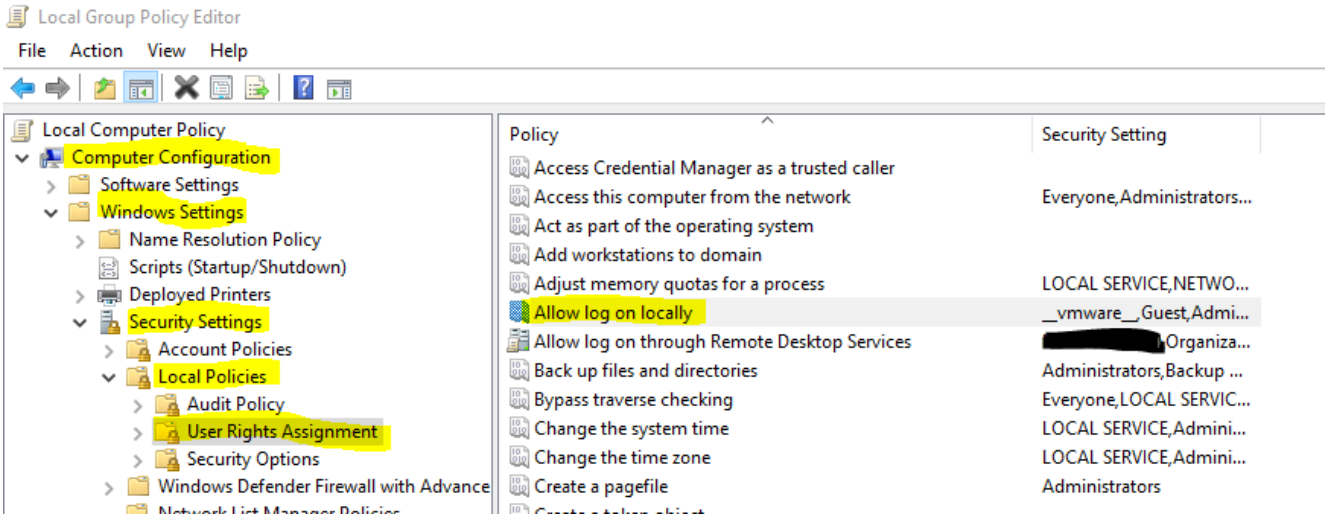
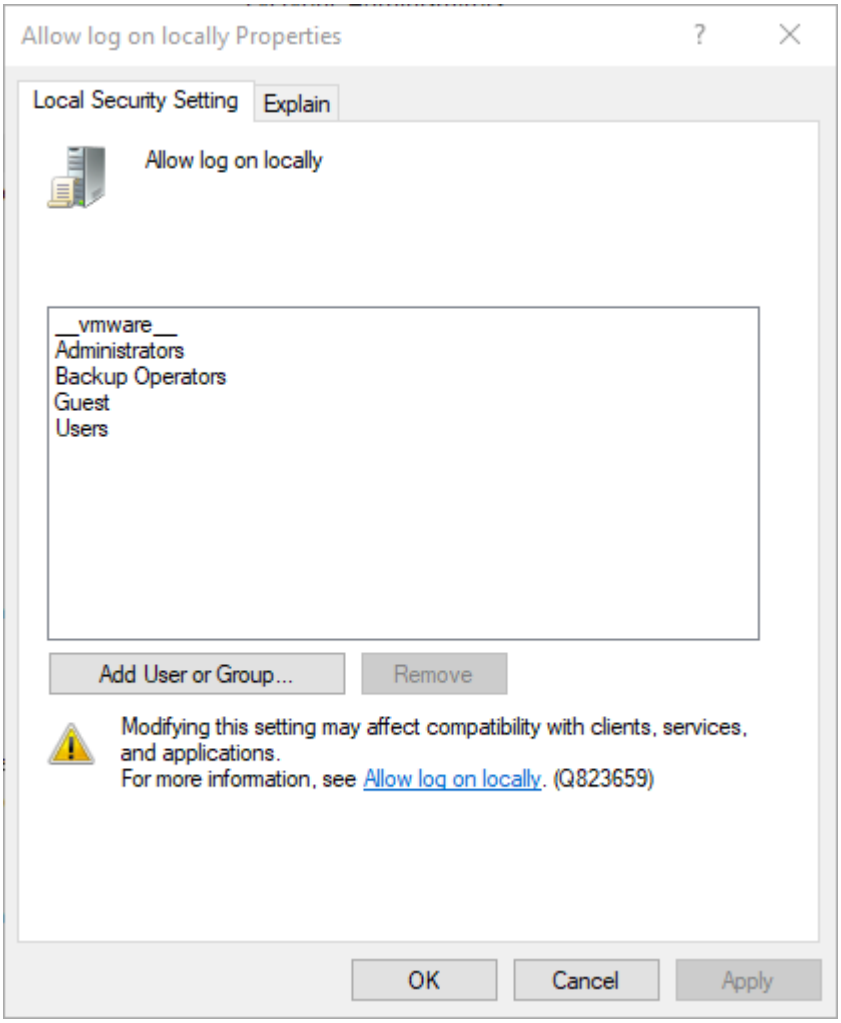
Domaindeki Bilgisayarda Oturum Açabilecek Kullanıcı Sınırlama

