S1-S3))' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bilgisayarı uyku durumuna geçirirken Windows'un bekleme durumlarını kullanmasına izin verilip verilmeyeceğini yönetir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe**:

Sistem uyku durumları (S1-S3), BitLocker birim şifreleme anahtarı gibi sırlar içerebilen RAM'e güç sağlar. Uyku durumundaki bir bilgisayarı (S1-S3) bulan bir saldırgan, bilgisayarın belleğine doğrudan saldırabilir ve RAM anımsatma ve doğrudan bellek erişimi (DMA) gibi tekniklerle sırlara erişebilir.

**Etki**:

Kullanıcılar, takılıyken Uyku (S3) özelliğini kullanamayacak ve bu, Hazırda Bekletme'den (S4) daha hızlı devam etmektedir.

**Denetim**:

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\abfc2519- 3608-4c2a-94ea-171b0ed546ab:ACSettingIndex*

**Düzeltme**:

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Güç Yönetimi\Uyku Ayarları\Uykudayken (fiş takılıyken) bekleme durumlarına izin ver (S1-S3)*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu Power.admx/adml tarafından sağlanır.

**18.8.34.6.5 (L1) 'Bilgisayar uyandığında (pille olduğunda) parola iste' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bilgisayarı uyku durumuna geçirirken Windows'un bekleme durumlarını kullanmasına izin verilip verilmeyeceğini yönetir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Sistem uyku durumları (S1-S3), BitLocker birim şifreleme anahtarı gibi sırlar içerebilen RAM'e güç sağlar. Uyku durumundaki bir bilgisayarı (S1-S3) bulan bir saldırgan, bilgisayarın belleğine doğrudan saldırabilir ve RAM anımsatma ve doğrudan bellek erişimi (DMA) gibi tekniklerle sırlara erişebilir.

**Etki:**

Kullanıcılar, takılıyken Uyku (S3) özelliğini kullanamayacak ve bu, Hazırda Bekletme'den (S4) daha hızlı devam etmektedir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\abfc2519- 3608-4c2a-94ea-171b0ed546ab:ACSettingIndex*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Güç Yönetimi\Uyku Ayarları\Uykudayken (fiş takılıyken) bekleme durumlarına izin ver (S1-S3)*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu Power.admx/adml tarafından sağlanır**.**

**18.8.34.6.6 (L1) 'Bilgisayar uyandığında parola iste (prize takılı)' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Sistem uyku modundan çıktığında kullanıcıdan parola istenip istenmeyeceğini belirtir. Bu ayar için önerilen durum: Etkin.

**Gerekçe**:

Bu ayarın etkinleştirilmesi, gözetimsiz bir bilgisayarı uyku durumundan uyandıran herkesin sisteme erişmeden önce oturum açma kimlik bilgilerini sağlamasını sağlar.

**Etki**:

Yok - bu varsayılan davranıştır.

**Denetim**:

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Power\PowerSettings\0e796bdb 100d-47d6-a2d5-f7d2daa51f51:ACSettingIndex*

**Düzeltme:**

GP yolu aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki kullanıcı arabirimini ayarlayın Etkinleştirildi:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Güç Yönetimi\Uyku Ayarları\Bilgisayar uyandığında (takılı) parola iste*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu Power.admx/adml tarafından sağlanır.

**18.8.35 Kurtarma**

**18.8.36 Uzaktan Yardım**

**18.8.36.1 (L1) 'Uzaktan Yardım Teklifini Yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bu bilgisayarda Teklif (İstenmeyen) Uzaktan Yardım'ı açmanıza veya kapatmanıza olanak tanır. Yardım masası ve destek personeli, kullanıcı yardım taleplerine yanıt verebilmelerine rağmen proaktif olarak yardım sunamayacaktır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bir kullanıcı kandırılabilir ve kötü niyetli bir kullanıcıdan istenmeyen bir Uzaktan Yardım teklifini kabul edebilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fAllowUnsolicited*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Uzaktan Yardım\Yapılandır Teklifi Uzaktan Yardım*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu RemoteAssistance.admx/adml tarafından sağlanır.

**18.8.36.2 (L1) 'İstenen Uzaktan Yardımı Yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bu bilgisayarda İstenen (İsteyin) Uzaktan Yardım'ı açmanıza veya kapatmanıza olanak tanır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe**:

Hileli bir yöneticinin başka bir kullanıcının masaüstü oturumuna erişme riski çok düşüktür, ancak bir kullanıcının bilgisayarına habersiz bağlanamaz veya kullanıcının izni olmadan bilgisayarı kontrol edemezler. Bir uzman bağlanmaya çalıştığında, kullanıcı yine de bağlantıyı reddetmeyi veya uzmana yalnızca görüntüleme ayrıcalıkları vermeyi seçebilir. Uzmanın iş istasyonunu uzaktan kontrol etmesine izin vermek için kullanıcının açıkça Evet düğmesini tıklaması gerekir.

**Etki**:

Bu bilgisayardaki kullanıcılar, birinden yardım istemek için e-posta veya dosya aktarımını kullanamaz. Ayrıca, kullanıcılar bu bilgisayara bağlantılara izin vermek için anlık ileti programlarını kullanamazlar.

**Denetim**:

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fAllowToGetHelp*

**Düzeltme**:

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\ Yönetim Şablonları\Sistem\Uzaktan Yardım\İstenen Uzaktan Yardımı Yapılandır*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu RemoteAssistance.admx/adml tarafından sağlanır**.**

**18.8.37 Uzaktan Prosedür Çağrısı (RPC)**

**18.8.37.1 (L1) 'RPC Endpoint Eşleştiricisi İstemci Kimlik Doğrulamasını Etkinleştir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, RPC istemcilerinin yaptıkları arama kimlik doğrulama bilgilerini içerdiğinde Uç Nokta Eşleyici Hizmeti ile kimlik doğrulaması yapıp yapmayacağını denetler. Windows NT4 çalıştıran bilgisayarlarda (tüm hizmet paketleri) Uç Nokta Eşleyici Hizmeti, bu şekilde sağlanan kimlik doğrulama bilgilerini işleyemez. Bu ilke ayarı, güvenilen etki alanı DC'lerine uygulanırsa (bkz. [Microsoft KB3073942](https://support.microsoft.com/en-us/kb/3073942)) tek yönlü orman güvenleriyle ilgili belirli bir soruna neden olabilir, bu nedenle Etki Alanı Denetleyicilerine uygulanmasını önermiyoruz. Not: Bu politika, sistem yeniden başlatılıncaya kadar geçerli olmayacaktır. Bu ayar için önerilen durum: Etkin.

**Gerekçe**:

RPC hizmetlerine anonim erişim, bilgilerin kimliği doğrulanmamış kullanıcılara yanlışlıkla ifşa edilmesine neden olabilir.

**Etki**:

RPC istemcileri, kimlik doğrulama bilgileri içeren çağrılar için Uç Nokta Eşleyici Hizmeti'nde kimlik doğrulaması yapacaktır. Bu tür aramaları yapan istemciler, Windows NT4 Server Endpoint Mapper Service ile iletişim kuramaz.

**Denetim**:

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsNT\Rpc:EnableAuthEpResolution*

**Düzeltme**:

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\System\Uzaktan Yordam Çağrısı\RPC Bitiş Noktası Eşleştiricisi İstemci Kimlik Doğrulamasını Etkinleştir*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu RPC.admx/adml tarafından sağlanır.

**18.8.37.2 (L1) 'Kimliği Doğrulanmamış RPC istemcilerini kısıtla' seçeneği 'Etkin: Kimliği Doğrulanmış' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, RPC sunucusu çalışma zamanının, RPC sunucularına bağlanan kimliği doğrulanmamış RPC istemcilerini nasıl işlediğini denetler. Bu ilke ayarı, tüm RPC uygulamalarını etkiler. Etki alanı ortamında bu ilke ayarı, grup ilkesi işlemenin kendisi de dahil olmak üzere çok çeşitli işlevleri etkileyebileceğinden dikkatli kullanılmalıdır. Bu ilke ayarında yapılan bir değişikliği geri almak, etkilenen her makinede manuel müdahale gerektirebilir. Bu ilke ayarı asla bir Etki Alanı Denetleyicisine uygulanmamalıdır. Bir istemci, sunucuyla iletişim kurmak için adlandırılmış bir kanal kullanıyorsa veya RPC Güvenliği kullanıyorsa kimliği doğrulanmış istemci olarak kabul edilecektir. Kimliği doğrulanmamış istemciler tarafından özellikle erişilebilir olmayı talep eden RPC Arabirimleri, bu ilke ayarı için seçilen değere bağlı olarak bu kısıtlamadan muaf olabilir. -- "Yok", tüm RPC istemcilerinin, ilke ayarının uygulandığı makinede çalışan RPC Sunucularına bağlanmasına izin verir. -- "Kimliği doğrulanmış", yalnızca kimliği doğrulanmış RPC İstemcilerinin (yukarıdaki tanıma göre) ilke ayarının uygulandığı makinede çalışan RPC Sunucularına bağlanmasına izin verir. Muafiyetler, onları talep eden arayüzlere verilir. -- "İstisnasız kimlik doğrulaması", yalnızca kimliği doğrulanmış RPC İstemcilerinin (yukarıdaki tanıma göre) ilke ayarının uygulandığı makinede çalışan RPC Sunucularına bağlanmasına izin verir. İstisnalara izin verilmez. Bu değerin ciddi sorunlara yol açma potansiyeli vardır ve tavsiye edilmez. Not: Bu ilke ayarı, sistem yeniden başlatılıncaya kadar uygulanmayacaktır. Bu ayar için önerilen durum: Etkinleştirildi: Kimliği doğrulandı.

**Gerekçe**: Kimliği doğrulanmamış RPC iletişimi bir güvenlik açığı oluşturabilir.

**Etki**:

Yok - bu varsayılan davranıştır.

**Denetim**:

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsNT\Rpc:RestrictRemoteClients*

**Düzeltme**:

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki kullanıcı arabirimi yolunu Etkin olarak ayarlayın: Doğrulanmış:

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Sistem\Uzak Yordam Çağrısı\Kimliği Doğrulanmamış RPC istemcilerini Kısıtla*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu RPC.admx/adml tarafından sağlanır.

**18.8.38 Çıkarılabilir Depolama Birimi Erişimi**

**18.8.39 Komut Dosyaları**

**18.8.40 Güvenlik Hesabı Yöneticisi**

**18.8.41 Sunucu Yöneticisi**

**18.8.42 Hizmet Denetim Yöneticisi Ayarları**

**18.8.43** **Kapatma**

**18.8.44 Kapatma Seçenekleri**

**18.8.45 Depolama Sağlığı**

**18.8.46 Akıllı** **Depolama**

**18.8.47 Sistem Geri Yükleme**

**18.8.48 Sorun Giderme ve Tanılama**

**18.8.48.1 Uygulama** **Uyumluluğu Tanılaması**

**18.8.48.2 Bozuk Dosya Kurtarma**

**18.8.48.3 Disk Tanılama**

**18.8.48.4 Hataya Dayanıklı Yığın**

**18.8.48.5 Microsoft Destek Tanılama**

**Araç 18.8.48.5.1 (L2) 'Microsoft Destek Tanılama Aracı: Destek sağlayıcısıyla MSDT etkileşimli iletişimini aç' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, destek sağlayıcı ile Microsoft Destek Tanılama Aracı (MSDT) etkileşimli iletişimini yapılandırır. MSDT, destek uzmanları tarafından analiz edilmek üzere tanılama verilerini toplar. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe**:

Gizlilik endişeleri nedeniyle, bu veriler hassas bilgiler içerebileceğinden, veriler hiçbir zaman 3. şahıslara gönderilmemelidir.

**Etki**:

MSDT, destek modunda çalışamaz ve destek sağlayıcısına hiçbir veri toplanamaz veya gönderilemez.

**Denetim**:

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\ScriptedDiagnosticsPro vider\Policy:DisableQueryRemoteServer*

**Düzeltme**:

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Sorun Giderme ve Tanılama\Microsoft Destek Tanı Aracı\Microsoft Destek Tanı Aracı: İle MSDT etkileşimli iletişimini açın destek sağlayıcı*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu MSDT.admx/adml tarafından sağlanır.

**18.8.48.6 MSI Bozuk Dosya Kurtarma**

**18.8.48.7 Planlı Bakım**

**18.8.48.8 Yazılı Tanılama**

**18.8.48.9 Windows Önyükleme Performansı Tanılama**

**18.8.48.10 Windows Bellek Sızıntısı Teşhisi**

**18.8.48.11 Windows Performans (PerfTrack)**

**18.8.48.11.1 (L2) 'PerfTrack'i Etkinleştir/Devre Dışı Bırak' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, yanıt verme olaylarının izlenmesinin etkinleştirilip etkinleştirilmeyeceğini belirtir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Etkinleştirildiğinde, belirli bir olayın toplu verileri Microsoft'a iletilecektir. Bu özelliği belirli bir kullanıcı için kısıtlama, izin düzeyini ayarlama ve hata raporlarının gönderilebileceği belirli programları belirleme seçeneği mevcuttur. Ancak, yetkisiz veya istenmeyen kullanım, veri sızıntısı veya kasıtsız iletişim potansiyelini sınırlamak için PerfTrack'i yürütme yeteneğinin merkezi olarak kısıtlanması şiddetle önerilir.

**Etki**:

Duyarlılık olayları işlenmez.

**Denetim**:

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WDI\{9c5a40da-b965- 4fc3-8781-88dd50a6299d}:ScenarioExecutionEnabled*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Sorun Giderme ve Tanılama\Windows Performansı PerfTrack\PerfTrack'i Etkinleştir/Devre Dışı Bırak*

**Not**: Bu Grup İlkesi yolu varsayılan olarak var. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan PerformancePerftrack.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.8.49 Güvenilir Platform Modülü Hizmetleri**

**18.8.50 Kullanıcı Profiller**i

**18.8.50.1 (L2) 'Reklam kimliğini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, reklam kimliğini kapatarak uygulamaların, uygulamalar arasındaki deneyimler için kimliği kullanmasını engeller. Bu ayar için önerilen durum: Etkin.

**Gerekçe**:

Reklam amaçlı, anonim olarak bile kullanıcı etkinliğini izlemek bir gizlilik endişesi olabilir. Kurumsal olarak yönetilen bir ortamda, uygulamaların hedeflenen reklamcılık için izlemeye ihtiyacı olmamalı veya bunu gerektirmemelidir.

**Etki:**

Reklam kimliği kapalı. Uygulamalar, uygulamalar arasındaki deneyimler için kimliği kullanamaz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\AdvertisingInfo:Disable edByGroupPolicy*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\Kullanıcı Profilleri\Reklam kimliğini kapatın*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.1 ve Server 2012 R2 Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu UserProfiles.admx/adml tarafından sağlanır.

**18.8.51 Windows Dosya Koruması**

**18.8.52 Windows HotStart**

**18.8.53 Windows Saati Hizmeti**

**18.8.53.1 Zaman Sağlayıcılar**

**18.8.53.1.1 (L2) 'Windows NTP İstemcisini Etkinleştir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows NTP İstemcisinin etkin olup olmadığını belirtir. Windows NTP İstemcisini etkinleştirmek, bilgisayarınızın bilgisayar saatini diğer NTP sunucularıyla senkronize etmesine olanak tanır. Üçüncü taraf bir zaman sağlayıcı kullanmaya karar verirseniz, bu hizmeti devre dışı bırakmak isteyebilirsiniz. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Dağıtılmış uygulamalar, kimlik doğrulama hizmetleri, çok kullanıcılı veritabanları ve günlük tutma hizmetleri dahil ancak bunlarla sınırlı olmamak üzere bir dizi hizmet ve güvenlik gereksinimi için güvenilir ve doğru bir zaman hesabı önemlidir. Bir NTP istemcisinin kullanımı (güvenli çalışma ile) işlevsel doğruluk sağlar ve güvenlikle ilgili olayları gözden geçirirken odak noktasıdır.

**Etki:**

Yerel bilgisayar saatini, zamanı NTP sunucularıyla senkronize edecek şekilde ayarlayabilirsiniz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\W32Time\TimeProviders\NtpClien t:Enabled*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Sistem\Windows Zaman Hizmeti\Zaman Sağlayıcıları\Windows NTP İstemcisini Etkinleştir*

**Not**: Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu W32Time.admx/adml tarafından sağlanır.

**18.8.53.1.2 (L2) 'Windows NTP Server'ı Etkinleştir' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows NTP Sunucusunun etkinleştirilip etkinleştirilmediğini belirlemenize olanak tanır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Hem Kerberos kimlik doğrulama zaman damgalarının hassasiyeti nedeniyle hem de doğru güvenlik günlüğünü sağlamak için kurumsal olarak yönetilen bir ortamda uygun zaman senkronizasyonunun yapılandırılması kritik derecede önemlidir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\W32Time\TimeProviders\NtpServe r:Enabled*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Sistem\Windows Zaman Hizmeti\Zaman Sağlayıcıları\Windows NTP Sunucusunu Etkinleştir*

**Not**: Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu W32Time.admx/adml tarafından sağlanır.

**18.9 Windows Bileşenleri**

**18.9.1 Active Directory Federasyon Hizmetleri**

**18.9.2 ActiveX Yükleyici Hizmeti**

**18.9.3 Windows 8 / 8.1 / 10'a özellikler ekleme (eski adıyla Windows Anytime Upgrade)**

**18.9.4 Uygulama Paketi Dağıtımı**

**18.9.4.1 (L2) 'Bir Windows uygulamasının uygulama verilerini kullanıcılar arasında paylaşmasına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bir Windows uygulamasının, uygulamayı yükleyen kullanıcılar arasında veri paylaşma yeteneğini yönetir. Veriler SharedLocal klasörü aracılığıyla paylaşılır. Bu klasör, Windows.Storage API aracılığıyla kullanılabilir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bir sistemin kullanıcıları, hassas verileri yanlışlıkla aynı sistemdeki diğer kullanıcılarla paylaşabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CurrentVersion\AppMode l\StateManager:AllowSharedLocalAppData*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Uygulama Paketi Dağıtımı\Bir Windows uygulamasının kullanıcılar arasında uygulama verilerini paylaşmasına izin verin*

**Not:** Bu Grup İlkesi path varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 RTM (Sürüm 1507) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu AppxPackageManager.admx/adml tarafından sağlanır.

**18.9.4.2 (L1) 'Yönetici olmayan kullanıcıların paketlenmiş Windows uygulamalarını yüklemesini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, Yönetici olmayan kullanıcıların Windows uygulama paketlerini yükleme yeteneğini yönetir. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Kurumsal olarak yönetilen bir ortamda uygulama kurulumları, son kullanıcılar tarafından değil, BT personeli tarafından merkezi olarak yönetilmelidir.

**Etki:**

Yönetici olmayan kullanıcılar, diğer ilkeler tarafından açıkça izin verilmedikçe Microsoft Store uygulama paketlerini yükleyemezler. Meşru kullanım için bir Microsoft Store uygulaması gerekiyorsa, bir Yöneticinin yüklemeyi Yönetici bağlamından gerçekleştirmesi gerekir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Appx:BlockNonAdminUserInstall

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki kullanıcı arabirimi yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\Windows Components\App Package Deployment\Yönetici olmayan kullanıcıların paketlenmiş Windows uygulamalarını yüklemesini engelle*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 2004 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu AppxPackageManager.admx/adml tarafından sağlanır.

**18.9.5 Uygulama Gizliliği**

**18.9.5.1 (L1) 'Sistem kilitliyken Windows uygulamalarının sesle etkinleştirilmesine izin ver' seçeneği 'Etkin: Reddetmeye Zorla' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, sistem kilitliyken Windows uygulamalarının sesle (uygulamalar ve Cortana) etkinleştirilip etkinleştirilemeyeceğini belirtir. Bu ayar için önerilen durum şudur: Etkin: Zorla Reddet.

**Gerekçe:**

Cihaz kilitliyken herhangi bir bilgisayar kaynağına erişime izin verilmemelidir.

**Etki:**

Kullanıcılar, bilgisayar kilitliyken uygulamaları etkinleştiremez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\AppPrivacy:LetAppsActi vateWithVoiceAboveLock*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Zorla Reddet:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Uygulama Gizliliği\Sistem kilitliyken Windows uygulamalarının sesle etkinleştirilmesine izin verin*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1903 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu AppPrivacy.admx/adml tarafından sağlanır.

**18.9.6 Uygulama çalışma zamanı**

**18.9.6.1 (L1) 'Microsoft hesaplarının isteğe bağlı olmasına izin ver' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, oturum açmak için bir hesap gerektiren Windows Mağazası uygulamaları için Microsoft hesaplarının isteğe bağlı olup olmadığını denetlemenize olanak tanır. Bu ilke yalnızca onu destekleyen Windows Mağazası uygulamalarını etkiler. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bu ayarın etkinleştirilmesi, bir kuruluşun Windows mağaza uygulamalarına erişirken Microsoft hesaplarını kullanmak yerine kurumsal kullanıcı hesaplarını kullanmasına olanak tanır. Bu, kuruluşa ilgili kimlik bilgileri üzerinde daha fazla kontrol sağlar. Microsoft hesapları merkezi olarak yönetilemez ve bu tür kurumsal kimlik bilgileri güvenlik ilkeleri bu hesaplara uygulanamaz, bu da Microsoft hesapları kullanılarak erişilen herhangi bir bilgiyi riske atabilir.

**Etki:**

Oturum açmak için genellikle bir Microsoft hesabı gerektiren Windows Mağazası uygulamaları, kullanıcıların bunun yerine bir kurumsal hesapla oturum açmasına olanak tanır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: MSAOptional*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Uygulama çalışma zamanı\Microsoft hesaplarının isteğe bağlı olmasına izin verin*

**Not:** Bu Grup İlkesi yolu, varsayılan. Microsoft Windows 8.1 ve Server 2012 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu AppXRuntime.admx/adml tarafından sağlanır.

**18.9.6.2 (L2) 'Barındırılan içerikten Windows Çalışma Zamanı API erişimi olan Evrensel Windows uygulamalarının başlatılmasını engelle.' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, doğrudan web içeriğinden Windows Runtime API erişimine sahip Microsoft Store uygulamalarının başlatılıp başlatılamayacağını denetler. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Windows API'sine doğrudan erişimi olan uygulamaları web'den engellemek, kötü amaçlı uygulamaların bir sistemde çalıştırılmasını engelleyebilir. Onaylı uygulamaları yalnızca sistem yöneticileri yüklemelidir.

**Etki:**

Bildirimin ApplicationContentUriRules bölümünde Windows Çalışma Zamanı API erişimi bildiren evrensel Windows uygulamaları başlatılamaz (bildirimde Windows Çalışma Zamanı API erişimi beyan etmeyen Evrensel Windows uygulamaları etkilenmeyecektir).

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: BlockHostedAppAccessWinRT*

**Düzeltme:** GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Uygulama çalışma zamanı\Barındırılan içerikten Windows Çalışma Zamanı API erişimiyle Evrensel Windows uygulamalarının başlatılmasını engelle.*

**Not:** Ayar uygulandıktan sonra yeniden başlatma gerekebilir.

**Not #2:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 RTM (Sürüm 1507) Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu AppXRuntime.admx/adml tarafından sağlanır.

**Not #3:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta barındırılan içerikten Windows Çalışma Zamanı API erişimi olan Windows Mağazası uygulamalarının başlatılmasını engelle olarak adlandırıldı, ancak Windows 10 Sürüm 1803 Yönetim Şablonlarından başlayarak yeniden adlandırıldı.

**18.9.7 Uygulama Uyumluluğu**

**18.9.8 Otomatik Oynatma Politikaları**

**18.9.8.1 (L1) 'Ses düzeyi olmayan cihazlar için Otomatik Oynatmaya İzin Verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kameralar veya telefonlar gibi MTP cihazları için Otomatik Kullan'a izin vermez. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Saldırgan, istemci bilgisayara veya bilgisayardaki verilere zarar verecek bir programı başlatmak için bu özelliği kullanabilir.

**Etki:**

Kamera veya telefon gibi MTP cihazları için Otomatik Kullan'a izin verilmeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Explorer:NoAutoplayfor nonVolume*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Otomatik Kullan İlkeleri\Birim olmayan aygıtlar için Otomatik Oynatmaya İzin Verme*

**Not**: Bu Grup İlkesi yolu mevcut olmayabilir varsayılan olarak. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu AutoPlay.admx/adml tarafından sağlanır.

**18.9.8.2 (L1) 'Otomatik Çalıştır için varsayılan davranışı ayarla' seçeneği 'Etkin: Otomatik çalıştırma komutu yürütme' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Otomatik Çalıştır komutları için varsayılan davranışı belirler. Otomatik çalıştırma komutları genellikle autorun.inf dosyalarında saklanır. Genellikle yükleme programını veya diğer rutinleri başlatırlar. Bu ayar için önerilen durum: Etkin: Herhangi bir otomatik çalıştırma komutu yürütme.

**Gerekçe:**

Windows Vista'dan önce, bir otomatik çalıştırma komutu içeren ortam eklendiğinde, sistem, kullanıcı müdahalesi olmadan programı otomatik olarak yürütür. Bu, kullanıcının bilgisi olmadan kod çalıştırılabileceğinden büyük bir güvenlik sorunu yaratır. Windows Vista ile başlayan varsayılan davranış, kullanıcıya autorun komutunun çalıştırılıp çalıştırılmayacağını sormaktır. Otomatik çalıştırma komutu, Otomatik Oynat iletişim kutusunda bir işleyici olarak gösterilir.

**Etki:**

AutoRun komutları tamamen devre dışı bırakılacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore r:NoAutorun*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Herhangi bir otomatik çalıştırma komutunu çalıştırmayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Otomatik Kullan İlkeleri\Otomatik Çalıştırma için varsayılan davranışı ayarlayın*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu AutoPlay.admx/adml tarafından sağlanır.

**18.9.8.3 (L1) 'Otomatik Oynatmayı kapat' seçeneği 'Etkin: Tüm sürücüler' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Otomatik oynatma, sürücüye ortam yerleştirdiğiniz anda sürücüden okumaya başlar, bu da programların veya ses ortamının kurulum dosyasının hemen başlamasına neden olur. Saldırgan, bilgisayara veya bilgisayardaki verilere zarar verecek bir programı başlatmak için bu özelliği kullanabilir. Otomatik oynatma, disket ve ağ sürücüleri gibi bazı çıkarılabilir sürücü türlerinde varsayılan olarak devre dışıdır, ancak CD-ROM sürücülerinde devre dışı bırakılır.

**Not:** Disket ve ağ sürücüleri gibi varsayılan olarak devre dışı bırakıldığı bilgisayar sürücülerinde Otomatik Oynat'ı etkinleştirmek için bu ilke ayarını kullanamazsınız. Bu ayar için önerilen durum: Etkin: Tüm sürücüler.

**Gerekçe:**

Saldırgan, istemci bilgisayara veya bilgisayardaki verilere zarar verecek bir programı başlatmak için bu özelliği kullanabilir.

**Etki:**

Otomatik oynatma devre dışı bırakılacak - kullanıcıların çıkarılabilir medyada sağlanan kurulum veya yükleme programlarını manuel olarak başlatması gerekecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore r:NoDriveTypeAutoRun*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Tüm sürücüler:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Otomatik Kullan İlkeleri\Otomatik Oynatmayı Kapat*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu AutoPlay.admx/adml

**18.9.9 Yedekleme**

**18.9.10 Biyometri**

**18.9.10.1 Yüz Özellikleri**

**18.9.10.1.1 (L1) 'Gelişmiş adres sahteciliği önleme yapılandır’ seçeneği ‘Etkin’ (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gelişmiş kimlik sahtekarlığının onu destekleyen aygıtlar için yapılandırılıp yapılandırılmadığını belirler. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Kurumsal yönetilen ortamlar artık daha geniş bir mobil cihaz yelpazesini desteklemektedir; bu cihazlarda güvenliği artırmak, ağınıza yetkisiz erişime karşı korunmaya yardımcı olacaktır.

**Etki:**

Windows, cihazdaki tüm kullanıcıların, onu destekleyen cihazlarda yüz özellikleri için kimlik sahtekarlığı önleme kullanmasını gerektirecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Biometrics\FacialFeatures:Enha ncedAntiSpoofing*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\Windows Components\Biometrics\Facial Features\Gelişmiş sahteciliğe karşı korumayı yapılandır*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1511 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu Biometrics.admx/adml tarafından sağlanır.

**Not #2:** Windows 10 Sürüm 1511 ve Windows 10 Sürüm 1607 ve Server 2016 Yönetim Şablonlarında, bu ayar başlangıçta mevcut olduğunda gelişmiş kimlik sahtekarlığı önleme kullan olarak adlandırıldı. Windows 10 Sürüm 1703 Yönetim Şablonlarından başlayarak, gelişmiş sahteciliğe karşı korumayı yapılandır olarak yeniden adlandırıldı.

**18.9.11 BitLocker Sürücü Şifrelemesi**

**18.9.11.1 Sabit Veri Sürücüleri**

**18.9.11.1.1 (BL) 'Windows'un önceki sürümlerinden BitLocker korumalı sabit veri sürücülerine erişime izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, FAT dosya sistemiyle biçimlendirilmiş sabit veri sürücülerinin kilidinin açılıp açılmayacağını ve Windows Server 2008 (R2 olmayan), Windows Vista, Windows XP Service Pack 3 (SP3) veya Windows çalıştıran bilgisayarlarda görüntülenebileceğini yapılandırır. Service Pack 2 (SP2) işletim sistemlerine sahip XP. Not: Bu ilke ayarı, NTFS dosya sistemiyle biçimlendirilmiş sürücüler için geçerli değildir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Varsayılan olarak BitLocker, Windows'un önceki sürümlerinde BitLocker To Go Okuyucu aracılığıyla erişime izin vermek için FAT biçimli sürücüleri sanallaştırır. Ek olarak BitLocker To Go Reader uygulaması, sürücünün şifrelenmemiş kısmına uygulanır. BitLocker To Go Reader uygulaması, diğer tüm uygulamalar gibi, yanıltmaya tabidir ve kötü amaçlı yazılımı yaymak için bir mekanizma olabilir.

**Etki:**

BitLocker korumalı FAT dosya sistemiyle biçimlendirilmiş sabit veri sürücülerinin kilidi, Windows Server 2008 (R2 olmayan), Windows Vista, Windows XP SP3 veya Windows XP SP2 çalıştıran bilgisayarlarda açılamaz. BitLockerToGo.exe yüklenmeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:FDVDiscoveryVolumeType*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki kullanıcı arabirimi yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\Windows'un önceki sürümlerinden BitLocker korumalı sabit veri sürücülerine erişime izin ver*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.1.2 (BL) 'BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçin' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli kimlik bilgileri olmadığında BitLocker korumalı sabit veri sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. "Veri kurtarma aracısına izin ver" onay kutusu, bir Veri Kurtarma Aracısının BitLocker korumalı sabit veri sürücüleriyle kullanılıp kullanılamayacağını belirtmek için kullanılır. Bir Veri Kurtarma Aracısı kullanılmadan önce, Grup İlkesi Yönetim Konsolu'ndaki veya Yerel Grup İlkesi Düzenleyicisi'ndeki Ortak Anahtar İlkeleri öğesinden eklenmelidir. Veri Kurtarma Aracıları ekleme hakkında daha fazla bilgi için Microsoft TechNet'teki BitLocker Sürücü Şifrelemesi Dağıtım Kılavuzu'na bakın. "BitLocker kurtarma bilgilerinin kullanıcı depolamasını yapılandır" bölümünde, kullanıcıların 48 basamaklı bir kurtarma parolası veya 256 bitlik bir kurtarma anahtarı oluşturmasına izin verilip verilmediğini, gerekli olup olmadığını veya izin verilmediğini seçin. Kullanıcıların bir sürücüde BitLocker'ı etkinleştirdiklerinde kurtarma seçeneklerini belirlemelerini önlemek için "BitLocker kurulum sihirbazından kurtarma seçeneklerini atla"yı seçin. Bu, BitLocker'ı etkinleştirdiğinizde hangi kurtarma seçeneğinin kullanılacağını belirleyemeyeceğiniz, bunun yerine sürücü için BitLocker kurtarma seçeneklerinin ilke ayarı tarafından belirlendiği anlamına gelir.

"BitLocker kurtarma bilgilerini Active Directory Etki Alanı Hizmetlerine kaydet" bölümünde, sabit veri sürücüleri için AD DS'de hangi BitLocker kurtarma bilgilerinin depolanacağını seçin. "Kurtarma parolasını ve anahtar paketini yedekle"yi seçerseniz, hem BitLocker kurtarma parolası hem de anahtar paketi AD DS'de depolanır. Anahtar paketinin depolanması, fiziksel olarak bozulmuş bir sürücüden verilerin kurtarılmasını destekler. "Yalnızca kurtarma parolasını yedekle"yi seçerseniz, AD DS'de yalnızca kurtarma parolası depolanır. Bilgisayar etki alanına bağlı olmadığı ve BitLocker kurtarma bilgilerinin AD DS'ye yedeklenmesi başarılı olmadığı sürece kullanıcıların BitLocker'ı etkinleştirmesini engellemek istiyorsanız "Sabit veri sürücüleri için kurtarma bilgileri AD DS'de depolanana kadar BitLocker'ı etkinleştirme" onay kutusunu seçin. Not: "Sabit veri sürücüleri için kurtarma bilgileri AD DS'de depolanana kadar BitLocker'ı etkinleştirme" onay kutusu seçilirse, otomatik olarak bir kurtarma parolası oluşturulur. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Yöneticiler, kullanıcıların verilerine erişememeleri durumunda şifrelenmiş verilere erişmek için her zaman güvenli ve güvenli bir yola sahip olmalıdır. Ek olarak, herhangi bir kimlik doğrulama yönteminde olduğu gibi, sürücüye erişmek için kullanılan kimlik doğrulama bilgilerini tahmin ederek veya bularak bir sürücünün güvenliği ihlal edilebilir.

**Etki:**

BitLocker'ı kullanmak için, sabit sürücüler için bir Veri Kurtarma Aracısının yapılandırılması gerekir. Bir sürücüyü kurtarmak için, Veri Kurtarma Aracısı özel anahtarına yüksek düzeyde kontrollü erişim gerekir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:FDVRecovery*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\Fixed Data Drives\BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçin*

**Not** : Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.1.3 (BL) 'BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçin: Veri kurtarma aracısına izin ver' seçeneği 'Etkin: Doğru' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli kimlik bilgileri olmadığında BitLocker korumalı sabit veri sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. "Veri kurtarma aracısına izin ver" onay kutusu, bir Veri Kurtarma Aracısının BitLocker korumalı sabit veri sürücüleriyle kullanılıp kullanılamayacağını belirtmek için kullanılır. Bir Veri Kurtarma Aracısı kullanılmadan önce, Grup İlkesi Yönetim Konsolu'ndaki veya Yerel Grup İlkesi Düzenleyicisi'ndeki Ortak Anahtar İlkeleri öğesinden eklenmelidir. Veri Kurtarma Aracıları ekleme hakkında daha fazla bilgi için Microsoft TechNet'teki BitLocker Sürücü Şifrelemesi Dağıtım Kılavuzu'na bakın. Bu ayar için önerilen durum: Etkin: Doğru (işaretli).

**Gerekçe:**

Yöneticiler, kullanıcıların verilerine erişememeleri durumunda şifrelenmiş verilere erişmek için her zaman güvenli ve güvenli bir yola sahip olmalıdır. Ek olarak, herhangi bir kimlik doğrulama yönteminde olduğu gibi, sürücüye erişmek için kullanılan kimlik doğrulama bilgilerini tahmin ederek veya bularak bir sürücünün güvenliği ihlal edilebilir. BitLocker'ı kullanmak için, sabit sürücüler için bir Veri Kurtarma Aracısının yapılandırılması gerekir. Bir sürücüyü kurtarmak için, Veri Kurtarma Aracısı özel anahtarına yüksek düzeyde kontrollü erişim gerekir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:FDVManageDRA*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Etkin olarak ayarlayın: Doğru (işaretli):

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\Sabit Veri Sürücüleri\BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçin: Veri kurtarma aracısına izin ver*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.1.4 (BL) 'BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçme: Kurtarma Parolası' seçeneği 'Etkin: 48 basamaklı kurtarma parolasına izin ver' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli kimlik bilgileri olmadığında BitLocker korumalı sabit veri sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. "BitLocker kurtarma bilgilerinin kullanıcı depolamasını yapılandır" bölümünde, kullanıcıların 48 basamaklı bir kurtarma parolası veya 256 bitlik bir kurtarma anahtarı oluşturmasına izin verilip verilmediğini, gerekli olup olmadığını veya izin verilmediğini seçin. Bu ayar için önerilen durum: Etkin: 48 basamaklı kurtarma parolasına izin ver.

**Gerekçe:**

Yöneticiler, kullanıcıların verilerine erişememeleri durumunda şifrelenmiş verilere erişmek için her zaman güvenli ve güvenli bir yola sahip olmalıdır. Ek olarak, herhangi bir kimlik doğrulama yönteminde olduğu gibi, sürücüye erişmek için kullanılan kimlik doğrulama bilgilerini tahmin ederek veya bularak bir sürücünün güvenliği ihlal edilebilir. BitLocker'ı kullanmak için, sabit sürücüler için bir Veri Kurtarma Aracısının yapılandırılması gerekir. Bir sürücüyü kurtarmak için, Veri Kurtarma Aracısı özel anahtarına yüksek düzeyde kontrollü erişim gerekir.

**Etki:**

Sabit sürücüler için 48 basamaklı bir kurtarma parolasına izin verilecek. 789 | Sayfa Denetimi: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:FDVRecoveryPassword*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: 48 basamaklı kurtarma parolasına izin ver:

*Bilgisayar Yapılandırması \Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\BitLocker korumalı sabit sürücülerin nasıl kurtarılacağını seçin: Kurtarma Parolası*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.1.5 (BL) 'BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçin: Kurtarma Anahtarı' seçeneği 'Etkin: 256 bit kurtarma anahtarına izin ver' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli kimlik bilgileri olmadığında BitLocker korumalı sabit veri sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. "BitLocker kurtarma bilgilerinin kullanıcı depolamasını yapılandır" bölümünde, kullanıcıların 48 basamaklı bir kurtarma parolası veya 256 bitlik bir kurtarma anahtarı oluşturmasına izin verilip verilmediğini, gerekli olup olmadığını veya izin verilmediğini seçin. Bu ayar için önerilen durum: Etkin: 256 bit kurtarma anahtarına izin ver.

**Gerekçe:**

Yöneticiler, kullanıcıların verilerine erişememeleri durumunda şifrelenmiş verilere erişmek için her zaman güvenli ve güvenli bir yola sahip olmalıdır. Ek olarak, herhangi bir kimlik doğrulama yönteminde olduğu gibi, sürücüye erişmek için kullanılan kimlik doğrulama bilgilerini tahmin ederek veya bularak bir sürücünün güvenliği ihlal edilebilir. BitLocker'ı kullanmak için, sabit sürücüler için bir Veri Kurtarma Aracısının yapılandırılması gerekir. Bir sürücüyü kurtarmak için, Veri Kurtarma Aracısı özel anahtarına yüksek düzeyde kontrollü erişim gerekir.

**Etki:**

Sabit sürücüler için 256 bit kurtarma anahtarına izin verilecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:FDVRecoveryKey*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: 256 bit kurtarma anahtarına izin ver:

*Bilgisayar Yapılandırması \Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\BitLocker korumalı sabit sürücülerin nasıl kurtarılacağını seçin: Kurtarma Anahtarı*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.1.6 (BL) 'BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçme: BitLocker kurulum sihirbazından kurtarma seçeneklerini çıkar' seçeneği 'Etkin: Doğru' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli kimlik bilgileri olmadığında BitLocker korumalı sabit veri sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. Kullanıcıların bir sürücüde BitLocker'ı etkinleştirdiklerinde kurtarma seçeneklerini belirlemelerini önlemek için "BitLocker kurulum sihirbazından kurtarma seçeneklerini atla"yı seçin. Bu, BitLocker'ı etkinleştirdiğinizde hangi kurtarma seçeneğinin kullanılacağını belirleyemeyeceğiniz, bunun yerine sürücü için BitLocker kurtarma seçeneklerinin ilke ayarı tarafından belirlendiği anlamına gelir. Bu ayar için önerilen durum: Etkin: Doğru (işaretli).

**Gerekçe:**

Yöneticiler, kullanıcıların verilerine erişememeleri durumunda şifrelenmiş verilere erişmek için her zaman güvenli ve güvenli bir yola sahip olmalıdır. Ek olarak, herhangi bir kimlik doğrulama yönteminde olduğu gibi, sürücüye erişmek için kullanılan kimlik doğrulama bilgilerini tahmin ederek veya bularak bir sürücünün güvenliği ihlal edilebilir. BitLocker'ı kullanmak için, sabit sürücüler için bir Veri Kurtarma Aracısının yapılandırılması gerekir. Bir sürücüyü kurtarmak için, Veri Kurtarma Aracısı özel anahtarına yüksek düzeyde kontrollü erişim gerekir.

**Etki:**

Sabit sürücüler için kurtarma seçeneklerini manuel olarak seçme yeteneği, BitLocker kurulum sihirbazında kullanıcıya sunulmayacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:FDVHideRecoveryPage*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki kullanıcı arabirimi yolunu Etkin olarak ayarlayın: Doğru (işaretli):

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\Sabit Veri Sürücüleri\BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçin: BitLocker kurulum sihirbazından kurtarma seçeneklerini atlayın*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.1.7 (BL) 'BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçin: BitLocker kurtarma bilgilerini sabit veri sürücüleri için AD DS'ye kaydet' seçeneği 'Etkin: Yanlış' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli kimlik bilgileri olmadığında BitLocker korumalı sabit veri sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. "BitLocker kurtarma bilgilerini Active Directory Etki Alanı Hizmetlerine kaydet" bölümünde, sabit veri sürücüleri için AD DS'de hangi BitLocker kurtarma bilgilerinin depolanacağını seçin. "Kurtarma parolasını ve anahtar paketini yedekle"yi seçerseniz, hem BitLocker kurtarma parolası hem de anahtar paketi AD DS'de depolanır. Anahtar paketinin depolanması, fiziksel olarak bozulmuş bir sürücüden verilerin kurtarılmasını destekler. "Yalnızca kurtarma parolasını yedekle"yi seçerseniz, AD DS'de yalnızca kurtarma parolası depolanır. Bu ayar için önerilen durum: Etkin: Yanlış (işaretlenmemiş).

**Gerekçe:**

Yöneticiler, kullanıcıların verilerine erişememeleri durumunda şifrelenmiş verilere erişmek için her zaman güvenli ve güvenli bir yola sahip olmalıdır. Ek olarak, herhangi bir kimlik doğrulama yönteminde olduğu gibi, sürücüye erişmek için kullanılan kimlik doğrulama bilgilerini tahmin ederek veya bularak bir sürücünün güvenliği ihlal edilebilir. BitLocker'ı kullanmak için, sabit sürücüler için bir Veri Kurtarma Aracısının yapılandırılması gerekir. Bir sürücüyü kurtarmak için, Veri Kurtarma Aracısı özel anahtarına yüksek düzeyde kontrollü erişim gerekir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:FDVActiveDirectoryBackup*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Yanlış (işaretlenmemiş):

*Bilgisayar Yapılandırması\İlkeler \Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçin: Sabit veri sürücüleri için BitLocker kurtarma bilgilerini AD DS'ye kaydedin*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.1.8 (BL) 'BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçin: BitLocker kurtarma bilgilerinin depolanmasını AD DS'ye yapılandır' seçeneği 'Etkin: Kurtarma parolalarını ve anahtar paketlerini yedekle' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli kimlik bilgileri olmadığında BitLocker korumalı sabit veri sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. "BitLocker kurtarma bilgilerini Active Directory Etki Alanı Hizmetlerine kaydet" bölümünde, sabit veri sürücüleri için AD DS'de hangi BitLocker kurtarma bilgilerinin depolanacağını seçin. "Kurtarma parolasını ve anahtar paketini yedekle"yi seçerseniz, hem BitLocker kurtarma parolası hem de anahtar paketi AD DS'de depolanır. Anahtar paketinin depolanması, fiziksel olarak bozulmuş bir sürücüden verilerin kurtarılmasını destekler. "Yalnızca kurtarma parolasını yedekle"yi seçerseniz, AD DS'de yalnızca kurtarma parolası depolanır. Bu ayar için önerilen durum: Etkin: Kurtarma parolalarını ve anahtar paketlerini yedekleyin.

**Gerekçe:**

Yöneticiler, kullanıcıların verilerine erişememeleri durumunda şifrelenmiş verilere erişmek için her zaman güvenli ve güvenli bir yola sahip olmalıdır. Ek olarak, herhangi bir kimlik doğrulama yönteminde olduğu gibi, sürücüye erişmek için kullanılan kimlik doğrulama bilgilerini tahmin ederek veya bularak bir sürücünün güvenliği ihlal edilebilir. BitLocker'ı kullanmak için, sabit sürücüler için bir Veri Kurtarma Aracısının yapılandırılması gerekir. Bir sürücüyü kurtarmak için, Veri Kurtarma Aracısı özel anahtarına yüksek düzeyde kontrollü erişim gerekir.

**Etki:**

Yok - Kural 18.9.11.1.7'de gerektiği gibi, üstündeki onay kutusu (BitLocker kurtarma bilgilerini sabit veri sürücüleri için AD DS'ye kaydet) Yanlış (işaretlenmemiş) olduğunda bu değer yok sayılır. Bu onay kutusu True (işaretli) olarak ayarlanırsa, hem kurtarma parolaları hem de sabit sürücüler için anahtar paketleri AD DS'ye kaydedilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:FDVActiveDirectoryInfoToStore*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Kurtarma parolalarını ve anahtar paketlerini yedekle:

*Bilgisayar Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Fixed Data Drives\BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçin: BitLocker kurtarma bilgilerinin AD DS'ye depolanmasını yapılandırın:*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir . Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.1.9 (BL) 'BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçin: Kurtarma bilgileri sabit veri sürücüleri için AD DS'de depolanana kadar BitLocker'ı etkinleştirmeyin' seçeneği 'Etkin: Yanlış' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli kimlik bilgileri olmadığında BitLocker korumalı sabit veri sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. Bilgisayar etki alanına bağlı olmadığı ve BitLocker kurtarma bilgilerinin AD DS'ye yedeklenmesi başarılı olmadığı sürece kullanıcıların BitLocker'ı etkinleştirmesini engellemek istiyorsanız "Sabit veri sürücüleri için kurtarma bilgileri AD DS'de depolanana kadar BitLocker'ı etkinleştirme" onay kutusunu seçin.

**Not:** "Sabit veri sürücüleri için kurtarma bilgileri AD DS'de depolanana kadar BitLocker'ı etkinleştirme" onay kutusu seçilirse, otomatik olarak bir kurtarma parolası oluşturulur.

Bu ayar için önerilen durum: Etkin: Yanlış (işaretlenmemiş).

**Gerekçe:**

Yöneticiler, kullanıcıların verilerine erişememeleri durumunda şifrelenmiş verilere erişmek için her zaman güvenli ve güvenli bir yola sahip olmalıdır. Ek olarak, herhangi bir kimlik doğrulama yönteminde olduğu gibi, sürücüye erişmek için kullanılan kimlik doğrulama bilgilerini tahmin ederek veya bularak bir sürücünün güvenliği ihlal edilebilir. BitLocker'ı kullanmak için, sabit sürücüler için bir Veri Kurtarma Aracısının yapılandırılması gerekir. Bir sürücüyü kurtarmak için, Veri Kurtarma Aracısı özel anahtarına yüksek düzeyde kontrollü erişim gerekir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:FDVRequireActiveDirectoryB ackup*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Yanlış (işaretlenmemiş):

*Bilgisayar Yapılandırması\ İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\Sabit Veri Sürücüleri\BitLocker korumalı sabit sürücülerin nasıl kurtarılabileceğini seçin: Sabit veri sürücüleri için kurtarma bilgileri AD DS'de depolanana kadar BitLocker'ı etkinleştirmeyin*

**Not**: Bu Grup İlkesi yolu, varsayılan olarak mevcut değil. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.1.10 (BL) 'Sabit veri sürücüleri için donanım tabanlı şifreleme kullanımını yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, BitLocker'ın sabit veri sürücülerinde donanım tabanlı şifreleme kullanımını yönetmenize ve donanım tabanlı şifreleme ile hangi şifreleme algoritmalarını kullanabileceğini belirlemenize olanak tanır. Donanım tabanlı şifrelemenin kullanılması, verilerin sürücüye sık sık okunmasını veya yazılmasını içeren sürücü işlemlerinin performansını iyileştirebilir. Donanım tabanlı şifrelemeyi desteklemeyen bilgisayarlarda donanım tabanlı şifreleme yerine BitLocker yazılım tabanlı şifrelemenin kullanılıp kullanılmayacağını ve donanım tabanlı şifrelemeyle kullanılan şifreleme algoritmalarını ve şifreleme paketlerini kısıtlamak isteyip istemediğinizi denetleyen ek seçenekler belirleyebilirsiniz. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Satıcı ve/veya kullanıcı, güvenlik açığını gidermek için bellenimi güncellemediyse, güvenlik açısından donanım tabanlı şifreleme, belirli kendi kendini şifreleyen sürücülerin (SED'ler) donanım şifrelemesinde güvenlik açıkları oluşturabilir. Daha fazla bilgi için [ADV180028 - Güvenlik Güncelleştirme Kılavuzu - Microsoft - BitLocker'ı yazılım şifrelemesini zorunlu kılacak şekilde yapılandırma kılavuzu](https://msrc.microsoft.com/update-guide/en-US/vulnerability/ADV180028) sayfasını ziyaret edin.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:FDVHardwareEncryption*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\Sabit Veri Sürücüleri\Sabit veri sürücüleri için donanım tabanlı şifreleme kullanımını yapılandır*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.1.11 (BL) 'Sabit veri sürücüleri için parola kullanımını yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, BitLocker korumalı sabit veri sürücülerinin kilidini açmak için parola gerekip gerekmediğini belirtir.

**Not**: Bu ayar, bir birimin kilidini açarken değil, BitLocker açıldığında uygulanır. BitLocker, sürücüde bulunan koruyuculardan herhangi biriyle sürücünün kilidinin açılmasına izin verir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Sözlük tarzı bir saldırı kullanarak, bir sürücünün kilidini tekrar tekrar açmaya çalışarak parolalar tahmin edilebilir veya keşfedilebilir. Bu tür BitLocker parolası, örneğin bir TPM tarafından sağlanan sözlük karşıtı saldırı korumalarını içerdiğinden, bunlara yönelik hızlı kaba kuvvet saldırılarını yavaşlatacak bir mekanizma yoktur.

**Etki:**

BitLocker'ı sabit sürücüler için yapılandırırken parola seçeneği kullanılamayacak. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:FDVPassphrase*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\Sabit Veri Sürücüleri\Sabit veri sürücüleri için parola kullanımını yapılandır*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.1.12 (BL) 'Sabit veri sürücülerinde akıllı kart kullanımını yapılandır' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir bilgisayardaki BitLocker korumalı sabit veri sürücülerine kullanıcı erişiminin kimliğini doğrulamak için akıllı kartların kullanılıp kullanılamayacağını belirlemenize olanak tanır. Sürücüye kullanıcı erişimini doğrulamak için akıllı kartlar kullanılabilir. "Sabit veri sürücülerinde akıllı kartların kullanılmasını gerektir" onay kutusunu seçerek akıllı kart kimlik doğrulamasını zorunlu kılabilirsiniz.

**Not:** Bu ayar, bir sürücünün kilidini açarken değil, BitLocker açılırken uygulanır. BitLocker, sürücüde bulunan koruyuculardan herhangi biriyle sürücünün kilidinin açılmasına izin verir.

Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bir sürücü, sürücüye erişmek için kullanılan kimlik doğrulama bilgilerini tahmin ederek veya bularak tehlikeye girebilir. Örneğin, bir parola tahmin edilebilir veya otomatik olarak kilidini açmak üzere ayarlanmış bir sürücü, otomatik olarak kilidini açtığı bilgisayarla birlikte kaybolabilir veya çalınabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:FDVAllowUserCert*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\Sabit Veri Sürücüleri\Sabit veri sürücülerinde akıllı kartların kullanımını yapılandır*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.1.13 (BL) 'Sabit veri sürücülerinde akıllı kart kullanımını yapılandırma: Sabit veri sürücülerinde akıllı kart kullanımını gerektir' seçeneği 'Etkin: Doğru' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir bilgisayardaki BitLocker korumalı sabit veri sürücülerine kullanıcı erişiminin kimliğini doğrulamak için akıllı kartların kullanılması gerekip gerekmediğini belirlemenize olanak tanır. Sürücüye kullanıcı erişimini doğrulamak için akıllı kartlar kullanılabilir. "Sabit veri sürücülerinde akıllı kartların kullanılmasını gerektir" onay kutusunu seçerek bir akıllı kart kimlik doğrulaması talep edebilirsiniz.

**Not**: Bu ayar, bir sürücünün kilidini açarken değil, BitLocker açılırken uygulanır. BitLocker, sürücüde bulunan koruyuculardan herhangi biriyle sürücünün kilidinin açılmasına izin verir.

Bu ayar için önerilen durum: Etkin: Doğru (işaretli).

**Gerekçe:**

Bir sürücü, sürücüye erişmek için kullanılan kimlik doğrulama bilgilerini tahmin ederek veya bularak tehlikeye girebilir. Örneğin, bir parola tahmin edilebilir veya otomatik olarak kilidini açmak üzere ayarlanmış bir sürücü, otomatik olarak kilidini açtığı bilgisayarla birlikte kaybolabilir veya çalınabilir.

**Etki:**

Sabit veri sürücülerine kullanıcı erişimini doğrulamak için akıllı kartlar gerekli olacaktır. Akıllı kartların kullanımı PKI altyapısı gerektirir. Kullanıcıların, bilgisayarı her yeniden başlattıklarında sabit veri sürücüsünün kilidini açmak için akıllı kartla kimlik doğrulaması yapmaları gerekecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:FDVEnforceUserCert*

**Düzeltme**:

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Doğru (işaretli):

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\Fixed Data Drives\Fixed Data Drives\ sabit veri sürücüleri: Sabit veri sürücülerinde akıllı kartların kullanılmasını gerektir*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.2 İşletim Sistemi Sürücüleri**

**18.9.11.2.1 (BL) 'Başlangıç için geliştirilmiş PIN'lere izin ver' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, BitLocker ile geliştirilmiş başlangıç PIN'lerinin kullanılıp kullanılmayacağını yapılandırmanıza olanak tanır. Gelişmiş başlangıç PIN'leri, büyük ve küçük harfler, simgeler, sayılar ve boşluklar dahil karakterlerin kullanılmasına izin verir. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Yalnızca sayısal bir PIN, alfa sayısal bir PIN'den daha az entropi sağlar. Başlangıç için gelişmiş PIN kullanılmadığında, PIN, yerelleştirme desteği mevcut olmadan önce işletim sistemi öncesi ortama girildiğinden, BitLocker PIN girişi için [F1-F10] işlev tuşlarının kullanılmasını gerektirir. Bu, her PIN basamağını on olasılıktan biriyle sınırlar. TPM, PIN yeniden deneme girişimleri için gecikmeyi katlanarak artıran bir mekanizma içeren bir darbe önleme özelliğine sahiptir; ancak, bir saldırgan, işlev tuşlarının 10 basamaklı bir alanını kullanarak bir kaba kuvvet saldırısını daha etkili bir şekilde gerçekleştirebilir.

**Etki:**

Ayarlanan tüm yeni BitLocker başlangıç PIN'leri gelişmiş PIN'ler olacaktır. Not: İşletim Sistemi Öncesi ortamda tüm bilgisayarlar tam klavye desteğini etkinleştirmez. Bazı anahtarlar mevcut olmayabilir. Bu işlevin, dağıtılmadan önce ortamınızdaki bilgisayarlar kullanılarak test edilmesi önerilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:UseEnhancedPin*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Components\BitLocker Sürücü Şifrelemesi\İşletim Sistemi Sürücüleri\Başlangıç için gelişmiş PIN'lere izin ver*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.2.2 (BL) 'Bütünlük doğrulaması için Güvenli Önyüklemeye İzin Ver' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, BitLocker işletim sistemi sürücüleri için platform bütünlüğü sağlayıcısı olarak Güvenli Önyüklemeye izin verilip verilmeyeceğini yapılandırmanıza olanak tanır. Güvenli Önyükleme, bilgisayarın önyükleme öncesi ortamının yalnızca yetkili yazılım yayıncıları tarafından dijital olarak imzalanmış bellenimi yüklemesini sağlar. Güvenli Önyükleme ayrıca, önyükleme öncesi yapılandırmayı yönetmek için eski BitLocker bütünlük denetimlerinden daha fazla esneklik sağlar. Güvenli Önyükleme, Sınıf 2 ve Sınıf 3 bilgisayarlar için UEFI 2.3.1 Spesifikasyonlarını karşılayan bir sistem gerektirir. Bu ilke etkinleştirildiğinde ve donanım BitLocker senaryoları için Güvenli Önyükleme kullanma yeteneğine sahip olduğunda, "Gelişmiş Önyükleme Yapılandırma Veri doğrulama profilini kullan" grup ilkesi ayarı yok sayılır ve Güvenli Önyükleme, yapılandırılan Güvenli Önyükleme ilkesi ayarına göre BCD ayarlarını doğrular. BitLocker'dan ayrı olarak.

**Not**: "Yerel UEFI üretici yazılımı yapılandırmaları için TPM platform doğrulama profilini yapılandır" grup ilkesi ayarı etkinleştirilirse ve PCR 7 atlanırsa, BitLocker'ın platform için Güvenli Önyükleme veya Önyükleme Yapılandırma Verileri (BCD) bütünlük doğrulamasını kullanması engellenir. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Güvenli Önyükleme, bilgisayar başlatılırken yalnızca yetkili yazılım yayıncıları tarafından dijital olarak imzalanmış bellenimin yüklenmesini sağlar, bu da rootkit'lerin ve diğer kötü amaçlı yazılım türlerinin sistemin kontrolünü ele geçirme riskini azaltır. Ayrıca, alternatif bir işletim sisteminden önyükleme yapan kötü niyetli kullanıcılara karşı koruma sağlamaya yardımcı olur.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:OSAllowSecureBootForIntegrity*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\ Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\İşletim Sistemi Sürücüleri\Bütünlük doğrulaması için Güvenli Önyüklemeye İzin Ver*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.2.3 (BL) 'BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılabileceğini seçin' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli başlangıç anahtarı bilgilerinin yokluğunda BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. "Sertifika tabanlı veri kurtarma aracısına izin ver" onay kutusu, bir Veri Kurtarma Aracısının BitLocker korumalı işletim sistemi sürücüleriyle kullanılıp kullanılamayacağını belirtmek için kullanılır. Bir Veri Kurtarma Aracısı kullanılmadan önce, Grup İlkesi Yönetim Konsolu'ndaki veya Yerel Grup İlkesi Düzenleyicisi'ndeki Ortak Anahtar İlkeleri öğesinden eklenmelidir. Veri Kurtarma Aracıları ekleme hakkında daha fazla bilgi için Microsoft TechNet'teki BitLocker Sürücü Şifrelemesi Dağıtım Kılavuzu'na bakın. "BitLocker kurtarma bilgilerinin kullanıcı depolamasını yapılandır" bölümünde, kullanıcıların 48 basamaklı bir kurtarma parolası veya 256 bitlik bir kurtarma anahtarı oluşturmasına izin verilip verilmediğini, gerekli olup olmadığını veya izin verilmediğini seçin. Kullanıcıların bir sürücüde BitLocker'ı etkinleştirdiklerinde kurtarma seçeneklerini belirlemelerini önlemek için "BitLocker kurulum sihirbazından kurtarma seçeneklerini atla"yı seçin. Bu, BitLocker'ı etkinleştirdiğinizde hangi kurtarma seçeneğinin kullanılacağını belirleyemeyeceğiniz, bunun yerine sürücü için BitLocker kurtarma seçeneklerinin ilke ayarı tarafından belirlendiği anlamına gelir. "BitLocker kurtarma bilgilerini Active Directory Etki Alanı Hizmetlerine kaydet" bölümünde, işletim sistemi sürücüleri için AD DS'de hangi BitLocker kurtarma bilgilerinin depolanacağını seçin. "Kurtarma parolasını ve anahtar paketini yedekle"yi seçerseniz, hem BitLocker kurtarma parolası hem de anahtar paketi AD DS'de depolanır. Anahtar paketinin depolanması, fiziksel olarak bozulmuş bir sürücüden verilerin kurtarılmasını destekler. "Yalnızca kurtarma parolasını yedekle"yi seçerseniz, AD DS'de yalnızca kurtarma parolası depolanır. Bilgisayar etki alanına bağlı olmadığı ve BitLocker kurtarma bilgilerinin AD DS'ye yedeklenmesi başarılı olmadığı sürece kullanıcıların BitLocker'ı etkinleştirmesini engellemek istiyorsanız "İşletim sistemi sürücüleri için kurtarma bilgileri AD DS'de depolanana kadar BitLocker'ı etkinleştirme" onay kutusunu seçin.

**Not**: "İşletim sistemi sürücüleri için AD DS'de kurtarma bilgileri depolanana kadar BitLocker'ı etkinleştirme" onay kutusu seçilirse, otomatik olarak bir kurtarma parolası oluşturulur.

Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bir kullanıcı, şifrelenmiş bir işletim sistemi birimine erişmek için birincil yolunu kaybederse veya sistem, önyükleme zamanı bütünlük denetimlerini geçemezse, sistem kurtarma moduna geçecektir. Kurtarma anahtarı Active Directory'ye yedeklenmemişse, kullanıcının kurtarma anahtarını USB flash sürücü gibi başka bir konuma kaydetmesi veya kurtarma parolasını yazdırmış olması ve şimdi bunlardan birine erişimi olması gerekir. sistemi kurtarmak için. Kullanıcı kurtarma anahtarını üretemezse, kullanıcının şifrelenmiş birime ve ardından orada depolanan tüm verilere erişimi reddedilecektir.

**Etki:**

BitLocker'ı açmak için kullanıcıların etki alanına bağlı olması gerekir. Bu politika FIPS şikayeti değildir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:OSRecovery*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\İşletim Sistemi Sürücüleri\BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılabileceğini seçin*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.2.4 (BL) 'BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılabileceğini seçin: Veri kurtarma aracısına izin ver' seçeneği 'Etkin: Yanlış' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli başlangıç anahtarı bilgilerinin yokluğunda BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. "Sertifika tabanlı veri kurtarma aracısına izin ver" onay kutusu, bir Veri Kurtarma Aracısının BitLocker korumalı işletim sistemi sürücüleriyle kullanılıp kullanılamayacağını belirtmek için kullanılır. Bir Veri Kurtarma Aracısı kullanılmadan önce, Grup İlkesi Yönetim Konsolu'ndaki veya Yerel Grup İlkesi Düzenleyicisi'ndeki Ortak Anahtar İlkeleri öğesinden eklenmelidir. Veri Kurtarma Aracıları ekleme hakkında daha fazla bilgi için Microsoft TechNet'teki BitLocker Sürücü Şifrelemesi Dağıtım Kılavuzu'na bakın. Bu ayar için önerilen durum: Etkin: Yanlış (işaretlenmemiş).

**Gerekçe**:

Bir kullanıcı, şifrelenmiş bir işletim sistemi birimine erişmek için birincil yolunu kaybederse veya sistem, önyükleme zamanı bütünlük denetimlerini geçemezse, sistem kurtarma moduna geçecektir. Kurtarma anahtarı Active Directory'ye yedeklenmemişse, kullanıcının kurtarma anahtarını USB flash sürücü gibi başka bir konuma kaydetmesi veya kurtarma parolasını yazdırmış olması ve şimdi bunlardan birine erişimi olması gerekir. sistemi kurtarmak için. Kullanıcı kurtarma anahtarını üretemezse, kullanıcının şifrelenmiş birime ve ardından orada depolanan tüm verilere erişimi reddedilecektir.

**Etki:**

İşletim sistemi sürücüsü için bir Veri Kurtarma Aracısına izin verilmeyecektir. BitLocker'ı açmak için kullanıcıların etki alanına bağlı olması gerekir. Bu politika FIPS şikayeti değildir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:OSManageDRA*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın: Yanlış (işaretlenmemiş):

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\İşletim Sistemi Sürücüleri\BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılabileceğini seçin: Veri kurtarma aracısına izin ver*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.2.5 (BL) 'BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılabileceğini seçin: Kurtarma Parolası' seçeneği 'Etkin: 48 basamaklı kurtarma parolası iste' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli başlangıç anahtarı bilgilerinin yokluğunda BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. "BitLocker kurtarma bilgilerinin kullanıcı depolamasını yapılandır" bölümünde, kullanıcıların 48 basamaklı bir kurtarma parolası veya 256 bitlik bir kurtarma anahtarı oluşturmasına izin verilip verilmediğini, gerekli olup olmadığını veya izin verilmediğini seçin. Bu ayar için önerilen durum: Etkin: 48 basamaklı kurtarma parolası gerektir.

**Gerekçe:**

Bir kullanıcı, şifrelenmiş bir işletim sistemi birimine erişmek için birincil yolunu kaybederse veya sistem, önyükleme zamanı bütünlük denetimlerini geçemezse, sistem kurtarma moduna geçecektir. Kurtarma anahtarı Active Directory'ye yedeklenmemişse, kullanıcının kurtarma anahtarını USB flash sürücü gibi başka bir konuma kaydetmesi veya kurtarma parolasını yazdırmış olması ve şimdi bunlardan birine erişimi olması gerekir. sistemi kurtarmak için. Kullanıcı kurtarma anahtarını üretemezse, kullanıcının şifrelenmiş birime ve ardından orada depolanan tüm verilere erişimi reddedilecektir.

**Etki**:

İşletim sistemi sürücüsü için 48 basamaklı bir kurtarma parolası gerekecektir. BitLocker'ı açmak için kullanıcıların etki alanına bağlı olması gerekir. Bu politika FIPS şikayeti değildir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:OSRecoveryPassword*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: 48 basamaklı kurtarma parolası iste:

*Bilgisayar Yapılandırması \Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Operating System Drives\BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılabileceğini seçin: Kurtarma Parolası*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.2.6 (BL) 'BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılabileceğini seçin: Kurtarma Anahtarı' seçeneği 'Etkin: 256 bit kurtarma anahtarına izin verme' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli başlangıç anahtarı bilgilerinin yokluğunda BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. "BitLocker kurtarma bilgilerinin kullanıcı depolamasını yapılandır" bölümünde, kullanıcıların 48 basamaklı bir kurtarma parolası veya 256 bitlik bir kurtarma anahtarı oluşturmasına izin verilip verilmediğini, gerekli olup olmadığını veya izin verilmediğini seçin. Bu ayar için önerilen durum: Etkin: 256 bit kurtarma anahtarına izin verme.

**Gerekçe:**

Bir kullanıcı, şifrelenmiş bir işletim sistemi birimine erişmek için birincil yolunu kaybederse veya sistem, önyükleme zamanı bütünlük denetimlerini geçemezse, sistem kurtarma moduna geçecektir. Kurtarma anahtarı Active Directory'ye yedeklenmemişse, kullanıcının kurtarma anahtarını USB flash sürücü gibi başka bir konuma kaydetmesi veya kurtarma parolasını yazdırmış olması ve şimdi bunlardan birine erişimi olması gerekir. sistemi kurtarmak için. Kullanıcı kurtarma anahtarını üretemezse, kullanıcının şifrelenmiş birime ve ardından orada depolanan tüm verilere erişimi reddedilecektir.

**Etki:**

İşletim sistemi sürücüsü için 256 bit kurtarma anahtarına izin verilmeyecek. BitLocker'ı açmak için kullanıcıların etki alanına bağlı olması gerekir. Bu politika FIPS şikayeti değildir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:OSRecoveryKey*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: 256 bit kurtarma anahtarına izin verme:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\İşletim Sistemi Sürücüleri\BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılacağını seçin: Kurtarma Anahtarı*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.2.7 (BL) 'BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılabileceğini seçin: BitLocker kurulum sihirbazından kurtarma seçeneklerini çıkar' seçeneği 'Etkin: Doğru' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli başlangıç anahtarı bilgilerinin yokluğunda BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. Kullanıcıların bir sürücüde BitLocker'ı etkinleştirdiklerinde kurtarma seçeneklerini belirlemelerini önlemek için "BitLocker kurulum sihirbazından kurtarma seçeneklerini atla"yı seçin. Bu, BitLocker'ı etkinleştirdiğinizde hangi kurtarma seçeneğinin kullanılacağını belirleyemeyeceğiniz, bunun yerine sürücü için BitLocker kurtarma seçeneklerinin ilke ayarı tarafından belirlendiği anlamına gelir. Bu ayar için önerilen durum: Etkin: Doğru (işaretli).

**Gerekçe:**

Bir kullanıcı, şifrelenmiş bir işletim sistemi birimine erişmek için birincil yolunu kaybederse veya sistem, önyükleme zamanı bütünlük denetimlerini geçemezse, sistem kurtarma moduna geçecektir. Kurtarma anahtarı Active Directory'ye yedeklenmemişse, kullanıcının kurtarma anahtarını USB flash sürücü gibi başka bir konuma kaydetmesi veya kurtarma parolasını yazdırmış olması ve şimdi bunlardan birine erişimi olması gerekir. sistemi kurtarmak için. Kullanıcı kurtarma anahtarını üretemezse, kullanıcının şifrelenmiş birime ve ardından orada depolanan tüm verilere erişimi reddedilecektir.

**Etki:**

Çalışan sürücü için kurtarma seçeneklerini manuel olarak seçme yeteneği, BitLocker kurulum sihirbazında kullanıcıya sunulmayacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:OSHideRecoveryPage*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Etkin olarak ayarlayın: Doğru (işaretli):

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\İşletim Sistemi Sürücüleri\BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılacağını seçin: BitLocker kurulum sihirbazından kurtarma seçeneklerini atlayın*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.2.8 (BL) 'BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılabileceğini seçin: BitLocker kurtarma bilgilerini işletim sistemi sürücüleri için AD DS'ye kaydet' seçeneği 'Etkin: Doğru' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli başlangıç anahtarı bilgilerinin yokluğunda BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. Kullanıcıların bir sürücüde BitLocker'ı etkinleştirdiklerinde kurtarma seçeneklerini belirlemelerini önlemek için "BitLocker kurulum sihirbazından kurtarma seçeneklerini atla"yı seçin. Bu, BitLocker'ı etkinleştirdiğinizde hangi kurtarma seçeneğinin kullanılacağını belirleyemeyeceğiniz, bunun yerine sürücü için BitLocker kurtarma seçeneklerinin ilke ayarı tarafından belirlendiği anlamına gelir. Bu ayar için önerilen durum: Etkin: Doğru (işaretli).

**Gerekçe:**

Bir kullanıcı, şifrelenmiş bir işletim sistemi birimine erişmek için birincil yolunu kaybederse veya sistem, önyükleme zamanı bütünlük denetimlerini geçemezse, sistem kurtarma moduna geçecektir. Kurtarma anahtarı Active Directory'ye yedeklenmemişse, kullanıcının kurtarma anahtarını USB flash sürücü gibi başka bir konuma kaydetmesi veya kurtarma parolasını yazdırmış olması ve şimdi bunlardan birine erişimi olması gerekir. sistemi kurtarmak için. Kullanıcı kurtarma anahtarını üretemezse, kullanıcının şifrelenmiş birime ve ardından orada depolanan tüm verilere erişimi reddedilecektir.

**Etki:**

Çalışan sürücü için kurtarma seçeneklerini manuel olarak seçme yeteneği, BitLocker kurulum sihirbazında kullanıcıya sunulmayacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:OSHideRecoveryPage*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Etkin olarak ayarlayın: Doğru (işaretli):

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\İşletim Sistemi Sürücüleri\BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılacağını seçin: BitLocker kurulum sihirbazından kurtarma seçeneklerini atlayın*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.2.9 (BL) 'BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılabileceğini seçin: BitLocker kurtarma bilgilerinin depolanmasını AD DS'ye yapılandırın:' seçeneği 'Etkin: Kurtarma parolalarını ve anahtar paketlerini depola' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli başlangıç anahtarı bilgilerinin yokluğunda BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. "BitLocker kurtarma bilgilerini Active Directory Etki Alanı Hizmetlerine kaydet" bölümünde, işletim sistemi sürücüleri için AD DS'de hangi BitLocker kurtarma bilgilerinin depolanacağını seçin. "Kurtarma parolasını ve anahtar paketini yedekle"yi seçerseniz, hem BitLocker kurtarma parolası hem de anahtar paketi AD DS'de depolanır. Anahtar paketinin depolanması, fiziksel olarak bozulmuş bir sürücüden verilerin kurtarılmasını destekler. "Yalnızca kurtarma parolasını yedekle"yi seçerseniz, AD DS'de yalnızca kurtarma parolası depolanır. Bu ayar için önerilen durum: Etkin: Doğru (işaretli).

**Gerekçe:**

Bir kullanıcı, şifrelenmiş bir işletim sistemi birimine erişmek için birincil yolunu kaybederse veya sistem, önyükleme zamanı bütünlük denetimlerini geçemezse, sistem kurtarma moduna geçecektir. Kurtarma anahtarı Active Directory'ye yedeklenmemişse, kullanıcının kurtarma anahtarını USB flash sürücü gibi başka bir konuma kaydetmesi veya kurtarma parolasını yazdırmış olması ve şimdi bunlardan birine erişimi olması gerekir. sistemi kurtarmak için. Kullanıcı kurtarma anahtarını üretemezse, kullanıcının şifrelenmiş birime ve ardından orada depolanan tüm verilere erişimi reddedilecektir.

**Etki:**

İşletim sistemi sürücüsü için BitLocker kurtarma bilgileri AD DS'ye yedeklenecek. BitLocker'ı açmak için kullanıcıların etki alanına bağlı olması gerekir. Bu politika FIPS şikayeti değildir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:OSActiveDirectoryBackup*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Doğru (işaretli):

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\İşletim Sistemi Sürücüleri\BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılacağını seçin: İşletim sistemi sürücüleri için BitLocker kurtarma bilgilerini AD DS'ye kaydedin*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.2.10 (BL) 'BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılabileceğini seçin: Kurtarma bilgileri işletim sistemi sürücüleri için AD DS'de depolanana kadar BitLocker'ı etkinleştirmeyin' seçeneği 'Etkin: Doğru' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli başlangıç anahtarı bilgilerinin yokluğunda BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. Bilgisayar etki alanına bağlı olmadığı ve BitLocker kurtarma bilgilerinin AD DS'ye yedeklenmesi başarılı olmadığı sürece kullanıcıların BitLocker'ı etkinleştirmesini engellemek istiyorsanız "İşletim sistemi sürücüleri için kurtarma bilgileri AD DS'de depolanana kadar BitLocker'ı etkinleştirme" onay kutusunu seçin.

**Not**: "İşletim sistemi sürücüleri için AD DS'de kurtarma bilgileri depolanana kadar BitLocker'ı etkinleştirme" onay kutusu seçilirse, otomatik olarak bir kurtarma parolası oluşturulur.

Bu ayar için önerilen durum: Etkin: Doğru (işaretli).

**Gerekçe:**

Bir kullanıcı, şifrelenmiş bir işletim sistemi birimine erişmek için birincil yolunu kaybederse veya sistem, önyükleme zamanı bütünlük denetimlerini geçemezse, sistem kurtarma moduna geçecektir. Kurtarma anahtarı Active Directory'ye yedeklenmemişse, kullanıcının kurtarma anahtarını USB flash sürücü gibi başka bir konuma kaydetmesi veya kurtarma parolasını yazdırmış olması ve şimdi bunlardan birine erişimi olması gerekir. sistemi kurtarmak için. Kullanıcı kurtarma anahtarını üretemezse, kullanıcının şifrelenmiş birime ve ardından orada depolanan tüm verilere erişimi reddedilecektir.

**Etki:**

BitLocker'ı açmak için kullanıcıların etki alanına bağlı olması ve işletim sistemi sürücüsü için BitLocker kurtarma bilgilerinin yedeklenmesinin başarılı olması gerekir. Bu politika FIPS şikayeti değildir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:OSRequireActiveDirectoryBa ckup*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Doğru (işaretli):

*Bilgisayar Yapılandırması\ İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\İşletim Sistemi Sürücüleri\BitLocker korumalı işletim sistemi sürücülerinin nasıl kurtarılacağını seçin: Kurtarma bilgileri işletim sistemi sürücüleri için AD DS'de depolanana kadar BitLocker'ı etkinleştirmeyin*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.2.11 (BL) 'İşletim sistemi sürücüleri için donanım tabanlı şifreleme kullanımını yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, BitLocker'ın işletim sistemi sürücülerinde donanım tabanlı şifreleme kullanımını yönetmenize ve donanım tabanlı şifreleme ile hangi şifreleme algoritmalarını kullanabileceğini belirlemenize olanak tanır. Donanım tabanlı şifrelemenin kullanılması, verilerin sürücüye sık sık okunmasını veya yazılmasını içeren sürücü işlemlerinin performansını iyileştirebilir. Donanım tabanlı şifrelemeyi desteklemeyen bilgisayarlarda donanım tabanlı şifreleme yerine BitLocker yazılım tabanlı şifrelemenin kullanılıp kullanılmayacağını ve donanım tabanlı şifrelemeyle kullanılan şifreleme algoritmalarını ve şifreleme paketlerini kısıtlamak isteyip istemediğinizi denetleyen ek seçenekler belirleyebilirsiniz. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Satıcı ve/veya kullanıcı, güvenlik açığını gidermek için bellenimi güncellemediyse, güvenlik açısından donanım tabanlı şifreleme, belirli kendi kendini şifreleyen sürücülerin (SED'ler) donanım şifrelemesinde güvenlik açıkları oluşturabilir. Daha fazla bilgi için [ADV180028 - Güvenlik Güncelleştirme Kılavuzu - Microsoft - BitLocker'ı yazılım şifrelemesini zorunlu kılacak şekilde yapılandırma kılavuzu](https://msrc.microsoft.com/update-guide/en-US/vulnerability/ADV180028) sayfasını ziyaret edin.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:OSHardwareEncryption*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\İşletim Sistemi Sürücüleri\İşletim sistemi sürücüleri için donanım tabanlı şifreleme kullanımını yapılandır*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.2.12 (BL) 'İşletim sistemi sürücüleri için parola kullanımını yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, BitLocker korumalı işletim sistemi sürücülerinin kilidini açmak için kullanılan parolaların kısıtlamalarını belirtir.

**Not**: Bu ayar, bir birimin kilidini açarken değil, BitLocker açıldığında uygulanır. BitLocker, sürücüde bulunan koruyuculardan herhangi biriyle sürücünün kilidinin açılmasına izin verir.

Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Sözlük tarzı bir saldırı kullanarak, bir sürücünün kilidini tekrar tekrar açmaya çalışarak parolalar tahmin edilebilir veya keşfedilebilir. Bu tür BitLocker parolası, örneğin bir TPM tarafından sağlanan sözlük karşıtı saldırı korumalarını içerdiğinden, bunlara yönelik hızlı kaba kuvvet saldırılarını yavaşlatacak bir mekanizma yoktur.

**Etki:**

BitLocker'ı işletim sistemi sürücüsü için yapılandırırken parola seçeneği kullanılamayacak. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:OSPassphrase*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\İşletim Sistemi Sürücüleri\İşletim sistemi sürücüleri için parola kullanımını yapılandır*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.2.13 (BL) 'Başlangıçta ek kimlik doğrulaması gerektir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bilgisayar her başlatıldığında BitLocker'ın ek kimlik doğrulaması gerektirip gerektirmediğini ve BitLocker'ı bir Güvenilir Platform Modülü (TPM) ile veya bunlar olmadan kullanıp kullanmadığınızı yapılandırmanıza olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır.

**Not:** Başlangıçta ek kimlik doğrulama seçeneklerinden yalnızca biri gerekli olabilir, aksi takdirde bir ilke hatası oluşur. BitLocker'ı TPM olmayan bir bilgisayarda kullanmak istiyorsanız, "Uyumlu bir TPM olmadan BitLocker'a izin ver" onay kutusunu seçin. Bu modda, başlatma için bir USB sürücüsü gereklidir ve sürücüyü şifrelemek için kullanılan temel bilgiler, bir USB anahtarı oluşturarak USB sürücüsünde depolanır. USB anahtarı takıldığında, sürücüye erişim doğrulanır ve sürücüye erişilebilir. USB anahtarı kaybolursa veya kullanılamıyorsa, sürücüye erişmek için BitLocker kurtarma seçeneklerinden birini kullanmanız gerekecektir. Uyumlu bir TPM'ye sahip bir bilgisayarda, şifrelenmiş veriler için ek koruma sağlamak üzere başlangıçta dört tür kimlik doğrulama yöntemi kullanılabilir. Bilgisayar başlatıldığında, kimlik doğrulama için yalnızca TPM'yi kullanabilir veya ayrıca bir başlangıç anahtarı içeren bir USB flash sürücünün takılmasını, 4 basamaklı ila 20 basamaklı kişisel kimlik numarasının (PIN) girilmesini veya her ikisini de gerektirebilir. Kullanıcılar, BitLocker kurulum sihirbazında gelişmiş başlatma seçeneklerini yapılandırabilir.

**Not #2:** Bir başlangıç PIN'i ve bir USB flash sürücü kullanılmasını zorunlu kılmak istiyorsanız, BitLocker ayarlarını BitLocker Sürücü Şifrelemesi kurulum sihirbazı yerine komut satırı aracı manager-bde'yi kullanarak yapılandırmanız gerekir.

Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

PIN kullanılmadan TPM, yalnızca erken önyükleme bileşenlerini doğrular ve kullanıcının herhangi bir ek kimlik doğrulama bilgisi girmesini gerektirmez. Bu yapılandırmada bir bilgisayar kaybolur veya çalınırsa, erken önyükleme bileşenleri değiştirilmedikçe veya şifreli sürücü makineden kaldırılmadıkça BitLocker, yerel Windows kimlik doğrulamasının sağladığının ötesinde herhangi bir ek koruma önlemi sağlamayacaktır.

**Etki:**

PIN, bilgisayarı yeniden başlatmak için fiziksel varlığı gerektirir. Bu işlev, Wake on LAN çözümleriyle uyumlu değildir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:UseAdvancedStartup*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Components\BitLocker Drive Encryption\İşletim Sistemi Sürücüleri\Başlangıçta ek kimlik doğrulaması gerektir*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.2.14 (BL) 'Başlangıçta ek kimlik doğrulaması gerektir: BitLocker'a uyumlu TPM olmadan izin ver' seçeneği 'Etkin: Yanlış' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir USB flash sürücüde bir parola veya başlangıç anahtarı kullanmak yerine BitLocker'ı Güvenilir Platform Modülü (TPM) olmadan kullanıp kullanamayacağınızı yapılandırmanıza olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. Bu ayar için önerilen durum: Etkin: Yanlış (işaretlenmemiş).

**Gerekçe:**

PIN kullanılmadan TPM, yalnızca erken önyükleme bileşenlerini doğrular ve kullanıcının herhangi bir ek kimlik doğrulama bilgisi girmesini gerektirmez. Bu yapılandırmada bir bilgisayar kaybolur veya çalınırsa, erken önyükleme bileşenleri değiştirilmedikçe veya şifreli sürücü makineden kaldırılmadıkça, BitLocker yerel Windows kimlik doğrulamasının sağladığının ötesinde herhangi bir ek koruma önlemi sağlamayacaktır.