Kurumun domain yapısına dahil olan bilgisayarlara varsayılan ayarda bütün domain kullanıcıları oturum açabilir. Bilgisayarlarda sadece izin verilen kullanıcıların oturum açmasına izin verilebilir.

Bunun için gpedit.msc komutu ile Local Group Policy Editor açılır. Ve aşağıdaki yol takip edilerek ilgili listeye izin verilecek kullanıcılar eklenir.



Kullanıcı belirleme ekranı:



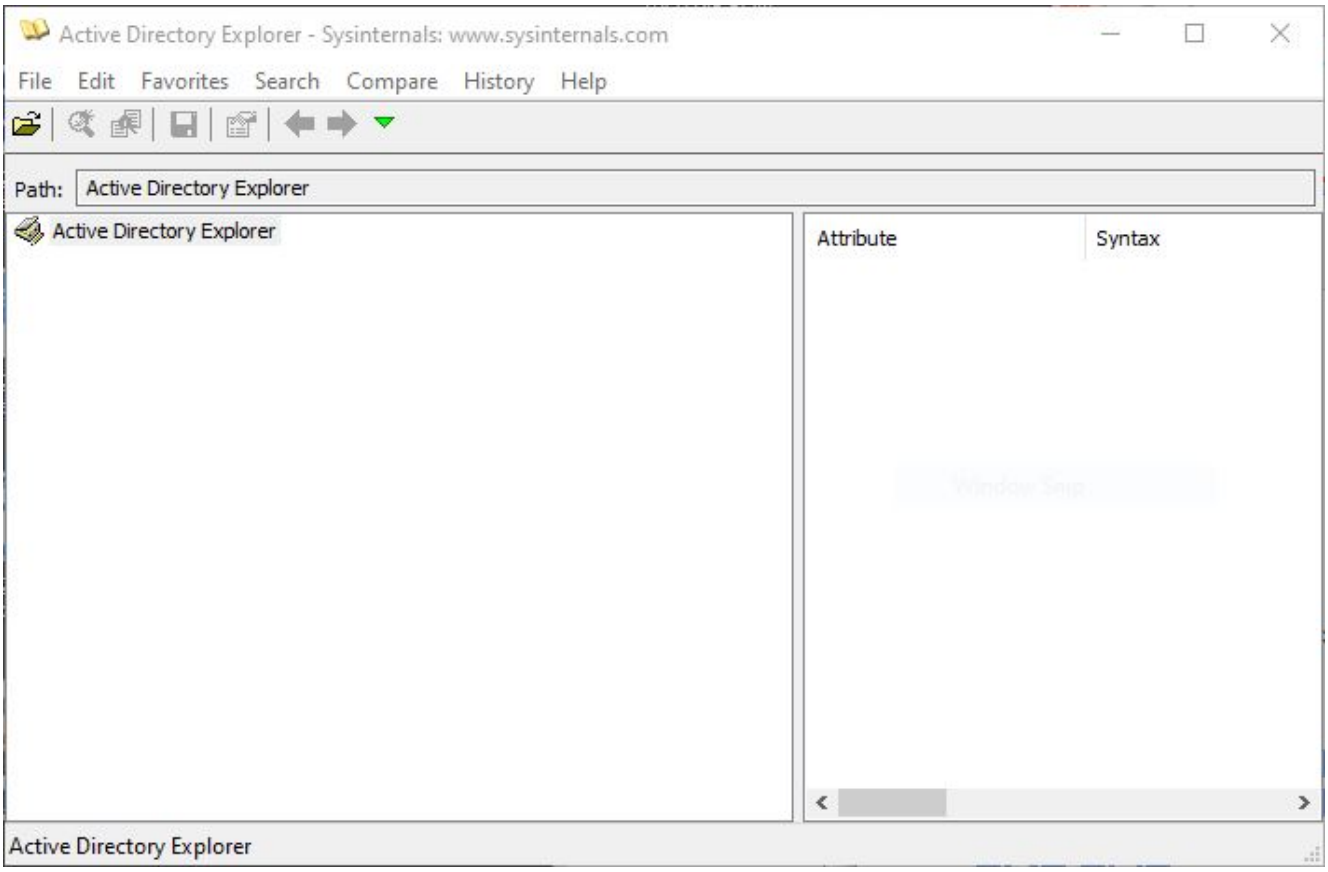
İşlemin Videolu Anlatımı

Active Directory Explorer İle AD Yapınızı Hızlıca Gözden Geçirin

Microsoft Active Directory