**Etki:**

BitLocker'ı kullanmak için uyumlu bir TPM gerekli olacaktır. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:EnableBDEWithNoTPM*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Yanlış (işaretlenmemiş):

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\İşletim Sistemi Sürücüleri\Başlangıçta ek kimlik doğrulaması gerektir: BitLocker'a uyumlu bir TPM olmadan izin ver*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.3 Çıkarılabilir Veri Sürücüleri**

**18.9.11.3.1 (BL) 'Windows'un önceki sürümlerinden BitLocker korumalı çıkarılabilir veri sürücülerine erişime izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, FAT dosya sistemiyle biçimlendirilmiş çıkarılabilir veri sürücülerinin kilidinin açılıp açılmayacağını ve Windows Server 2008 (R2 olmayan), Windows Vista, Windows XP Service Pack 3 (SP3) veya Windows çalıştıran bilgisayarlarda görüntülenip görüntülenmeyeceğini yapılandırır. Service Pack 2 (SP2) işletim sistemlerine sahip XP.

**Not**: Bu ilke ayarı, NTFS dosya sistemiyle biçimlendirilmiş sürücüler için geçerli değildir.

Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Varsayılan olarak BitLocker, Windows'un önceki sürümlerinde BitLocker To Go Okuyucu aracılığıyla erişime izin vermek için FAT biçimli sürücüleri sanallaştırır. Ek olarak BitLocker To Go Reader uygulaması, sürücünün şifrelenmemiş kısmına uygulanır. BitLocker To Go Reader uygulaması, diğer tüm uygulamalar gibi, yanıltmaya tabidir ve kötü amaçlı yazılımı yaymak için bir mekanizma olabilir.

**Etki:**

BitLocker korumalı FAT dosya sistemiyle biçimlendirilmiş çıkarılabilir veri sürücülerinin kilidi Windows Server 2008 (R2 olmayan), Windows Vista, Windows XP SP3 veya Windows XP SP2 çalıştıran bilgisayarlarda açılamaz. BitLockerToGo.exe yüklenmeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:RDVDiscoveryVolumeType*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Components\BitLocker Drive Encryption\Removable Data Drives\Windows'un önceki sürümlerinden BitLocker korumalı çıkarılabilir veri sürücülerine erişime izin ver*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.3.2 (BL) 'BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılabileceğini seçin' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli kimlik bilgileri olmadığında BitLocker korumalı çıkarılabilir veri sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. "Veri kurtarma aracısına izin ver" onay kutusu, bir Veri Kurtarma Aracısının BitLocker korumalı çıkarılabilir veri sürücüleri ile kullanılıp kullanılamayacağını belirtmek için kullanılır. Bir Veri Kurtarma Aracısı kullanılmadan önce, Grup İlkesi Yönetim Konsolu'ndaki veya Yerel Grup İlkesi Düzenleyicisi'ndeki Ortak Anahtar İlkeleri öğesinden eklenmelidir. Veri Kurtarma Aracıları ekleme hakkında daha fazla bilgi için Microsoft TechNet'teki BitLocker Sürücü Şifrelemesi Dağıtım Kılavuzu'na bakın. "BitLocker kurtarma bilgilerinin kullanıcı depolamasını yapılandır" bölümünde, kullanıcıların 48 basamaklı bir kurtarma parolası veya 256 bitlik bir kurtarma anahtarı oluşturmasına izin verilip verilmediğini, gerekli olup olmadığını veya izin verilmediğini seçin. Kullanıcıların bir sürücüde BitLocker'ı etkinleştirdiklerinde kurtarma seçeneklerini belirlemelerini önlemek için "BitLocker kurulum sihirbazından kurtarma seçeneklerini atla"yı seçin. Bu, BitLocker'ı etkinleştirdiğinizde hangi kurtarma seçeneğinin kullanılacağını belirleyemeyeceğiniz, bunun yerine sürücü için BitLocker kurtarma seçeneklerinin ilke ayarı tarafından belirlendiği anlamına gelir.

"BitLocker kurtarma bilgilerini Active Directory Etki Alanı Hizmetlerine kaydet" bölümünde, çıkarılabilir veri sürücüleri için AD DS'de hangi BitLocker kurtarma bilgilerinin depolanacağını seçin. "Kurtarma parolasını ve anahtar paketini yedekle"yi seçerseniz, hem BitLocker kurtarma parolası hem de anahtar paketi AD DS'de depolanır. "Yalnızca kurtarma parolasını yedekle"yi seçerseniz, AD DS'de yalnızca kurtarma parolası depolanır. Bilgisayar etki alanına bağlı olmadığı ve BitLocker kurtarma bilgilerinin AD DS'ye yedeklenmesi başarılı olmadığı sürece kullanıcıların BitLocker'ı etkinleştirmesini engellemek istiyorsanız "Çıkarılabilir veri sürücüleri için kurtarma bilgileri AD DS'de depolanana kadar BitLocker'ı etkinleştirme" onay kutusunu seçin.

**Not:** "Çıkarılabilir veri sürücüleri için kurtarma bilgileri AD DS'de depolanana kadar BitLocker'ı etkinleştirme" onay kutusu seçilirse, otomatik olarak bir kurtarma parolası oluşturulur.

Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Yöneticiler, kullanıcıların verilerine erişememeleri durumunda şifrelenmiş verilere erişmek için her zaman güvenli ve güvenli bir yola sahip olmalıdır. Ek olarak, herhangi bir kimlik doğrulama yönteminde olduğu gibi, sürücüye erişmek için kullanılan kimlik doğrulama bilgilerini tahmin ederek veya bularak bir sürücünün güvenliği ihlal edilebilir.

**Etki:**

BitLocker'ı kullanmak için bir Veri Kurtarma Aracısının çıkarılabilir sürücüler için yapılandırılması gerekir. Bir sürücüyü kurtarmak için, Veri Kurtarma Aracısı özel anahtarına yüksek düzeyde kontrollü erişim gerekir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:RDVRecovery*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\Çıkarılabilir Veri Sürücüleri\BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılabileceğini seçin*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.3.3 (BL) 'BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılabileceğini seçin: Veri kurtarma aracısına izin ver' seçeneği 'Etkin: Doğru' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli kimlik bilgileri olmadığında BitLocker korumalı çıkarılabilir veri sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. "Veri kurtarma aracısına izin ver" onay kutusu, bir Veri Kurtarma Aracısının BitLocker korumalı çıkarılabilir veri sürücüleri ile kullanılıp kullanılamayacağını belirtmek için kullanılır. Bir Veri Kurtarma Aracısı kullanılmadan önce, Grup İlkesi Yönetim Konsolu'ndaki veya Yerel Grup İlkesi Düzenleyicisi'ndeki Ortak Anahtar İlkeleri öğesinden eklenmelidir. Veri Kurtarma Aracıları ekleme hakkında daha fazla bilgi için Microsoft TechNet'teki BitLocker Sürücü Şifrelemesi Dağıtım Kılavuzu'na bakın. Bu ayar için önerilen durum: Etkin: Doğru (işaretli).

**Gerekçe:**

Yöneticiler, kullanıcıların verilerine erişememeleri durumunda şifrelenmiş verilere erişmek için her zaman güvenli ve güvenli bir yola sahip olmalıdır. Ek olarak, herhangi bir kimlik doğrulama yönteminde olduğu gibi, sürücüye erişmek için kullanılan kimlik doğrulama bilgilerini tahmin ederek veya bularak bir sürücünün güvenliği ihlal edilebilir. BitLocker'ı kullanmak için, çıkarılabilir sürücüler için bir Veri Kurtarma Aracısının yapılandırılması gerekir. Bir sürücüyü kurtarmak için, Veri Kurtarma Aracısı özel anahtarına yüksek düzeyde kontrollü erişim gerekir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:RDVManageDRA*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki kullanıcı arabirimi yolunu Etkin olarak ayarlayın: Doğru (işaretli):

*Bilgisayar Yapılandırması\İlkeler \Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılabileceğini seçin: Veri kurtarma aracısına izin ver*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.3.4 (BL) 'BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılabileceğini seçme: Kurtarma Parolası' seçeneği 'Etkin: 48 basamaklı kurtarma parolasına izin verme' olarak ayarlanmalıdır. (Otomatik)**

**Açıklama:**

Bu ilke ayarı, gerekli kimlik bilgileri olmadığında BitLocker korumalı çıkarılabilir veri sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. "BitLocker kurtarma bilgilerinin kullanıcı depolamasını yapılandır" bölümünde, kullanıcıların 48 basamaklı bir kurtarma parolası veya 256 bitlik bir kurtarma anahtarı oluşturmasına izin verilip verilmediğini, gerekli olup olmadığını veya izin verilmediğini seçin. Bu ayar için önerilen durum: Etkin: 48 basamaklı kurtarma parolasına izin verme.

**Gerekçe:**

Yöneticiler, kullanıcıların verilerine erişememeleri durumunda şifrelenmiş verilere erişmek için her zaman güvenli ve güvenli bir yola sahip olmalıdır. Ek olarak, herhangi bir kimlik doğrulama yönteminde olduğu gibi, sürücüye erişmek için kullanılan kimlik doğrulama bilgilerini tahmin ederek veya bularak bir sürücünün güvenliği ihlal edilebilir. BitLocker'ı kullanmak için, çıkarılabilir sürücüler için bir Veri Kurtarma Aracısının yapılandırılması gerekir. Bir sürücüyü kurtarmak için, Veri Kurtarma Aracısı özel anahtarına yüksek düzeyde kontrollü erişim gerekir.

**Etki:**

Çıkarılabilir sürücüler için 48 basamaklı bir kurtarma parolasına izin verilmeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:RDVRecoveryPassword*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: 48 basamaklı kurtarma parolasına izin verme:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\Çıkarılabilir Veri Sürücüleri\BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılacağını seçin: Kurtarma Parolası*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.3.5 (BL) 'BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılabileceğini seçin: Kurtarma Anahtarı' seçeneği 'Etkin: 256 bit kurtarma anahtarına izin verme' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli kimlik bilgileri olmadığında BitLocker korumalı çıkarılabilir veri sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. "BitLocker kurtarma bilgilerinin kullanıcı depolamasını yapılandır" bölümünde, kullanıcıların 48 basamaklı bir kurtarma parolası veya 256 bitlik bir kurtarma anahtarı oluşturmasına izin verilip verilmediğini, gerekli olup olmadığını veya izin verilmediğini seçin. Bu ayar için önerilen durum: Etkin: 48 basamaklı kurtarma parolasına izin verme.

**Gerekçe:**

Yöneticiler, kullanıcıların verilerine erişememeleri durumunda şifrelenmiş verilere erişmek için her zaman güvenli ve güvenli bir yola sahip olmalıdır. Ek olarak, herhangi bir kimlik doğrulama yönteminde olduğu gibi, sürücüye erişmek için kullanılan kimlik doğrulama bilgilerini tahmin ederek veya bularak bir sürücünün güvenliği ihlal edilebilir. BitLocker'ı kullanmak için, çıkarılabilir sürücüler için bir Veri Kurtarma Aracısının yapılandırılması gerekir. Bir sürücüyü kurtarmak için, Veri Kurtarma Aracısı özel anahtarına yüksek düzeyde kontrollü erişim gerekir.

**Etki:**

Çıkarılabilir sürücüler için 48 basamaklı bir kurtarma parolasına izin verilmeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:RDVRecoveryPassword*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: 48 basamaklı kurtarma parolasına izin verme:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\Çıkarılabilir Veri Sürücüleri\BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılacağını seçin: Kurtarma Parolası*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.3.6 (BL) 'BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılabileceğini seçin: Kurtarma seçeneklerini BitLocker kurulum sihirbazından çıkar' seçeneği 'Etkin: Doğru' (Otomatik) olarak ayarlandığından emin olun**

**Açıklama:**

Bu ilke ayarı, gerekli kimlik bilgileri olmadığında BitLocker korumalı çıkarılabilir veri sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. Kullanıcıların bir sürücüde BitLocker'ı etkinleştirdiklerinde kurtarma seçeneklerini belirlemelerini önlemek için "BitLocker kurulum sihirbazından kurtarma seçeneklerini atla"yı seçin. Bu, BitLocker'ı etkinleştirdiğinizde hangi kurtarma seçeneğinin kullanılacağını belirleyemeyeceğiniz, bunun yerine sürücü için BitLocker kurtarma seçeneklerinin ilke ayarı tarafından belirlendiği anlamına gelir. Bu ayar için önerilen durum: Etkin: Doğru (işaretli).

**Gerekçe:**

Yöneticiler, kullanıcıların verilerine erişememeleri durumunda şifrelenmiş verilere erişmek için her zaman güvenli ve güvenli bir yola sahip olmalıdır. Ek olarak, herhangi bir kimlik doğrulama yönteminde olduğu gibi, sürücüye erişmek için kullanılan kimlik doğrulama bilgilerini tahmin ederek veya bularak bir sürücünün güvenliği ihlal edilebilir. BitLocker'ı kullanmak için, çıkarılabilir sürücüler için bir Veri Kurtarma Aracısının yapılandırılması gerekir. Bir sürücüyü kurtarmak için, Veri Kurtarma Aracısı özel anahtarına yüksek düzeyde kontrollü erişim gerekir.

**Etki:**

Çıkarılabilir sürücüler için kurtarma seçeneklerini manuel olarak seçme yeteneği, BitLocker kurulum sihirbazında kullanıcıya sunulmayacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:RDVHideRecoveryPage*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Doğru (işaretli):

*Bilgisayar Yapılandırması\İlkeler \Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılabileceğini seçin: BitLocker kurulum sihirbazından kurtarma seçeneklerini atlayın*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.3.7 (BL) 'BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılabileceğini seçin: BitLocker kurtarma bilgilerini çıkarılabilir veri sürücüleri için AD DS'ye kaydet' seçeneği 'Etkin: Yanlış' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli kimlik bilgileri olmadığında BitLocker korumalı çıkarılabilir veri sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. "BitLocker kurtarma bilgilerini Active Directory Etki Alanı Hizmetlerine kaydet" bölümünde, çıkarılabilir veri sürücüleri için AD DS'de hangi BitLocker kurtarma bilgilerinin depolanacağını seçin. "Kurtarma parolasını ve anahtar paketini yedekle"yi seçerseniz, hem BitLocker kurtarma parolası hem de anahtar paketi AD DS'de depolanır. "Yalnızca kurtarma parolasını yedekle"yi seçerseniz, AD DS'de yalnızca kurtarma parolası depolanır. Bu ayar için önerilen durum: Etkin: Yanlış (işaretlenmemiş).

**Gerekçe:**

Yöneticiler, kullanıcıların verilerine erişememeleri durumunda şifrelenmiş verilere erişmek için her zaman güvenli ve güvenli bir yola sahip olmalıdır. Ek olarak, herhangi bir kimlik doğrulama yönteminde olduğu gibi, sürücüye erişmek için kullanılan kimlik doğrulama bilgilerini tahmin ederek veya bularak bir sürücünün güvenliği ihlal edilebilir. BitLocker'ı kullanmak için, çıkarılabilir sürücüler için bir Veri Kurtarma Aracısının yapılandırılması gerekir. Bir sürücüyü kurtarmak için, Veri Kurtarma Aracısı özel anahtarına yüksek düzeyde kontrollü erişim gerekir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:RDVActiveDirectoryBackup*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Yanlış (işaretlenmemiş):

*Bilgisayar Yapılandırması\İlkeler \Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılacağını seçin: Çıkarılabilir veri sürücüleri için BitLocker kurtarma bilgilerini AD DS'ye kaydedin*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.3.8 (BL) 'BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılabileceğini seçin: BitLocker kurtarma bilgilerinin depolanmasını AD DS'ye yapılandırın:' seçeneği 'Etkin: Kurtarma parolalarını ve anahtar paketlerini yedekle' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli kimlik bilgileri olmadığında BitLocker korumalı çıkarılabilir veri sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. "BitLocker kurtarma bilgilerini Active Directory Etki Alanı Hizmetlerine kaydet" bölümünde, çıkarılabilir veri sürücüleri için AD DS'de hangi BitLocker kurtarma bilgilerinin depolanacağını seçin. "Kurtarma parolasını ve anahtar paketini yedekle"yi seçerseniz, hem BitLocker kurtarma parolası hem de anahtar paketi AD DS'de depolanır. "Yalnızca kurtarma parolasını yedekle"yi seçerseniz, AD DS'de yalnızca kurtarma parolası depolanır. Bu ayar için önerilen durum: Etkin: Kurtarma parolalarını ve anahtar paketlerini yedekleyin.

**Gerekçe:**

Yöneticiler, kullanıcıların verilerine erişememeleri durumunda şifrelenmiş verilere erişmek için her zaman güvenli ve güvenli bir yola sahip olmalıdır. Ek olarak, herhangi bir kimlik doğrulama yönteminde olduğu gibi, sürücüye erişmek için kullanılan kimlik doğrulama bilgilerini tahmin ederek veya bularak bir sürücünün güvenliği ihlal edilebilir. BitLocker'ı kullanmak için, çıkarılabilir sürücüler için bir Veri Kurtarma Aracısının yapılandırılması gerekir. Bir sürücüyü kurtarmak için, Veri Kurtarma Aracısı özel anahtarına yüksek düzeyde kontrollü erişim gerekir.

**Etki:**

Yok - Kural 18.9.11.3.7'de gerektiği gibi, üstündeki onay kutusu (BitLocker kurtarma bilgilerini çıkarılabilir veri sürücüleri için AD DS'ye kaydet) Yanlış (işaretlenmemiş) olduğunda bu değer yok sayılır. Bu onay kutusu True (işaretli) olarak ayarlanırsa, hem kurtarma parolaları hem de çıkarılabilir sürücüler için anahtar paketleri AD DS'ye kaydedilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:RDVActiveDirectoryInfoToSt cevher*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Kurtarma parolalarını ve anahtar paketlerini yedekle:

*Bilgisayar Configuration\Policies\Administrative Templates\Windows Components\BitLocker Drive Encryption\Removable Data Drives\BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılabileceğini seçin: BitLocker kurtarma bilgilerinin AD DS'ye depolanmasını yapılandırın*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir . Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.3.9 (BL) 'BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılabileceğini seçin: Kurtarma bilgileri çıkarılabilir veri sürücüleri için AD DS'de depolanana kadar BitLocker'ı etkinleştirmeyin' seçeneği 'Etkin: Yanlış' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, gerekli kimlik bilgileri olmadığında BitLocker korumalı çıkarılabilir veri sürücülerinin nasıl kurtarılacağını denetlemenize olanak tanır. Bu ilke ayarı, BitLocker'ı açtığınızda uygulanır. Bilgisayar etki alanına bağlı olmadığı ve BitLocker kurtarma bilgilerinin AD DS'ye yedeklenmesi başarılı olmadığı sürece kullanıcıların BitLocker'ı etkinleştirmesini engellemek istiyorsanız "Çıkarılabilir veri sürücüleri için kurtarma bilgileri AD DS'de depolanana kadar BitLocker'ı etkinleştirme" onay kutusunu seçin.

**Not:** "Çıkarılabilir veri sürücüleri için kurtarma bilgileri AD DS'de depolanana kadar BitLocker'ı etkinleştirme" onay kutusu seçilirse, otomatik olarak bir kurtarma parolası oluşturulur.

Bu ayar için önerilen durum: Etkin: Yanlış (işaretlenmemiş).

**Gerekçe:**

Yöneticiler, kullanıcıların verilerine erişememeleri durumunda şifrelenmiş verilere erişmek için her zaman güvenli ve güvenli bir yola sahip olmalıdır. Ek olarak, herhangi bir kimlik doğrulama yönteminde olduğu gibi, sürücüye erişmek için kullanılan kimlik doğrulama bilgilerini tahmin ederek veya bularak bir sürücünün güvenliği ihlal edilebilir. BitLocker'ı kullanmak için, çıkarılabilir sürücüler için bir Veri Kurtarma Aracısının yapılandırılması gerekir. Bir sürücüyü kurtarmak için, Veri Kurtarma Aracısı özel anahtarına yüksek düzeyde kontrollü erişim gerekir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:RDVRequireActiveDirectoryB ackup*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Yanlış (işaretlenmemiş):

*Bilgisayar Yapılandırması\ İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\Çıkarılabilir Veri Sürücüleri\BitLocker korumalı çıkarılabilir sürücülerin nasıl kurtarılacağını seçin: Çıkarılabilir veri sürücüleri için kurtarma bilgileri AD DS'de depolanana kadar BitLocker'ı etkinleştirmeyin*

**Not:** Bu Grup İlkesi yolu, varsayılan olarak mevcut değil. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.3.10 (BL) 'Çıkarılabilir veri sürücüleri için donanım tabanlı şifreleme kullanımını yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, BitLocker'ın çıkarılabilir veri sürücülerinde donanım tabanlı şifreleme kullanımını yönetmenize ve donanım tabanlı şifreleme ile hangi şifreleme algoritmalarını kullanabileceğini belirlemenize olanak tanır. Donanım tabanlı şifrelemenin kullanılması, verilerin sürücüye sık sık okunmasını veya yazılmasını içeren sürücü işlemlerinin performansını iyileştirebilir. Donanım tabanlı şifrelemeyi desteklemeyen bilgisayarlarda donanım tabanlı şifreleme yerine BitLocker yazılım tabanlı şifrelemenin kullanılıp kullanılmayacağını ve donanım tabanlı şifrelemeyle kullanılan şifreleme algoritmalarını ve şifreleme paketlerini kısıtlamak isteyip istemediğinizi denetleyen ek seçenekler belirleyebilirsiniz. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Satıcı ve/veya kullanıcı, güvenlik açığını gidermek için bellenimi güncellemediyse, güvenlik açısından donanım tabanlı şifreleme, belirli kendi kendini şifreleyen sürücülerin (SED'ler) donanım şifrelemesinde güvenlik açıkları oluşturabilir. Daha fazla bilgi için [ADV180028 - Güvenlik Güncelleştirme Kılavuzu - Microsoft - BitLocker'ı yazılım şifrelemesini zorunlu kılacak şekilde yapılandırma kılavuzu](https://msrc.microsoft.com/update-guide/en-US/vulnerability/ADV180028) sayfasını ziyaret edin.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:RDVHardwareEncryption*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\Çıkarılabilir Veri Sürücüleri\Çıkarılabilir veri sürücüleri için donanım tabanlı şifreleme kullanımını yapılandırın*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.3.11 (BL) 'Çıkarılabilir veri sürücüleri için parola kullanımını yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, BitLocker korumalı çıkarılabilir veri sürücülerinin kilidini açmak için parola gerekip gerekmediğini belirtmenize olanak tanır.

**Not:** Bu ayar, bir sürücünün kilidini açarken değil, BitLocker açıldığında uygulanır. BitLocker, sürücüde bulunan koruyuculardan herhangi biriyle sürücünün kilidinin açılmasına izin verir.

Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Sözlük tarzı bir saldırı kullanarak, bir sürücünün kilidini tekrar tekrar açmaya çalışarak parolalar tahmin edilebilir veya keşfedilebilir. Bu tür BitLocker parolası, örneğin bir TPM tarafından sağlanan sözlük karşıtı saldırı korumalarını içermediğinden, bunlara karşı hızlı kaba kuvvet saldırılarının kullanımını yavaşlatacak bir mekanizma yoktur.

**Etki:**

BitLocker'ı çıkarılabilir sürücüler için yapılandırırken parola seçeneği kullanılamayacak. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:RDVPassphrase*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\Çıkarılabilir Veri Sürücüleri\Çıkarılabilir veri sürücüleri için parola kullanımını yapılandır*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.3.12 (BL) 'Çıkarılabilir veri sürücülerinde akıllı kart kullanımını yapılandır' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir bilgisayardaki BitLocker korumalı çıkarılabilir veri sürücülerine kullanıcı erişiminin kimliğini doğrulamak için akıllı kartların kullanılıp kullanılamayacağını belirtir. Sürücüye kullanıcı erişimini doğrulamak için akıllı kartlar kullanılabilir. "Akıllı kartların çıkarılabilir veri sürücülerinde kullanılmasını gerektir" onay kutusunu seçerek akıllı kart kimlik doğrulamasını zorunlu kılabilirsiniz.

**Not:** Bu ayar, bir birimin kilidini açarken değil, BitLocker açıldığında uygulanır. BitLocker, sürücüde bulunan koruyuculardan herhangi biriyle sürücünün kilidinin açılmasına izin verir.

Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bir sürücü, sürücüye erişmek için kullanılan kimlik doğrulama bilgilerini tahmin ederek veya bularak tehlikeye girebilir. Örneğin, bir parola tahmin edilebilir veya otomatik olarak kilidini açmak üzere ayarlanmış bir sürücü, otomatik olarak kilidini açtığı bilgisayarla birlikte kaybolabilir veya çalınabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:RDVAllowUserCert*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\Çıkarılabilir Veri Sürücüleri\Çıkarılabilir veri sürücülerinde akıllı kartların kullanımını yapılandır*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.3.13 (BL) 'Çıkarılabilir veri sürücülerinde akıllı kart kullanımını yapılandırma: Çıkarılabilir veri sürücülerinde akıllı kart kullanımını gerektir' seçeneği 'Etkin: Doğru' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir bilgisayardaki BitLocker korumalı çıkarılabilir veri sürücülerine kullanıcı erişiminin kimliğini doğrulamak için akıllı kartların kullanılması gerekip gerekmediğini belirtir. Sürücüye kullanıcı erişimini doğrulamak için akıllı kartlar kullanılabilir. "Akıllı kartların çıkarılabilir veri sürücülerinde kullanılmasını gerektir" onay kutusunu seçerek akıllı kart kimlik doğrulamasını zorunlu kılabilirsiniz.

**Not:** Bu ayar, bir birimin kilidini açarken değil, BitLocker açıldığında uygulanır. BitLocker, sürücüde bulunan koruyuculardan herhangi biriyle sürücünün kilidinin açılmasına izin verir.

Bu ayar için önerilen durum: Etkin: Doğru (işaretli).

**Gerekçe:**

Bir sürücü, sürücüye erişmek için kullanılan kimlik doğrulama bilgilerini tahmin ederek veya bularak tehlikeye girebilir. Örneğin, bir parola tahmin edilebilir veya otomatik olarak kilidini açmak üzere ayarlanmış bir sürücü, otomatik olarak kilidini açtığı bilgisayarla birlikte kaybolabilir veya çalınabilir.

**Etki:**

Çıkarılabilir veri sürücülerine kullanıcı erişimini doğrulamak için akıllı kartlar gerekecektir. Akıllı kartların kullanımı PKI altyapısı gerektirir. Kullanıcıların, bilgisayarı her yeniden başlattıklarında çıkarılabilir veri sürücüsünün kilidini açmak için akıllı kartla kimlik doğrulaması yapmaları gerekir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:RDVEnforceUserCert*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Doğru (işaretli):

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\Çıkarılabilir Veri Sürücüleri\Akıllı kartların çıkarılabilir veri sürücüleri: Çıkarılabilir veri sürücülerinde akıllı kartların kullanılmasını gerektir*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.3.14 (BL) 'BitLocker tarafından korunmayan çıkarılabilir sürücülere yazma erişimini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir bilgisayarın çıkarılabilir veri sürücüsüne veri yazabilmesi için BitLocker korumasının gerekli olup olmadığını yapılandırır. BitLocker korumalı olmayan tüm çıkarılabilir veri sürücüleri salt okunur olarak bağlanacaktır. Sürücü BitLocker tarafından korunuyorsa, okuma ve yazma erişimiyle bağlanacaktır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Kullanıcılar, önemli verileri sürücüye kaydetmeden önce çıkarılabilir sürücüleri gönüllü olarak şifreleyemez.

**Etki:**

BitLocker korumalı olmayan tüm çıkarılabilir veri sürücüleri salt okunur olarak bağlanacaktır. Sürücü BitLocker tarafından korunuyorsa, okuma ve yazma erişimiyle bağlanacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\Policies\Microsoft\FVE:RDVDenyWri teAccess*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\Çıkarılabilir Veri Sürücüleri\BitLocker tarafından korunmayan çıkarılabilir sürücülere yazma erişimini engelle*

**Not :** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.3.15 (BL) 'BitLocker tarafından korunmayan çıkarılabilir sürücülere yazma erişimini reddet: Başka bir kuruluşta yapılandırılmış cihazlara yazma erişimine izin verme' seçeneği 'Etkin: Yanlış' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bilgisayarın başka bir kuruluşta yapılandırılmış BitLocker korumalı çıkarılabilir sürücülere veri yazıp yazamayacağını yapılandırır. Bu ayar için önerilen durum: Etkin: Yanlış (işaretlenmemiş).

**Gerekçe:**

Başka bir kuruluşta yapılandırılmış BitLocker korumalı çıkarılabilir sürücülere yazma erişimini kısıtlamak, şifreli veri paylaşımının gerekli olduğu meşru iş operasyonlarını engelleyebilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:RDVDenyCrossOrg*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Yanlış (işaretlenmemiş):

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\BitLocker Sürücü Şifrelemesi\Çıkarılabilir Veri Sürücüleri\Çıkarılabilir sürücülere yazma erişimini engelle BitLocker tarafından korunmaz: Başka bir kuruluşta yapılandırılmış aygıtlara yazma erişimine izin verme*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.11.4 (BL) 'Bu bilgisayar kilitliyken yeni DMA aygıtlarını devre dışı bırak' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir kullanıcı Windows'ta oturum açana kadar tüm çalışırken takılabilir PCI aşağı akış bağlantı noktaları için doğrudan bellek erişimini (DMA) engellemenize olanak tanır. Bu ayar için önerilen durum: Etkin. Not: Microsoft, yaptırımını güçlendirmek için Windows 10 R1709'da bu ayarın uygulamasını değiştirmiştir. Sonuç olarak, sorunu düzeltmek için satıcıdan güncelleştirilmiş bellenim ve/veya sürücüler yüklenene kadar, bazı donanım yapılandırmaları bu sürümde (veya daha yenisinde) bu ayarla beklenmeyen sorunlarla karşılaşabilir. Daha fazla bilgi için Etki Bildirimine bakın.

**Gerekçe:**

BitLocker ile korunan bir bilgisayar, bilgisayar açıldığında veya Bekleme güç durumundayken Doğrudan Bellek Erişimi (DMA) saldırılarına karşı savunmasız olabilir - buna iş istasyonu kilitliyken de dahildir. Bu ayarın etkinleştirilmesi, bilgisayar gözetimsiz bırakıldığında bu tür bir saldırının önlenmesine yardımcı olacaktır.

**Etki:**

DMA kullanan yeni eklenen donanım aygıtları, kullanıcı oturumun kilidini açana veya oturum açana kadar kilitli (veya oturumu kapatılmış) bir iş istasyonunda çalışmayacaktır. Windows 10 R1709'da (veya daha yenisinde) bazı donanım yapılandırmalarında bu ayarla beklenmeyen sorunlar yaşanabilir. , sorunu düzeltmek için güncellenmiş bellenim ve/veya sürücüler gerektirir. Daha fazla bilgi için [MSKB 4057300](https://support.microsoft.com/en-us/help/4057300/devices-not-working-before-log-on-a-computer-running-windows-10-1709)'e bakın. Bu ayarı, büyük ölçekte dağıtmadan önce tüm iş istasyonu donanımı örneklerinde test etmenizi öneririz - ilk olarak satıcı üretici yazılımı ve/veya sürücü güncellemelerinin gerekli olup olmadığını görmek için.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\FVE:DisableExternalDMAUnderLock*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\ Windows Components\BitLocker Drive Encryption\Bu bilgisayar kilitliyken yeni DMA aygıtlarını devre dışı bırak*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1703 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu VolumeEncryption.admx/adml tarafından sağlanır.

**18.9.12 Kamera**

**18.9.12.1 (L2) 'Kamera Kullanımına İzin Ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, makinede Kamera cihazlarının kullanımına izin verilip verilmediğini kontrol eder. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Yüksek güvenlikli bir ortamda bulunan kameralar, ciddi gizlilik ve veri hırsızlığı riskleri oluşturabilir - bu riski azaltmaya yardımcı olmak için devre dışı bırakılmalıdır.

**Etki:**

Kullanıcılar kamerayı bir sistemde kullanamayacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Camera:AllowCamera*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Kamera\Kamera Kullanımına İzin Ver*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1607 ve Server 2016 Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu Camera.admx/adml tarafından sağlanır.

**18.9.13 Sohbet**

**18.9.14 Bulut İçeriği**

**18.9.14.1 (L1) 'Bulut kullanıcı hesabı durum içeriğini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, tüm Windows deneyimlerinde bulut tüketici hesabı durumu içeriğine izin verilip verilmeyeceğini belirler. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Kurumsal olarak yönetilen bir ortamda tüketici hesaplarının kullanılması, olası veri sızıntılarına yol açabileceğinden iyi bir güvenlik uygulaması değildir.

**Etki:**

Kullanıcılar, sistemde Microsoft tüketici hesaplarını kullanamayacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CloudContent:DisableCo nsumerAccountStateContent*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Bulut İçeriği\Bulut tüketici hesabı durum içeriğini kapat*

**Not:** Bu Grup İlkesi yolu mevcut olmayabilir varsayılan olarak. Microsoft Windows 10 Sürüm 21H2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu CloudContent.admx/adml tarafından sağlanır.

**18.9.14.2 (L2) 'Bulut için optimize edilmiş içeriği kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, tüm Windows deneyimlerinde bulut için optimize edilmiş içeriği kapatır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Gizlilik endişeleri nedeniyle, bu veriler hassas bilgiler içerebileceğinden, veriler hiçbir zaman 3. şahıslara gönderilmemelidir.

**Etki:**

Bulut için optimize edilmiş içerik istemcisi bileşenini kullanan Windows deneyimleri, özelleştirilmiş içerik yerine varsayılan yedek içeriği sunacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CloudContent:DisableCl oudOptimizedContent*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonlar\Windows Bileşenleri\Bulut İçeriği\Bulut için optimize edilmiş içeriği kapat*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 20H2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu CloudContent.admx/adml tarafından sağlanır.

**18.9.14.3 (L1) 'Microsoft tüketici deneyimlerini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, tüketicilerin cihazlarından ve Microsoft hesabından en iyi şekilde yararlanmasına yardımcı olan deneyimleri kapatır. Bu ayar için önerilen durum: Etkin.

**Not:** [Microsoft TechNet](https://technet.microsoft.com/en-us/itpro/windows/manage/group-policies-for-enterprise-and-education-editions)'e göre bu ilke ayarı yalnızca Windows 10 Enterprise ve Windows 10 Education sürümleri için geçerlidir.

**Gerekçe:**

Uygulamaların kurumsal olarak yönetilen bir ortamda sessizce yüklenmesi iyi bir güvenlik uygulaması değildir - özellikle uygulamalar üçüncü bir tarafa veri gönderiyorsa.

**Etki:**

Kullanıcılar artık Microsoft'tan kişiselleştirilmiş önerileri ve Microsoft hesaplarıyla ilgili bildirimleri görmeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CloudContent:DisableWi ndowsConsumerFeatures*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\Windows Components\Cloud Content\Microsoft tüketici deneyimlerini kapat*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1511 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu CloudContent.admx/adml tarafından sağlanır.

**18.9.15 Bağlantı**

**18.9.15.1 (L1) 'Eşleştirme için pin iste' seçeneği 'Etkin: İlk kez' VEYA 'Etkin: Her Zaman' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir kablosuz görüntüleme cihazıyla eşleştirme için bir PIN'in gerekli olup olmadığını kontrol eder. Bu ayar için önerilen durum: Etkin: İlk Kez VEYA Etkin: Her Zaman.

**Gerekçe:**

Bu ayar yapılandırılmazsa veya devre dışı bırakılmazsa, kablosuz görüntüleme aygıtlarını sistemle eşleştirirken PIN istenmez, bu da yetkisiz kullanım riskini artırır.

**Etki:**

Yeni kablosuz görüntüleme cihazlarına bağlanmak için yapılan eşleştirme töreni için her zaman bir PIN gerekir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Connect:RequirePinForPairing*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: İlk Kez VEYA Etkin: Her Zaman:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Bağlan\Eşleştirme için pin gerektir*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1607 ve Server 2016 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu WirelessDisplay.admx/adml tarafından sağlanır. Yeni Aşağıdaki eylemlerden birini seçin alt seçeneği daha sonra Windows 10 Sürüm 1809 Yönetim Şablonlarından itibaren eklenmiştir. Eski şablonlarda Etkin'i seçmek, yeni şablonlarda Etkin: İlk Kez'i seçmeye eşdeğerdir.

**18.9.16 Kimlik Bilgileri Kullanıcı Arayüzü**

**18.9.16.1 (L1) 'Parola göster düğmesini görüntüleme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, parola girişi kullanıcı deneyimlerinde parola açığa çıkarma düğmesinin görüntülenmesini yapılandırmanıza olanak tanır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bu, özellikle dokunmatik ekran kullanırken uzun ve karmaşık bir parola girerken yararlı bir özelliktir. Potansiyel risk, ekranınızı gizlice gözlemlerken başka birinin şifrenizi görebilmesidir.

**Etki:**

Bir kullanıcı parola girişi metin kutusuna bir parola yazdıktan sonra parola ifşa düğmesi görüntülenmeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CredUI:DisablePassword Reveal*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Kimlik Bilgisi Kullanıcı Arabirimi\Şifreyi gösterme düğmesini görüntüleme*

**Not:** Bu Grup İlkesi yolu varsayılan olarak var. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu CredUI.admx/adml tarafından sağlanır.

**18.9.16.2 (L1) 'Yönetici hesaplarını yükseklikte numaralandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, parola girişi kullanıcı deneyimlerinde parola açığa çıkarma düğmesinin görüntülenmesini yapılandırmanıza olanak tanır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bu, özellikle dokunmatik ekran kullanırken uzun ve karmaşık bir parola girerken yararlı bir özelliktir. Potansiyel risk, ekranınızı gizlice gözlemlerken başka birinin şifrenizi görebilmesidir.

**Etki:**

Bir kullanıcı parola girişi metin kutusuna bir parola yazdıktan sonra parola ifşa düğmesi görüntülenmeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\CredUI:DisablePassword Reveal*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Kimlik Bilgisi Kullanıcı Arabirimi\Şifreyi gösterme düğmesini görüntüleme*

**Not:** Bu Grup İlkesi yolu varsayılan olarak var. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu CredUI.admx/adml tarafından sağlanır.

**18.9.16.3 (L1) 'Yerel hesaplar için güvenlik sorularının kullanılmasını engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, yerel hesap parolalarını sıfırlamak için güvenlik sorularının kullanılıp kullanılamayacağını denetler. Güvenlik sorusu özelliği, etki alanı hesapları için geçerli değildir, yalnızca iş istasyonundaki yerel hesaplar için geçerlidir. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Kullanıcılar, kullanıcının sosyal medya hesaplarını gözlemleyerek kolayca tahmin edilebilecek veya gizlenebilecek güvenlik soruları oluşturabilir, bu da kötü niyetli bir aktörün yerel kullanıcı hesabı şifresini değiştirmesini ve bilgisayara o kullanıcı hesabı olarak erişmesini kolaylaştırır.

**Etki:**

Yerel kullanıcı hesapları, parolalarını sıfırlamak için güvenlik soruları oluşturamayacak ve kullanamayacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:NoLocalPassword ResetQuestions*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\Windows Components\Credential User Interface\Yerel hesaplar için güvenlik sorularının kullanımını engelle*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1903 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu CredUI.admx/adml tarafından sağlanır.

**18.9.17 Veri toplama ve önizleme yapıları**

**18.9.17.1 (L1) 'Tanılama Verilerine İzin Ver' seçeneği 'Etkin: Tanılama verileri kapalı (önerilmez)' veya 'Etkin: Gerekli tanılama verilerini gönder' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Microsoft'a bildirilen tanılama ve kullanım verilerinin miktarını belirler:

* Değer (0) Tanılama verileri kapalı (önerilmez). Bu değer kullanılarak cihazdan hiçbir tanılama verisi gönderilmez. Bu değer yalnızca Enterprise, Education ve Server sürümlerinde desteklenir. Bu ayarı seçerseniz, kuruluşunuzdaki cihazlar yine güvende olur.
* Değer (1) Gerekli tanılama verilerini gönderin. Bu, Windows'un güvenli, güncel ve beklendiği gibi çalışmasını sağlamak için gereken minimum tanılama verileridir. Bu değerin kullanılması, Ayarlar uygulamasında İsteğe bağlı tanılama verileri kontrolünü devre dışı bırakır.
* Değer (3) İsteğe bağlı tanılama verilerini gönder değeri. Sorunları tespit etmemize, teşhis etmemize ve düzeltmemize ve ayrıca ürün iyileştirmeleri yapmamıza yardımcı olan ek teşhis verileri toplanır. İsteğe bağlı tanılama verilerini göndermeyi seçtiğinizde, gerekli tanı verileri her zaman dahil edilecektir. İsteğe bağlı tanılama verileri, tanılama günlük dosyalarını ve kilitlenme dökümlerini de içerebilir. Hangi isteğe bağlı tanılama verilerinin gönderildiğini daha ayrıntılı bir şekilde kontrol etmek için Döküm Toplama Sınırı ve Tanılama Günlük Toplama Sınırı ilkelerini kullanın.

Windows telemetri ayarları, Windows işletim sistemi ve bazı birinci taraf uygulamalar için geçerlidir. Bu ayar, Windows 10/11 üzerinde çalışan üçüncü taraf uygulamalar için geçerli değildir.

Bu ayar için önerilen durum: Etkin: Tanılama verileri kapalı (önerilmez) veya Etkin: Gerekli tanılama verilerini gönder.

**Not:** Kuruluşunuz Windows Update'e güveniyorsa, önerilen minimum ayar Gerekli tanılama verileri'dir. Tanılama verileri kapalıyken hiçbir Windows Update bilgisi toplanmadığından, güncelleme hatalarıyla ilgili önemli bilgiler gönderilmez. Microsoft bu bilgileri, bu hataların nedenlerini düzeltmek ve güncellemelerin kalitesini artırmak için kullanır.

**Not #2:** Tanılama verilerini etkinleştirme ayarlarını yapılandır kullanıcı arabirimi grup ilkesi, son kullanıcıların veri toplama ayarlarını değiştirmesini önlemek için kullanılabilir.

**Not 3:** Gelişmiş tanılama verileri ayarı, Windows 11 ve Windows Server 2022'de mevcut değildir ve gönderilen isteğe bağlı tanılama verilerinin miktarını denetleyebilen ilkelerle değiştirilmiştir. Bu ayarlar hakkında daha fazla bilgi için Tanılama verilerini Grup İlkesi ve MDM Gerekçesini kullanarak yönetme sayfasını ziyaret edin: Herhangi bir veriyi bir üçüncü taraf satıcıya göndermek bir güvenlik sorunudur ve yalnızca gerektiğinde yapılmalıdır.