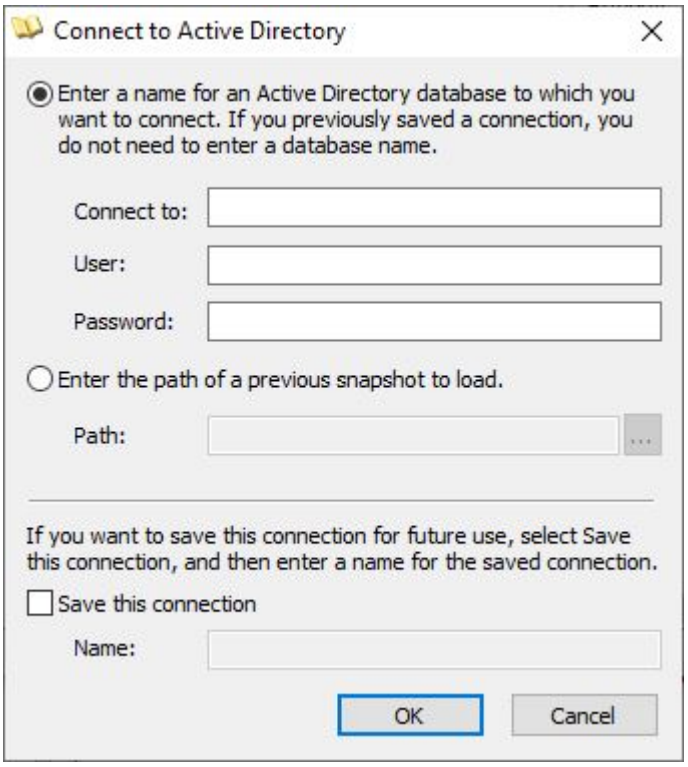
Active Directory şirketlerde gerek kaynak gerek kullanıcı yönetiminde görev alan bir yapı olarak karşımıza çıkmaktadır. Yapısı ve üstlendiği görevler gereği kullanıcıya dair bütün bilgileri üzerinde tutmaktadır. Bu bilgilerden bazıları sistem yöneticisi için önemli verilerdir. Örneğin kullanıcının en son ne zaman şifre değiştirdiği, en son ne zaman oturum açtığı vb.

Bu verileri okumak için kullanılabilecek faydalı uygulamalardan biri de Actice Directory Explorer aracıdır.