**Etki:**

0 veya 1 değerlerinin ayarlanmasının cihazdaki belirli deneyimleri bozacağını unutmayın.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection:AllowTe metri*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın: Tanılama verileri kapalı (önerilmez ) veya Etkin: Gerekli tanılama verilerini gönderin:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Veri Toplama ve Önizleme Yapıları\Tanılama Verilerine İzin Ver*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 11 Sürüm 21H2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu DataCollection.admx/adml tarafından sağlanır.

**Not 2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Telemetriye İzin Ver olarak adlandırılmıştı, ancak Windows 11 Sürüm 21H2 Yönetim Şablonlarından başlayarak Tanılama Verilerine İzin Ver olarak yeniden adlandırıldı.

**18.9.17.2 (L2) 'Bağlı Kullanıcı Deneyimi ve Telemetri hizmeti için Kimliği Doğrulanmış Proxy kullanımını yapılandır' seçeneği 'Etkin: Kimliği Doğrulanmış Proxy kullanımını devre dışı bırak' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Bağlı Kullanıcı Deneyimi ve Telemetri hizmetinin, verileri Microsoft'a geri göndermek için otomatik olarak kimliği doğrulanmış bir proxy kullanıp kullanamayacağını denetler. Bu ayar için önerilen durum: Etkin: Kimliği Doğrulanmış Proxy kullanımını devre dışı bırakın.

**Gerekçe:**

Herhangi bir veriyi bir üçüncü taraf satıcıya göndermek bir güvenlik sorunudur ve yalnızca gerektiğinde yapılmalıdır.

**Etki:**

Bağlı Kullanıcı Deneyimi ve Telemetri hizmetinin, kimliği doğrulanmış bir proxy kullanılarak otomatik olarak engellenecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection:Disable EnterpriseAuthProxy*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Kimliği Doğrulanmış Proxy kullanımını devre dışı bırakın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Veri Toplama ve Önizleme Yapıları\Bağlı Kullanıcı için Kimliği Doğrulanmış Proxy kullanımını yapılandırın Deneyim ve Telemetri hizmeti*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1703 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu DataCollection.admx/adml tarafından sağlanır.

**18.9.17.3 (L1) ‘OneSettings indirmelerini devre dışı bırak’ seçeneği ‘Etkin’(Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows'un yapılandırma ayarlarını indirmek için OneSettings hizmetine bağlanmaya çalışıp çalışmayacağını denetler. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bir üçüncü taraf satıcıya veri göndermek bir güvenlik sorunudur ve yalnızca gerektiği şekilde yapılmalıdır.

**Etki:**

Windows, yapılandırma ayarlarını indirmek için OneSettings hizmetine bağlanmayacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection:Disable OneSettingsDownloads*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonlar\Windows Bileşenleri\Veri Toplama ve Önizleme Yapıları\OneSettings İndirmelerini Devre Dışı Bırak*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 21H2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu DataCollection.admx/adml tarafından sağlanır.

**18.9.17.4 (L1) 'Geri bildirim bildirimlerini gösterme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir kuruluşun cihazlarının Microsoft'tan gelen geri bildirim sorularını göstermesini engellemesine olanak tanır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Kullanıcılar, kurumsal olarak yönetilen bir ortamda 3. taraf satıcılara herhangi bir geri bildirim göndermemelidir.

**Etki:**

Kullanıcılar artık Windows Geri Bildirim uygulaması aracılığıyla geri bildirim bildirimlerini görmeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection:DoNotSh owFeedbackNotifications*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonlar\Windows Bileşenleri\Veri Toplama ve Önizleme Yapıları\Geri bildirim bildirimlerini gösterme*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1511 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu FeedbackNotifications.admx/adml tarafından sağlanır.

**18.9.17.5 (L1) 'OneSettings Denetimini Etkinleştir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows kayıtlarının OneSettings hizmetiyle Operational EventLog'a bağlanma girişiminde bulunup bulunmayacağını denetler. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Olaylar kaydedilmezse, sistem sorunlarının veya kötü niyetli kullanıcıların yetkisiz faaliyetlerinin temel nedenini belirlemek zor veya imkansız olabilir.

**Etki:**

Sisteme herhangi bir etkisi olmamalıdır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\DataCollection:EnableOneSettin gsAuditing*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\ Windows Bileşenleri\Veri Toplama ve Önizleme Yapıları\OneSettings Denetimini Etkinleştir*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 21H2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu DataCollection.admx/adml tarafından sağlanır.

**18.9.17.6 (L1) 'Tanılama Günlüğü Toplamayı Sınırla' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, cihazdaki bir sorunu gidermek için daha fazla bilgi gerektiğinde ek tanı günlüklerinin toplanıp toplanmadığını kontrol eder. Bu ayar için önerilen durum: Etkin.

**Not:** Tanılama günlükleri yalnızca, aygıt isteğe bağlı tanılama verilerini göndermek üzere yapılandırıldığında gönderilir. Tanılama verileri öneriyle sınırlıdır Tanı Verilerine İzin Ver Etkin olarak ayarlanmıştır: Tanılama verileri kapalı (önerilmez) veya Etkin: Yalnızca temel bilgileri göndermek için gerekli tanı verilerini gönderin.

**Gerekçe:**

Bir üçüncü taraf satıcıya veri göndermek bir güvenlik sorunudur ve yalnızca gerektiğinde yapılmalıdır.

**Etki:**

Tanılama günlükleri ve kilitlenme dökümleri gibi bilgiler Microsoft'a iletilmek üzere toplanmaz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection:LimitDi agnosticLogCollection*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Veri Toplama ve Önizleme Yapıları\Limit Tanılama Günlük Toplama*

**Not:** Bu Grup İlkesi yolu mevcut olmayabilir varsayılan olarak. Microsoft Windows 10 Sürüm 21H2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu DataCollection.admx/adml tarafından sağlanır.

**18.9.17.7 (L1) 'Limit Dump Collection' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir sorunu gidermek için daha fazla bilgi gerektiğinde toplanabilecek dökümlerin türünü sınırlar. Bu ayar için önerilen durum: Etkin.

**Not:** Dökümler, yalnızca cihaz isteğe bağlı tanılama verileri göndermek üzere yapılandırıldığında gönderilir. Tanılama verileri öneriyle sınırlıdır Tanılama Verilerine İzin Ver'in Etkin olarak ayarlandığından emin olun: Tanılama verileri kapalı (önerilmez) veya Etkin: Yalnızca temel bilgileri göndermek için gerekli tanı verilerini gönderin.

**Gerekçe:**

Bir üçüncü taraf satıcıya veri göndermek bir güvenlik sorunudur ve yalnızca gerektiği şekilde yapılmalıdır.

**Etki:**

Windows Hata Bildirimi, çekirdek mini ve kullanıcı modu triyaj bellek dökümleri göndermekle sınırlıdır ve hassas bilgilerin Microsoft'a gönderilmesi riskini azaltır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DataCollection:LimitDu mpCollection*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın.

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Veri Toplama ve Önizleme Yapıları\Limit Döküm Toplama*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 21H2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu DataCollection.admx/adml tarafından sağlanır.

**18.9.17.8 (L1) 'Insider derlemeleri üzerinde kullanıcı denetimini değiştir' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların Windows Update için Gelişmiş Seçenekler'deki Insider derleme denetimlerine erişip erişemeyeceğini belirler. Bu denetimler, "Insider derlemelerini alın" altında bulunur ve kullanıcıların cihazlarını Windows önizleme yazılımını indirmek ve yüklemek için kullanılabilir hale getirmelerini sağlar. Bu ayar için önerilen durum: Devre Dışı.

**Not:** Bu ilke ayarı, Sürüm 1703'e kadar yalnızca Windows 10 Pro veya Windows 10 Enterprise çalıştıran cihazlar için geçerlidir. Sürüm 1709 veya daha yenisi için Microsoft, Önizleme yapılarını yönet ayarının (Kural 18.9.103.1.1) kullanılmasını önerir. Ortamdaki daha eski Windows 10 yapılarının hala zorunlu kılınmasını sağlamak için bu ayarı karşılaştırmalı değerlendirmede tuttuk.

**Gerekçe:**

Kurumsal olarak yönetilen bir ortamda deneysel özelliklere izin verilmesi riskli olabilir, çünkü bu, sistemlerde hatalar ve güvenlik açıkları oluşturarak bir saldırganın erişmesini kolaylaştırabilir. Genellikle yalnızca üretime hazır yapıların kullanılması tercih edilir.

**Etki:**

"Insider derlemelerini edinin" öğesi kullanılamayacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PreviewBuilds:AllowBui ldPreview*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Veri Toplama ve Önizleme Yapıları\Insider yapıları üzerinde kullanıcı denetimini değiştir*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değil. Microsoft Windows 10 RTM (Sürüm 1507) Yönetim Şablonları (veya daha yenisi) ile birlikte verilen Grup İlkesi şablonu AllowBuildPreview.admx/adml tarafından sağlanır.

**18.9.18 Teslimat Optimizasyonu**

**18.9.18.1 (L1) 'İndirme Modu' seçeneği 'Etkin: İnternet' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Teslim İyileştirme'nin Windows Güncellemeleri, Uygulamalar ve Uygulama güncellemelerinin indirilmesinde kullanabileceği indirme yöntemini belirtir. Aşağıdaki yöntemler desteklenir:

* 0 = yalnızca HTTP, eşleme yok.
* 1 = HTTP, aynı NAT arkasında eşleme ile harmanlanmıştır.
* 2 = HTTP, özel bir grup üzerinden eşleme ile harmanlanmıştır. Eşleme, varsayılan olarak aynı Active Directory Sitesindeki (varsa) veya aynı etki alanındaki cihazlarda gerçekleşir. Bu seçenek seçildiğinde, eşleme NAT'ları geçecektir. Özel bir grup oluşturmak için Grup Kimliğini Mod 2 ile birlikte kullanın.
* 3 = İnternet Eşlemesi ile harmanlanmış HTTP.
* 99 = Eşleme olmadan basit indirme modu. Teslim İyileştirme yalnızca HTTP kullanarak indirilir ve Teslim İyileştirme bulut hizmetleriyle iletişim kurmaya çalışmaz.
* 100 = Baypas modu. Teslimat Optimizasyonu'nu kullanmayın ve bunun yerine BITS'yi kullanın.

Bu ayar için önerilen durum, DIŞINDA herhangi bir değerdir: Etkin: İnternet (3).

**Not:** Enterprise, Enterprise LTSB veya Education dışındaki tüm SKU'larda varsayılan, Etkin'dir: İnternet (3), bu nedenle diğer SKU'larda bunu farklı bir değere ayarladığınızdan emin olun.

**Gerekçe:**

Gizlilik endişeleri ve güvenlik riskleri nedeniyle, güncellemeler yalnızca doğrudan Microsoft'tan veya dahili ağdaki, güncellemelerini güvenilir bir kaynaktan alan ve ağ yöneticisi tarafından onaylanan güvenilir bir makineden indirilmelidir.

**Etki:**

Makineler, İnternet'teki benzerlerinden güncellemeleri indiremeyecek. Etkin: Yalnızca HTTP (0), Etkin: Basit (99) veya Etkin: Atlama (100) olarak ayarlanırsa, makineler aynı LAN üzerindeki diğer makinelerden güncellemeleri indiremez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\DeliveryOptimization:D ODownloadMode*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Etkin dışında herhangi bir değere ayarlayın: İnternet ( 3):

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Teslim İyileştirme\İndirme Modu*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 RTM (Sürüm 1507) Yönetim Şablonları (veya daha yenisi) ile birlikte verilen Grup İlkesi şablonu DeliveryOptimization.admx/adml tarafından sağlanır.

**18.9.19 Masaüstü Gadget'ları**

**18.9.20 Masaüstü** **Pencere Yöneticisi**

**18.9.21 Aygıt ve Sürücü Uyumluluğu**

**18.9.22 Cihaz kaydı (eski adıyla Workplace Join)**

**18.9.23 Dijital Dolap**

**18.9.24 Uç kullanıcı arayüzü**

**18.9.25 NUMBER**

**18.9.26 Etkinlik Yönlendirme**

**18.9.27 Olay Günlüğü** **Hizmeti**

**18.9.27.1 Uygulama**

**18.9.27.1.1 (L1) 'Uygulama: Günlük dosyası maksimum boyutuna ulaştığında Olay Günlüğü davranışını denetle' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, günlük dosyası maksimum boyutuna ulaştığında Olay Günlüğü davranışını denetler. Bu ayar için önerilen durum: Devre Dışı.

**Not:** Eski olaylar, tam ilke ayarı yapıldığında Yedekleme günlüğüne göre otomatik olarak tutulabilir veya tutulmayabilir. Gerekçe: Yeni olaylar kaydedilmezse, sistem sorunlarının veya kötü niyetli kullanıcıların yetkisiz faaliyetlerinin temel nedenini belirlemek zor veya imkansız olabilir.

**Etki:** Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Application:R etention*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Windows Bileşenleri\Olay Günlüğü Hizmeti\Application\Kontrol Günlük dosyası maksimum boyutuna ulaştığında Olay Günlüğü davranışı*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan EventLog.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**Not #2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Eski olayları koru olarak adlandırılmıştı, ancak Windows 8.0 ve Server 2012 (R2 olmayan Yönetim Şablonları) ile başlayarak yeniden adlandırıldı.

**18.9.27.1.2 (L1) 'Uygulama: Maksimum günlük dosyası boyutunu belirtin' seçeneği 'Etkin: 32.768 veya üzeri' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, günlük dosyasının maksimum boyutunu kilobayt olarak belirtir. Maksimum günlük dosyası boyutu, kilobayt artışlarla 1 megabayt (1,024 kilobayt) ile 4 terabayt (4,194,240 kilobayt) arasında yapılandırılabilir. Bu ayar için önerilen durum: Etkin: 32.768 veya üstü.

**Gerekçe:**

Olaylar kaydedilmezse, sistem sorunlarının veya kötü niyetli kullanıcıların yetkisiz faaliyetlerinin temel nedenini belirlemek zor veya imkansız olabilir.

**Etki:**

Olay günlükleri kapasiteye kadar dolduğunda, her biri için saklama yöntemi, bilgisayarın en eski girişlerin üzerine en yeni girişlerin üzerine yazacağı şekilde ayarlanmadıkça, bilgi kaydetmeyi durduracaktır. Son verilerin kaybolması riskini azaltmak için, gerektiğinde eski olayların üzerine yazılacak şekilde saklama yöntemini yapılandırabilirsiniz. Bu yapılandırmanın sonucu, daha eski olayların günlüklerden kaldırılmasıdır. Saldırganlar, saldırılarının herhangi bir kanıtının üzerine yazmak için çok sayıda yabancı olay üretebildikleri için bu tür bir yapılandırmadan yararlanabilirler. Olay günlüğü verilerinin arşivlenmesini ve yedeklenmesini otomatikleştirirseniz bu riskler biraz azaltılabilir. İdeal olarak, özel olarak izlenen tüm olaylar, Microsoft System Center Operations Manager (SCOM) veya başka bir otomatik izleme aracı kullanan bir sunucuya gönderilmelidir. Böyle bir yapılandırma özellikle önemlidir çünkü bir sunucunun güvenliğini başarıyla ihlal eden bir saldırgan Güvenlik günlüğünü temizleyebilir. Tüm olaylar bir izleme sunucusuna gönderilirse, saldırganın faaliyetleri hakkında adli bilgi toplayabilirsiniz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Application:M axSize*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın: 32.768 veya üstü:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Olay Günlüğü Hizmeti\Uygulama\Maksimum günlük dosyası boyutunu (KB) belirtin*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerde bulunan EventLog.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**Not 2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Maksimum Günlük Boyutu (KB) olarak adlandırılmıştı, ancak Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonlarından başlayarak yeniden adlandırıldı.

**18.9.27.2 Güvenlik**

**18.9.27.2.1 (L1) 'Güvenlik: Günlük dosyası maksimum boyutuna ulaştığında Olay Günlüğü davranışını denetle' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, günlük dosyası maksimum boyutuna ulaştığında Olay Günlüğü davranışını denetler. Bu ayar için önerilen durum: Devre Dışı.

**Not:** Eski olaylar, tam ilke ayarı yapıldığında Yedekleme günlüğüne göre otomatik olarak tutulabilir veya tutulmayabilir.

**Gerekçe:**

Yeni olaylar kaydedilmezse, sistem sorunlarının veya kötü niyetli kullanıcıların yetkisiz faaliyetlerinin temel nedenini belirlemek zor veya imkansız olabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Security:Rete ntion*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Olay Günlüğü Hizmeti\Güvenlik\Kontrol Günlük dosyası maksimum boyutuna ulaştığında Olay Günlüğü davranışı*

**Not :** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu EventLog.admx/adml tarafından sağlanır.

**Not #2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Eski olayları koru olarak adlandırıldı, ancak Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonlarından başlayarak yeniden adlandırıldı.

**18.9.27.2.2 (L1) 'Güvenlik: Maksimum günlük dosyası boyutunu belirtin (KB)' seçeneği 'Etkin: 196.608 veya üzeri' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, günlük dosyasının maksimum boyutunu kilobayt olarak belirtir. Maksimum günlük dosyası boyutu, kilobayt artışlarla 1 megabayt (1,024 kilobayt) ile 4 terabayt (4,194,240 kilobayt) arasında yapılandırılabilir. Bu ayar için önerilen durum: Etkin: 196.608 veya üstü.

**Gerekçe:**

Olaylar kaydedilmezse, sistem sorunlarının veya kötü niyetli kullanıcıların yetkisiz faaliyetlerinin temel nedenini belirlemek zor veya imkansız olabilir.

**Etki:**

Olay günlükleri kapasiteye kadar dolduğunda, her biri için saklama yöntemi, bilgisayarın en eski girişlerin üzerine en yeni girişlerin üzerine yazacağı şekilde ayarlanmadıkça, bilgi kaydetmeyi durduracaktır. Son verilerin kaybolması riskini azaltmak için, gerektiğinde eski olayların üzerine yazılacak şekilde saklama yöntemini yapılandırabilirsiniz. Bu yapılandırmanın sonucu, daha eski olayların günlüklerden kaldırılmasıdır. Saldırganlar, saldırılarının herhangi bir kanıtının üzerine yazmak için çok sayıda yabancı olay üretebildikleri için bu tür bir yapılandırmadan yararlanabilirler. Olay günlüğü verilerinin arşivlenmesini ve yedeklenmesini otomatikleştirirseniz bu riskler biraz azaltılabilir. İdeal olarak, özel olarak izlenen tüm olaylar, Microsoft System Center Operations Manager (SCOM) veya başka bir otomatik izleme aracı kullanan bir sunucuya gönderilmelidir. Böyle bir yapılandırma özellikle önemlidir çünkü bir sunucunun güvenliğini başarıyla ihlal eden bir saldırgan Güvenlik günlüğünü temizleyebilir. Tüm olaylar bir izleme sunucusuna gönderilirse, saldırganın faaliyetleri hakkında adli bilgi toplayabilirsiniz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Security:MaxSize*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: 196.608 veya üstü:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Olay Günlüğü Hizmeti\Güvenlik\Maksimum günlük dosyası boyutunu (KB) belirtin*

**Not:** Bu Grup İlkesi yolu, tüm sürümlerde bulunan EventLog.admx/adml Grup İlkesi şablonu tarafından sağlanır. Microsoft Windows Yönetim Şablonları.

**Not 2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Maksimum Günlük Boyutu (KB) olarak adlandırılmıştı, ancak Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonlarından başlayarak yeniden adlandırıldı.

**18.9.27.3 Kurulum**

**18.9.27.3.1 (L1) 'Kurulum: Günlük dosyası maksimum boyutuna ulaştığında Olay Günlüğü davranışını denetle' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, günlük dosyası maksimum boyutuna ulaştığında Olay Günlüğü davranışını denetler. Bu ayar için önerilen durum: Devre Dışı.

**Not:** Eski olaylar, tam ilke ayarı yapıldığında Yedekleme günlüğüne göre otomatik olarak tutulabilir veya tutulmayabilir.

**Gerekçe:**

Yeni olaylar kaydedilmezse, sistem sorunlarının veya kötü niyetli kullanıcıların yetkisiz faaliyetlerinin temel nedenini belirlemek zor veya imkansız olabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Setup:Retenti on*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Olay Günlüğü Hizmeti\Kur\Kontrol Günlük dosyası maksimum boyutuna ulaştığında Olay Günlüğü davranışı*

**Not :** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu EventLog.admx/adml tarafından sağlanır.

**Not #2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Eski olayları koru olarak adlandırıldı, ancak Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonlarından başlayarak yeniden adlandırıldı.

**18.9.27.3.2 (L1) 'Kurulum: Maksimum günlük dosyası boyutunu belirtin' seçeneği 'Etkin: 32.768 veya üzeri' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, günlük dosyasının maksimum boyutunu kilobayt olarak belirtir. Maksimum günlük dosyası boyutu, kilobayt artışlarla 1 megabayt (1,024 kilobayt) ile 4 terabayt (4,194,240 kilobayt) arasında yapılandırılabilir. Bu ayar için önerilen durum: Etkin: 32.768 veya üstü.

**Gerekçe:**

Olaylar kaydedilmezse, sistem sorunlarının veya kötü niyetli kullanıcıların yetkisiz faaliyetlerinin temel nedenini belirlemek zor veya imkansız olabilir

**Etki:**

Olay günlükleri kapasiteye dolduğunda, her biri için saklama yöntemi ayarlanmadıkça bilgileri kaydetmeyi durdururlar. böylece bilgisayar en eski girişlerin üzerine en yenilerini yazacaktır. Son verilerin kaybolması riskini azaltmak için, gerektiğinde eski olayların üzerine yazılacak şekilde saklama yöntemini yapılandırabilirsiniz. Bu yapılandırmanın sonucu, daha eski olayların günlüklerden kaldırılmasıdır. Saldırganlar, saldırılarının herhangi bir kanıtının üzerine yazmak için çok sayıda yabancı olay üretebildikleri için bu tür bir yapılandırmadan yararlanabilirler. Olay günlüğü verilerinin arşivlenmesini ve yedeklenmesini otomatikleştirirseniz bu riskler biraz azaltılabilir. İdeal olarak, özel olarak izlenen tüm olaylar, Microsoft System Center Operations Manager (SCOM) veya başka bir otomatik izleme aracı kullanan bir sunucuya gönderilmelidir. Böyle bir yapılandırma özellikle önemlidir çünkü bir sunucunun güvenliğini başarıyla ihlal eden bir saldırgan Güvenlik günlüğünü temizleyebilir. Tüm olaylar bir izleme sunucusuna gönderilirse, saldırganın faaliyetleri hakkında adli bilgi toplayabilirsiniz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\Setup:MaxSize*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın: 32.768 veya üstü:

*Bilgisayar Yapılandırma\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Olay Günlüğü Hizmeti\Kurulum\Maksimum günlük dosyası boyutunu (KB) belirtin*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan EventLog.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**Not 2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Maksimum Günlük Boyutu (KB) olarak adlandırıldı, ancak Windows 8.0 ve Server 2012 (R2 olmayan Yönetim Şablonları) ile yeniden adlandırıldı.

**18.9.27.4 Sistem**

**18.9.27.4.1 (L1) 'Sistem: Günlük dosyası maksimum boyutuna ulaştığında Olay Günlüğü davranışını kontrol et' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, günlük dosyası maksimum boyutuna ulaştığında Olay Günlüğü davranışını denetler. Bu ayar için önerilen durum: Devre Dışı.

**Not:** Eski olaylar, tam ilke ayarı yapıldığında Yedekleme günlüğüne göre otomatik olarak tutulabilir veya tutulmayabilir.

**Gerekçe:**

Yeni olaylar kaydedilmezse, sistem sorunlarının veya kötü niyetli kullanıcıların yetkisiz faaliyetlerinin temel nedenini belirlemek zor veya imkansız olabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\System:Retent ion*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Olay Günlüğü Hizmeti\Sistem\Kontrol Günlük dosyası maksimum boyutuna ulaştığında Olay Günlüğü davranışı*

**Not :** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu EventLog.admx/adml tarafından sağlanır.

**Not 2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Eski olayları koru olarak adlandırıldı, ancak Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonlarından başlayarak yeniden adlandırıldı.

**18.9.27.4.2 (L1) 'Sistem: Maksimum günlük dosyası boyutunu belirtin' seçeneği 'Etkin: 32.768 veya üzeri' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, günlük dosyasının maksimum boyutunu kilobayt olarak belirtir. Maksimum günlük dosyası boyutu, kilobayt artışlarla 1 megabayt (1,024 kilobayt) ile 4 terabayt (4,194,240 kilobayt) arasında yapılandırılabilir. Bu ayar için önerilen durum: Etkin: 32.768 veya üstü.

**Gerekçe:**

Olaylar kaydedilmezse, sistem sorunlarının veya kötü niyetli kullanıcıların yetkisiz faaliyetlerinin temel nedenini belirlemek zor veya imkansız olabilir

**Etki:**

Olay günlükleri kapasiteye dolduğunda, her biri için saklama yöntemi ayarlanmadıkça bilgileri kaydetmeyi durdururlar. böylece bilgisayar en eski girişlerin üzerine en yenilerini yazacaktır. Son verilerin kaybolması riskini azaltmak için, gerektiğinde eski olayların üzerine yazılacak şekilde saklama yöntemini yapılandırabilirsiniz. Bu yapılandırmanın sonucu, daha eski olayların günlüklerden kaldırılmasıdır. Saldırganlar, saldırılarının herhangi bir kanıtının üzerine yazmak için çok sayıda yabancı olay üretebildikleri için bu tür bir yapılandırmadan yararlanabilirler. Olay günlüğü verilerinin arşivlenmesini ve yedeklenmesini otomatikleştirirseniz bu riskler biraz azaltılabilir. İdeal olarak, özel olarak izlenen tüm olaylar, Microsoft System Center Operations Manager (SCOM) veya başka bir otomatik izleme aracı kullanan bir sunucuya gönderilmelidir. Böyle bir yapılandırma özellikle önemlidir çünkü bir sunucunun güvenliğini başarıyla ihlal eden bir saldırgan Güvenlik günlüğünü temizleyebilir. Tüm olaylar bir izleme sunucusuna gönderilirse, saldırganın faaliyetleri hakkında adli bilgi toplayabilirsiniz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\EventLog\System:MaxSize*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın: 32.768 veya üstü:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Olay Günlüğü Hizmeti\Sistem\Maksimum günlük dosyası boyutunu (KB) belirtin*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerde bulunan Grup İlkesi şablonu EventLog.admx/adml tarafından sağlanır.

**Not 2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Maksimum Günlük Boyutu (KB) olarak adlandırıldı, ancak Windows 8.0 ve Server 2012 (R2 olmayan Yönetim Şablonları) ile yeniden adlandırıldı.

**18.9.28 Etkinlik Kaydı**

**18.9.29 Olay Görüntüleyicisi**

**18.9.30 Aile Koruması (eski adıyla Ebeveyn Denetimleri)**

**18.9.31 Dosya Gezgini (eski adıyla Windows Gezgini)**

**18.9.31.2 (L1) 'Explorer için Veri Yürütme Engellemesini Kapat' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Veri Yürütme Engellemesi'ni devre dışı bırakmak, belirli eski eklenti uygulamalarının Explorer'ı sonlandırmadan çalışmasına izin verebilir. Bu ayar için önerilen durum: Devre Dışı.

**Not:** Bazı eski eklenti uygulamaları ve diğer yazılımlar Veri Yürütme Engellemesi ile çalışmayabilir ve söz konusu eklenti/yazılım için bir istisna tanımlanmasını gerektirir.

**Gerekçe:**

Veri Yürütme Engellemesi, Explorer tarafından desteklenen ve belirli kötü amaçlı yazılım türlerinin etkisini sınırlamaya yardımcı olan önemli bir güvenlik özelliğidir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Explorer:NoDataExecutionPrevention*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\Windows Components\File Explorer\Explorer için Veri Yürütme Engellemesini Kapat*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu Explorer.admx/adml tarafından sağlanır.

**18.9.31.3 (L1) 'Bozulmada yığın sonlandırmayı kapat' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bozulma durumunda yığın sonlandırması olmadan, bir Dosya Gezgini oturumu bozulduğunda eski eklenti uygulamaları çalışmaya devam edebilir. Yolsuzlukta yığın sonlandırmanın etkin olduğundan emin olmak bunu önleyecektir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bir uygulamanın oturumu bozulduktan sonra çalışmasına izin vermek, sistemin risk duruşunu artırır.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Explorer:NoHeapTermina tionOnCorruption*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonlar\Windows Bileşenleri\Dosya Gezgini\Yolsuzluk durumunda yığın sonlandırmayı kapat*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu Explorer.admx/adml tarafından sağlanır.

**18.9.31.4 (L1) 'Kabuk protokolü korumalı modunu kapat' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kabuk protokolünün sahip olabileceği işlevsellik miktarını yapılandırmanıza olanak tanır. Bu protokolün tam işlevselliğini kullanırken, uygulamalar klasörleri açabilir ve dosyaları başlatabilir. Korumalı mod, bu protokolün işlevselliğini azaltır ve uygulamaların yalnızca sınırlı sayıda klasör açmasına izin verir. Uygulamalar, korumalı moddayken bu protokolle dosyaları açamaz. Windows'un güvenliğini artırmak için bu protokolü korumalı modda bırakmanız önerilir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Dosya ve klasörlerin açılmasını sınırlı bir kümeyle sınırlamak, sistemin saldırı yüzeyini azaltır.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\Explore r:PreXPSP2ShellProtocolBehavior*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Windows Bileşenleri\Dosya Gezgini\Kabuk protokolü korumalı modunu kapat*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan WindowsExplorer.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.9.32 Dosya Geçmişi**

**18.9.33 Cihazımı Bul**

**18.9.34 Oyun Gezgini**

**18.9.35 El yazısı**

**18.9.36 Ev Grubu**

**18.9.36.1 (L1) 'Bilgisayarın ev grubuna katılmasını engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Varsayılan olarak, kullanıcılar bilgisayarlarını bir ev ağındaki Ev Grubuna ekleyebilir. Bu ayar için önerilen durum: Etkin.

**Not:** Ev Grubu özelliği, Windows 7'den Windows 10 Sürüm 1709'a kadar Windows'un tüm iş istasyonu sürümlerinde mevcuttur. Microsoft, Windows 10 Sürüm 1803'ten başlayarak bu özelliği tamamen kaldırmıştır. Ancak ortamınızda hala Windows 10 Sürüm 1709 (veya daha eski) varsa iş istasyonlarındaysa, bu ayar bu sistemlerde Ev Grubunu devre dışı bırakmak için önemli olmaya devam eder.

**Gerekçe:**

Etki alanına katılmış bir bilgisayardaki kaynaklar bir Ev Grubu ile paylaşılamazken, etki alanına katılmış bilgisayardan gelen bilgiler Ev Grubundaki diğer bilgisayarlara sızdırılabilir. Etki: Bu bilgisayardaki bir kullanıcı bu bilgisayarı bir Ev Grubuna ekleyemez. Bu ayar, diğer ağ paylaşım özelliklerini etkilemez. Ev ağlarındaki yazıcılara ve diğer paylaşılan cihazlara erişen mobil kullanıcılar, Ev Grubu işlevselliğinin sağladığı kullanım kolaylığından yararlanamaz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\HomeGroup:DisableHomeGroup*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*BilgisayarYapılandırması\İlkeler\YönetimTemplates\WindowsComponents\HomeGroup\Bilgisayarın bir ev grubuna katılmasını engelle*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu Sharing.admx/adml tarafından sağlanır.

**18.9.37 İnsan Varlığı**

**18.9.38 Video İçe Aktar**

**18.9.39 Internet Explorer**

**18.9.40 İnternet Bilgi Hizmetleri**

**18.9.41 Konum ve Sensörler**

**18.9.41.1 (L2) 'Konumu kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bilgisayarın konum özelliğini kapatır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bu ayar, konum özelliğini etkiler (ör. GPS veya diğer konum izleme). Güvenlik açısından, çoğu durumda yazılıma konumunuzu açıklamak iyi bir fikir değildir, ancak haritalama yazılımı gibi meşru kullanımlar vardır. Ancak, yüksek güvenlikli ortamlarda kullanılmamalıdırlar.

**Etki:**

Konum özelliği kapatılır ve bilgisayardaki tüm programların konum özelliğinden alınan konum bilgilerini kullanması engellenir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\LocationAndSensors:DisableLocation*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Konum ve Sensörler\Konumu kapat*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu Sensors.admx/adml tarafından sağlanır.

**18.9.42 Bakım Zamanlayıcı**

**18.9.43 Haritalar**

**18.9.44 MDM**

**18.9.45 Mesajlaşma**

**18.9.45.1 (L2) 'Message Service Cloud** **Senkronizasyonuna İzin Ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, hücresel metin mesajlarının Microsoft'un bulut hizmetlerine yedeklenmesine ve geri yüklenmesine izin verir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Yüksek güvenlikli bir ortamda, bu veriler hassas bilgiler içerebileceğinden, veriler hiçbir zaman 3. şahıslara gönderilmemelidir.

**Etki:**

Hücresel metin mesajları Microsoft'un bulut hizmetlerine yedeklenmeyecek (veya geri yüklenmeyecek).

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Messaging:AllowMessage Sync*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Messaging\İleti Hizmetine İzin Ver Bulut Senkronizasyonu*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1709 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu Messaging.admx/adml tarafından sağlanır.

**18.9.46 Microsoft hesabı**

**18.9.46.1 (L1) 'Tüm tüketiciler için Microsoft hesabı kullanıcı kimlik doğrulamasını engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, cihazdaki uygulamaların ve hizmetlerin Windows OnlineID ve WebAccountManager API'leri aracılığıyla yeni tüketici Microsoft hesabı kimlik doğrulamasını kullanıp kullanamayacağını belirler. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Kimlik yönetimi ilkelerini etkin bir şekilde uygulamak ve bilgisayarlarında hangi hesapların kullanıldığını sıkı bir şekilde kontrol etmek isteyen kuruluşlar, muhtemelen Microsoft hesaplarını engellemek isteyeceklerdir. Kuruluşların ayrıca bilgi sistemleri için geçerli olan uyumluluk standartlarının gereksinimlerini karşılamak için Microsoft hesaplarını engellemesi gerekebilir.

**Etki:**

Cihazdaki tüm uygulamaların ve hizmetlerin, Windows OnlineID ve WebAccountManager API'leri aracılığıyla tüketici Microsoft hesaplarını kullanan yeni kimlik doğrulamaları engellenecektir. Web tarayıcılarında veya OAuth kullanan uygulamalarda doğrudan kullanıcı tarafından gerçekleştirilen kimlik doğrulama işlemleri etkilenmeyecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftAccount:DisableUserAuth*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\ Windows Bileşenleri\Microsoft hesapları\Tüm tüketici Microsoft hesabı kullanıcı kimlik doğrulamasını engelle*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1703 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu MSAPolicy.admx/adml tarafından sağlanır.

**18.9.47 Microsoft Defender Antivirüs (eski adıyla Windows Defender ve Windows Defender Antivirus)**

**18.9.47.1 İstemci Arayüzü**

**18.9.47.2 Cihaz Kontrolü**

**18.9.47.3 İstisnalar**

**18.9.47.4 MAPS**

**18.9.47.4.1 (L1) 'Microsoft MAPS'e raporlama için yerel ayar geçersiz kılma özelliğini yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, cihazdaki uygulamaların ve hizmetlerin Windows OnlineID ve WebAccountManager API'leri aracılığıyla yeni tüketici Microsoft hesabı kimlik doğrulamasını kullanıp kullanamayacağını belirler. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Kimlik yönetimi ilkelerini etkin bir şekilde uygulamak ve bilgisayarlarında hangi hesapların kullanıldığını sıkı bir şekilde kontrol etmek isteyen kuruluşlar, muhtemelen Microsoft hesaplarını engellemek isteyeceklerdir. Kuruluşların ayrıca bilgi sistemleri için geçerli olan uyumluluk standartlarının gereksinimlerini karşılamak için Microsoft hesaplarını engellemesi gerekebilir.

**Etki:**

Cihazdaki tüm uygulamaların ve hizmetlerin, Windows OnlineID ve WebAccountManager API'leri aracılığıyla tüketici Microsoft hesaplarını kullanan yeni kimlik doğrulamaları engellenecektir. Web tarayıcılarında veya OAuth kullanan uygulamalarda doğrudan kullanıcı tarafından gerçekleştirilen kimlik doğrulama işlemleri etkilenmeyecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftAccount:DisableUserAuth*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\ Windows Bileşenleri\Microsoft hesapları\Tüm tüketici Microsoft hesabı kullanıcı kimlik doğrulamasını engelle*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1703 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu MSAPolicy.admx/adml tarafından sağlanır.

**18.9.47.4.2 (L2) 'Microsoft MAPS'e Katıl' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Microsoft'un Windows Defender Virüsten Koruma Bulut Koruma Hizmeti ve ardından Microsoft Defender Virüsten Koruma Bulut Koruma Hizmeti olarak yeniden adlandırdığı Microsoft Etkin Koruma Hizmetine (MAPS) katılmanıza olanak tanır. Microsoft MAPS / Microsoft Defender Antivirus Bulut Koruma Hizmeti, olası tehditlere nasıl yanıt vereceğinizi seçmenize yardımcı olan çevrimiçi topluluktur. Topluluk ayrıca yeni kötü amaçlı yazılım bulaşmalarının yayılmasını durdurmaya da yardımcı olur. Algılanan yazılım hakkında temel veya ek bilgiler göndermeyi seçebilirsiniz. Ek bilgiler, Microsoft'un yeni tanımlar oluşturmasına ve bilgisayarınızı korumasına yardımcı olur. Olası seçenekler şunlardır:

* (0x0) Devre dışı (varsayılan)
* (0x1) Temel üyelik
* (0x2) Gelişmiş üyelik

Temel üyelik, uyguladığınız eylemlerden veya yazılımın nereden geldiği dahil olmak üzere algılanan yazılım hakkında Microsoft'a temel bilgileri gönderir veya otomatik olarak uygulanan ve eylemlerin başarılı olup olmadığı. Temel bilgilere ek olarak gelişmiş üyelik, Microsoft'a kötü amaçlı yazılım casus yazılımları ve yazılım dosya adlarının konumu, yazılımın nasıl çalıştığı ve bilgisayarınızı nasıl etkilediği dahil olmak üzere potansiyel olarak istenmeyen yazılımlar hakkında daha fazla bilgi gönderir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Gönderilecek bilgiler, zararlı yazılımların kaldırılması durumunda bilgisayarınızda algılanan öğelerin konumu gibi bilgileri içerebilir. Bilgiler otomatik olarak toplanır ve gönderilir. Bazı durumlarda kişisel bilgiler istemeden Microsoft'a gönderilebilir. Ancak Microsoft, bu bilgileri sizi tanımlamak veya sizinle iletişim kurmak için kullanmayacağını belirtir. Yüksek güvenlikli ortamlarda gizlilik nedenleriyle bu veri gönderimlerini tamamen engellemek en iyisidir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri değeri olmadığında veya 0 değeriyle mevcut olduğunda geçerlidir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsDefender\Spynet:SpynetReporting*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki kullanıcı arabirimi yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Microsoft Defender Antivirus\MAPS\Microsoft MAPS'a Katılın*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.1 ve Server 2012 R2 Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu WindowsDefender.admx/adml tarafından sağlanır.

**18.9.47.5 Microsoft Defender Exploit Guard (eski adıyla Windows Defender Exploit**  **Guard)**

**18.9.47.5.1 Saldırı Yüzeyinin Azaltılması**

**18.9.47.5.1.1 (L1) 'Saldırı Yüzeyi Azaltma kurallarını yapılandır' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Saldırı Yüzeyi Azaltma (ASR) kurallarının durumunu kontrol eder. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Saldırı yüzeyinin azaltılması, genellikle makinelere bulaşmak için kötü amaçlı yazılım arayan istismarlar tarafından kullanılan eylemlerin ve uygulamaların önlenmesine yardımcı olur.

**Etki:**

Bir kural tetiklendiğinde, Eylem Merkezi'nden bir bildirim görüntülenecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsDefender\WindowsDefender Exploit Guard\ASR:ExploitGuard\_ASR\_Rules*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Configuration\Policies\Administrative Templates\Windows Components\Microsoft Defender Antivirus\Microsoft Defender Exploit Guard\Attack Surface Reduction\Configure Attack Surface Reduction kuralları*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1709 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu WindowsDefender.admx/adml tarafından sağlanır.