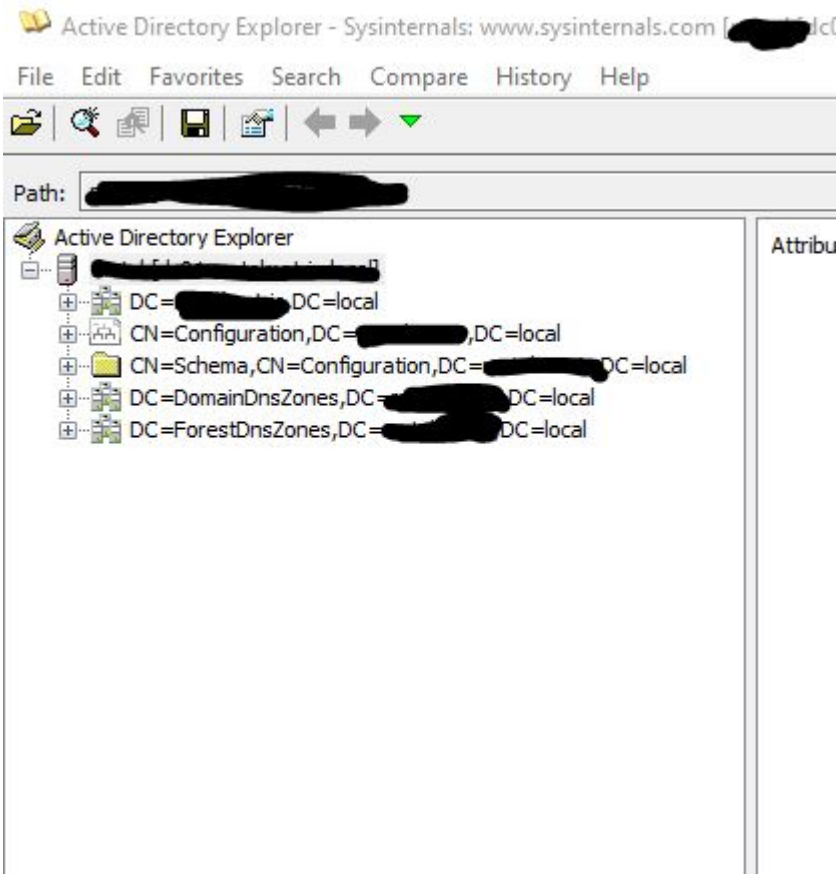
Active Directory Explorer

Öncelikle Active Directory sunucusuna bağlanmak gerekiyor. Bağlantı için File => Connect yolu izlenir. Açılan aşağıdaki ekranda AD sunucusu ve yetkili bir kullanıcı hesabı ve şifresi girilir.