**18.9.47.5.1.2 (L1) 'Saldırı Yüzeyi Azaltma kurallarını yapılandır: Her ASR kuralı için durumu ayarla' olarak yapılandır.(Otomatik)**

**Açıklama:**

Bu ilke ayarı, Saldırı Yüzeyi Azaltma kurallarını belirler. Bu ayar için önerilen durum:

* 26190899-1602-49e8-8b27-eb1d0a1ce869 - 1 (Ofis iletişim uygulamasının alt süreçler oluşturmasını engelle)
* 3b576869-a4ec-4529-8536-b80a7769e899 - 1 (Ofis uygulamalarının yürütülebilir içerik oluşturmasını engelle)
* 5beb7efe -fd9a-4556-801d-275e5ffc04cc - 1 (Gizlenmiş olabilecek komut dosyalarının yürütülmesini engelle)
* 75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84 - 1 (Office uygulamalarının diğer işlemlere kod enjekte etmesini engelleyin)
* 7674ba52-37eb-4a4f-a9a1-f0f9 - 1 (Adobe Reader'ın alt işlemler oluşturmasını engelle)
* 92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b - 1 (Office makrosundan Win32 API çağrılarını engelle)
* 9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2 - 1 (Windows yerel güvenliğinden kimlik bilgilerinin çalınmasını engelle yetki alt sistemi (lsass.exe))
* b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4 - 1 (USB'den çalışan güvenilmeyen ve imzasız işlemleri engelle)
* be9ba2d9-53ea-4cdc-84e5-9b1eeee46550 - 1 (E-posta istemcisinden ve web postasından çalıştırılabilir içeriği engelle) )
* d3e037e1-3eb8-44c8-a917-5792794759 6d - 1 (JavaScript veya VBScript'in indirilen yürütülebilir içeriği başlatmasını engelle)
* d4f940ab-401b-4efc-aadc-ad5f3c50688a - 1 (Ofis uygulamalarının alt işlemler oluşturmasını engelle)
* e6db77e5-3df2-4cf1-b95a-636979351e5b - 1 (Şu şekilde kalıcılığı engelle) olay aboneliği)

**Not:** ASR kuralları hakkında daha fazla bilgiyi aşağıdaki bağlantıda bulabilirsiniz: [Kötü amaçlı yazılım bulaşmasını önlemek için Saldırı yüzeyi azaltma kurallarını kullanın | Microsoft Docs](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-exploit-guard/attack-surface-reduction-exploit-guard)

**Gerekçe:**

Saldırı yüzeyini azaltma, makinelere bulaşmak için kötü amaçlı yazılım arayan istismarlar tarafından tipik olarak kullanılan eylemlerin ve uygulamaların önlenmesine yardımcı olur. Etki: Bir kural tetiklendiğinde, Eylem Merkezi'nden bir bildirim görüntülenecektir. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:26190899-1602-49e8-8b27-eb1d0a1ce869*

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:3b576869-a4ec-4529-8536-b80a7769e899*

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:5beb7efe-fd9a-4556-801d-275e5ffc04cc*

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:75668c1f-73b5-4cf0-bb93-3ecf5cb7cc84*

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c*

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b*

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:9e6c4e1f-7d60-472f-ba1a-a39ef669e4b2*

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:b2b3f03d-6a65-4f7b-a9c7-1c7ef74a9ba4*

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:be9ba2d9-53ea-4cdc-84e5-9b1eeee46550*

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:d3e037e1-3eb8-44c8-a917-57927947596d*

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:d4f940ab-401b-4efc-aadc-ad5f3c50688a*

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Windows Defender Exploit Guard\ASR\Rules:e6db77e5-3df2-4cf1-b95a-636979351e5b*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu 26190899-1602-49e8-8b27-eb1d0a1ce869, 3b576869-a4ec-4529-8536-b80a7769e899, 5beb7efe-fd9a-4556-801d-275, 7ff5ffe5c4fc1c3b576869-a4ec-4529-8536-b80a7769e899, 5beb7efe-fd9a-4556-801d-275, 7ff5ffs -73b5-4cf0-bb93-3ecf5cb7cc84, 7674ba52-37eb-4a4f-a9a1-f0f9a1619a2c, 92e97fa1-2edf-4476-bdd6-9dd0b4dddc7b, 9e6c4e1f-7d60-47239f-ba669e-a4a9ef-ba-7a4a9ef-ba7a4a9e9d9d9dd -53ea-4cdc-84e5-9b1eeee46550, d3e037e1-3eb8-44c8-a917-57927947596d, d4f940ab-401b-4efc-aadc-ad5f3c50688a ve e6db77e5-3df2-4cf197e5-3df2-4cf197-b95a-6'nın her biri 1:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenler\Microsoft Defender Antivirus\Microsoft Defender Exploit Koruma\Saldırı Yüzeyi Azaltma\Saldırı Yüzeyi Azaltma kurallarını yapılandırın: Ayarla her ASR kuralı için durum*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1709 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu WindowsDefender.admx/adml tarafından sağlanır.

**18.9.47.5.2 Kontrollü Klasör Erişimi**

**18.9.47.5.3 Ağ** **Koruması**

**18.9.47.5.3.1 (L1) 'Kullanıcıların ve uygulamaların tehlikeli web sitelerine erişmesini engelle' seçeneği 'Etkin: Engelle' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Microsoft Defender Exploit Guard ağ korumasını denetler. Bu ayar için önerilen durum: Etkin: Engelle.

**Gerekçe:**

Bu ayar, çalışanların İnternet'te kimlik avı dolandırıcılığı, istismar barındıran siteler ve diğer kötü amaçlı içerikler barındırabilecek tehlikeli etki alanlarına erişmek için herhangi bir uygulamayı kullanmasını önlemeye yardımcı olabilir.

**Etki:**

Kullanıcılar ve uygulamalar tehlikeli etki alanlarına erişemeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\windows Defender\Windows Defender Exploit Guard\Network Protection:EnableNetworkProtection*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Engelle:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Windows Defender Antivirus\Windows Defender Exploit Guard\Ağ Koruması\Kullanıcıların ve uygulamaların tehlikeli web sitelerine erişim*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1709 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu WindowsDefender.admx/adml tarafından sağlanır**.**

**18.9.47.6 MpEngine**

**18.9.47.6.1 (L2) 'Dosya karması hesaplama özelliğini etkinleştir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, Microsoft Defender tarafından taranan dosyalar için karma değerlerinin hesaplanıp hesaplanmayacağını belirler. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Microsoft Defender Antivirus gibi bir virüsten koruma çözümü çalıştırırken, bunun şüpheli ve bilinen kötü amaçlı etkinlikleri izleyecek şekilde yapılandırıldığından emin olmak önemlidir. Dosya karmaları, dosyalardaki değişiklikleri algılamanın güvenilir bir yoludur ve en son tarandıklarından ve güvenli oldukları belirlendiğinden beri değişmeyen dosyaları atlayarak tarama sürecini hızlandırabilir. Değişen bir dosya karması da ek incelemeye neden olabilir.

**Etki:**

Bu ayar, ilk dağıtım sırasında ve sık sık yeni yürütülebilir içeriğin oluşturulduğu (yazılım geliştiricileri gibi) veya uygulamaların sık sık yüklendiği veya güncellendiği kullanıcılar için performansın düşmesine neden olabilir. Bu ayar hakkında daha fazla bilgi için lütfen Güvenlik temeli (SON) sayfasını ziyaret edin: [Windows 10 ve Windows Server, sürüm 2004 - Microsoft Tech Community - 1543631.](https://techcommunity.microsoft.com/t5/microsoft-security-baselines/security-baseline-final-windows-10-and-windows-server-version/ba-p/1543631)

**Not:**

Kullanıcı ve sistem performansının etkisini sağlamak için dağıtım sırasında bu ayarın etkisi yakından izlenmelidir. kabul edilebilir sınırlar içindedir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsDefender\MpEngine:EnableFileHashComputation*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\Windows Components\Microsoft Defender Antivirus\MpEngine\Enable file hash hesaplama özelliği*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1709 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu WindowsDefender.admx/adml tarafından sağlanır.

**18.9.47.7 Ağ Denetim Sistemi**

**18.9.47.8 Karantina**

**18.9.47.9 Gerçek zamanlı koruma**

**18.9.47.9.1 (L1) 'İndirilen tüm dosyaları ve ekleri tara' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, indirilen tüm dosyalar ve ekler için taramayı yapılandırır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Microsoft Defender Antivirus gibi bir virüsten koruma çözümü çalıştırırken, şüpheli ve bilinen kötü amaçlı etkinlikleri gerçek zamanlı olarak buluşsal olarak izleyecek şekilde yapılandırıldığından emin olmak önemlidir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Gerçek Zamanlı Koruma:DisableIOAVProtection*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Microsoft Defender Antivirus\Gerçek Zamanlı Koruma\İndirilen tüm dosyaları ve ekleri tara*

**Not**: Bu Grup İlke yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.1 ve Server 2012 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu WindowsDefender.admx/adml tarafından sağlanır.

**18.9.47.9.2 (L1) 'Gerçek zamanlı korumayı kapat' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bilinen kötü amaçlı yazılım algılaması için gerçek zamanlı koruma istemlerini yapılandırır. Microsoft Defender Antivirus, kötü amaçlı yazılımlar veya potansiyel olarak istenmeyen yazılımlar kendi kendini yüklemeye veya bilgisayarınızda çalıştırmaya çalıştığında sizi uyarır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Microsoft Defender Antivirus gibi bir virüsten koruma çözümü çalıştırırken, şüpheli ve bilinen kötü amaçlı etkinlikleri gerçek zamanlı olarak buluşsal olarak izleyecek şekilde yapılandırıldığından emin olmak önemlidir.

**Etki:**

Yok - bu varsayılan davranıştır. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Gerçek Zamanlı Koruma:DisableRealtimeMonitoring*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\ İlkeler\Yönetim Şablonları\Windows Bileşenleri\Microsoft Defender Antivirus\Gerçek Zamanlı Koruma\Gerçek zamanlı korumayı kapat*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.1 ve Server 2012 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu WindowsDefender.admx/adml tarafından sağlanır.

**18.9.47.9.3 (L1) 'Davranış izlemeyi aç' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:** Bu ilke ayarı, Microsoft Defender Antivirus için davranış izlemeyi yapılandırmanıza olanak tanır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Microsoft Defender Antivirus gibi bir virüsten koruma çözümü çalıştırırken, şüpheli ve bilinen kötü amaçlı etkinlikleri gerçek zamanlı olarak buluşsal olarak izleyecek şekilde yapılandırıldığından emin olmak önemlidir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Gerçek Zamanlı Koruma:DisableBehaviorMonitoring*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\ İlkeler\Yönetim Şablonları\Windows Bileşenleri\Microsoft Defender Antivirus\Gerçek Zamanlı Koruma\Davranış izlemeyi aç*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.1 ve Server 2012 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu WindowsDefender.admx/adml tarafından sağlanır.

**18.9.47.9.4 (L1) 'Komut dosyası taramasını aç' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama**:

Bu ilke ayarı, komut dosyası taramasının açılmasına/kapatılmasına izin verir. Komut dosyası taraması komut dosyalarını yakalar ve ardından sistemde yürütülmeden önce bunları tarar. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Microsoft Defender Antivirus gibi bir virüsten koruma çözümü çalıştırırken, şüpheli ve bilinen kötü amaçlı etkinlikleri gerçek zamanlı olarak buluşsal olarak izleyecek şekilde yapılandırıldığından emin olmak önemlidir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender\Gerçek Zamanlı Koruma:DisableScriptScanning*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\ İlkeler\Yönetim Şablonları\Windows Bileşenleri\Microsoft Defender Antivirus\Gerçek Zamanlı Koruma\Komut dosyası taramasını aç*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 21H2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu WindowsDefender.admx/adml tarafından sağlanır.

**18.9.47.10 İyileştirme**

**18.9.47.11 Raporlama**

**18.9.47.11.1 (L2) 'Watson olaylarını yapılandır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Watson olaylarının gönderilip gönderilmeyeceğini yapılandırmanıza olanak tanır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Watson olayları, bir program veya hizmet çöktüğünde veya başarısız olduğunda, otomatik gönderme olasılığı da dahil olmak üzere Microsoft'a gönderilen raporlardır. Bu bilgilerin gönderilmesini önlemek, gizlilik endişelerini azaltmaya yardımcı olabilir.

**Etki:**

Bir program veya hizmet çöktüğünde veya başarısız olduğunda Watson olayları otomatik olarak Microsoft'a gönderilmez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsDefender\Reporting:DisableGenericRePorts*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Microsoft Defender Antivirus\Reporting\Configure Watson olaylarını*

: Bu Grup İlkesi yolu, varsayılan. Microsoft Windows 8.1 ve Server 2012 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu WindowsDefender.admx/adml tarafından sağlanır.

**18.9.47.12 Tarama**

**18.9.47.12.1 (L1) 'Çıkarılabilir sürücüleri tara' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, tam bir tarama çalıştırırken USB flash sürücüler gibi çıkarılabilir sürücülerin içeriğinde kötü amaçlı yazılım ve istenmeyen yazılım taraması yapılıp yapılmayacağını yönetmenize olanak tanır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Çıkarılabilir sürücülerin harici, yönetilmeyen bir bilgisayardan kurumsal yönetilen ortama getirilen kötü amaçlı yazılımları içerme olasılığı daha yüksek olduğundan, mevcut çıkarılabilir sürücülerin her tür taramaya her zaman dahil edilmesini sağlamak önemlidir.

**Etki:**

Çıkarılabilir sürücüler, Microsoft Defender Antivirus tarafından her tür tarama sırasında taranacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsDefender\Scan:DisableRemovableDriveScanning*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Microsoft Defender Antivirus\Scan\Scan çıkarılabilir sürücüleri*

**Not:** Bu Grup İlkesi yolu, varsayılan. Microsoft Windows 8.1 ve Server 2012 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu WindowsDefender.admx/adml tarafından sağlanır.

**18.9.47.12.2 (L1) 'E-posta taramasını aç' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, e-posta taramasını yapılandırmanıza olanak tanır. E-posta taraması etkinleştirildiğinde, motor, posta gövdelerini ve eklerini analiz etmek için posta kutusunu ve posta dosyalarını belirli biçimlerine göre ayrıştırır. Şu anda çeşitli e-posta biçimleri desteklenmektedir, örneğin: pst (Outlook), dbx, mbx, mime (Outlook Express), binhex (Mac). Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

E-posta ekleri, bilgisayarlara kötü amaçlı yazılım sızmak için yaygın olarak kullanılan bir saldırı vektörü olduğundan, gelen e-postalar Microsoft Defender Antivirus gibi bir virüsten koruma çözümü tarafından taranmalıdır.

**Etki:**

Microsoft Defender Antivirus tarafından e-posta taraması etkinleştirilecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsDefender\Scan:DisableEmailScanning*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\Windows Components\Microsoft Defender Antivirus\Scan\E-posta taramasını aç*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.1 ve Server 2012 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu WindowsDefender.admx/adml tarafından sağlanır.

**18.9.47.13 Güvenlik İstihbaratı Güncellemeleri (eski adıyla İmza Güncellemeleri)**

**18.9.47.14 Tehditler**

**18.9.47.15 (L1) 'İstenmeyen türden olabilecek uygulamalar için algılamayı yapılandır' seçeneği 'Etkin: Engelle' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, reklam yazılımı veya kötü amaçlı yazılım sunabilen gizli istenmeyen uygulama paketleyicileri veya bunların paket uygulamaları olan Potansiyel Olarak İstenmeyen Uygulamaların (PUA) algılanmasını ve eylemini kontrol eder. Bu ayar için önerilen durum: Etkin: Engelle. Daha fazla bilgi için şu bağlantıya bakın: [Microsoft Defender Antivirus ile olası istenmeyen uygulamaları engelleyin | Microsoft Belgeleri](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-antivirus/detect-block-potentially-unwanted-apps-windows-defender-antivirus)

**Gerekçe:**

İstenmeyen olabilecek uygulamalar, ağınıza kötü amaçlı yazılım bulaşma riskini artırabilir, kötü amaçlı yazılım bulaşmalarının tespit edilmesini zorlaştırabilir ve uygulamaları temizlerken BT kaynaklarını boşa harcayabilir. Kurulumdan engellenmelidirler.

**Etki:**

Microsoft tarafından PUA olarak tanımlanan uygulamalar, indirme ve yükleme sırasında engellenecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender:PUAProtection*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın: Engelle:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Microsoft Defender Antivirus\İstenmeyen olabilecek uygulamalar için algılamayı yapılandır*

**Not:** Bu Grup İlkesi yolu Microsoft Windows 10 Sürüm 1809 ve Sunucu 2019 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu WindowsDefender.admx/adml tarafından sağlanır

**18.9.47.16 (L1) 'Microsoft Defender Antivirüs'ü kapat' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı Microsoft Defender Antivirus'ü kapatır. Ayar Devre Dışı olarak yapılandırılırsa, Microsoft Defender Antivirus çalışır ve bilgisayarlar kötü amaçlı yazılımlara ve diğer olası istenmeyen yazılımlara karşı taranır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Geçerli, güncellenmiş bir virüsten koruma ürününün her bilgisayarı kötü amaçlı dosya etkinliğine karşı taradığından emin olmak önemlidir. Microsoft, Microsoft Defender Antivirus'te kutudan çıktığı gibi yetkin bir çözüm sunar. Saygın bir üçüncü taraf antivirüs çözümü satın almayı seçen kuruluşlar, ticari alternatif yerine kendilerini bu öneriden muaf tutmayı seçebilirler.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsDefender:DisableAntiSpyware*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Microsoft Defender Antivirus\Turn off Microsoft Defender AntiVirus*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu WindowsDefender.admx/adml.

**Not #2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Windows Defender'ı Kapat olarak adlandırıldı, ancak Windows 10 Sürüm 1703 Yönetim Şablonlarından başlayarak Windows Defender Antivirus olarak yeniden adlandırıldı. Windows 10 Sürüm 2004 Yönetim Şablonlarından başlayarak yeniden Microsoft Defender Antivirus'ü Kapat olarak yeniden adlandırıldı.

**18.9.48 Microsoft Defender Application Guard (eski adıyla Windows Defender Application Guard)**

**18.9.48.1 (NG) 'Microsoft Defender Application Guard'da olayların denetlenmesine izin ver' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, denetleme olaylarının Microsoft Defender Application Guard'dan toplanıp toplanamayacağına karar vermenizi sağlar. Bu ayar için önerilen durum: Etkin.

**Not:** Microsoft Defender Uygulama Koruması, Windows'un 64 bit sürümünü ve donanım destekli CPU sanallaştırmasını (Intel VT-x veya AMD-V) destekleyen bir CPU gerektirir. Bu özellik sanal donanımda resmi olarak desteklenmez, ancak donanım destekli CPU sanallaştırma özelliğinin ana bilgisayar tarafından konuk VM'ye gösterilmesi koşuluyla VM'lerde (özellikle test için) çalışabilir.

Bu özelliğin sistem gereksinimleri hakkında daha fazla bilgiyi [Microsoft Defender Application Guard için Sistem gereksinimleri (Windows 10) | Microsoft Docs](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/reqs-wd-app-guard)

**Not #2**: Azure IaaS VM'leri kullanılırken Credential Guard ve Device Guard şu anda desteklenmemektedir.

**Gerekçe:**

Microsoft Defender Application Guard olaylarının denetlenmesi, bir güvenlik olayı araştırılırken faydalı olabilir.

**Etki:**

Microsoft Defender Application Guard, denetim ilkelerini Microsoft Edge'den devralacak ve özellikle Microsoft Defender Application Guard için sistem olaylarını denetlemeye başlayacak. Toplanan günlükler, Application Guard dışında Microsoft Edge'de gözden geçirilebilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\AppHVSI:AuditApplicationGuard*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Components\Microsoft Defender Application Guard\Microsoft Defender Application Guard'da olayları denetlemeye izin ver*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1709 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu AppHVSI.admx/adml tarafından sağlanır.

**Not 2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Windows Defender Uygulama Korumasında denetim olaylarına izin ver olarak adlandırılmıştı, ancak Windows 10 Sürüm 2004 Yönetim Şablonlarından başlayarak Microsoft Defender Uygulama Korumasında denetim olaylarına izin ver olarak yeniden adlandırıldı.

**18.9.48.2 (NG) 'Microsoft Defender Application Guard'da kamera ve mikrofon erişimine izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

İlke, Microsoft Defender Application Guard içindeki uygulamaların cihazın kamerasına ve mikrofonuna erişip erişemeyeceğini belirlemenize olanak tanır. Bu ayar için önerilen durum: Devre Dışı.

**Not:**

Microsoft Defender Uygulama Koruması, Windows'un 64 bit sürümünü ve donanım destekli CPU sanallaştırmasını (Intel VT-x veya AMD-V) destekleyen bir CPU gerektirir. Bu özellik sanal donanımda resmi olarak desteklenmez, ancak donanım destekli CPU sanallaştırma özelliğinin ana bilgisayar tarafından konuk VM'ye gösterilmesi koşuluyla VM'lerde (özellikle test için) çalışabilir. Bu özelliğin sistem gereksinimleri hakkında daha fazla bilgi için [Microsoft Defender Application Guard için Sistem gereksinimleri (Windows 10) | Microsoft Docs](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/reqs-wd-app-guard)

**Not #2:** Azure IaaS VM'leri kullanılırken Credential Guard ve Device Guard şu anda desteklenmemektedir.

**Gerekçe:** Hassas bilgilerin kötü amaçlı kullanım için elde edilmesini engellemek amacıyla, Microsoft Defender Application Guard kapsayıcısı içindeki güvenilmeyen siteler bilgisayarın mikrofonuna veya kamerasına erişmemelidir.

**Etki:**

Bu varsayılan değerdir, bu nedenle bu ayarın uygulanması için etki minimum düzeyde olmalıdır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\AppHVSI:AllowCameraMicrophoneR edirection*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Devre Dışı Bırakılmış

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows olarak ayarlayın Components\Microsoft Defender Application Guard\Microsoft Defender Application Guard'da kamera ve mikrofon erişimine izin ver*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1809 ve Sunucu 2019 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu AppHVSI.admx/adml tarafından sağlanır.

**Not 2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Windows Defender Uygulama Korumasında kamera ve mikrofon erişimine izin ver olarak adlandırılmıştı, ancak Windows 10 Sürüm 2004 Yönetim Sürümü'nden başlayarak Microsoft Defender Uygulama Korumasında kamera ve mikrofon erişimine izin ver olarak yeniden adlandırıldı.

**18.9.48.3 (NG) 'Microsoft Defender Application Guard için veri kalıcılığına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, verilerin Microsoft Defender Application Guard'daki farklı oturumlarda kalıcı olup olmayacağına karar vermenize olanak tanır. Bu ayar için önerilen durum: Devre Dışı.

**Not:** Microsoft Defender Uygulama Koruması, Windows'un 64 bit sürümünü ve donanım destekli CPU sanallaştırmasını (Intel VT-x veya AMD-V) destekleyen bir CPU gerektirir. Bu özellik sanal donanımda resmi olarak desteklenmez, ancak donanım destekli CPU sanallaştırma özelliğinin ana bilgisayar tarafından konuk VM'ye gösterilmesi koşuluyla VM'lerde (özellikle test için) çalışabilir. Bu özelliğin sistem gereksinimleri hakkında daha fazla bilgi için [Microsoft Defender Application Guard için Sistem gereksinimleri (Windows 10) | Microsoft Docs](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/reqs-wd-app-guard)

**Not #2:** Azure IaaS VM'leri kullanılırken Credential Guard ve Device Guard şu anda desteklenmemektedir.

**Gerekçe:**

Microsoft Defender Application Guard'ın birincil amacı, güvenilmeyen web sitelerini ziyaret etmek için "korumalı alan kapsayıcı" sunmaktır. Veri kalıcılığına izin verilirse, korumalı alanın etkinliğini azaltır ve kötü amaçlı içerik, oturumlar arasında Microsoft Defender Application Guard kapsayıcısında etkin kalabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\AppHVSI:AllowPersistence*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Components\Microsoft Defender Application Guard\Microsoft Defender Application Guard için veri kalıcılığına izin ver*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1709 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu AppHVSI.admx/adml tarafından sağlanır.

**Not 2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Windows Defender Uygulama Koruması için veri kalıcılığına izin ver olarak adlandırılmıştı, ancak Windows 10 Sürüm 2004 Yönetim Şablonlarından başlayarak Microsoft Defender Uygulama Koruması için veri kalıcılığına izin ver olarak yeniden adlandırıldı.

**18.9.48.4 (NG) 'Dosyaların Microsoft Defender Application Guard'dan ana bilgisayar işletim sistemine indirilmesine ve kaydedilmesine izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, indirilen dosyaların Microsoft Defender Application Guard kapsayıcısından ana bilgisayar işletim sistemine kaydedilip kaydedilmeyeceğini belirler. Bu ayar için önerilen durum: Devre Dışı.

**Not:** Microsoft Defender Uygulama Koruması, Windows'un 64 bit sürümünü ve donanım destekli CPU sanallaştırmasını (Intel VT-x veya AMD-V) destekleyen bir CPU gerektirir. Bu özellik sanal donanımda resmi olarak desteklenmez, ancak donanım destekli CPU sanallaştırma özelliğinin ana bilgisayar tarafından konuk VM'ye gösterilmesi koşuluyla VM'lerde (özellikle test için) çalışabilir. Bu özelliğin sistem gereksinimleri hakkında daha fazla bilgiyi [Microsoft Defender Application Guard için Sistem gereksinimleri (Windows 10) | Microsoft Docs](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/reqs-wd-app-guard)

**Not #2**: Azure IaaS VM'leri kullanılırken Credential Guard ve Device Guard şu anda desteklenmemektedir.

**Gerekçe:**

Microsoft Defender Application Guard'ın birincil amacı, bir "korumalı alan kapsayıcı" sunmaktır. Potansiyel olarak kötü amaçlı dosyalar, ana bilgisayarı riske atabilecek korumalı alan ortamından ana bilgisayar işletim sistemine kopyalanmamalıdır.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\AppHVSI:SaveFilesToHost*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Components\Microsoft Defender Application Guard\Dosyaların Microsoft Defender Application Guard'dan ana bilgisayar işletim sistemine indirilmesine ve kaydedilmesine izin ver*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1803 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu AppHVSI.admx/adml tarafından sağlanır.

**Not 2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Dosyaların Windows Defender Uygulama Korumasından ana bilgisayar işletim sistemine indirilmesine ve kaydedilmesine izin ver olarak adlandırılmıştı, ancak Dosyaların şuradan indirilmesine ve ana bilgisayar işletim sistemine kaydedilmesine izin ver olarak yeniden adlandırıldı.

**18.9.48.5 (NG) 'Microsoft Defender Application Guard pano ayarlarını yapılandırma: Pano davranış ayarı' seçeneği 'Etkin: Pano işlemini yalıtılmış bir oturumdan ana bilgisayara etkinleştir' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Microsoft Defender Application Guard'dayken panonun nasıl davranacağına karar vermenizi sağlar. Bu ayar için önerilen durum: Etkin: Yalıtılmış bir oturumdan ana bilgisayara pano işlemini etkinleştirin.

**Not:** Microsoft Defender Uygulama Koruması, Windows'un 64 bit sürümünü ve donanım destekli CPU sanallaştırmasını (Intel VT-x veya AMD-V) destekleyen bir CPU gerektirir. Bu özellik sanal donanımda resmi olarak desteklenmez, ancak donanım destekli CPU sanallaştırma özelliğinin ana bilgisayar tarafından konuk VM'ye gösterilmesi koşuluyla VM'lerde (özellikle test için) çalışabilir. Bu özelliğin sistem gereksinimleri hakkında daha fazla bilgiyi [Microsoft Defender Application Guard için Sistem gereksinimleri (Windows 10) | Microsoft Docs](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/reqs-wd-app-guard)

**Not #2:** Azure IaaS VM'leri kullanılırken Credential Guard ve Device Guard şu anda desteklenmemektedir.

**Gerekçe:**

Microsoft Defender Application Guard'ın birincil amacı, güvenilmeyen web sitelerini ziyaret etmek için "korumalı alan kapsayıcı" sunmaktır. Ana bilgisayar panosu Microsoft Defender Application Guard'a sunulursa, güvenliği ihlal edilmiş bir Microsoft Defender Application Guard oturumunun içeriğine erişimi olur ve hassas bilgileri kötü amaçlı bir web sitesine veya uygulamaya maruz bırakma olasılığı vardır. Ancak, Microsoft Defender Application Guard panosu ana bilgisayar tarafından erişilebilir hale getirilirse risk azalır ve aslında bu işlevsellik genellikle operasyonel açıdan gerekli olabilir.

**Etki:**

Microsoft Defender Uygulama Koruması oturumları, ana bilgisayar cihazının panosuna erişemez, ancak ana bilgisayar cihazı, Microsoft Defender Uygulama Koruması oturum panosuna erişebilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\AppHVSI:AppHVSIClipboardSetting gs*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Yalıtılmış bir oturumdan pano işlemini etkinleştir ana

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Microsoft Defender Uygulama Koruması\Yapılandır Microsoft Defender Uygulama Koruması pano ayarları: Pano davranışı ayarı*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1703 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu AppHVSI.admx/adml tarafından sağlanır.

**Not #2**: Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Windows Defender Uygulama Koruması pano ayarlarını yapılandır: Pano davranışı ayarı olarak adlandırıldı, ancak adı Microsoft Defender Uygulama Koruması pano ayarlarını yapılandır: Windows 10 Sürümü ile başlayan Pano davranışı ayarı olarak yeniden adlandırıldı.

**18.9.48.6 (NG) 'Microsoft Defender Application Guard'ı Yönetilen Mod'da Aç' seçeneği 'Etkin: 1' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Microsoft Defender Uygulama Koruması (Uygulama Koruması) aracılığıyla uygulama yalıtımını etkinleştirir. Kullanılabilir 4 seçenek vardır:

* 0. Microsoft Defender Uygulama Korumasını Devre Dışı Bırak
* 1. YALNIZCA Microsoft Edge için Microsoft Defender Uygulama Korumasını etkinleştirin
* 2. YALNIZCA Microsoft Office için Microsoft Defender Uygulama Korumasını etkinleştirin
* 3. Microsoft Edge için Microsoft Defender Uygulama Korumasını Etkinleştirin VE Microsoft Office

Bu ayar için önerilen durum: Etkin: 1 (YALNIZCA Microsoft Edge için Microsoft Defender Uygulama Korumasını Etkinleştir).

**Not:** Microsoft Defender Uygulama Koruması, Windows'un 64 bit sürümünü ve donanım destekli CPU sanallaştırmasını (Intel VT-x veya AMD-V) destekleyen bir CPU gerektirir. Bu özellik sanal donanımda resmi olarak desteklenmez, ancak donanım destekli CPU sanallaştırma özelliğinin ana bilgisayar tarafından konuk VM'ye gösterilmesi koşuluyla VM'lerde (özellikle test için) çalışabilir.

Bu özelliğin sistem gereksinimleri hakkında daha fazla bilgi [Microsoft Defender Application Guard için sistem gereksinimleri (Windows 10) | Microsoft Docs](https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-defender-application-guard/reqs-wd-app-guard)

**Not #2:**

Yayınlanma sırasında, Windows 10'un şu anda yayımlanmış tüm sürümlerinde Microsoft Defender Application Guard, yalnızca Microsoft Edge için Microsoft Office için korumayı henüz desteklememektedir. Bu nedenle, bu ayardaki ek kullanılabilir 2 ve 3 seçenekleri henüz geçerli değildir.

**Not 3:**

Azure IaaS VM'leri kullanılırken Credential Guard ve Device Guard şu anda desteklenmemektedir.

**Gerekçe:**

Microsoft Defender Application Guard, sanallaştırma tabanlı güvenlik yalıtımı kullanacak şekilde yapılandırılmış uygulamalar için sanallaştırılmış bir ortam oluşturmak üzere Windows Hiper Yönetici kullanır. İzolasyondayken, uygunsuz kullanıcı etkileşimleri ve uygulama güvenlik açıkları, çekirdeği veya sanallaştırılmış ortamın dışında çalışan diğer uygulamaları tehlikeye atamaz.

**Etki:**

Microsoft Edge için Microsoft Defender Uygulama Koruması açılacak.

**Not:** Microsoft Defender Uygulama Korumasının çalışması için İnternet Bağlantı Paylaşımı (ICS) (SharedAccess) hizmeti gerekir, bu nedenle Microsoft Defender Uygulama Korumasını etkinleştirmeyi seçerseniz bu hizmeti devre dışı bırakmak için bir istisna (bkz. Bölüm 5) gerekecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\AppHVSI:AllowAppHVSI\_ProviderS et*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın: 1:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Microsoft Defender Uygulama Koruması\Yönetilen Modda Microsoft Defender Uygulama Korumasını Aç*

**Not:**

Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1703 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu AppHVSI.admx/adml tarafından sağlanır.

**Not #2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Windows Defender Uygulama Korumasını Kurumsal Modda Aç olarak adlandırılmıştı, ancak Windows 10 Sürüm 1903 Yönetim Şablonlarından başlayarak Windows Defender Uygulama Korumasını Yönetilen Modda Aç olarak yeniden adlandırıldı. Windows 10 Sürüm 2004 Yönetim Şablonlarından başlayarak, Microsoft Defender Uygulama Korumasını Yönetilen Modda Aç olarak yeniden adlandırıldı.

**18.9.49 Microsoft Defender Exploit Guard (eski adıyla Windows Defender Exploit Guard)**

**18.9.50 Microsoft Edge**

**18.9.51 Microsoft FIDO Kimlik Doğrulaması**

**18.9.52 Microsoft İkincil Kimlik Doğrulama Faktörü**

**18.9.53 Microsoft Kullanıcı Deneyimi Sanallaştırma**

**18.9.54 NetMeeting**

**18.9.55 Ağ Erişim Koruması**

**18.9.56 Ağ Projektörü**

**18.9.57 Haberler ve ilgi alanları**

**18.9.57.1 (L2) 'Görev çubuğunda haberleri ve ilgi alanlarını etkinleştir' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, cihazda haber ve ilgi alanlarına izin verilip verilmediğini belirtir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Gizlilik endişeleri nedeniyle, Windows görev çubuğundaki haberler ve ilgi alanları gibi uygulamalar ve özellikler, verilerin Microsoft gibi 3. taraflara geri gönderilme potansiyeli nedeniyle olası bir güvenlik riski olarak değerlendirilmelidir. Ek olarak, uygulama, besleme içinde uygunsuz haberleri ve ilgi alanlarını görüntüleyebilir.

**Etki:**

Windows görev çubuğundaki haberler ve ilgi alanları özelliği cihazda kullanılamayacak.

**Not:** Karşılaştırma yayını sırasında, bu ayar, haberler ve ilgi alanları özelliği için görev çubuğu menü seçeneklerini gizlemez veya devre dışı bırakmaz, ancak özelliği yeniden açmaya çalışmak herhangi bir görünür değişikliğe neden olmaz. Microsoft'un gelecekteki bir işletim sistemi güncellemesinde görev çubuğu menü seçeneklerini "grileştirmek" için bu davranışı değiştirmesi mümkündür.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Feeds:EnableFeeds*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonlar\Windows Bileşenleri\Haberler ve ilgi alanları\Görev çubuğunda haberleri ve ilgi alanlarını etkinleştir*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 21H1 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu Feeds.admx/adml tarafından sağlanır.

**18.9.58 OneDrive (eski adıyla SkyDrive)**

**18.9.58.1 (L1) 'Dosya depolama alanı için OneDrive kullanımını engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, uygulamaların ve özelliklerin Yeni Nesil Eşitleme İstemcisi kullanarak OneDrive'daki dosyalarla çalışmasını engellemenize olanak tanır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bu ayarın etkinleştirilmesi, kullanıcıların Yeni Nesil Eşitleme İstemcisini kullanarak yanlışlıkla (veya kasıtlı olarak) gizli veya hassas kurumsal bilgileri OneDrive bulut hizmetine yüklemesini önler.

**Not:**

Bu güvenlik sorunu, yalnızca Windows ile birlikte sağlananlar için değil, bir iş istasyonuna yüklenen herhangi bir bulut tabanlı dosya depolama uygulaması için geçerlidir.

**Etki:**

Kullanıcılar OneDrive uygulamasından ve dosya seçiciden OneDrive'a erişemez. Windows Mağazası uygulamaları, WinRT API'sini kullanarak OneDrive'a erişemez. OneDrive, Dosya Gezgini'ndeki gezinme bölmesinde görünmüyor. OneDrive dosyaları bulutla senkronize tutulmaz. Kullanıcılar, film rulosu klasöründen otomatik olarak fotoğraf ve video yükleyemez.

**Not:** Kuruluşunuz Office 365 kullanıyorsa, bu ayarın kullanıcıların dosyaları OneDrive/SkyDrive'a kaydetmesini engelleyeceğini unutmayın.

**Not #2:** Kuruluşunuz OneDrive İş'i uygulamaya karar verdiyse ve bu nedenle kendisini bu öneriden muaf tutması gerekiyorsa, en son OneDrive istemcisiyle birlikte verilen OneDrive.admx/adml şablonunu da edinmenizi ve kullanmanızı kesinlikle öneririz: [bu bağlantıda](https://docs.microsoft.com/en-us/onedrive/use-group-policy) belirtilmiştir (bu şablon Windows Yönetim Şablonlarına dahil değildir).

Özellikle bu şablondaki iki alternatif OneDrive ayarı dikkate almaya değer:

* Yalnızca belirli kuruluşlar için OneDrive hesaplarının eşitlenmesine izin ver - OneDrive istemci bağlantılarını yalnızca onaylanmış kiracı kimlikleriyle sınırlayan bilgisayar tabanlı bir ayar.
* Kullanıcıların kişisel OneDrive hesaplarını senkronize etmesini önleyin - tüketici OneDrive'ın (yani iş dışı) kullanımını engelleyen kullanıcı tabanlı bir ayar.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\OneDrive:DisableFileSy ncNGSC*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\OneDrive\Dosya depolama için OneDrive kullanımını engelle*

**Not:** Bu Grup İlkesi yolu mevcut olmayabilir varsayılan olarak. Microsoft Windows 8.1 ve Server 2012 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu SkyDrive.admx/adml tarafından sağlanır. Ancak, yalnızca Microsoft Windows 10 Sürüm 1607 ve Server 2016 Yönetim Şablonlarında (veya daha yenisinde) bulunan sürümü kullanmanızı şiddetle öneririz. Şablonların eski sürümleri, yukarıdaki sürümde düzgün şekilde temizlenene kadar hem OneDrive hem de SkyDrive için farklı şablon dosyalarında çakışan ayarlara sahipti.

**Not 2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar dosya depolama için SkyDrive kullanımını engelle olarak adlandırılmıştır, ancak Windows 10 RTM (Sürüm 1507) Yönetim Şablonlarından başlayarak yeniden adlandırılmıştır.

**18.9.59 Çevrimiçi Yardım**

**18.9.60 OOBE**

**18.9.61 Parola Senkronizasyonu**

**18.9.62 Taşınabilir İşletim Sistemi**

**18.9.63 Sunum Ayarları**

**18.9.64 Yüklemeye Zorla**

**18.9.64.1 (L2) 'Yüklemeye Zorla hizmetini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır**

**Açıklama:**

Bu ilke ayarı, kullanıcıların diğer cihazlarda veya web'de çalışan Microsoft Store Uygulamasından Uygulamaları cihaza aktarıp aktaramayacağını kontrol eder. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Yüksek güvenlikli yönetilen bir ortamda, uygulama kurulumları son kullanıcılar tarafından değil, BT personeli tarafından merkezi olarak yönetilmelidir.

**Etki:**

Kullanıcılar, diğer cihazlarda veya web'de çalışan Microsoft Store'dan Uygulamaları bu cihaza aktaramayacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\PushToInstall:DisablePushToIns uzun*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Yüklemek İçin Bastır\Yüklemek İçin Bastır hizmetini kapat*

**Not:** Bu Grup İlkesi yolu mevcut olmayabilir varsayılan olarak. Microsoft Windows 10 Sürüm 1709 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu PushToInstall.admx/adml tarafından sağlanır.

**18.9.65 Uzak Masaüstü Hizmetleri (eski adıyla Terminal Hizmetleri)**

**18.9.65.1 RD Lisansı (eski adıyla TH Lisansı)**

**18.9.65.2 Uzak Masaüstü Bağlantısı İstemcisi**

**18.9.65.2.1 RemoteFX USB Aygıt Yeniden Yönlendirme**

**18.9.65.2.2 (L1) 'Şifrelerin kaydedilmesine izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Uzak Masaüstü istemcilerinin parolaları bir bilgisayara kaydetmesini önlemeye yardımcı olur. Bu ayar için önerilen durum: Etkin.

**Not:**

Bu ilke ayarı daha önce Devre Dışı veya Yapılandırılmadı olarak yapılandırıldıysa, Uzak Masaüstü istemcisinin herhangi bir sunucuyla bağlantısı ilk kez kesildiğinde önceden kaydedilmiş parolalar silinir.

**Gerekçe:**

Bilgisayara fiziksel erişimi olan bir saldırgan, kayıtlı parolaları koruyan korumayı kırabilir. Bir kullanıcının hesabını tehlikeye atan ve bilgisayarına bağlanan bir saldırgan, ek ana bilgisayarlara erişmek için kayıtlı parolaları kullanabilir.

**Etki:**

Uzak Masaüstü istemcileri için parola kaydetme onay kutusu devre dışı bırakılacak ve kullanıcılar parolaları kaydedemeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:DisablePasswordSaving*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Uzak Masaüstü Hizmetleri\Uzak Masaüstü Bağlantısı İstemcisi\Parolaların kaydedilmesine izin verme*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu TerminalServer.admx/adml tarafından sağlanır.

**18.9.65.3 Uzak Masaüstü Oturum Ana Bilgisayarı (eski adıyla Terminal Server)**

**18.9.65.3.1 Uygulama Uyumluluğu**

**18.9.65.3.2 Bağlantılar**

**18.9.65.3.2.1 (L2) 'Kullanıcıların Uzak Masaüstü Hizmetleri'ni kullanarak uzaktan bağlanmasına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Uzak Masaüstü Hizmetleri'ni kullanarak bilgisayarlara uzaktan erişimi yapılandırmanıza olanak tanır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Uzak Masaüstü Hizmetleri aracılığıyla oturum açmaya izin ver kullanıcı hakkına sahip herhangi bir hesap, bilgisayarın uzak konsolunda oturum açabilir. Bilgisayarın konsolunda oturum açması gereken meşru kullanıcılara erişimi kısıtlamazsanız, yetkisiz kullanıcılar ayrıcalıklarını yükseltmek için kötü amaçlı kod indirebilir ve çalıştırabilir.

**Etki:**

Yok - Sistem Özellikleri sayfasındaki Uzak sekmesinde Uzak Masaüstü Hizmetleri manuel olarak etkinleştirilmediği sürece bu varsayılan yapılandırmadır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fDenyTSConnections*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Uzak Masaüstü Hizmetleri\Uzak Masaüstü Oturum Ana Bilgisayarı\Bağlantılar\Kullanıcıların Uzak kullanarak uzaktan bağlanmasına izin ver Masaüstü Hizmetleri*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu TerminalServer.admx/adml tarafından sağlanır.

**Not 2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Kullanıcıların Terminal Hizmetlerini kullanarak uzaktan bağlanmasına izin ver olarak adlandırılmıştı, ancak Windows 7 ve Server 2008 R2 Yönetim Şablonlarında Kullanıcıların Uzak Masaüstü Hizmetlerini kullanarak uzaktan bağlanmasına izin ver olarak yeniden adlandırıldı. Sonunda (tekrar) Windows 8.0 ve Server 2012 (R2 olmayan Yönetim Şablonları) ile başlayarak Kullanıcıların Uzak Masaüstü Hizmetlerini kullanarak uzaktan bağlanmasına izin ver olarak yeniden adlandırıldı.

**18.9.65.3.3 Cihaz ve Kaynak Yeniden Yönlendirme**

**18.9.65.3.3.1 (L2) 'UI Otomasyonu yeniden yönlendirmesine izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, yerel bilgisayarda çalışan Kullanıcı Arabirimi (UI) Otomasyonu istemci uygulamalarının sunucudaki UI öğelerine erişip erişemeyeceğini belirler. UI Otomasyonu, programların çoğu UI öğesine erişim sağlar ve bu da, düzgün çalışması için UI ile etkileşime girmesi gereken Büyüteç ve Ekran Okuyucusu gibi yardımcı teknoloji ürünlerinin kullanılmasına izin verir. Kullanıcı arabirimi bilgileri, otomatikleştirilmiş test komut dosyalarının kullanıcı arabirimi ile etkileşime girmesine de olanak tanır. Örneğin, yerel bilgisayarın Ekran Okuyucusu ve Büyüteç istemcileri, uzak bir oturumda açılan bir web sayfasında UI ile etkileşim kurmak için kullanılabilir. Bu ayar için önerilen durum: Devre Dışı.

**Not:** Uzak Masaüstü oturumları şu anda UI Otomasyonu yeniden yönlendirmesini desteklememektedir.

**Gerekçe:**

Güvenlik açısından daha hassas bir ortamda, olası saldırı yüzeyinin azaltılması arzu edilir. Bir Uzak Masaüstü oturumu içinde UI Otomasyonu yeniden yönlendirme ihtiyacı nadirdir ve şu anda desteklenmemektedir, ancak kötü niyetli etkinliklerin gerçekleşmesi için beklenmeyen yolların sayısını azaltmak mantıklıdır.

**Etki:**

Yerel bilgisayardaki UI Otomasyonu istemcileri uzak uygulamalarla etkileşim kuramayacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:EnableUiaRedirection*

**Düzeltme**:

Önerilen yapılandırmayı GP aracılığıyla kurmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\Yönetim Şablonları \Windows Bileşenleri\Uzak Masaüstü Hizmetleri\Uzak Masaüstü Oturum Ana Bilgisayarı\Aygıt ve Kaynak Yeniden Yönlendirme\Kullanıcı Arabirimi Otomasyonu yeniden yönlendirmesine izin ver*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 21H2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu TerminalServer.admx/adml tarafından sağlanır.

**18.9.65.3.3.2 (L2) 'COM bağlantı noktası yeniden yönlendirmesine izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir Uzak Masaüstü Hizmetleri oturumunda verilerin uzak bilgisayardan istemci COM bağlantı noktalarına yeniden yönlendirilmesini engellenip engellenmeyeceğini belirtir. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Güvenlik açısından daha hassas bir ortamda, olası saldırı yüzeyinin azaltılması arzu edilir. Uzak Masaüstü oturumu içinde COM bağlantı noktası yeniden yönlendirme ihtiyacı çok nadirdir, bu nedenle veri hırsızlığı ve/veya kötü amaçlı kod aktarımı için beklenmeyen yolların sayısını azaltmak mantıklıdır.

**Etki:**

Uzak Masaüstü Hizmetleri oturumundaki kullanıcılar, sunucu verilerini yerel (istemci) COM bağlantı noktalarına yeniden yönlendiremez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fDisableCcm*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\ Yönetim Şablonları\Windows Bileşenleri\Uzak Masaüstü Hizmetleri\Uzak Masaüstü Oturum Ana Bilgisayarı\Aygıt ve Kaynak Yeniden Yönlendirme\COM bağlantı noktası yeniden yönlendirmesine izin verme*

**Not**: Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerde bulunan Grup İlkesi şablonu TerminalServer.admx/adml tarafından sağlanır.

**18.9.65.3.3.3 (L1) 'Sürücü yeniden yönlendirmesine izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların istemci bilgisayarlarındaki yerel sürücüleri eriştikleri Uzak Masaüstü Sunucularıyla paylaşmasını engeller. Eşlenen sürücüler, Windows Gezgini'ndeki oturum klasör ağacında aşağıdaki biçimde görünür: \\TSClient\$ Yerel sürücüler paylaşılırsa, üzerlerinde depolanan verileri kullanmak isteyen davetsiz misafirlere karşı savunmasız kalırlar. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Veriler, herhangi bir doğrudan kullanıcı etkileşimi olmaksızın, kullanıcının Uzak Masaüstü Hizmetleri oturumundan kullanıcının yerel bilgisayarına iletilebilir. Güvenliği ihlal edilmiş bir sunucuda zaten bulunan kötü amaçlı yazılımlar, Uzak Masaüstü oturumu sırasında kullanıcının yerel bilgisayarına doğrudan ve gizli disk erişimine sahip olacaktır.

**Etki:**

Sürücü yeniden yönlendirmesi mümkün olmayacak. Çoğu durumda, bağlı kullanıcı tarafından manuel olarak gerçekleştirilen dosya paylaşımlarına (yönetimsel paylaşımlar dahil) geleneksel ağ sürücüsü eşlemesi, gerektiğinde dosya aktarımlarına izin vermek için yetenekli bir yedek olarak hizmet edecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fDisableCdm*

**Düzeltme:** GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Uzak Masaüstü Hizmetleri\Uzak Masaüstü Oturum Ana Bilgisayarı\Aygıt ve Kaynak Yeniden Yönlendirme\Sürücü yeniden yönlendirmesine izin verme*

**Not**: Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu TerminalServer.admx/adml tarafından sağlanır.

**18.9.65.3.3.4 (L2) 'Konum yeniden yönlendirmeye izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Uzak Masaüstü Hizmetleri oturumunda konum verilerinin uzak bilgisayara yeniden yönlendirilmesini denetler. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Güvenlik açısından daha hassas bir ortamda, olası saldırı yüzeyinin azaltılması arzu edilir. Bir Uzak Masaüstü oturumu içinde konum verilerinin yeniden yönlendirilmesi ihtiyacı nadirdir, bu nedenle kötü amaçlı etkinliklerin gerçekleşmesi için beklenmeyen yolların sayısını azaltmak mantıklıdır.

**Etki:**

Kullanıcılar, konum verilerini uzak bilgisayara yeniden yönlendiremez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fDisableLocationRedir*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\Yönetim Şablonları \Windows Bileşenleri\Uzak Masaüstü Hizmetleri\Uzak Masaüstü Oturum Ana Bilgisayarı\Aygıt ve Kaynak Yeniden Yönlendirme\Konum yeniden yönlendirmesine izin verme*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 21H2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu TerminalServer.admx/adml tarafından sağlanır.

**18.9.65.3.3.5 (L2) 'LPT bağlantı noktası yeniden yönlendirmesine izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bir Uzak Masaüstü Hizmetleri oturumu sırasında verilerin istemci LPT bağlantı noktalarına yeniden yönlendirilmesinin engellenip engellenmeyeceğini belirtir. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Güvenlik açısından daha hassas bir ortamda, olası saldırı yüzeyinin azaltılması arzu edilir. Bir Uzak Masaüstü oturumu içinde LPT bağlantı noktası yeniden yönlendirme ihtiyacı çok nadirdir, bu nedenle veri hırsızlığı ve/veya kötü amaçlı kod aktarımı için beklenmeyen yolların sayısını azaltmak mantıklıdır.

**Etki:**

Uzak Masaüstü Hizmetleri oturumundaki kullanıcılar, sunucu verilerini yerel (istemci) LPT bağlantı noktalarına yeniden yönlendiremez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fDisableLPT*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\ Yönetim Şablonları\Windows Bileşenleri\Uzak Masaüstü Hizmetleri\Uzak Masaüstü Oturum Ana Bilgisayarı\Aygıt ve Kaynak Yeniden Yönlendirme\LPT bağlantı noktası yeniden yönlendirmesine izin verme*

**Not**: Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerde bulunan Grup İlkesi şablonu TerminalServer.admx/adml tarafından sağlanır.

**18.9.65.3.3.6 (L2) 'Desteklenen Tak ve Kullan cihaz yeniden yönlendirmesine izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows Taşınabilir Aygıtlar gibi desteklenen Tak ve Kullan aygıtlarının Uzak Masaüstü Hizmetleri oturumunda uzak bilgisayara yeniden yönlendirilmesini denetlemenize olanak tanır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Güvenlik açısından daha hassas bir ortamda, olası saldırı yüzeyinin azaltılması arzu edilir. Uzak Masaüstü oturumu içinde Tak ve Kullan cihaz yeniden yönlendirme ihtiyacı çok nadirdir, bu nedenle veri hırsızlığı ve/veya kötü amaçlı kod aktarımı için beklenmeyen yolların sayısını azaltmak mantıklıdır.

**Etki:**

Uzak Masaüstü Hizmetleri oturumundaki kullanıcılar, desteklenen (yerel istemci) Tak ve Kullan aygıtlarını uzak bilgisayara yeniden yönlendiremez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fDisablePNPRedir*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Uzak Masaüstü Hizmetleri\Uzak Masaüstü Oturum Ana Bilgisayarı\Aygıt ve Kaynak Yeniden Yönlendirme\Desteklenen Fişe izin verme ve Play cihazı yeniden yönlendirmesi*

**Not**: Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu TerminalServer.admx/adml tarafından sağlanır.

**18.9.65.3.4 Lisanslama**

**18.9.65.3.5 Yazıcı Yeniden Yönlendirme**

**18.9.65.3.6 Profiller**

**18.9.65.3.7 RD Bağlantı Aracısı (eski adıyla TH Bağlantı Aracısı)**

**18.9.65.3.8 Uzak Oturum Ortamı**

**18.9.65.3.9 Güvenlik**

**18.9.65.3.9.1 (L1) 'Bağlantı sırasında her zaman parola sor' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Uzak Masaüstü Hizmetleri'nin bağlantı sırasında istemci bilgisayardan her zaman bir parola isteyip istemediğini belirtir. Bu ilke ayarını, Parolayı Uzak Masaüstü Bağlantısı istemcisinde zaten sağlamış olsalar bile, Uzak Masaüstü Hizmetleri'nde oturum açan kullanıcılar için parola istemini zorlamak için kullanabilirsiniz. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Kullanıcılar, yeni bir Uzak Masaüstü Bağlantısı kısayolu oluşturduklarında hem kullanıcı adlarını hem de parolalarını saklama seçeneğine sahiptir. Uzak Masaüstü Hizmetlerini çalıştıran sunucu, bu özelliği kullanan kullanıcıların sunucuda oturum açmasına izin veriyor ancak parolalarını girmiyorsa, kullanıcının bilgisayarına fiziksel erişim kazanmış bir saldırganın bir Uzak Masaüstü Sunucusuna bağlanması olasıdır. Kullanıcının parolasını bilmeseler bile Uzak Masaüstü Bağlantısı kısayolu aracılığıyla.

**Etki:**

Kullanıcılar, Uzak Masaüstü Bağlantısı istemcisinde parolalarını sağlayarak Uzak Masaüstü Hizmetleri'nde otomatik olarak oturum açamaz. Onlardan oturum açmak için bir parola istenir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fPromptForPassword*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\ Yönetim Şablonları\Windows Bileşenleri\Uzak Masaüstü Hizmetleri\Uzak Masaüstü Oturum Ana Bilgisayarı\Güvenlik\Bağlantı sırasında her zaman parola ister*

**Not:** Bu Grup İlkesi yolu, Microsoft'un tüm sürümlerinde bulunan Grup İlkesi şablonu TerminalServer.admx/adml tarafından sağlanır. Windows Yönetim Şablonları.

**Not #2:** Microsoft Windows Vista Yönetim Şablonlarında bu ayar, bağlantıda her zaman istemciden parola iste olarak adlandırılmıştır, ancak Windows Server 2008 (R2 olmayan Yönetim Şablonları) ile başlayarak yeniden adlandırılmıştır.

**18.9.65.3.9.2 (L1) 'Güvenli RPC iletişimi gerektir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Uzak Masaüstü Hizmetlerinin tüm istemcilerle güvenli Uzaktan Yordam Çağrısı (RPC) iletişimi gerektirip gerektirmediğini veya güvenli olmayan iletişime izin verip vermediğini belirlemenize olanak tanır. Yalnızca kimliği doğrulanmış ve şifrelenmiş isteklere izin vererek istemcilerle RPC iletişiminin güvenliğini güçlendirmek için bu ilke ayarını kullanabilirsiniz. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Güvenli olmayan RPC iletişimine izin vermek, sunucuyu ortadaki adam saldırılarına ve veri ifşa saldırılarına maruz bırakabilir.

**Etki:**

Uzak Masaüstü Hizmetleri, güvenli istekleri destekleyen RPC istemcilerinden gelen istekleri kabul eder ve güvenilmeyen istemcilerle güvenli olmayan iletişime izin vermez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:fEncryptRPCTraffic*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Uzak Masaüstü Hizmetleri\Uzak Masaüstü Oturum Ana Bilgisayarı\Güvenlik\Güvenli RPC iletişimi gerektirir*

**Not:** Bu Grup İlke yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu TerminalServer.admx/adml tarafından sağlanır.

**18.9.65.3.9.3 (L1) 'Uzak (RDP) bağlantılar için belirli güvenlik katmanının kullanılmasını gerektir' seçeneği 'Etkin: SSL' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Uzak Masaüstü Protokolü (RDP) bağlantıları sırasında istemciler ve RD Oturum Ana Bilgisayarı sunucuları arasındaki iletişimin güvenliğini sağlamak için belirli bir güvenlik katmanının kullanılmasının gerekip gerekmediğini belirtir. Bu ayar için önerilen durum: Etkin: SSL.

**Not:** Bu ayarın SSL olarak etiketlenmesine rağmen, aslında eski (ve daha az güvenli) SSL protokolünü değil, Aktarım Katmanı Güvenliği (TLS) sürüm 1.0'ı zorunlu kılar. Gerekçe: Yerel Uzak Masaüstü Protokolü (RDP) şifrelemesi artık zayıf bir protokol olarak kabul edilir, bu nedenle istemciler ve RD Oturum Ana Bilgisayarı sunucuları arasındaki tüm RDP iletişimleri için daha güçlü Aktarım Katmanı Güvenliği (TLS) şifrelemesinin kullanılması tercih edilir.

**Etki:**

RD Oturum Ana Bilgisayarı sunucusunda kimlik doğrulaması yapmak için TLS 1.0 gerekli olacaktır. TLS desteklenmiyorsa bağlantı başarısız olur.

**Not:** Varsayılan olarak bu ayar, RDP bağlantıları için kendinden imzalı bir sertifika kullanır. Kuruluşunuz SSL/TLS şifrelemesi için bir Ortak Anahtar Altyapısı (PKI) kullanımını kurduysa, RDP'ye kendinden imzalı bir sertifika yerine PKI'nızdan bir sertifika kullanma talimatı vermek için Sunucu kimlik doğrulama sertifikası şablonu ayarını da yapılandırmanızı öneririz. bir. Bu amaçla kullanılan sertifika şablonunun, Amaçlanan Amaç olarak yapılandırılmış "İstemci Kimlik Doğrulaması" olması gerektiğini unutmayın. Ayrıca, belirtilen şablonu kullanan geçerli, süresi dolmamış bir sertifikanın çalışması için iş istasyonunda önceden kurulmuş olması gerektiğini unutmayın.

**Not #2**: SSL/TLS güvenlik katmanı, ilk bağlantı girişiminde (RDP oturum açma ekranından önce) kullanıcının Windows parolasını bekleyeceğinden, bazı üçüncü taraf iki faktörlü kimlik doğrulama çözümleri (ör. RSA Kimlik Doğrulama Aracısı) bu ayardan olumsuz etkilenebilir. , ve kimliği başarılı bir şekilde doğrulandıktan sonra, kimlik bilgilerini RDP ana bilgisayarındaki o Windows oturumuna iletin (oturum açma işlemini tamamlamak için). İki faktörlü bir aracı varsa ve RDP oturum açma ekranında farklı bir kimlik bilgisi bekliyorsa, bu ilk bağlantı başarısız bir oturum açma girişimine neden olabilir ve ayrıca her yeni RDP oturumu için etkin bir şekilde "çift oturum açma" gereksinimine neden olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:SecurityLayer*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın: SSL:

*Bilgisayar Yapılandırması\ İlkeler\Yönetim Şablonları\Windows Bileşenleri\Uzak Masaüstü Hizmetleri\Uzak Masaüstü Oturum Ana Bilgisayarı\Güvenlik\Uzak (RDP) bağlantılar için özel güvenlik katmanı kullanılmasını gerektirir*

**Not:** Bu Grup İlkesi yolu, Grup İlkesi şablonu TerminalServer.admx/adml tarafından sağlanır. Microsoft Windows Yönetim Şablonlarının tüm sürümlerine dahildir.

**18.9.65.3.9.4 (L1) 'Ağ Düzeyinde Kimlik Doğrulama kullanarak uzak bağlantılar için kullanıcı kimlik doğrulaması gerektir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Ağ Düzeyinde Kimlik Doğrulamayı kullanarak RD Oturum Ana Bilgisayarı sunucusuna yapılan uzak bağlantılar için kullanıcı kimlik doğrulamasının gerekip gerekmediğini belirtmenize olanak tanır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Uzak bağlantı sürecinde kullanıcı kimlik doğrulamasının daha erken gerçekleşmesini zorunlu kılmak, güvenliği artırır.

**Etki:**

Yalnızca Ağ Düzeyinde Kimlik Doğrulamayı destekleyen istemci bilgisayarlar RD Oturum Ana Bilgisayarı sunucusuna bağlanabilir.

**Not:** Bazı üçüncü taraf iki faktörlü kimlik doğrulama çözümleri (ör. RSA Kimlik Doğrulama Aracısı) bu ayardan olumsuz etkilenebilir, çünkü Ağ Düzeyinde Kimlik Doğrulama, ilk bağlantı girişiminde (RDP oturum açma ekranından önce) ve başarılı bir şekilde kimlik doğrulaması yapıldığında kullanıcının Windows parolasını bekleyecektir. , kimlik bilgilerini RDP ana bilgisayarındaki o Windows oturumuna iletin (oturum açma işlemini tamamlamak için). İki faktörlü bir aracı varsa ve RDP oturum açma ekranında farklı bir kimlik bilgisi bekliyorsa, bu ilk bağlantı başarısız bir oturum açma girişimine neden olabilir ve ayrıca her yeni RDP oturumu için etkin bir şekilde "çift oturum açma" gereksinimine neden olabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:UserAuthentication*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Uzak Masaüstü Hizmetleri\Uzak Masaüstü Oturum Ana Bilgisayarı\Güvenlik\Kullanarak uzak bağlantılar için kullanıcı kimlik doğrulaması gerektir Ağ Düzeyinde Kimlik Doğrulama*

**Not**: Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu TerminalServer.admx/adml tarafından sağlanır.

**Not #2:** Microsoft Windows Vista Yönetim Şablonlarında, bu ayar başlangıçta Uzak bağlantılar için RDP 6.0 kullanılarak kullanıcı kimlik doğrulaması iste olarak adlandırılmıştı, ancak Windows Server 2008 (R2 olmayan Yönetim Şablonları) ile başlayarak yeniden adlandırıldı.

**18.9.65.3.9.5 (L1) 'İstemci bağlantısı şifreleme düzeyini ayarla' seçeneği 'Etkin: Yüksek Düzey' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Uzak Masaüstü Protokolü (RDP) bağlantıları sırasında istemci bilgisayarlar ile RD Oturum Ana Bilgisayarı sunucuları arasındaki iletişimi güvenli hale getirmek için belirli bir şifreleme düzeyinin kullanılmasının gerekip gerekmediğini belirtir. Bu politika yalnızca yerel RDP şifrelemesi kullandığınızda geçerlidir. Ancak, yerel RDP şifrelemesi (SSL şifrelemesinin aksine) önerilmez. Bu politika, SSL şifrelemesi için geçerli değildir. Bu ayar için önerilen durum: Etkin: Yüksek Düzey.

**Gerekçe:**

Düşük seviyeli şifreleme kullanan Uzak Masaüstü istemci bağlantılarına izin verilirse, bir saldırganın yakalanan Uzak Masaüstü Hizmetleri ağ trafiğinin şifresini çözmesi daha olasıdır.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:MinEncryptionLevel*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın: Yüksek Düzey:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Uzak Masaüstü Hizmetleri\Uzak Masaüstü Oturum Ana Bilgisayarı\Güvenlik\İstemci bağlantısı şifreleme düzeyini ayarlayın*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu TerminalServer.admx/adml tarafından sağlanır.

**18.9.65.3.10 Oturum Süresi Sınırları**

**18.9.65.3.10.1 (L2) 'Etkin ancak boşta olan Uzak Masaüstü Hizmetleri oturumları için zaman sınırı ayarla' seçeneği 'Etkin: 15 dakika veya daha az, ancak Hiçbir Zaman (0)’ olarak ayarlanmalıdır. (Otomatik)**

**Açıklama:**

Bu ilke ayarı, etkin bir Uzak Masaüstü Hizmetleri oturumunun otomatik olarak bağlantısı kesilmeden önce (kullanıcı girişi olmadan) boşta kalabileceği maksimum süreyi belirtmenize olanak tanır. Bu ayar için önerilen durum: Etkin: 15 dakika veya daha az, ancak Hiçbir Zaman (0) değil.

**Gerekçe:**

Bu ayar, etkin Uzak Masaüstü oturumlarının kullanılmadığı sırada bilgisayarı uzun süre bağlamasını ve bilgi işlem kaynaklarının çok sayıda etkin olmayan oturum tarafından tüketilmesini önlemeye yardımcı olur. Ayrıca, hala etkin olan eski, unutulmuş Uzak Masaüstü oturumları, kullanıcının parolası değiştiyse ancak eski oturum hala çalışıyorsa parola kilitlenmesine neden olabilir. Bağlı kullanıcı sayısını sınırlayan sistemler için (örneğin, varsayılan Yönetim modundaki sunucular - yalnızca 2 oturum), diğer kullanıcıların eski ancak hala etkin oturumları, başka bir kullanıcının bağlanmasını engelleyebilir ve bu da etkin bir hizmet reddine neden olabilir

**Etki:**

Uzak Masaüstü Hizmetleri, etkin ancak boşta olan oturumların bağlantısını 15 dakika (veya belirtilen süre kadar) sonra otomatik olarak kesecektir. Kullanıcı, oturumun bağlantısı kesilmeden iki dakika önce bir uyarı alır; bu, kullanıcının oturumu etkin tutmak için bir tuşa basmasına veya fareyi hareket ettirmesine olanak tanır. Boşta oturum süresi sınırlarının konsol oturumları için geçerli olmadığını unutmayın.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:MaxIdleTime*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: 15 dakika veya daha az, ama Asla (0):

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Uzak Masaüstü Hizmetleri\Uzak Masaüstü Oturum Ana Bilgisayarı\Oturum Zaman Sınırları\Etkin ancak boşta Uzak Masaüstü Hizmetleri oturumları için zaman sınırı ayarla*

**Not:** Bu Grup İlkesi yolu sağlanır Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu TerminalServer.admx/adml tarafından.

**Not #2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar Etkin ancak boştaki Terminal Hizmetleri oturumları için süre sınırı ayarla olarak adlandırılmıştır, ancak Windows 7 ve Server 2008 R2 Yönetim Şablonlarından başlayarak yeniden adlandırılmıştır.

**18.9.65.3.10.2 (L2) 'Bağlantısı kesilmiş oturumlar için süre sınırı ayarla' seçeneği 'Etkin: 1 dakika' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, bağlantısı kesilmiş Uzak Masaüstü Hizmetleri oturumları için bir zaman sınırı yapılandırmanıza olanak tanır. Bu ayar için önerilen durum: Etkin: 1 dakika.

**Gerekçe:**

Bu ayar, etkin Uzak Masaüstü oturumlarının kullanılmadığı sırada bilgisayarı uzun süre bağlamasını önlemeye yardımcı olur ve bilgi işlem kaynaklarının çok sayıda bağlantısı kesilmiş ancak etkin oturum tarafından tüketilmesini önler. Ayrıca, hala etkin olan eski, unutulmuş Uzak Masaüstü oturumları, kullanıcının parolası değiştiyse ancak eski oturum hala çalışıyorsa parola kilitlenmesine neden olabilir. Bağlı kullanıcı sayısını sınırlayan sistemler için (örneğin, varsayılan Yönetim modundaki sunucular - yalnızca 2 oturum), diğer kullanıcıların eski ancak hala etkin oturumları, başka bir kullanıcının bağlanmasını engelleyebilir ve bu da etkin bir hizmet reddine neden olabilir. Bu ayar, bağlantısı kesilmiş bir oturumun düzgün bir şekilde sonlandırıldığından emin olmak için önemlidir.

**Etki:**

Bağlantısı kesilen Uzak Masaüstü oturumları 1 dakika sonra sunucudan silinir. Bağlantısı kesilen oturum süresi sınırlarının konsol oturumları için geçerli olmadığını unutmayın.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:MaxDisconnectionTime*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: 1 dakika:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Uzak Masaüstü Hizmetleri\Uzak Masaüstü Oturum Ana Bilgisayarı\Oturum Süresi Sınırları\Zaman sınırını ayarla bağlantısı kesilen oturumlar için*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu TerminalServer.admx/adml tarafından sağlanır.

**18.9.65.3.11 Geçici klasörler**

**18.9.65.3.11.1 (L1) 'Çıkışta geçici klasörleri silme' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Uzak Masaüstü Hizmetleri'nin oturum kapatıldığında kullanıcının oturum başına geçici klasörlerini tutup tutmayacağını belirtir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Geçici klasörlerin içinde hassas bilgiler bulunabilir ve sistemde oturum açan diğer yöneticiler tarafından görülebilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\Terminal Services:DeleteTempDirsOnExit*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Uzak Masaüstü Hizmetleri\Uzak Masaüstü Oturum Ana Bilgisayarı\Geçici Klasörler\Çıkışta geçici klasörleri silme*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu TerminalServer.admx/adml tarafından sağlanır.

**Not 2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar Çıkışta geçici klasörü silme olarak adlandırılmıştır, ancak Windows 8.0 ve Server 2012 (R2 olmayan Yönetim Şablonları) ile başlayarak yeniden adlandırılmıştır.

**18.9.66 RSS Beslemeleri**

**18.9.66.1 (L1) 'Kasaların indirilmesini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcının bir RSS beslemesinden kullanıcının bilgisayarına ekleri (dosya ekleri) indirmesini engeller. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Eklerin RSS beslemesi aracılığıyla indirilmesine izin vermek, kötü niyetli olabilecek dosyaların ortaya çıkmasına neden olabilir.

**Etki:**

Kullanıcılar, Feed özelliği sayfası aracılığıyla bir ek indirmek için Feed Sync Engine'i ayarlayamaz. Geliştiriciler, feed API'leri aracılığıyla indirme ayarını değiştiremez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\InternetExplorer\Feeds:DisableEnclosureDownload*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\RSS Akışları\Kasaların indirilmesini engelle*

**Not:** Bu Grup İlkesi yolu, Grup İlkesi tarafından sağlanır. Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan şablon InetRes.admx/adml.

**Not #2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayarın adı Muhafazaların indirilmesini kapat, ancak Windows 8.0 ve Server 2012 (R2 olmayan Yönetim Şablonları) ile başlayarak yeniden adlandırıldı.

**18.9.67 Arama**

**18.9.67.1 OCR**

**18.9.67.2 (L2) 'Cloud Sear****ch'e İzin Ver' seçeneği 'Etkin: Cloud Search'ü Devre Dışı Bırak' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcının bir RSS beslemesinden kullanıcının bilgisayarına ekleri (dosya ekleri) indirmesini engeller. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Eklerin RSS beslemesi aracılığıyla indirilmesine izin vermek, kötü niyetli olabilecek dosyaların ortaya çıkmasına neden olabilir.

**Etki:**

Kullanıcılar, Feed özelliği sayfası aracılığıyla bir ek indirmek için Feed Sync Engine'i ayarlayamaz. Geliştiriciler, feed API'leri aracılığıyla indirme ayarını değiştiremez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\InternetExplorer\Feeds:DisableEnclosureDownload*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\RSS Akışları\Kasaların indirilmesini engelle*

**Not**: Bu Grup İlkesi yolu, Grup İlkesi tarafından sağlanır. Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan şablon InetRes.admx/adml.

**Not #2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayarın adı Muhafazaların indirilmesini kapat, ancak Windows 8.0 ve Server 2012 (R2 olmayan Yönetim Şablonları) ile başlayarak yeniden adlandırıldı.

**18.9.67.3 (L1) 'Cortana'ya** **izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, cihazda Cortana'ya izin verilip verilmediğini belirtir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Cortana etkinleştirilirse, hassas bilgiler arama geçmişinde bulunabilir ve Microsoft'a gönderilebilir.

**Etki:**

Cortana kapatılacak. Kullanıcılar, cihazda ve İnternette bir şeyler bulmak için aramayı kullanmaya devam edebilecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search:AllowCortana*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\Windows Components\Search\Cortana'ya İzin Ver*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 RTM (Sürüm 1507) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu Search.admx/adml tarafından sağlanır.

**18.9.67.4 (L1) 'Cortana'nın kilit ekranının üzerinde olmasına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, sistem kilitliyken kullanıcının Cortana ile konuşma kullanarak etkileşime girip giremeyeceğini belirler. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Cihaz kilitliyken herhangi bir bilgisayar kaynağına erişime izin verilmemelidir.

**Etki:**

Kullanıcının Cortana ile konuşarak etkileşim kurabilmesi için sistemin kilidinin açılması gerekir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search:AllowCortanaAboveLock*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\Windows Components\Search\Cortana'ya izin ver kilit ekranının üzerinde*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1607 ve Server 2016 Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu Search.admx/adml tarafından sağlanır.

**18.9.67.5 (L1) 'Şifrelenmiş dosyaların dizine eklenmesine izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, şifrelenmiş öğelerin dizine eklenmesine izin verilip verilmeyeceğini kontrol eder. Bu ayar değiştirildiğinde, dizin tamamen yeniden oluşturulur. Şifrelenmiş dosyaların güvenliğini sağlamak için dizinin konumu için tam birim şifrelemesi (BitLocker Sürücü Şifrelemesi veya Microsoft'a ait olmayan bir çözüm gibi) kullanılmalıdır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Dizin oluşturma ve kullanıcıların şifrelenmiş dosyaları aramasına izin verme, şifrelenmiş dosyalar içinde saklanan gizli verileri potansiyel olarak açığa çıkarabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search:AllowIndexingEncryptedStoresOrItems*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\Windows Components\Search\Şifreli dosyaların dizine eklenmesine izin ver*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu Search.admx/adml tarafından sağlanır.

**18.9.67.6 (L1) 'Aramanın ve Cortana'nın konumu kullanmasına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, aramanın ve Cortana'nın konuma duyarlı arama ve Cortana sonuçları sağlayıp sağlayamayacağını belirtir. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Kurumsal olarak yönetilen bir ortamda Cortana ve Arama'nın konum verilerine erişmesine izin vermek gereksizdir. Kuruluşlar muhtemelen bu bilgilerin paylaşılmasını istemezler. Etki: Arama ve Cortana'nın konum bilgilerine erişimi olmayacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Windows Search:AllowSearchToUseLocation*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\Windows Components\Search\Aramaya ve Cortana'nın konumu kullanmasına izin ver*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 RTM (Sürüm 1507) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu Search.admx/adml tarafından sağlanır.

**18.9.68 Güvenlik Merkezi**

**18.9.69 NIS Sunucusu**

**18.9.70 Kapatma Seçenekleri**

**18.9.71 Akıllı Kart**

**18.9.72 Yazılım Koruma Platformu**

**18.9.72.1 (L2) 'KMS Client Online AVS Doğrulamasını Kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Anahtar Yönetim Hizmeti (KMS), yazılım lisanslarını depolamak için yerel bir sunucu kurmayı gerektiren bir Microsoft lisans etkinleştirme yöntemidir. KMS hizmetini etkinleştirmek için KMS sunucusunun kendisinin Microsoft'a bağlanması gerekir, ancak sonraki ağ üzerindeki istemciler, doğrudan Microsoft'a bağlanmak yerine Microsoft Windows işletim sistemini ve/veya Microsoft Office'lerini KMS sunucusu aracılığıyla etkinleştirebilir. Bu ilke ayarı, KMS istemci etkinleştirme verilerini Microsoft'a otomatik olarak göndermeyi devre dışı bırakmanıza olanak tanır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

KMS lisanslama yöntemi, KMS istemcilerinin Microsoft'a bağlanmasını gerektirmese de, KMS istemcisi etkinleştirme durumu verilerini Microsoft'a otomatik olarak gönderirler. Bu bilgilerin gönderilmesini önlemek, yüksek güvenlikli ortamlarda gizlilik endişelerini azaltmaya yardımcı olabilir.

**Etki:**

Bilgisayarın, KMS istemcisi etkinleştirme durumuyla ilgili olarak Microsoft'a veri göndermesi engellenir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows NT\CurrentVersion\Software Protection Platform:NoGenTicket*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması \İlkeler\Yönetim Şablonları\Windows Bileşenleri\Yazılım Koruma Platformu\KMS İstemci Çevrimiçi AVS Doğrulamasını Kapat*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 RTM (Sürüm 1507) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu AVSValidationGP.admx/adml tarafından sağlanır.

**18.9.73 Ses Kaydedici**

**18.9.74 Konuşma**

**18.9.75 Mağaza**

**18.9.75.1 (L2) 'Microsoft Store'daki tüm uygulamaları devre dışı bırak' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, Microsoft Store'dan önceden yüklenmiş veya indirilmiş tüm uygulamaların başlatılmasını yapılandırır. Bu ayar için önerilen durum: Devre Dışı.

**Not:** Bu ilke ayarı yalnızca Windows 10 Enterprise ve Windows 10 Education sürümleri için geçerlidir.

**Not #2:** Bu ayarın adı ve Etkin/Devre Dışı değerleri yanlış ifade edilmiştir – mantıksal olarak başlık, Etkin olarak yapılandırmanın Microsoft Store'daki tüm uygulamaları devre dışı bırakacağını ve Devre Dışı olarak yapılandırmanın Microsoft'tan tüm uygulamaları etkinleştireceğini ima eder. Mağaza. Bunun tersi doğrudur (ve GPME yardım metniyle uyumludur). Bu, Yönetim Şablonunda Microsoft tarafından yapılan mantıksal bir ifade hatasıdır.

**Gerekçe:**

Mağaza hizmeti, öncelikle tüketici kullanımı için Windows'ta yerleşik bir perakende satış noktasıdır. Kurumsal olarak yönetilen bir ortamda BT departmanı, güvenlik açığı bulunan yazılımların yüklenmesi riskini azaltmak için tüm uygulamaların kurulumunu yönetmelidir.

**Etki:**

Microsoft Store'dan önceden yüklenmiş veya indirilmiş tüm uygulamaların başlatılması engellenir. Mevcut Microsoft Store uygulamaları güncellenmeyecek. Microsoft Mağazası devre dışı.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsStore:DisableStoreApps*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Components\Store\Microsoft Store'dan tüm uygulamaları devre dışı bırak*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1511 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu WindowsStore.admx/adml tarafından sağlanır.

**Not 2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Windows Mağazasından tüm uygulamaları devre dışı bırak olarak adlandırılmıştı, ancak Windows 10 Sürüm 1803 Yönetim Şablonlarından başlayarak yeniden adlandırıldı.

**18.9.75.2 (L1) 'Yalnızca Microsoft Store'daki özel mağazayı göster' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Microsoft Store'daki perakende kataloğuna erişimi reddeder ancak özel mağazayı görüntüler. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Özel mağazaya izin vermek, bir kuruluşun, kullanıcıların bir sisteme eklemek için erişime sahip olduğu uygulamaları kontrol etmesine olanak tanır. Bu, onaylanmamış kötü amaçlı uygulamaların bir sistemde çalışmamasını sağlamaya yardımcı olacaktır.

**Etki:**

Kullanıcılar Microsoft Store'daki perakende kataloğunu görüntüleyemeyecek, ancak özel mağazadaki uygulamaları görüntüleyebilecekler.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsStore:RequirePrivateSto reOnly*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Mağaza\Yalnızca Microsoft Mağazasındaki özel mağazayı görüntüle*

**Not:** Bu Grup İlkesi yolu, varsayılan olarak var. Microsoft Windows 10 Sürüm 1607 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu WindowsStore.admx/adml tarafından sağlanır.

**Not #2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Yalnızca Windows Mağazası uygulamasındaki özel mağazayı görüntüle olarak adlandırılmıştı, ancak Windows 10 Sürüm 1803 Yönetim Şablonlarından başlayarak yeniden adlandırıldı.

**18.9.75.3 (L1) 'Güncellemelerin Otomatik İndirilmesini ve Yüklenmesini Kapat' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, Microsoft Store uygulama güncellemelerinin otomatik olarak indirilmesini ve yüklenmesini etkinleştirir veya devre dışı bırakır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Sisteminizi düzgün bir şekilde yamalanmış halde tutmak, 0 günlük güvenlik açıklarına karşı korunmaya yardımcı olabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsStore:AutoDownload*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki kullanıcı arabirimi yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Components\Store\Güncelleştirmelerin Otomatik İndirilmesini ve Yüklenmesini Kapat*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.1 ve Server 2012 R2 Yönetim Şablonlarında bulunan Grup İlkesi şablonu WinStoreUI.admx/adml tarafından veya Microsoft Windows 10 Sürüm 1511 Yönetim Sisteminde bulunan Grup İlkesi şablonu WindowsStore.admx/adml tarafından sağlanır. Şablonlar (veya daha yenisi)

**18.9.75.4 (L1) 'Windows'un en son sürümüne güncelleme teklifini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Windows'un en son sürümüne güncellemek için Microsoft Store teklifini etkinleştirir veya devre dışı bırakır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Planlanmamış işletim sistemi yükseltmeleri, daha önlenebilir destek çağrılarına yol açabilir. BT departmanı, tüm yükseltmeleri ve güncellemeleri yönetiyor ve onaylıyor olmalıdır.

**Etki:**

Microsoft Store uygulaması, Windows'un en son sürümü için güncellemeler sunmayacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsStore:DisableOSUpgrade*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki kullanıcı arabirimi yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Components\Store\Windows'un en son sürümüne güncelleme teklifini kapatın*

Not: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.1 ve Server 2012 R2 Yönetim Şablonlarında bulunan Grup İlkesi şablonu WinStoreUI.admx/adml tarafından veya Microsoft Windows 10 Sürüm 1511 Yönetim Sisteminde Şablonlar (veya daha yenisi) bulunan Grup İlkesi şablonu WindowsStore.admx/adml tarafından sağlanır.

**18.9.75.5 (L2) 'Mağaza uygulamasını kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama**:

Bu ayar, Mağaza uygulamasına erişimi reddeder veya izin verir. Bu ayar için önerilen durum: Etkin.

**Not:** [Microsoft TechNet](https://technet.microsoft.com/en-us/itpro/windows/manage/group-policies-for-enterprise-and-education-editions) ve [MSKB 3135657](https://support.microsoft.com/en-us/help/3135657/can-t-disable-windows-store-in-windows-10-pro-through-group-policy) uyarınca, bu ilke ayarı Enterprise ve Education dışındaki Windows 10 sürümleri için geçerli değildir.

**Gerekçe:**

Yalnızca bir BT departmanı tarafından onaylanan uygulamalar yüklenmelidir. Kullanıcıların 3. taraf uygulamaları yüklemesine izin vermek, yamaların kaçırılmasına ve potansiyel sıfır gün güvenlik açıklarına neden olabilir.

**Etki:**

Microsoft Store uygulamasına erişim reddedildi.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsStore:RemoveWindowsStore*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Mağaza\Mağaza uygulamasını kapatın*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonlarında bulunan Grup İlkesi şablonu WinStoreUI.admx/adml tarafından veya Microsoft Windows 10 Sürüm 1511 Yönetim Şablonlarında (veya daha yenisi) bulunan Grup İlkesi şablonu WindowsStore.admx/adml tarafından sağlanır.

**18.9.76 Ayarlarınızı senkronize edin**

**18.9.77 Tablet PC**

**18.9.78 Görev Zamanlayıcı**

**18.9.79 Kiracı Kısıtlamaları**

**18.9.80 Metin Girişi**

**18.9.81 Widget'lar**

**18.9.81.1 (L1) 'Widget'lara izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlandığından emin olun**

**Açıklama:**

Bu ilke ayarı, aygıtta pencere öğeleri özelliğine izin verilip verilmediğini belirtir. Widget özelliği hava durumu, haberler, spor, hisse senetleri, trafik ve eğlence (kapsayıcı bir liste değil) gibi bilgiler sağlar. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Gizlilik endişeleri nedeniyle, Windows görev çubuğundaki widget'lar gibi uygulamalar ve özellikler, verilerin Microsoft gibi 3. taraflara geri gönderilme potansiyeli nedeniyle olası bir güvenlik riski olarak değerlendirilmelidir.

**Etki:**

Windows görev çubuğundaki widget özelliği cihazda kullanılamayacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Dsh:AllowNewsAndInterests*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\WindowsBileşenleri\Widgets\Widgets'a İzin Ver*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 21H2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu NewsAndInterests.admx/adml tarafından sağlanır.

**18.9.82 Windows Takvim**

**18.9.83 Windows Renk Sistemi**

**18.9.84 Windows Müşteri Deneyimini Geliştirme Programı**

**18.9.85 Windows Defender Akıllı Ekran**

**18.9.85.1 Gezgin**

**18.9.85.1.1 (L1) 'Windows Defender SmartScreen'i Yapılandır' seçeneği 'Etkin: Uyar ve atlamayı önle' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows Defender SmartScreen'in davranışını yönetmenize olanak tanır. Windows Defender SmartScreen, İnternet'ten indirilen tanınmayan programları çalıştırmadan önce kullanıcıları uyararak bilgisayarların daha güvenli kalmasına yardımcı olur. Bu özelliğin etkinleştirildiği bilgisayarlarda çalışan dosyalar ve programlar hakkında Microsoft'a bazı bilgiler gönderilir. Bu ayar için önerilen durum: Etkin: Uyar ve baypası engelle.