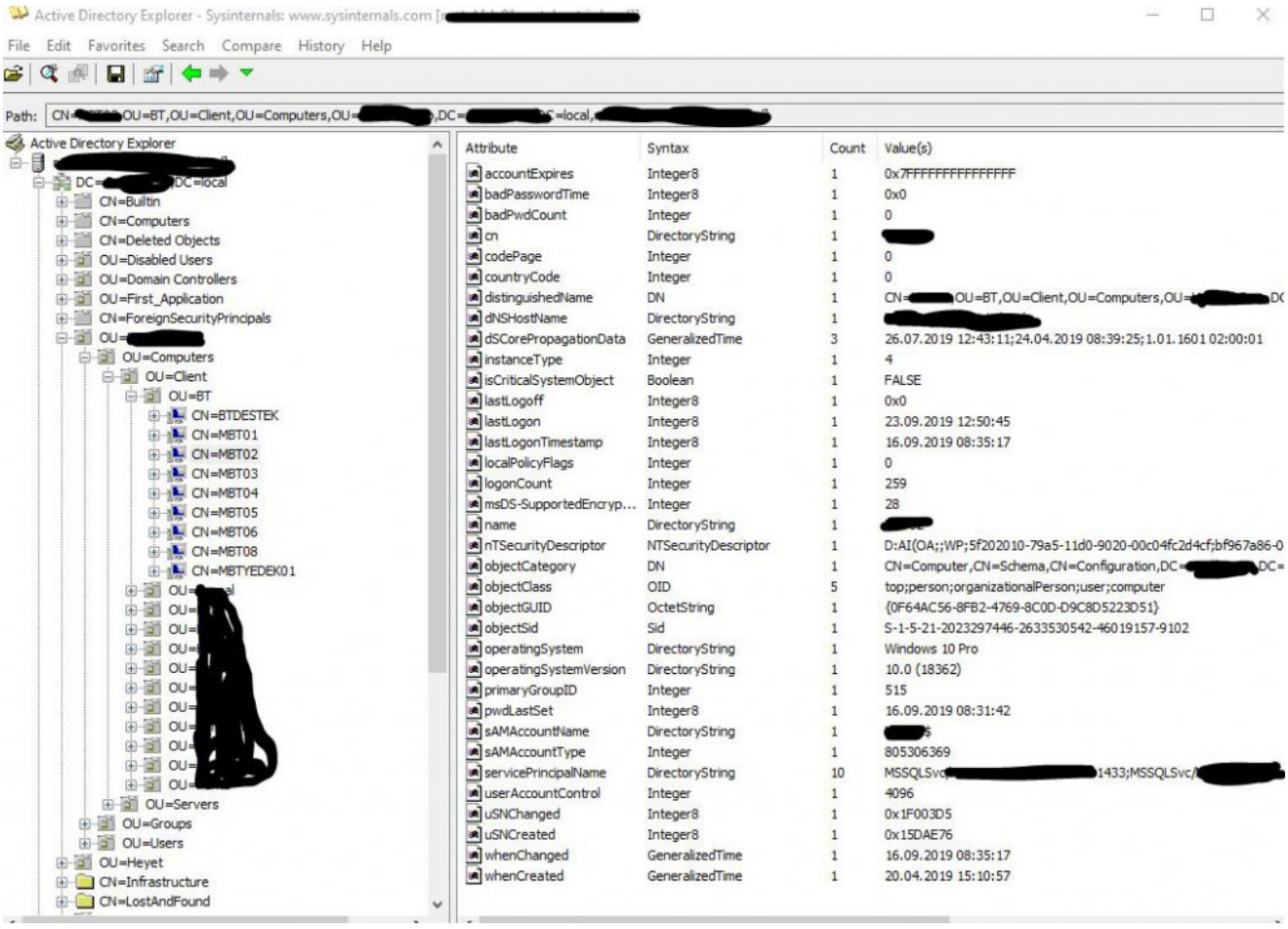
AD Server Bağlantı Ekranı

Bağlantı için gerekli bilgiler girildikten sonra aşağıdaki ekranda göründüğü gibi AD yapısı ekrana gelecektir.