**Gerekçe:**

Windows Defender SmartScreen, İnternet'ten indirilen tanınmayan programları çalıştırmadan önce kullanıcıları uyararak bilgisayarların daha güvenli kalmasına yardımcı olur. Ancak, PC'lerde çalışan dosya ve programlarla ilgili bazı bilgilerin Microsoft'a gönderilmesi nedeniyle bazı kuruluşlar bunu devre dışı bırakmayı tercih edebilir.

**Etki:**

Kullanıcılar, İnternet'ten indirilen tanınmayan programları çalıştırmalarına izin verilmeden önce uyarılacaktır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumları tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:EnableSmartScre tr*

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\System:ShellSmartScree nLevel*

**Düzeltme**:

GP aracılığıyla önerilen yapılandırmayı oluşturmak için: aşağıdaki UI yolunu Etkin olarak ayarlayın: Uyar ve atlamayı engelle:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Windows Defender SmartScreen\Explorer\Windows Defender SmartScreen'i Yapılandır*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu WindowsExplorer.admx/adml tarafından sağlanır.

**Not #2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Windows SmartScreen'i Yapılandır olarak adlandırıldı, ancak Windows 10 Sürüm 1703 Yönetim Şablonlarından başlayarak yeniden adlandırıldı.

**18.9.85.2 Microsoft Edge**

**18.9.85.2.1 (L1) 'Windows Defender SmartScreen'i Yapılandır' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, SmartScreen Filtresini açıp açmamaya karar vermenizi sağlar. SmartScreen Filtresi, çalışanlarınızı olası kimlik avı dolandırıcılıklarından ve kötü amaçlı yazılımlardan korumaya yardımcı olmak için uyarı mesajları sağlar. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

SmartScreen, kullanıcıları olası kötü amaçlı siteler ve dosyalar konusunda uyarmaya yardımcı olduğu için önemli bir amaca hizmet eder. Kullanıcıların bu ayarı kapatmasına izin vermek, tarayıcıyı tehlikeye karşı daha savunmasız hale getirebilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\PhishingFilter:E nabledV9*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Windows Defender SmartScreen\Microsoft Edge\Windows Defender SmartScreen'i Yapılandır

**Not:** Bu Grup İlkesi yolu varsayılan olarak var. Microsoft Windows 10 RTM (Sürüm 1507) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu MicrosoftEdge.admx/adml tarafından sağlanır.

**Not #2:** Microsoft Windows 10 RTM (1507 Sürümü) Yönetim Şablonlarında, bu ayar başlangıçta SmartScreen'i yapılandırmanıza izin verir. Microsoft Windows 10 Sürüm 1511 Yönetim Şablonlarında, SmartScreen Filtresini Kapat olarak yeniden adlandırıldı. Microsoft Windows 10 Sürüm 1607 ve Server 2016 Yönetim Şablonlarında (tekrar) SmartScreen Filtresini Yapılandır olarak yeniden adlandırıldı. Son olarak, Windows 10 Sürüm 1703 Yönetim Şablonlarından başlayarak şu anki Windows Defender SmartScreen'i Yapılandır adı verildi.

**18.9.85.2.2 (L1) 'Siteler için Windows Defender SmartScreen istemlerinin atlanmasını engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, çalışanların potansiyel olarak kötü amaçlı web siteleri hakkındaki SmartScreen Filtresi uyarılarını geçersiz kılıp kılamayacağına karar vermenizi sağlar. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

SmartScreen, bir web sitesi potansiyel olarak kötü amaçlıysa bir çalışanı uyarır. Bu ayarın etkinleştirilmesi, bu uyarıların atlanmasını önler.

**Etki:**

Çalışanlar SmartScreen Filtresi uyarılarını görmezden gelemeyecek ve SmartScreen'in algıladığı potansiyel olarak kötü amaçlı web sitelerine gitmeleri engellenecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\PhishingFilter:P reventOverride*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Windows Defender SmartScreen\Microsoft Edge\Siteler için Windows Defender SmartScreen istemlerini atlamayı önleyin*

**Not:** Bu Grup İlke yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1511 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu MicrosoftEdge.admx/adml tarafından sağlanır.

**Not #2:** Microsoft Windows 10 Sürüm 1511 Yönetim Şablonlarında, bu ayar başlangıçta SmartScreen Filtresi uyarı geçersiz kılmalarına izin verme olarak adlandırılmıştır. Microsoft Windows 10 Sürüm 1607 ve Server 2016 Yönetim Şablonlarında bu ayar, siteler için SmartScreen istemlerini atlamayı engelle olarak yeniden adlandırılmıştır. Son olarak, Windows 10 Sürüm 1703 Yönetim Şablonları ile başlayan siteler için Windows Defender SmartScreen istemlerini atlayarak şu anki Önle adı verildi.

**18.9.86 Windows Hata Bildirimi**

**18.9.87 Windows Oyun Kaydı ve Yayını**

**18.9.87.1 (L1) 'Windows Oyun Kaydını ve Yayınını etkinleştirir veya devre dışı bırakır' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, çalışanların potansiyel olarak kötü amaçlı web siteleri hakkındaki SmartScreen Filtresi uyarılarını geçersiz kılıp kılamayacağına karar vermenizi sağlar. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

SmartScreen, bir web sitesi potansiyel olarak kötü amaçlıysa bir çalışanı uyarır. Bu ayarın etkinleştirilmesi, bu uyarıların atlanmasını önler.

**Etki:**

Çalışanlar SmartScreen Filtresi uyarılarını görmezden gelemeyecek ve SmartScreen'in algıladığı potansiyel olarak kötü amaçlı web sitelerine gitmeleri engellenecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\MicrosoftEdge\PhishingFilter:P reventOverride*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Windows Defender SmartScreen\Microsoft Edge\Siteler için Windows Defender SmartScreen istemlerini atlamayı önleyin*

**Not:** Bu Grup İlke yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1511 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu MicrosoftEdge.admx/adml tarafından sağlanır.

**Not #2:** Microsoft Windows 10 Sürüm 1511 Yönetim Şablonlarında, bu ayar başlangıçta SmartScreen Filtresi uyarı geçersiz kılmalarına izin verme olarak adlandırılmıştı. Microsoft Windows 10 Sürüm 1607 ve Server 2016 Yönetim Şablonlarında bu ayar, siteler için SmartScreen istemlerini atlamayı engelle olarak yeniden adlandırılmıştır. Son olarak, Windows 10 Sürüm 1703 Yönetim Şablonları ile başlayan siteler için Windows Defender SmartScreen istemlerini atlayarak şu anki Önle adı verildi.

**18.9.88 İş için Windows Hello (eski adıyla Microsoft Passport for Work)**

**18.9.89 Windows Ink Çalışma Alanı**

**18.9.89.1 (L2) 'Windows Ink Çalışma Alanı'nda önerilen uygulamalara izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, Windows Oyun Kaydı ve Yayını özelliklerini etkinleştirir veya devre dışı bırakır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bu ayara izin verilirse, kullanıcılar oturum bilgilerini kaydedebilir ve harici sitelere yayınlayabilir; bu, hem hassas şirket verilerinin (ekranda) yanlışlıkla şirket dışında ifşa edilmesi riski hem de gizlilik endişesidir.

**Etki:**

Windows Oyun Kaydı'na izin verilmeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\GameDVR:AllowGameDVR*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Windows Oyun Kaydı ve Yayını\Windows Oyun Kaydı ve Yayınını etkinleştirir veya devre dışı bırakır*

**Not:** Bu Grup İlkesi path varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 RTM (Sürüm 1507) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu GameDVR.admx/adml tarafından sağlanır.

**18.9.89.2 (L1) ' Windows Ink Çalışma Alanına İzin Ver' seçeneği 'Etkin: Açık, ancak kilidin üstünde erişime izin verme' veya ‘Devre Dışı’ olarak ayarlanmalıdır, ‘Etkin’ yapılmamalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows Ink Workspace'te önerilen uygulamalara izin verilip verilmeyeceğini belirler. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bu Microsoft özelliği, veri toplamak ve toplanan verilere dayalı olarak uygulamalar önermek için tasarlanmıştır. Bu ayarın devre dışı bırakılması, verilerinizin herhangi bir üçüncü tarafla paylaşılmamasına yardımcı olur.

**Etki:**

Windows Ink Workspace'te önerilen uygulamalara izin verilmeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsInkWorkspace:AllowSugge stedAppsInWindowsInkWorkspace*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Windows Ink Çalışma Alanı\Windows Ink Çalışma Alanında önerilen uygulamalara izin ver*

**Not:** Bu Grup İlkesi yolu varsayılan olarak var. Microsoft Windows 10 Sürüm 1607 ve Server 2016 Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu WindowsInkWorkspace.admx/adml tarafından sağlanır.

**18.9.90 Windows Installer**

**18.9.90.1 (L1) 'Yüklemeler üzerinde kullanıcı kontrolüne izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kilit ekranının üzerinde Windows Ink öğelerine izin verilip verilmeyeceğini belirler. Bu ayar için önerilen durum: Etkin: Açık, ancak kilidin üzerinde erişime izin vermiyor VEYA Devre Dışı.

**Gerekçe:**

Sistem kilitliyken herhangi bir uygulamaya erişilmesine izin verilmesi önerilmez. Bu özelliğe izin veriliyorsa, yalnızca kullanıcı uygun kimlik bilgileriyle kimlik doğrulaması yaptığında erişilebilir olmalıdır.

**Etki:**

Windows Ink Workspace'e kilit ekranının üzerinde izin verilmeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\WindowsInkWorkspace:AllowWindo wsInkWorkspace*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: Açık, ancak kilidin üzerinde erişime izin verme VEYA Devre Dışı:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Windows Ink Çalışma Alanı\Windows Ink Çalışma Alanına İzin Ver*

**Not :** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1607 ve Server 2016 Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu WindowsInkWorkspace.admx/adml tarafından sağlanır.

**18.9.90.2 (L1) 'Her zaman yükseltilmiş ayrıcalıklarla yükle' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, kullanıcıların genellikle yalnızca sistem yöneticileri tarafından kullanılabilen yükleme seçeneklerini değiştirmesine izin verilip verilmediğini denetler. Windows Installer'ın güvenlik özellikleri, normalde kullanıcıların, dosyaların yükleneceği dizini belirlemek gibi, genellikle sistem yöneticileri için ayrılmış olan yükleme seçeneklerini değiştirmelerini engeller. Windows Installer, bir yükleme paketinin kullanıcının korumalı bir seçeneği değiştirmesine izin verdiğini algılarsa, yüklemeyi durdurur ve bir mesaj görüntüler. Bu güvenlik özellikleri, yalnızca yükleme programı, kullanıcı tarafından reddedilen dizinlere erişimi olan ayrıcalıklı bir güvenlik bağlamında çalışırken çalışır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Kurumsal olarak yönetilen bir ortamda, bir sisteme yalnızca yönetici haklarına sahip BT personelinin yazılım yüklemesi veya değiştirmesi gerekir. Kullanıcılara yüklemeler üzerinde herhangi bir denetime sahip olma olanağı vermek, onaylanmamış yazılımların bir sisteme yüklenmesi veya sistemden kaldırılması riskini doğurabilir ve bu da sistemin tehlikeye açık hale gelmesine neden olabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer:EnableUserCo ntrol*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için, aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Templates\Windows Components\Windows Installer\Yüklemeler üzerinde kullanıcı denetimine izin ver*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu MSI.admx/adml tarafından sağlanır.

**Not #2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar Yüklemeler üzerinde kullanıcı denetimini etkinleştir olarak adlandırılmıştır, ancak Windows 8.0 ve Server 2012 (R2 olmayan Yönetim Şablonları) ile başlayarak yeniden adlandırılmıştır.

**18.9.90.3 (L2) 'Windows Installer komut dosyaları için Internet Explorer güvenlik istemini engelle' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, Windows Installer'ın sisteme herhangi bir program yüklediğinde sistem izinlerini kullanıp kullanmayacağını denetler.

**Not:** Bu ayar hem Bilgisayar Yapılandırması hem de Kullanıcı Yapılandırması klasörlerinde görünür. Bu ayarı etkin kılmak için, her iki klasörde de ayarı etkinleştirmelisiniz.

**Dikkat:** Etkinleştirilirse, yetenekli kullanıcılar, ayrıcalıklarını değiştirmek ve kısıtlı dosya ve klasörlere kalıcı erişim elde etmek için bu ayarın verdiği izinlerden yararlanabilir. Bu ayarın Kullanıcı Yapılandırma sürümünün güvenli olduğunun garanti edilmediğini unutmayın.

Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Sınırlı ayrıcalıklara sahip kullanıcılar, yerel yerleşik Yöneticiler grubuna ait yeni bir yerel hesap oluşturan, mevcut hesaplarını yerel yerleşik Yöneticiler grubuna ekleyen, kötü amaçlı yazılımlar yükleyen bir Windows Installer yükleme paketi oluşturarak bu özellikten yararlanabilir. veya diğer yetkisiz faaliyetlerde bulunur.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer:AlwaysInstal lElevated*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Windows Installer\Her zaman yükseltilmiş ayrıcalıklarla yükleyin*

**Not**: Bu Grup İlkesi yolu Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan ilke şablonu MSI.admx/adml Grup tarafından sağlanır.

**18.9.91 Windows Oturum Açma Seçenekleri**

**18.9.91.1 (L1) 'Yeniden başlatmadan sonra oturum aç ve son etkileşimli kullanıcıyı otomatik olarak kilitle' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Web tabanlı programların, kullanıcıyı bilgilendirmeden bilgisayara yazılım yüklemesine izin verilip verilmeyeceğini denetler. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Sistem uyarısının bastırılması bir güvenlik riski oluşturabilir ve sistemdeki saldırı yüzeyini artırabilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Installer:SafeForScripting*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Windows Installer\Windows Installer komut dosyaları için Internet Explorer güvenlik istemini önleyin*

**Not:** Bu Grup İlkesi yolu Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu MSI.admx/adml tarafından sağlanır.

**Not #2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Windows Installer komut dosyaları için IE güvenlik istemini devre dışı bırak olarak adlandırılmıştı, ancak Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonlarından başlayarak yeniden adlandırıldı.

**18.9.92 Windows Mail**

**18.9.93 Windows Media Center**

**18.9.94 Windows Media Dijital Hak Yönetimi**

**18.9.95 Windows Media Player**

**18.9.96 Windows Toplantı Alanı**

**18.9.97 Windows Messenger**

**18.9.98 Windows Mobility Center**

**18.9.99 Windows Movie Maker**

**18.9.100 Windows PowerShell**

**18.9.100.1 (L1) 'PowerShell Betik Blok Günlüğünü Aç' seçeneği 'Etkin' (Otomatik) olarak ayarlanlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows Update sistemi yeniden başlattıktan sonra bir aygıtın son etkileşimli kullanıcıda otomatik olarak oturum açıp açmayacağını denetler. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Bu özelliğin devre dışı bırakılması, kullanıcının kimlik bilgilerinin önbelleğe alınmasını ve cihazın yetkisiz kullanımını engeller ve ayrıca kullanıcının yeniden başlatmanın farkında olmasını sağlar.

**Etki:**

Cihaz, Windows Update yeniden başlatıldıktan sonra otomatik oturum açma için kullanıcının kimlik bilgilerini saklamaz. Sistem yeniden başlatıldıktan sonra kullanıcıların kilit ekranı uygulamaları yeniden başlatılmaz. Yeniden başlattıktan sonra devam etmek için kullanıcının oturum açma kimlik bilgilerini sunması gerekir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System: DisableAutomaticRestartSignOn*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Windows Oturum Açma Seçenekleri\Oturum açın ve yeniden başlatmanın ardından son etkileşimli kullanıcıyı otomatik olarak kilitleyin*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.1 ve Server 2012 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan WinLogon.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**Not #2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta sistem tarafından başlatılan bir yeniden başlatmanın ardından otomatik olarak son etkileşimli kullanıcı oturum aç olarak adlandırıldı, ancak Windows 10 Sürüm 1903 Yönetim Şablonlarından başlayarak yeniden adlandırıldı.

**18.9.100.2 (L1) 'PowerShell Transkripsiyonunu Aç' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Applications and Services Logs\Microsoft\Windows\PowerShell\Operational Event Log kanalına tüm PowerShell komut dosyası girdilerinin günlüğe kaydedilmesini sağlar. Bu ayar için önerilen durum: Etkin.

**Not:** Komut Dosyası Blok Çağırma Başlat/Durdur Olaylarının günlüğe kaydedilmesi etkinse (seçenek kutusu işaretli), bir komut, komut dosyası bloğu, işlev veya komut dosyası başlatıldığında veya durduğunda PowerShell ek olayları günlüğe kaydeder. Bu seçeneğin etkinleştirilmesi, yüksek hacimli olay günlüğü oluşturur. CIS, çok sayıda olay ürettiği için bu seçenek için bir öneride bulunmamayı bilinçli olarak seçmiştir. Bir kuruluş isteğe bağlı ayarı etkinleştirmeyi seçerse (işaretli), bu aynı zamanda kıyaslamayla da uyumludur. Gerekçe: PowerShell komut dosyası girişi günlükleri, ne olduğunu belirlemek için PowerShell saldırı olaylarının adli incelemelerini gerçekleştirirken çok değerli olabilir.

**Etki:**

PowerShell komut dosyası girişi, kimlik bilgileri ve hassas bilgiler içerebilen Applications and Services Logs\Microsoft\Windows\PowerShell\Operational Event Logs kanalına kaydedilecektir. Uyarı: PowerShell günlüklerinde, bu günlüklere okuma erişimi olan kullanıcılara maruz kalabilecek kimlik bilgilerini ve hassas bilgileri yakalama riskleri vardır. Microsoft, olay günlüğü verilerini daha iyi korumak için "Korumalı Olay Günlüğü" adlı bir özellik sağlar. Olay günlüğünü korumayla ilgili yardım için şu adresi ziyaret edin: [Windows'u Günlüğe Kaydetme Hakkında - PowerShell | Microsoft Belgeleri.](https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_logging_windows?view=powershell-7.2#protected-event-logging)

Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\PowerShell\ScriptBlock Logging:EnableScriptBlockLogging*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Windows Bileşenleri\Windows PowerShell\PowerShell Komut Dosyası Blok Günlüğünü Açın*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 RTM (Sürüm 1507) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu PowerShellExecutionPolicy.admx/adml tarafından sağlanır.

**18.9.101 Windows Güvenilirlik Analizi**

**18.9.102 Windows Uzaktan Yönetim (WinRM)**

**18.9.102.1 WinRM İstemcisi**

**18.9.102.1.1 (L1) 'Temel kimlik doğrulamasına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows Uzaktan Yönetim (WinRM) istemcisinin Temel kimlik doğrulamasını kullanıp kullanmadığını yönetmenize olanak tanır. Bu ayar için önerilen durum: Devre Dışı.

**Not:** Microsoft'un Exchange Online hizmetini (Office 365) kullanan istemciler, bu ayarın Etkin olarak ayarlanması için bu öneride bir istisna gerektirecektir. Exchange Online, HTTPS üzerinden Temel kimlik doğrulamasını kullanır ve bu nedenle Exchange Online kimlik doğrulama trafiği güvenli bir şekilde şifrelenmeye devam eder.

**Gerekçe:**

Temel kimlik doğrulama, WinRM'de bulunan diğer kimlik doğrulama yöntemlerinden daha az sağlamdır çünkü parolalar da dahil olmak üzere kimlik bilgileri düz metin olarak iletilir. WinRM'nin çalıştığı ağdaki paketleri yakalayabilen bir saldırgan, WinRM aracılığıyla uzak ana bilgisayarlara erişmek için kullanılan kimlik bilgilerini belirleyebilir

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Client:AllowBasic*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Windows Bileşenleri\Windows Uzaktan Yönetim (WinRM)\WinRM İstemcisi\Temel kimlik doğrulamasına izin ver*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan WindowsRemoteManagement.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.9.102.1.2 (L1) 'Şifrelenmemiş trafiğe izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows Uzaktan Yönetim (WinRM) istemcisinin ağ üzerinden şifrelenmemiş iletiler gönderip almayacağını yönetmenize olanak tanır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

WinRM ağ trafiğini şifrelemek, bir saldırganın ağdan geçerken WinRM mesajlarını görüntüleme veya değiştirme riskini azaltır.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Client:AllowUnen cryptedTraffic*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Windows Bileşenleri\Windows Uzaktan Yönetim (WinRM)\WinRM İstemcisi\Şifrelenmemiş trafiğe izin ver*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan WindowsRemoteManagement.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.9.102.1.3 (L1) 'Özet kimlik doğrulamasına izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows Uzaktan Yönetim (WinRM) istemcisinin Özet kimlik doğrulamasını kullanıp kullanmayacağını yönetmenize olanak tanır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Özet kimlik doğrulama, WinRM'de bulunan diğer kimlik doğrulama yöntemlerinden daha az sağlamdır; WinRM'nin çalıştığı ağdaki paketleri yakalayabilen bir saldırgan, WinRM aracılığıyla uzak ana bilgisayarlara erişmek için kullanılan kimlik bilgilerini belirleyebilir.

**Etki:**

WinRM istemcisi Özet kimlik doğrulamasını kullanmayacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Client:AllowDigest*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Windows Bileşenleri\Windows Uzaktan Yönetim (WinRM)\WinRM İstemcisi\Özet kimlik doğrulamasına izin verme*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan WindowsRemoteManagement.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.9.102.2 WinRM Hizmeti**

**18.9.102.2.1 (L1) 'Temel kimlik doğrulamasına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlandığından emin olun**

**Açıklama:**

Bu ilke ayarı, Windows Uzaktan Yönetim (WinRM) hizmetinin bir uzak istemciden Temel kimlik doğrulamasını kabul edip etmediğini yönetmenize olanak tanır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Temel kimlik doğrulama, WinRM'de bulunan diğer kimlik doğrulama yöntemlerinden daha az sağlamdır çünkü parolalar da dahil olmak üzere kimlik bilgileri düz metin olarak iletilir. WinRM'nin çalıştığı ağdaki paketleri yakalayabilen bir saldırgan, WinRM aracılığıyla uzak ana bilgisayarlara erişmek için kullanılan kimlik bilgilerini belirleyebilir.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:AllowBas ic*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Windows Uzaktan Yönetimi (WinRM)\WinRM Hizmeti\Temel kimlik doğrulamasına izin ver*

**Not:** Bu Grup İlkesi yolu Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu WindowsRemoteManagement.admx/adml tarafından sağlanır

**18.9.102.2.2 (L2) 'WinRM aracılığıyla uzaktan sunucu yönetimine izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows Uzaktan Yönetim (WinRM) hizmetinin varsayılan HTTP bağlantı noktası üzerinden HTTP aktarımındaki istekleri ağda otomatik olarak dinleyip dinlemediğini yönetmenize olanak tanır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Herhangi bir özellik potansiyel bir saldırı yoludur, gelen ağ bağlantılarını etkinleştirenler özellikle risklidir. Yalnızca güvenilir ağlarda Windows Uzaktan Yönetim (WinRM) hizmetinin kullanımını etkinleştirin ve mümkün olduğunda IPsec gibi ek denetimler kullanın.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi nesnesi aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:AllowAutoConfig*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\Yönetim Şablonları\Windows Bileşenleri\Windows Uzaktan Yönetim (WinRM)\WinRM Hizmeti\WinRM aracılığıyla uzak sunucu yönetimine izin ver*

**Not:** Bu Grup İlkesi yol, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu WindowsRemoteManagement.admx/adml tarafından sağlanır.

**Not #2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Dinleyicilerin otomatik yapılandırılmasına izin ver olarak adlandırılmıştı, ancak Windows 8.0 ve Server 2012 (R2 olmayan Yönetim Şablonları) ile başlayarak yeniden adlandırıldı.

**18.9.102.2.3 (L1) 'Şifrelenmemiş trafiğe izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows Uzaktan Yönetim (WinRM) hizmetinin ağ üzerinden şifrelenmemiş iletiler gönderip almayacağını yönetmenize olanak tanır. Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

WinRM ağ trafiğini şifrelemek, bir saldırganın ağdan geçerken WinRM mesajlarını görüntüleme veya değiştirme riskini azaltır.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:AllowUnencryptedTraffic*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Windows Bileşenleri\Windows Uzaktan Yönetim (WinRM)\WinRM Hizmeti\Şifrelenmemiş trafiğe izin ver*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan WindowsRemoteManagement.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.9.102.2.4 (L1) 'WinRM'nin RunAs kimlik bilgilerini depolamasına izin verme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows Uzaktan Yönetim (WinRM) hizmetinin herhangi bir eklenti için RunAs kimlik bilgilerinin depolanmasına izin verip vermeyeceğini yönetmenize olanak tanır. Bu ayar için önerilen durum: Etkin.

**Not:** Bu ilke ayarını etkinleştirir ve ardından devre dışı bırakırsanız, RunAsPassword için önceden yapılandırılmış tüm değerlerin sıfırlanması gerekir.

**Gerekçe:**

RunAs kimlik bilgilerini saklama yeteneği kullanışlı bir özellik olsa da, hesaptan ödün verme riskini biraz artırır. Örneğin, masaüstünüzü birkaç dakika gözetimsiz bırakmadan önce kilitlemeyi unutursanız, başka bir kişi yalnızca bilgisayarınızın masaüstüne değil, aynı zamanda önbelleğe alınmış RunAs kimlik bilgileriyle WinRM aracılığıyla yönettiğiniz tüm ana bilgisayarlara da erişebilir.

**Etki:**

WinRM hizmeti, herhangi bir eklenti için RunAsUser veya RunAsPassword yapılandırma değerlerinin ayarlanmasına izin vermez. Bir eklenti RunAsUser ve RunAsPassword yapılandırma değerlerini zaten ayarladıysa, RunAsPassword yapılandırma değeri bilgisayardaki kimlik bilgisi deposundan silinecektir. Bu ayar daha sonra tekrar Devre Dışı bırakılırsa, RunAsPassword için önceden yapılandırılmış tüm değerlerin sıfırlanması gerekir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service:DisableR unAs*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Windows Uzaktan Yönetimi (WinRM)\WinRM Hizmeti\WinRM'nin RunAs kimlik bilgilerini depolamasına izin verme*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu WindowsRemoteManagement.admx/adml tarafından sağlanır.

**18.9.103 Windows Uzak Kabuk**

**18.9.103.1 (L2) 'Uzaktan Kabuk Erişimine İzin Ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, komut dosyalarını ve komutları yürütmek için desteklenen tüm kabuklara uzaktan erişim yapılandırmasını yönetmenize olanak tanır. Bu ayar için önerilen durum: Devre Dışı.

**Not:** Bu ayar için GPME yardım metni yanlış yazılmıştır; bu, Etkin olarak yapılandırılmasının yeni Uzak Kabuk bağlantılarını reddedeceğini ve Devre Dışı olarak ayarlanması Uzak Kabuk bağlantılarına izin vereceğini gösterir. Bunun tersi doğrudur (ve ayarın başlığı ile tutarlıdır). Bu, Yönetim Şablonunda Microsoft tarafından yapılan bir ifade hatasıdır.

**Gerekçe:**

Herhangi bir özellik potansiyel bir saldırı yoludur, gelen ağ bağlantılarını etkinleştirenler özellikle risklidir. Windows Uzak Kabuğunun yalnızca güvenilir ağlarda kullanımını etkinleştirin ve mümkün olduğunda IPsec gibi ek denetimler kullanın.

**Etki:**

Yeni Uzak Kabuk bağlantılarına izin verilmez ve iş istasyonu tarafından reddedilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi nesnesi aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WinRM\Service\WinRS:Al lowRemoteShellAccess*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması \Yönetim Şablonları\Windows Bileşenleri\Windows Uzak Kabuk\Uzaktan Kabuk Erişimine İzin Ver*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan WindowsRemoteShell.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.9.104 Windows Sandbox**

**18.9.104.1 (L1) 'Windows Sandbox ile pano paylaşımına izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows sanal alanıyla pano paylaşımını etkinleştirir veya devre dışı bırakır. Bu ayar için önerilen durum: Devre Dışı. Not: Windows Sandbox özelliği ilk olarak Windows 10 R1903'te tanıtıldı ve ana bilgisayarda değişiklik yapmadan uygulamaları test etme gibi görünen bir amaç için Windows'un geçici bir "temiz yükleme" sanal örneğinin ana bilgisayar içinde çalıştırılmasına izin verir.

**Gerekçe:**

Kopyala ve yapıştırın devre dışı bırakılması, Windows Sandbox'ın maruz kaldığı saldırı yüzeyini ve güvenilmeyen uygulamaların dahili ağa olası maruz kalmasını azaltır. Etki: Windows Sandbox'a/dan kopyala ve yapıştır işlevi devre dışı bırakılacak. Bu nedenle, dosyalar pano aracılığıyla Windows Sandbox'a/Bu alandan taşınamaz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Sandbox:AllowClipboard Redirection*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Windows Korumalı Alanı\Windows Korumalı Alan ile pano paylaşımına izin ver*

**Not:** Bu Grup İlkesi yolu, varsayılan. Microsoft Windows 10 Sürüm 21H2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu WindowsSandbox.admx/adml tarafından sağlanır.

**18.9.104.2 (L1) 'Windows Sandbox'ta ağa izin ver' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows Sandbox'ta ağı etkinleştirir veya devre dışı bırakır. Ağ iletişimi, ana bilgisayarda sanal bir anahtar oluşturularak ve Windows Sandbox'ı bir sanal Ağ Arabirim Kartı (NIC) aracılığıyla ona bağlayarak elde edilir. Bu ayar için önerilen durum: Devre Dışı.

**Not:** Windows Sandbox özelliği ilk olarak Windows 10 R1903'te tanıtıldı ve ana bilgisayarda değişiklik yapmadan uygulamaları test etme gibi görünen bir amaç için Windows'un geçici bir "temiz yükleme" sanal örneğinin ana bilgisayar içinde çalıştırılmasına izin verir.

**Gerekçe:**

Ağ erişimini devre dışı bırakmak, Windows Sandbox'ın maruz kaldığı saldırı yüzeyini ve güvenilmeyen uygulamaların dahili ağa maruz kalmasını azaltır. Not: Microsoft'a göre, Windows Sandbox'ta ağ oluşturmayı etkinleştirmek, güvenilmeyen uygulamaları dahili ağa maruz bırakabilir.

**Etki:**

Windows Sandbox'a/Windows Sandbox'tan ağ erişimi devre dışı bırakılacak. Bu nedenle, dosyalar ağ üzerinden Windows Sandbox'a/Bu Alandan taşınamaz. Denetim: Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\Sandbox:AllowNetworkin g*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Windows Korumalı Alanı\Windows Korumalı Alanında ağ oluşturmaya izin ver*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir . Microsoft Windows 10 Sürüm 21H2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu WindowsSandbox.admx/adml tarafından sağlanır.

**18.9.105 Windows Güvenliği (eski adıyla Windows Defender Güvenlik Merkezi)**

**18.9.105.1 Hesap koruması**

**18.9.105.2 Uygulama ve tarayıcı koruması**

**18.9.105.2.1 (L1) 'Kullanıcıların ayarları değiştirmesini engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların Windows Güvenlik ayarlarındaki Exploit koruma ayarları alanında değişiklik yapmasını engeller. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Kuruluşa özel yapılandırmanın değiştirilmemesini sağlamak için yalnızca yetkili BT personeli, açıklardan yararlanma koruması ayarlarında değişiklik yapabilmelidir.

**Etki:**

Yerel kullanıcılar, Açıklardan Yararlanma koruması ayarları alanında değişiklik yapamaz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows Defender Security Center\App and Browser protection:DisallowExploitProtectionOverride*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Windows Güvenliği\Uygulama ve tarayıcı koruması\Kullanıcıların ayarları değiştirmesini engelle*

**Not**: Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1709 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu WindowsDefenderSecurityCenter.admx/adml tarafından sağlanır.

**18.9.106 Windows SideShow**

**18.9.107 Windows Sistem Kaynağı Yöneticisi**

**18.9.108 Windows Güncelleme**

**18.9.108.1 Eski Politikalar**

**18.9.108.1.1 (L1) 'Zamanlanmış otomatik güncelleştirme yüklemeleri için oturum açmış kullanıcılarla otomatik yeniden başlatma yok' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Otomatik Güncelleştirmelerin, zamanlanmış bir yüklemeyi tamamlamak için oturum açan kullanıcılar tarafından bilgisayarların yeniden başlatılmasını bekleyeceğini belirtir. Bu ayar için önerilen durum: Devre Dışı.

**Not**: Bu ayar, yalnızca Otomatik Güncelleştirmeleri zamanlanmış güncelleme yüklemelerini gerçekleştirecek şekilde yapılandırdığınızda geçerlidir. Otomatik Güncelleştirmeleri Yapılandır ayarını Devre Dışı olarak yapılandırırsanız, bu ayarın hiçbir etkisi olmaz.

**Gerekçe:**

Bazı güvenlik güncelleştirmeleri, yüklemeyi tamamlamak için bilgisayarın yeniden başlatılmasını gerektirir. Bilgisayar otomatik olarak yeniden başlatılamıyorsa, en son güncelleme tamamen yüklenmeyecek ve yeniden başlatılana kadar bilgisayara yeni güncellemeler indirilmeyecektir. Otomatik yeniden başlatma işlevi olmadan, güvenlik bilincine sahip olmayan kullanıcılar yeniden başlatmayı süresiz olarak geciktirmeyi seçebilir, bu nedenle bilgisayarı daha az güvenli bir durumda tutar.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim**:

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU:NoAutoRebootWithLoggedOnUsers*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Windows Bileşenleri\Windows Update\Eski İlkeler\Zamanlanmış otomatik güncelleme yüklemeleri için oturum açmış kullanıcılarla otomatik yeniden başlatma yok*

**Not:** Bu Grup İlkesi yolu, tüm sürümlerde bulunan Grup İlkesi şablonu WindowsUpdate.admx/adml tarafından sağlanır Microsoft Windows Yönetim Şablonları.

**Not 2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Zamanlanmış Otomatik Güncelleştirmeler yüklemeleri için otomatik yeniden başlatma yok olarak adlandırılmıştı, ancak Windows 7 ve Server 2008 R2 Yönetim Şablonlarından başlayarak yeniden adlandırıldı.

**18.9.108.2 Son kullanıcı deneyimini yönetme**

**18.9.108.2.1 (L1) 'Otomatik Güncelleştirmeleri Yapılandır' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, ortamınızdaki bilgisayarların Windows Update'ten mi yoksa WSUS'tan mı güvenlik güncelleştirmeleri alacağını belirtir. Bu ilke ayarını Etkin olarak yapılandırırsanız, işletim sistemi bir ağ bağlantısının mevcut olduğunu algılar ve ardından kendileri için geçerli olan güncellemeler için Windows Update'i veya belirlenmiş intranet sitenizi aramak için ağ bağlantısını kullanır. Bu ilke ayarını Etkin olarak yapılandırdıktan sonra, hizmetin nasıl çalışacağını belirtmek için Otomatik Güncelleştirme Özelliklerini Yapılandır iletişim kutusunda aşağıdaki üç seçenekten birini seçin:

* 2 - İndirme ve otomatik yükleme için bildir (Herhangi bir güncellemeyi indirmeden önce bildir)
* 3 - Otomatik indir ve yükleme için bildir (Güncellemeleri otomatik olarak indir ve yüklenmeye hazır olduklarında bildir.) (Varsayılan ayar)
* 4 - Otomatik indir ve yüklemeyi planla (Güncellemeleri otomatik olarak indir ve aşağıda belirtilen programa göre kur.) )
* 5 - Yerel yöneticinin ayarı seçmesine izin verin (Yukarıdaki seçeneklerle ilgili kararı yerel Yöneticilere bırakın (Önerilmez))

Bu ayar için önerilen durum: Etkin.

**Not:** "Otomatik güncellemeyi yapılandır:" alt ayarının 4 olası değeri vardır - bunların tümü belirli kurumsal ihtiyaçlara bağlı olarak geçerlidir, ancak mümkünse 4 - Otomatik indirme ve kurulumu zamanlama değerini kullanmanızı öneririz. Bu öneri puanlanmış bir gereklilik değildir.

**Not #2**: Yama için bir 3. taraf çözümü kullanan kuruluşlar, kendilerini bu öneriden muaf tutmayı seçebilir ve bunun yerine yerel Windows Update mekanizmasının 3. taraf yama işlemine müdahale etmemesi için bunu Devre Dışı olarak yapılandırabilir.

**Gerekçe:**

Her ne kadar Windows'un her sürümü yayınlanmadan önce kapsamlı bir şekilde test edilse de, ürünler gönderildikten sonra sorunların keşfedilmesi olasıdır. Otomatik Güncelleştirmeleri Yapılandır ayarı, ortamınızdaki bilgisayarların her zaman en son kritik işletim sistemi güncellemelerine ve hizmet paketlerine sahip olmasını sağlamanıza yardımcı olabilir.

**Etki:**

Gerektiğinde kritik işletim sistemi güncellemeleri ve hizmet paketleri yüklenecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU:NoAutoUpdate*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler \Yönetim Şablonları\Windows Bileşenleri\Windows Update\Son kullanıcı deneyimini yönet\Otomatik Güncelleştirmeleri Yapılandır*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan WindowsUpdate.admx/adml Grup İlkesi şablonu tarafından sağlanır.

**18.9.108.2.2 (L1) 'Otomatik Güncellemeleri Yapılandır: Zamanlanmış yükleme günü' seçeneği '0 - Her gün' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, ortamınızdaki bilgisayarların Windows Update veya WSUS'tan ne zaman güvenlik güncelleştirmeleri alacağını belirtir. Bu ayar için önerilen durum: 0 - Her gün.

**Not:** Bu ayar yalnızca, 'Otomatik Güncelleştirmeleri Yapılandır' önerisinde 4 - Otomatik indirme ve yüklemeyi planla seçiliyse geçerlidir. Başka bir seçenek seçilirse hiçbir etkisi olmayacaktır.

**Gerekçe:**

Her Windows sürümü yayınlanmadan önce kapsamlı bir şekilde test edilse de, ürünler gönderildikten sonra sorunların keşfedilmesi olasıdır. Otomatik Güncelleştirmeleri Yapılandır ayarı, ortamınızdaki bilgisayarların her zaman en son kritik işletim sistemi güncellemelerine ve hizmet paketlerine sahip olmasını sağlamanıza yardımcı olabilir.

**Etki:**

**'**Otomatik Güncelleştirmeleri Yapılandır' önerisinde 4 - Otomatik indirme ve yükleme zamanlaması seçilirse, kritik işletim sistemi güncellemeleri ve hizmet paketleri her gün otomatik olarak indirilir (varsayılan olarak saat 03:00'te).

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate\AU:ScheduledInstallDay*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu 0 - Her gün olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Windows Update\Son kullanıcı deneyimini yönet\Otomatik Güncelleştirmeleri Yapılandır: Zamanlanmış yükleme günü*

**Not :** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu WindowsUpdate.admx/adml tarafından sağlanır.

**18.9.108.2.3 (L1) 'Güncellemeleri duraklat özelliğine erişimi kaldır' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu politika, "Güncellemeleri duraklat" özelliğine erişimi kaldırır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Güvenlik ve sistem güncellemelerinin uygulandığından emin olmak için sistem yöneticileri, sistemlere güncellemelerin ne zaman uygulanacağını kontrol etmelidir.

**Etki:**

Kullanıcılar, güncellemelerin bir sisteme yüklenmesini önlemek için Windows Update'te "Güncellemeleri duraklat" seçeneğini belirleyemez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:SetDisab lePauseUXAccess*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonlar\Windows Bileşenleri\Windows Update\Son kullanıcı deneyimini yönet\"Güncellemeleri duraklat" özelliğine erişimi kaldırın*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1809 ve Sunucu 2019 Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu WindowsUpdate.admx/adml tarafından sağlanır.

**18.9.108.3 Windows Server Update Service'ten sunulan güncellemeleri yönetme**

**18.9.108.4 Windows Update'ten (eski adıyla Windows Güncelleştirmelerini ve İş için Windows Update'i Ertele) sunulan güncelleştirmeleri yönetme**

**18.9.108.4.1 (L1) 'Önizleme yapılarını yönet' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, güncelleme yayınlanmadan önce hangi güncellemelerin alınacağını yönetir. Dev Channel: Son derece teknik kullanıcılar için idealdir. Dev Channel'daki kullanıcılar, bir geliştirme döngüsünde en erken olan aktif geliştirme şubemizden derlemeler alacaktır. Bu derlemeler belirli bir Windows 10 sürümüyle eşleşmiyor. Beta Kanalı: Yaklaşan Windows 10 özelliklerini görmek isteyen özellik kaşifleri için idealdir. Geri bildiriminiz, mühendislerimizin önemli sorunların büyük bir sürümden önce düzeltilmesine yardımcı olacağı için burada özellikle önemli olacaktır. Sürüm Önizleme Kanalı (varsayılan): Sürüm Önizleme Kanalındaki İçerdekiler, dünyaya yayınlanmadan önce Windows 10'un gelecek sürümüne erişebilecek. Bu yapılar Microsoft tarafından desteklenmektedir. Sürüm Önizleme Kanalı, şirketlere kuruluşlarında geniş dağıtımdan önce gelecek Windows 10 sürümlerini önizlemelerini ve doğrulamalarını önerdiğimiz yerdir. Bu ayar için önerilen durum: Devre Dışı.

**Not:** Önizleme Yapısı kaydı, 2 veya daha yüksek bir telemetri düzeyi ayarı ve alan adınızın insider.windows.com'da kayıtlı olmasını gerektirir. Önizleme Derlemeleri hakkında ek bilgi için bkz.: <https://aka.ms/wipforbiz>

**Gerekçe:**

Kurumsal yönetilen bir ortamda deneysel özelliklere izin verilmesi riskli olabilir, çünkü bu, sistemlerde hatalar ve güvenlik açıkları oluşturabilir, bu da işleri kolaylaştırır. erişim sağlamak için bir saldırgan. Genellikle yalnızca üretime hazır yapıların kullanılması tercih edilir.

**Etki:**

Önizleme derlemelerinin cihaza yüklenmesi engellenir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:ManagePreviewBuildsPolicyValue*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonlar\Windows Bileşenleri\Windows Update\Windows Update\Önizleme yapılarını yönet tarafından sunulan güncellemeleri yönet*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1709 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu WindowsUpdate.admx/adml tarafından sağlanır.

**18.9.108.4.2 (L1) 'Önizleme Derlemeleri ve Özellik Güncelleştirmelerinin ne zaman alınacağını seç' seçeneği 'Etkin: 180 gün veya daha fazla' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Önizleme Oluşturma veya Özellik Güncellemelerinin ne zaman alınacağını belirler.

Güncellemeleri Ertele Bu, cihazların, tüm yayın öncesi kanallar için 14 güne kadar ve Altı Aylık Kanal için 365 güne kadar kanalınızda kullanılabilen bir sonraki Özellik Güncellemesini almayı ertelemesini sağlar. Veya cihaz Altı Aylık Kanaldan güncelleniyorsa, politika güncellenene veya cihaz hizmet sonuna ulaşana kadar cihazın taşınacağı ve/veya açık kalacağı bir sürüm belirlenebilir.

**Not:** Her iki politikayı da ayarlarsanız, belirtilen sürüm öncelikli olur ve ertelemeler geçerli olmaz. İşletim sistemi sürümü bilgileri için lütfen Windows Sürüm Bilgileri sayfasına bakın.

Güncellemeleri Duraklat Özellik Güncellemelerinin planlanan zamanda alınmasını önlemek için Özellik Güncellemelerini geçici olarak duraklatabilirsiniz. Duraklatma, belirtilen başlangıç tarihinden itibaren veya alan temizlenene kadar 35 gün boyunca yürürlükte kalacaktır (Kalite Güncellemeleri sunulmaya devam edecektir).

**Not:** "Teşhis Verilerine İzin Ver" (eski adıyla "Telemetriye İzin Ver") politikası 0 olarak ayarlanırsa, bu politikanın hiçbir etkisi olmaz.

**Not #2:** Microsoft, Windows 10 R1607 ile başlayarak, bulut tabanlı güncelleme yönetimini göz önünde bulunduran Çift Tarama adlı yeni bir Windows Update (WU) istemci davranışını tanıttı. Bazı durumlarda, bu İkili Tarama özelliği, Windows Server Update Services (WSUS) ve/veya manuel WU güncellemelerinden gelen Windows Güncellemelerini etkileyebilir. Ortamınızda WSUS kullanıyorsanız, yukarıdaki ayarı Yapılandırılmadı olarak ayarlamanız veya Güncelleme erteleme ilkelerinin Windows Update'e (Windows 10 Sürüm 1709 Yönetim Şablonlarına eklenmiştir) karşı taramaya neden olmasına izin verme ayarını yapılandırmanız gerekebilir. İkili Tarama özelliğinin araya girmesini önleyin. İkili Tarama hakkında daha fazla bilgiyi şu bağlantılarda bulabilirsiniz:

[“İkili Tarama”nın gizemini giderme – WSUS Ürün Ekibi Blogu](https://blogs.technet.microsoft.com/wsus/2017/05/05/demystifying-dual-scan/)

[1607'de İkili Taramayı İyileştirme – WSUS Ürün Ekibi Blogu](https://blogs.technet.microsoft.com/wsus/2017/08/04/improving-dual-scan-on-1607/)

**Not 3:** Windows 10 R1703'ten önce, 180 günün üzerindeki değerler tanınmaz OS tarafından. Windows 10 R1703 ile başlayarak, erteleyebileceğiniz maksimum gün sayısı 365 gündür.

**Gerekçe:**

Bir üretim ortamında, beta sürümünde zorlu testlerden geçtikten sonra yalnızca herkese açık olan yazılım ve özelliklerin kullanılması tercih edilir.

**Etki:**

Özellik Güncelleştirmeleri, Microsoft tarafından genel kullanıma sunulana kadar ertelenecektir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:DeferFea tureUpdates HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:DeferFea tureUpdatesPeriodInDays*

**Düzeltme:**

Önerilen aşağıdaki UI yolunu Etkin olarak ayarlayın: 180 veya daha fazla gün:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Windows Update\Windows Update\Windows Update for Business\'tan sunulan güncellemeleri yönetin Önizleme Yapıları ve Özellik Güncellemeleri alındığında seçin*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1607 ve Server 2016 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu WindowsUpdate.admx/adml tarafından sağlanır.

**Not 2:** Daha eski Microsoft Windows Yönetim Şablonlarında, bu ayar başlangıçta Özellik Güncelleştirmeleri alındığında Seç olarak adlandırılmıştı, ancak Windows 10 Sürüm 1709 Yönetim Şablonlarından başlayarak Önizleme Derlemeleri ve Özellik Güncelleştirmeleri alındığında Seç olarak yeniden adlandırıldı**.**

**18.9.108.4.3 (L1) 'Kalite Güncellemelerinin ne zaman alınacağını seç' seçeneği 'Etkin: 0 gün' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayarlar, Kalite Güncellemelerinin ne zaman alınacağını kontrol eder. Bu ayar için önerilen durum: Etkin: 0 gün.

**Not:** "Teşhis Verilerine İzin Ver" (eski adıyla "Telemetriye İzin Ver") politikası 0 olarak ayarlanırsa, bu politikanın hiçbir etkisi olmaz.

**Not #2:** Microsoft, Windows 10 R1607 ile başlayarak, bulut tabanlı güncelleme yönetimine dikkat ederek, Çift Tarama adlı yeni bir Windows Update (WU) istemci davranışını tanıttı. Bazı durumlarda, bu İkili Tarama özelliği, Windows Server Update Services (WSUS) ve/veya manuel WU güncellemelerinden gelen Windows Güncellemelerini etkileyebilir. Ortamınızda WSUS kullanıyorsanız, yukarıdaki ayarı Yapılandırılmadı olarak ayarlamanız veya Güncelleme erteleme ilkelerinin Windows Update'e (Windows 10 Sürüm 1709 Yönetim Şablonlarına eklenmiştir) karşı taramaya neden olmasına izin verme ayarını yapılandırmanız gerekebilir. İkili Tarama özelliğinin araya girmesini önleyin. İkili Tarama hakkında daha fazla bilgi şu bağlantılarda mevcuttur:

[“İkili Tarama”nın Gizemini Çözme – WSUS Ürün Ekibi Blogu](https://blogs.technet.microsoft.com/wsus/2017/05/05/demystifying-dual-scan/)

[1607'de İkili Taramayı İyileştirme – WSUS Ürün Ekibi Blogu](https://blogs.technet.microsoft.com/wsus/2017/08/04/improving-dual-scan-on-1607/)

**Gerekçe:**

Kalite Güncellemeleri önemli hata düzeltmeleri ve/veya güvenlik yamaları içerebilir ve en kısa sürede kurulmalıdır.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:DeferQua lityUpdates HKEY\_LOCAL\_MACHINE\SOFTWARE\Policies\Microsoft\Windows\WindowsUpdate:DeferQua lity configurationD aracılığıylaUpdatesPeriodInDays*

**Düzeltme :**

GP aşağıdaki UI yolunu Etkin olarak ayarlayın:0 gün:

*Bilgisayar Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Windows Update\İş için Windows Update\Kalite Güncelleştirmelerinin ne zaman alınacağını seçin*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut değildir. Güncellenmiş bir Grup İlkesi şablonu (WindowsUpdate.admx/adml) gereklidir - Microsoft Windows 10 Sürüm 1607 ve Server 2016 Yönetim Şablonlarına (veya daha yenisine) dahildir

**19 Yönetim Şablonları (Kullanıcı)**

**19.1 Denetim** **Masası**

**19.1.1 Program Ekle veya Kaldır**

**19.1.2 Ekran**

**19.1.3 Kişiselleştirme (eski adıyla Masaüstü Temaları)**

**19.1.3.1 (L1) 'Ekran koruyucuyu etkinleştir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, masaüstü ekran koruyucularının kullanımını etkinleştirir/devre dışı bırakır. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bir kullanıcı uzaklaşırken bilgisayarını kilitlemeyi unutursa, yoldan geçen birinin onu ele geçirmesi olasıdır. Şifreli kilitli zaman ayarlı bir ekran koruyucuyu yapılandırmak, bu korsanlıklara karşı korunmaya yardımcı olacaktır.

**Etki:**

Aşağıdaki iki koşulun geçerli olması koşuluyla bir ekran koruyucu çalışır: İlk olarak, belirli ekran koruyucuyu zorla veya istemci bilgisayardaki Denetim Masası aracılığıyla öneri aracılığıyla istemcide geçerli bir ekran koruyucu belirtilir. İkinci olarak, öneri Ekran koruyucu zaman aşımı ayarı, ayar veya Kontrol Paneli aracılığıyla sıfırdan farklı bir değere ayarlanır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_USERS\[USER SID]\Software\Policies\Microsoft\Windows\Control Panel\Desktop:ScreenSaveActive*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Kullanıcı Yapılandırması\İlkeler\Yönetim Şablonları\Denetim Masası\Kişiselleştirme\Ekran koruyucuyu etkinleştir*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu ControlPanelDisplay.admx/adml tarafından sağlanır.

**19.1.3.2 (L1) 'Ekran koruyucuyu parola ile koru' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, bilgisayarda kullanılan ekran koruyucuların parola korumalı olup olmadığını belirler. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bir kullanıcı uzaklaşırken bilgisayarını kilitlemeyi unutursa, yoldan geçen birinin onu ele geçirmesi olasıdır. Şifreli kilitli zaman ayarlı bir ekran koruyucuyu yapılandırmak, bu korsanlıklara karşı korunmaya yardımcı olacaktır.

**Etki:**

Tüm ekran koruyucular parola korumalıdır. Kişiselleştirme veya Görüntü Denetim Masası'ndaki Ekran Koruyucu iletişim kutusundaki "Parola korumalı" onay kutusu devre dışı bırakılarak kullanıcıların parola koruma ayarını değiştirmesi engellenir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_USERS\[USER SID]\Software\Policies\Microsoft\Windows\Control Panel\Desktop:ScreenSaverIsSecure*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Kullanıcı Yapılandırması\İlkeler\Yönetim Şablonları\Denetim Masası\Kişiselleştirme\Parola ekran koruyucuyu korur*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu ControlPanelDisplay.admx/adml tarafından sağlanır.

**19.1.3.3 (L1) 'Ekran koruyucu zaman aşımı' seçeneği 'Etkin: 900 saniye veya daha az, ancak 0 değil' olarak ayarlanmalıdır. (Otomatik)**

**Açıklama:**

Bu ayar, ekran koruyucu başlatılmadan önce ne kadar kullanıcı boşta kalması gerektiğini belirtir. Bu ayar için önerilen durum: Etkin: 900 saniye veya daha az, ancak 0 değil.

**Not:** Bu ayarın aşağıdaki koşullarda hiçbir etkisi yoktur:

* Bekleme süresi sıfıra ayarlanır.
* "Ekran Koruyucuyu Etkinleştir" ayarı devre dışı bırakılır.
* Geçerli bir ekran koruyucusu manuel olarak veya "Ekran koruyucu yürütülebilir adı" ayarı aracılığıyla seçilmez

**Gerekçe:**

Bir kullanıcı uzaklaşırken bilgisayarını kilitlemeyi unutursa, yoldan geçen birinin onu ele geçirmesi olasıdır. Şifreli kilitli zaman ayarlı bir ekran koruyucuyu yapılandırmak, bu korsanlıklara karşı korunmaya yardımcı olacaktır.

**Etki:**

Bilgisayar belirtilen süre boyunca gözetimsiz bırakıldığında ekran koruyucu otomatik olarak etkinleşir ve kullanıcılar zaman aşımı değerini değiştiremez.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_USERS\[USER SID]\Software\Policies\Microsoft\Windows\Control Panel\Desktop:ScreenSaveTimeOut*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın: 900 veya daha az, ancak 0 değil:

*Kullanıcı Yapılandırması\İlkeler\Yönetim Şablonları\Denetim Masası\Kişiselleştirme\Ekran koruyucu zaman aşımı*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 7 ve Server 2008 R2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu ControlPanelDisplay.admx/adml tarafından sağlanır.

**19.2 Masaüstü**

**19.3 Ağ**

**19.4 Paylaşılan Klasörler**

**19.5 Başlat Menüsü ve Görev Çubuğu**

**19.5.1 Bildirimler**

**19.5.1.1 (L1) 'Kilit ekranında toast bildirimlerini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kilit ekranındaki tost bildirimlerini kapatır. Bu ayar için önerilen durum Etkin'dir.

**Gerekçe:**

Bu özellik kullanıcılar için kullanışlı olsa da, bildirimler sağlayan uygulamalar, cihaz gözetimsiz bırakıldığında hassas kişisel veya iş verilerini görüntüleyebilir.

**Etki:**

Uygulamalar, kilit ekranında tost bildirimleri oluşturamayacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_USERS[USERSID]\Software\Policies\Microsoft\Windows\CurrentVersion\PushNotifications:NoT oastApplicationNotificationOnLockScreen*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Kullanıcı Yapılandırması\İlkeler\Yönetim Şablonları\Başlat Menüsü ve Görev Çubuğu\Bildirimler\Kilit ekranında bildirimleri kapat*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 8.0 ve Server 2012 (R2 olmayan) Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu WPN.admx/adml tarafından sağlanır.

**19.6 Sistem**

**19.6.1 Ctrl+Alt+Del Seçenekleri**

**19.6.2 Ekran**

**19.6.3 Sürücü Kurulumu**

**19.6.4 Klasör Yeniden Yönlendirme**

**19.6.5 Grup İlkesi**

**19.6.6 İnternet İletişim Yönetimi**

**19.6.6.1 İnternet İletişimi ayarları**

**19.6.6.1.1 (L2) 'Yardım Deneyimini Geliştirme Programını Kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların Yardım Deneyimini Geliştirme programına katılıp katılamayacağını belirtir. Yardım Deneyimini Geliştirme programı, Microsoft'un iyileştirebilmesi için müşterilerin Windows Yardım'ı nasıl kullandığı hakkında bilgi toplar. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Büyük kurumsal yönetilen ortamlar, Microsoft tarafından yönetilen istemci bilgisayarlardan toplanan bilgilere sahip olmak istemeyebilir.

**Etki:**

Kullanıcılar, Yardım Deneyimini Geliştirme programına katılamaz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_USERS[USERSID]\Software\Policies\Microsoft\Assistance\Client\1.0:NoImplicitFeedback*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Kullanıcı Yapılandırması\İlkeler\Yönetim Şablonları\Sistem\İnternet İletişim Yönetimi\İnternet İletişim Ayarları\Yardım Deneyimi Geliştirme Programını Kapat*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu HelpAndSupport.admx/adml tarafından sağlanır.

**19.7 Windows** **Bileşenleri**

**19.7.1 Windows 8 / 8.1 / 10'a özellikler ekleme (eski adıyla Windows Anytime Upgrade)**

**19.7.2 Uygulama çalışma zamanı**

**19.7.3 Uygulama Uyumluluğu**

**19.7.4 Ek Yöneticisi**

**19.7.4.1 (L1) 'Dosya eklerindeki bölge bilgilerini koruma' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows'un dosya eklerini menşe bölgeleri (kısıtlı, İnternet, intranet, yerel gibi) hakkında bilgilerle işaretleyip işaretlemediğini yönetmenize olanak tanır. Bu, düzgün çalışması için NTFS gerektirir ve FAT32'de haber verilmeksizin başarısız olur. Windows, bölge bilgilerini korumayarak uygun risk değerlendirmeleri yapamaz. Bu ayar için önerilen durum: Devre Dışı.

**Not:** Ek Yöneticisi özelliği, dosyanın bölge bilgileri dosyanın özelliklerindeki "Engellemeyi kaldır" düğmesi veya aşağıdaki gibi ayrı bir araç aracılığıyla kaldırılmadığı sürece/olmadığı sürece, güvenilir olmayan bir kaynaktan geldiği işaretlenen dosyaları açarken veya yürütürken kullanıcıları uyarır. Microsoft Sysinternals Akışları.

**Gerekçe:** İnternet veya Kısıtlı Siteler bölgesindeki bir bilgisayardan indirilen bir dosya, intranet dosya paylaşımı gibi güvenli görünmesini sağlayan bir konuma taşınabilir ve şüphelenmeyen bir kullanıcı tarafından yürütülebilir. Ek Yöneticisi özelliği, dosyanın bölge bilgisi kaldırılmadıkça/kaldırılmadıkça, güvenilmeyen bir kaynaktan olarak işaretlenen dosyaları açarken veya yürütürken kullanıcıları uyarır.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_USERS[USERSID]\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments:SaveZoneI nformation*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Disabled olarak ayarlayın :

*Kullanıcı Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Ek Yöneticisi\Dosya eklerinde bölge bilgilerini koruma*

**Not**: Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu AttachmentManager.admx/adml tarafından sağlanır.

**19.7.4.2 (L1) 'Ekleri açarken virüsten koruma programlarını bilgilendir' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kayıtlı virüsten koruma programlarını bilgilendirme davranışını yönetir. Birden fazla program kayıtlıysa, hepsine bilgi verilecektir. Bu ayar için önerilen durum: Etkin.

**Not**: Bu ilke ayarının düzgün çalışması için güncelleştirilmiş bir virüsten koruma programı yüklenmelidir.

**Gerekçe:**

Erişim denetimi yapmayan virüsten koruma programları, indirilen dosyaları tarayamayabilir.

**Etki:**

Windows, kayıtlı virüsten koruma programlarına, bir kullanıcı bir dosya ekini açtığında dosyayı taramasını söyler. Virüsten koruma programı başarısız olursa, ekin açılması engellenir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_USERS[USERSID]\Software\Microsoft\Windows\CurrentVersion\Policies\Attachments:ScanWithAntiVirus*

**Düzeltme**:

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Kullanıcı Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Ek Yöneticisi\Ekleri açarken virüsten koruma programlarını bilgilendir*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu AttachmentManager.admx/adml tarafıdan sağlanır.

**19.7.5 Otomatik Oynatma Politikaları**

**19.7.6 Yedekleme**

**19.7.7 Hesap Makinesi**

**19.7.8 Bulut İçeriği**

**19.7.8.1 (L1) 'Windows spot ışığını kilit ekranında yapılandır' seçeneği Devre Dışı' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kilit ekranında Windows Spotlight'ı yapılandırmanıza olanak tanır. Bu ayar için önerilen durum: Devre Dışı.

**Not:** [Microsoft TechNet](https://technet.microsoft.com/en-us/itpro/windows/manage/group-policies-for-enterprise-and-education-editions)'e göre bu ilke ayarı yalnızca Windows 10 Enterprise ve Windows 10 Education sürümleri için geçerlidir.

**Gerekçe:**

Bu ayarın etkinleştirilmesi, verilerinizin herhangi bir üçüncü tarafla paylaşılmamasına yardımcı olacaktır. Windows Spotlight özelliği, verileri toplar ve bu verileri, önerilen uygulamaları ve internetten görüntüleri görüntülemek için kullanır.

**Etki:**

Windows Spotlight kapatılacak ve kullanıcılar artık bunu kilit ekranı olarak seçemeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir:

*HKEY\_USERS[USERSID]\Software\Policies\Microsoft\Windows\CloudContent:ConfigureWindowsSpotlight*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Kullanıcı Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Bulut İçeriği\Kilit ekranında Windows spot ışığını yapılandırın*

**Not:** Bu Grup İlkesi yolu, varsayılan. Microsoft Windows 10 Sürüm 1607 ve Server 2016 Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu CloudContent.admx/adml tarafından sağlanır.

**19.7.8.2 (L1) 'Windows spot ışığında üçüncü taraf içeriği önerme' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, Windows'un üçüncü taraf yazılım yayıncılarından uygulama ve içerik önerip önermeyeceğini belirler. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bu ayarın etkinleştirilmesi, verilerinizin herhangi bir üçüncü tarafla paylaşılmamasına yardımcı olacaktır. Windows Spotlight özelliği, verileri toplar ve bu verileri, önerilen uygulamaları ve internetten görüntüleri görüntülemek için kullanır.

**Etki:**

Kilit ekranında Windows Spotlight, Windows ipuçları, Microsoft tüketici özellikleri ve diğer ilgili özellikler artık üçüncü taraf yazılım yayıncılarından uygulama ve içerik önermeyecektir. Kullanıcılar, Microsoft özellikleri ve uygulamalarıyla daha üretken olmalarını sağlayacak önerileri ve ipuçlarını görmeye devam edebilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_USERS[USERSID]\Software\Policies\Microsoft\Windows\CloudContent:DisableThirdPartySuggestions*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Kullanıcı Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Bulut İçeriği\Windows spot ışığında üçüncü taraf içeriği önerme*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 1607 ve Server 2016 Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu CloudContent.admx/adml tarafından sağlanır.

**19.7.8.3 (L2) 'Tanılama verilerini uyarlanmış deneyimler için kullanma' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, Windows'un kullanıcıya uyarlanmış deneyimler sağlamak için tanılama verilerini kullanıp kullanamayacağını belirler. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Kişiselleştirilmiş verilerin izlenmesi, toplanması ve kullanılması, birçok kuruluşu ilgilendiren bir gizlilik ve güvenlik sorunudur.

**Etki:**

Windows, kilit ekranında gösterilen içeriği, Windows ipuçlarını, Microsoft tüketici özelliklerini özelleştirmek için bu cihazdan tanılama verilerini kullanmayacak ("Tanılama ve kullanım verileri" ayar değerine bağlı olarak bu veriler tarayıcı, uygulama ve özellik kullanımını içerebilir) ve diğer ilgili özellikler. Bu özellikler etkinleştirilirse kullanıcılar önerileri, ipuçlarını ve teklifleri görmeye devam eder, ancak bunlar daha az kişiselleştirilebilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_USERS[USERSID]\Software\Policies\Microsoft\Windows\CloudContent:DisableTailoredExperien cesWithDiagnosticData*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Kullanıcı Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Bulut İçeriği\Uyarlanmış deneyimler için tanılama verilerini kullanmayın*

**Not:** Bu Grup İlkesi yolu varsayılan olarak var. Microsoft Windows 10 Sürüm 1703 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu CloudContent.admx/adml tarafından sağlanır. Varsayılan Değer: Devre Dışı. (Microsoft, kişiselleştirilmiş öneriler, ipuçları ve teklifler sağlamak için tanı verilerini kullanacaktır.)

**19.7.8.4 (L2) 'Tüm Windows spot ışığı özelliklerini kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, tüm Windows Spotlight özelliklerinin açık/kapalı olup olmadığını (birlikte) belirler. Bu ayar için önerilen durum: Etkin.

**Not:** [Microsoft TechNet](https://technet.microsoft.com/en-us/itpro/windows/manage/group-policies-for-enterprise-and-education-editions)'e göre bu ilke ayarı yalnızca Windows 10 Enterprise ve Windows 10 Education sürümleri için geçerlidir.

**Gerekçe:**

Bu ayarın etkinleştirilmesi, verilerinizin herhangi bir üçüncü tarafla paylaşılmamasına yardımcı olacaktır. Windows Spotlight özelliği, verileri toplar ve bu verileri, önerilen uygulamaları ve internetten görüntüleri görüntülemek için kullanır.

**Etki:**

Kilit ekranında Windows Spotlight, Windows ipuçları, Microsoft tüketici özellikleri ve diğer ilgili özellikler kapatılacak.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_USERS[USERSID]\Software\Policies\Microsoft\Windows\CloudContent:DisableWindowsSpotlight Features*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Kullanıcı Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Bulut İçeriği\Tüm Windows spot özelliklerini kapatın*

**Not:** Bu Grup İlkesi yolu, varsayılan. Microsoft Windows 10 Sürüm 1607 ve Server 2016 Yönetim Şablonları (veya daha yenisi) ile birlikte gelen Grup İlkesi şablonu CloudContent.admx/adml tarafından sağlanır.

**19.7.8.5 (L1) 'Masaüstünde Spotlight koleksiyonunu kapat' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır**.

**Açıklama:**

Bu ilke ayarı, Kişiselleştirme'deki Spotlight koleksiyonu ayarını kaldırarak, kullanıcının Microsoft'tan günlük görüntüleri seçip ardından sistem masaüstüne indirmesini engeller. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Bu ayarın etkinleştirilmesi, verilerinizin herhangi bir üçüncü tarafla paylaşılmamasına yardımcı olacaktır. Windows Spotlight özelliği, verileri toplar ve bu verileri Microsoft'tan gelen görüntüleri görüntülemek için kullanır.

**Etki:**

Spotlight koleksiyonu özelliği, Kişiselleştirme ayarlarında bir seçenek olarak kullanılamayacak, bu nedenle kullanıcılar Microsoft'tan günlük görüntüleri indiremeyecek.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_USERS[USERSID]\SOFTWARE\Policies\Microsoft\Windows\CloudContent:DisableSpotlightCollect ionOnDesktop*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Kullanıcı Configuration\Policies\Administrative Templates\Windows Components\Cloud Content\Masaüstünde Spotlight koleksiyonunu kapat*

**Not:** Bu Grup İlkesi yolu varsayılan olarak mevcut olmayabilir. Microsoft Windows 10 Sürüm 21H2 Yönetim Şablonlarında (veya daha yenisinde) bulunan Grup İlkesi şablonu CloudContent.admx/adml tarafından sağlanır.

**19.7.9 Kimlik Bilgileri Kullanıcı Arayüzü**

**19.7.10 Veri toplama ve önizleme derlemeleri**

**19.7.11 Masaüstü Araçları**

**19.7.12 Masaüstü Pencere Yöneticisi**

**19.7.13 Dijital Dolap**

**19.7.14 Uç kullanıcı arayüzü**

**19.7.15** **Dosya Gezgini (eski adıyla Windows Gezgini)**

**19.7.16 Dosya İptali**

**19.7.17 İSİM**

**19.7.18 Video İçe Aktar**

**19.7.19 Anlık Arama**

**19.7.20 Internet Explorer**

**19.7.21 Konum ve Sensörler**

**19.7.22 Microsoft Edge**

**19.7.23 Microsoft Yönetim Konsolu**

**19.7.24 Microsoft Kullanıcı Deneyimi Sanallaştırma**

**19.7.25 Çoklu görev**

**19.7.26 NetMeeting**

**19.7.27 Ağ Projektörü**

**19.7.28 Ağ Paylaşımı**

**19.7.28.1 (L1) 'Kullanıcıların profillerinde dosya paylaşmasını engelle.' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ilke ayarı, kullanıcıların profillerinde dosya paylaşıp paylaşamayacağını belirler. Varsayılan olarak, bir yönetici bilgisayarı seçtikten sonra, kullanıcıların profillerindeki dosyaları ağlarındaki diğer kullanıcılarla paylaşmasına izin verilir. Yönetici, kendi profili içinde bir dosya paylaşmak için paylaşım sihirbazını kullanarak bilgisayarı seçebilir. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Düzgün yapılandırılmazsa, bir kullanıcı hassas verileri yanlışlıkla yetkisiz kullanıcılarla paylaşabilir. Kurumsal yönetilen bir ortamda, şirket, kullanıcının doğrudan kendi kullanıcı profilinden dosya paylaşması yerine dosya sunucusu veya SharePoint gibi dosya paylaşımı için yönetilen bir konum sağlamalıdır.

**Etki:**

Kullanıcılar, paylaşım sihirbazını kullanarak profillerinde dosya paylaşamaz. Ayrıca, paylaşım sihirbazı %root%\Users konumunda paylaşım oluşturamaz ve yalnızca klasörlerde SMB paylaşımları oluşturmak için kullanılabilir.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_USERS[USERSID]\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer:NoInplaceSha ring*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı kurmak için aşağıdaki UI yolunu Etkin olarak ayarlayın :

*Kullanıcı Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Ağ Paylaşımı\Kullanıcıların profillerinde dosya paylaşmasını engelle.*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu Sharing.admx/adml tarafından sağlanır.

**19.7.29 OOBE**

**19.7.30 Sunum Ayarları**

**19.7.31 Uzak Masaüstü Hizmetleri (eski adıyla Terminal Hizmetleri)**

**19.7.32 RSS Beslemeleri**

**19.7.33 Arama**

**19.7.34** **Ses Kaydedici**

**19.7.35** **Mağaza**

**19.7.36 Tablet PC**

**19.7.37 Görev Zamanlayıcı**

**19.7.38 Windows Takvim**

**19.7.39** **Windows Renk Sistemi**

**19.7.40 Windows Defender Akıllı Ekran**

**19.7.41 Windows Hata Bildirimi**

**19.7.42 İş için Windows Hello (eski adıyla Microsoft Passport for Work)**

**19.7.43 Windows Installer**

**19.7.43.1 (L1) 'Her zaman yükseltilmiş ayrıcalıklarla yükle' seçeneği 'Devre Dışı' (Otomatik) olarak ayarlandığından emin olun**

**Açıklama:**

Bu ayar, Windows Installer'ın sisteme herhangi bir program yüklediğinde sistem izinlerini kullanıp kullanmayacağını denetler.

**Not:** Bu ayar hem Bilgisayar Yapılandırması hem de Kullanıcı Yapılandırması klasörlerinde görünür. Bu ayarı etkin kılmak için, her iki klasörde de ayarı etkinleştirmelisiniz.

**Dikkat:** Etkinleştirilirse, yetenekli kullanıcılar, ayrıcalıklarını değiştirmek ve kısıtlı dosya ve klasörlere kalıcı erişim elde etmek için bu ayarın verdiği izinlerden yararlanabilir. Bu ayarın Kullanıcı Yapılandırma sürümünün güvenli olduğunun garanti edilmediğini unutmayın.

Bu ayar için önerilen durum: Devre Dışı.

**Gerekçe:**

Sınırlı ayrıcalıklara sahip kullanıcılar, yerel yerleşik Yöneticiler grubuna ait yeni bir yerel hesap oluşturan, mevcut hesaplarını yerel yerleşik Yöneticiler grubuna ekleyen, kötü amaçlı yazılımlar yükleyen bir Windows Installer yükleme paketi oluşturarak bu özellikten yararlanabilir. veya diğer yetkisiz faaliyetlerde bulunur.

**Etki:**

Yok - bu varsayılan davranıştır.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_USERS[USERSID]\Software\Policies\Microsoft\Windows\Installer:AlwaysInstallElevated*

**Düzeltme:**

Önerilen yapılandırmayı GP aracılığıyla kurmak için aşağıdaki UI yolunu Devre Dışı olarak ayarlayın:

*Kullanıcı Yapılandırması \Policies\Yönetim Şablonları\Windows Bileşenleri\Windows Installer\Her zaman yükseltilmiş ayrıcalıklarla yükleyin*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu MSI.admx/adml tarafından sağlanır.

**19.7.44 Windows Oturum Açma Seçenekleri**

**19.7.45** **Windows Posta**

**19.7.46 Windows Media Center**

**19.7.47 Windows Media Player**

**19.7.47.1 Ağ İletişimi**

**19.7.47.2 Oynatma**

**19.7.47.2.1 (L2) 'Codec Bileşeninin İndirilmesini Engelle' seçeneği 'Etkin' (Otomatik) olarak ayarlanmalıdır.**

**Açıklama:**

Bu ayar, Windows Media Player'ın henüz anlamadığı medya dosyalarının kodunu çözmek için ek codec bileşenleri indirmesine izin verilip verilmediğini denetler. Bu ayar için önerilen durum: Etkin.

**Gerekçe:**

Media Player'da ek bir codec bileşeninin yüklenmesini gerektiren kötü amaçlı bir veri dosyası açılırsa, bunun bazı risk potansiyeli vardır. Gerekli bir iş işlevi için özel bir codec bileşeni gerekiyorsa, bu codec bileşeninin yasal olduğundan emin olmak için önce test edilmeli ve kuruluştaki BT departmanı tarafından sağlanmalıdır.

**Etki:**

Windows Media Player'ın codec bileşenlerini bilgisayarınıza otomatik olarak indirmesi engellenir. Ayrıca, Player'daki Player sekmesindeki Codec bileşenlerini otomatik olarak indir onay kutusu kullanılamaz.

**Denetim:**

Düzeltme bölümünde açıklanan Kullanıcı Arabirimi Yoluna gidin ve belirtilen şekilde ayarlandığını onaylayın. Bu grup ilkesi ayarı, aşağıdaki kayıt defteri konumu tarafından desteklenir: *HKEY\_USERS[USERSID]\Software\Policies\Microsoft\WindowsMediaPlayer:PreventCodecDownload*

**Düzeltme:**

GP aracılığıyla önerilen yapılandırmayı oluşturmak için, aşağıdaki UI yolunu Etkin olarak ayarlayın:

*Kullanıcı Yapılandırması\İlkeler\Yönetim Şablonları\Windows Bileşenleri\Windows Media Player\Oynatma\Önleme Codec İndirme*

**Not:** Bu Grup İlkesi yolu, Microsoft Windows Yönetim Şablonlarının tüm sürümlerinde bulunan Grup İlkesi şablonu WindowsMediaPlayer.admx/adml tarafından sağlanır.

**Referanslar**

1. <https://www.cisecurity.org/white-papers/cis-password-policy-guide/>
2. <https://support.microsoft.com/en-us/topic/minimum-password-length-auditing-and-enforcement-on-certain-versions-of-windows-5ef7fecf-3325-f56b-cc10-4fd565aacc59>
3. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/access-credential-manager-as-a-trusted-caller>
4. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/act-as-part-of-the-operating-system>
5. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/adjust-memory-quotas-for-a-process>
6. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/allow-log-on-locally>
7. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/allow-log-on-through-remote-desktop-services>
8. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/back-up-files-and-directories>
9. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/change-the-system-time>
10. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/change-the-time-zone>
11. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/create-a-pagefile>
12. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/create-a-token-object>
13. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/create-global-objects>
14. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/create-permanent-shared-objects>
15. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/create-symbolic-links>
16. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/debug-programs>
17. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/access-this-computer-from-the-network>
18. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/load-and-unload-device-drivers>
19. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/lock-pages-in-memory>
20. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/log-on-as-a-batch-job>
21. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/log-on-as-a-service>
22. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/manage-auditing-and-security-log>
23. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/modify-an-object-label>
24. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/modify-firmware-environment-values>
25. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/perform-volume-maintenance-tasks>
26. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/profile-single-process>
27. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/profile-system-performance>
28. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/replace-a-process-level-token>
29. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/restore-files-and-directories>
30. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/shut-down-the-system>
31. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/take-ownership-of-files-or-other-objects>
32. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/accounts-administrator-account-status>
33. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/accounts-block-microsoft-accounts>
34. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/accounts-guest-account-status>
35. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/accounts-limit-local-account-use-of-blank-passwords-to-console-logon-only>
36. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/accounts-rename-administrator-account>
37. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/accounts-rename-guest-account>
38. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/audit-force-audit-policy-subcategory-settings-to-override>
39. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/audit-shut-down-system-immediately-if-unable-to-log-security-audits>
40. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/devices-allowed-to-format-and-eject-removable-media>
41. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/devices-prevent-users-from-installing-printer-drivers>
42. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/domain-member-digitally-encrypt-or-sign-secure-channel-data-always>
43. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/domain-member-digitally-encrypt-secure-channel-data-when-possible>
44. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/domain-member-digitally-sign-secure-channel-data-when-possible>
45. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/domain-member-disable-machine-account-password-changes>
46. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/domain-member-maximum-machine-account-password-age>
47. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/domain-member-require-strong-windows-2000-or-later-session-key>
48. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-do-not-require-ctrl-alt-del>
49. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-do-not-display-last-user-name>
50. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-machine-account-lockout-threshold>
51. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-machine-inactivity-limit>
52. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-message-text-for-users-attempting-to-log-on>
53. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-message-title-for-users-attempting-to-log-on>
54. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-number-of-previous-logons-to-cache-in-case-domain-controller-is-not-available>
55. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-prompt-user-to-change-password-before-expiration>
56. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/interactive-logon-smart-card-removal-behavior>
57. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-client-digitally-sign-communications-always>
58. <https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/jj852251(v=ws.11>)
59. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-client-send-unencrypted-password-to-third-party-smb-servers>
60. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-amount-of-idle-time-required-before-suspending-session>
61. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-digitally-sign-communications-always>
62. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/smbv1-microsoft-network-server-digitally-sign-communications-if-client-agrees>
63. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-disconnect-clients-when-logon-hours-expire>
64. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/microsoft-network-server-server-spn-target-name-validation-level>
65. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-allow-anonymous-sidname-translation>
66. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-anonymous-enumeration-of-sam-accounts>
67. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-anonymous-enumeration-of-sam-accounts-and-shares>
68. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-do-not-allow-storage-of-passwords-and-credentials-for-network-authentication>
69. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-let-everyone-permissions-apply-to-anonymous-users>
70. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-named-pipes-that-can-be-accessed-anonymously>
71. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-remotely-accessible-registry-paths>
72. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-remotely-accessible-registry-paths-and-subpaths>
73. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-anonymous-access-to-named-pipes-and-shares>
74. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-restrict-clients-allowed-to-make-remote-sam-calls>
75. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-shares-that-can-be-accessed-anonymously>
76. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-access-sharing-and-security-model-for-local-accounts>
77. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-allow-local-system-to-use-computer-identity-for-ntlm>
78. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-allow-localsystem-null-session-fallback>
79. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-allow-pku2u-authentication-requests-to-this-computer-to-use-online-identities>
80. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-configure-encryption-types-allowed-for-kerberos>
81. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-do-not-store-lan-manager-hash-value-on-next-password-change>
82. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-force-logoff-when-logon-hours-expire>
83. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-lan-manager-authentication-level>
84. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-ldap-client-signing-requirements>
85. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/network-security-minimum-session-security-for-ntlm-ssp-based-including-secure-rpc-clients>
86. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/system-objects-require-case-insensitivity-for-non-windows-subsystems>
87. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/system-objects-strengthen-default-permissions-of-internal-system-objects>
88. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-account-control-admin-approval-mode-for-the-built-in-administrator-account>
89. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-account-control-behavior-of-the-elevation-prompt-for-administrators-in-admin-approval-mode>
90. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-account-control-behavior-of-the-elevation-prompt-for-standard-users>
91. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-account-control-detect-application-installations-and-prompt-for-elevation>
92. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-account-control-only-elevate-uiaccess-applications-that-are-installed-in-secure-locations>
93. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-account-control-run-all-administrators-in-admin-approval-mode>
94. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-account-control-switch-to-the-secure-desktop-when-prompting-for-elevation>
95. <https://docs.microsoft.com/en-us/windows/security/threat-protection/security-policy-settings/user-account-control-virtualize-file-and-registry-write-failures-to-per-user-locations>
96. <https://blogs.technet.microsoft.com/filecab/2016/09/16/stop-using-smb1/>
97. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527>
98. <https://docs.microsoft.com/en-us/windows/security/threat-protection/auditing/audit-application-group-management>
99. <https://support.microsoft.com/en-us/topic/kb5005010-restricting-installation-of-new-printer-drivers-after-applying-the-july-6-2021-updates-31b91c02-05bc-4ada-a7ea-183b129578a7>
100. <https://support.microsoft.com/en-gb/topic/kb5005652-manage-new-point-and-print-default-driver-installation-behavior-cve-2021-34481-873642bf-2634-49c5-a23b-6d8e9a302872>
101. <https://docs.microsoft.com/en-us/windows-server/networking/dns/doh-client-support>
102. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527>
103. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-1675>
104. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34481>
105. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-34527>
106. <https://msrc.microsoft.com/update-guide/vulnerability/CVE-2021-36958>
107. <https://msrc-blog.microsoft.com/2021/08/10/point-and-print-default-behavior-change/>
108. <https://support.microsoft.com/en-us/topic/kb5005652-manage-new-point-and-print-default-driver-installation-behavior-cve-2021-34481-873642bf-2634-49c5-a23b-6d8e9a302872>
109. <https://support.microsoft.com/en-us/topic/kb5005652-manage-new-point-and-print-default-driver-installation-behavior-cve-2021-34481-873642bf-2634-49c5-a23b-6d8e9a302872>
110. <https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_logging_windows?view=powershell-7.2#protected-event-logging>
111. <https://docs.microsoft.com/en-us/windows/security/identity-protection/remote-credential-guard>
112. <https://msrc.microsoft.com/update-guide/en-US/vulnerability/ADV180028>
113. <https://msrc.microsoft.com/update-guide/en-US/vulnerability/ADV180028>
114. <https://msrc.microsoft.com/update-guide/en-US/vulnerability/ADV180028>
115. <https://docs.microsoft.com/en-us/windows/privacy/configure-windows-diagnostic-data-in-your-organization>
116. <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/configure-real-time-protection-microsoft-defender-antivirus>
117. <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/configure-real-time-protection-microsoft-defender-antivirus>
118. <https://docs.microsoft.com/en-us/windows/security/threat-protection/microsoft-defender-antivirus/configure-real-time-protection-microsoft-defender-antivirus>
119. <https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/configure-advanced-scan-types-microsoft-defender-antivirus?view=o365-worldwide>
120. <https://techcommunity.microsoft.com/t5/windows-it-pro-blog/group-configuration-news-and-interests-on-the-windows-taskbar/ba-p/2281005/page/2#comments>
121. <https://docs.microsoft.com/en-us/dotnet/framework/ui-automation/ui-automation-overview>
122. <https://docs.microsoft.com/en-us/powershell/module/microsoft.powershell.core/about/about_logging_windows?view=powershell-7.2#protected-event-logging>
123. <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-sandbox/windows-sandbox-configure-using-wsb-file>
124. <https://docs.microsoft.com/en-us/windows/security/threat-protection/windows-sandbox/windows-sandbox-configure-using-wsb-file>
125. <https://docs.microsoft.com/en-us/windows-insider/business/manage-builds>
126. <https://docs.microsoft.com/en-us/windows/configuration/windows-spotlight>
127. **İSTİSNALAR**

**Not: Bazı özelliklerin açıklaması bulunmamaktadır. Bu kısımlar bilerek boş bırakılmıştır ve Windows kıyaslamalarının yapısının tutarlı olmasını sağlamak için mevcuttur.**