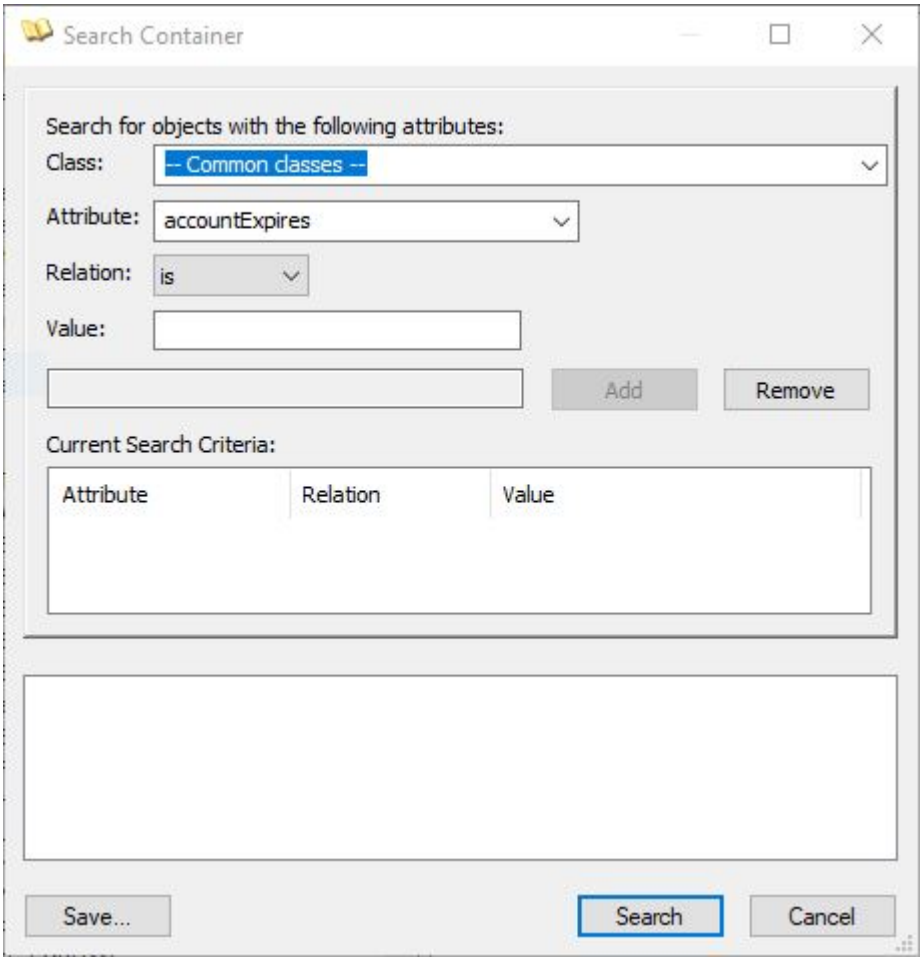
AD Yapısı

Yapı içerisinde gezinerek domainde bulunan kullanıcı ve bilgisayarlarla ilgili bilgiler incelenebilir. Örneğin aşağıdaki ekranda örnek bir bilgisayar hesabı inceleniyor.



Bilgisayar Hesabı

Yapı içerisinde arama yapmak için Search => Search Container seçeneği tıklanır.



Active Directory İçerisinde Arama

Arama ekranı kriterleri aşağıdaki gibidir:

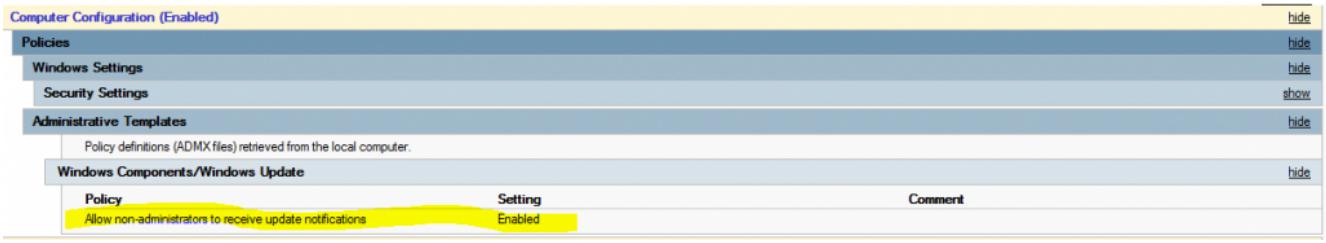
Class	Arama Yapılacak Nesne Türü
Attribute	Arama yapılacak nesne özelliği
Relation	Karşılaştırma kriteri
Value	Aranan değer

Arama kriterleri girildikten sonra “Add” butonu ile şart aramaya eklenir. Bu şekilde bütün şartlar ekrana girildikten sonra “Search” butonu ile arama yapılır.

Uygulamayı İndirmek için burayı **TIKLAYIN**

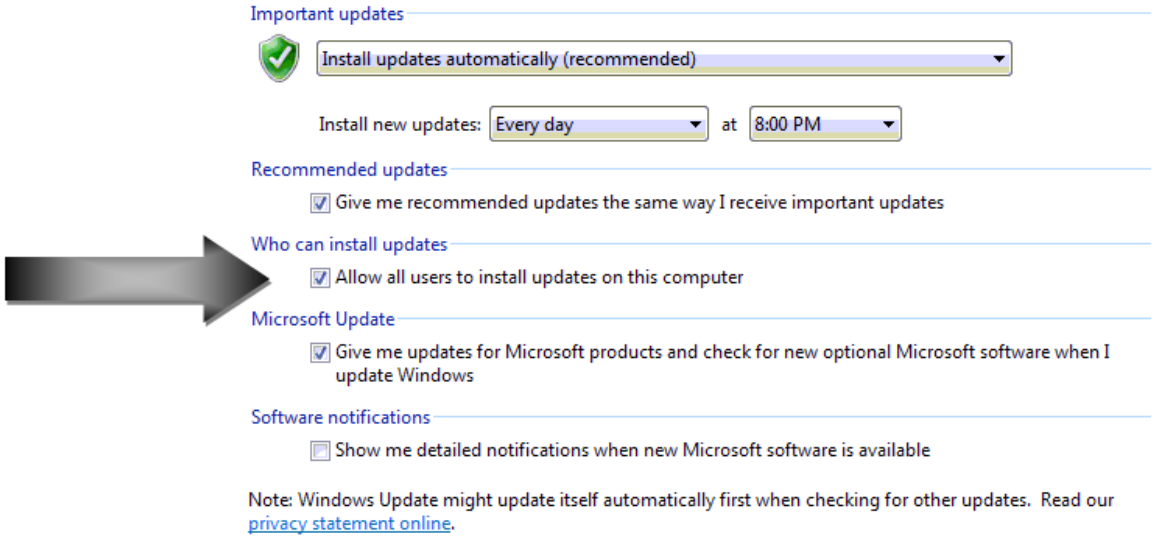
Standart Kullanıcıların Windows Güncellemelerini Yüklemelerine İzin Vermek

Firmalarda kullanılan güvenlik önlemlerinden biri kullanıcılardan local admin yetkilerini almaktır. Ancak bunu yapınca da standart kullanıcı hesapları Windows güncellemelerini yükleyemez hale geliyor. Bu sorunu çözmek için group policy üzerinden aşağıdaki ayar yapılır. Bu ayardan sonra standart kullanıcılar da windows güncellemelerini yükleyebilecek.



Standart Kullanıcı İçin Güncelleme Yetkisi

Bu işlem domain yapısında olmayan bir Windows makinesinde yapılmak istendiğinde aşağıdaki yok izlenir

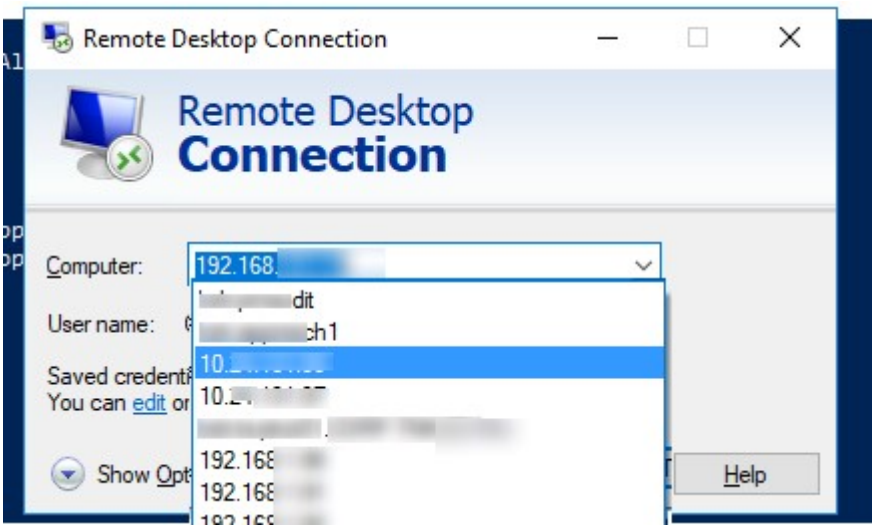


Standart Kullanıcıya Güncelleme Yetkisi Verme

Veya Local Policy üzerinden işlem yapılmak istenirse:

- Çalıştır satırına gpedit.msc yazıp ENTER tuşuna basın (Çalıştır satırı için Win + R)
- Computer Configuration -> Administrative Templates -> Windows Component -> Windows Update yolunu izleyin
- “Allow non administrative to receive update notifications” seçeneğini ENABLE olarak değiştirin.

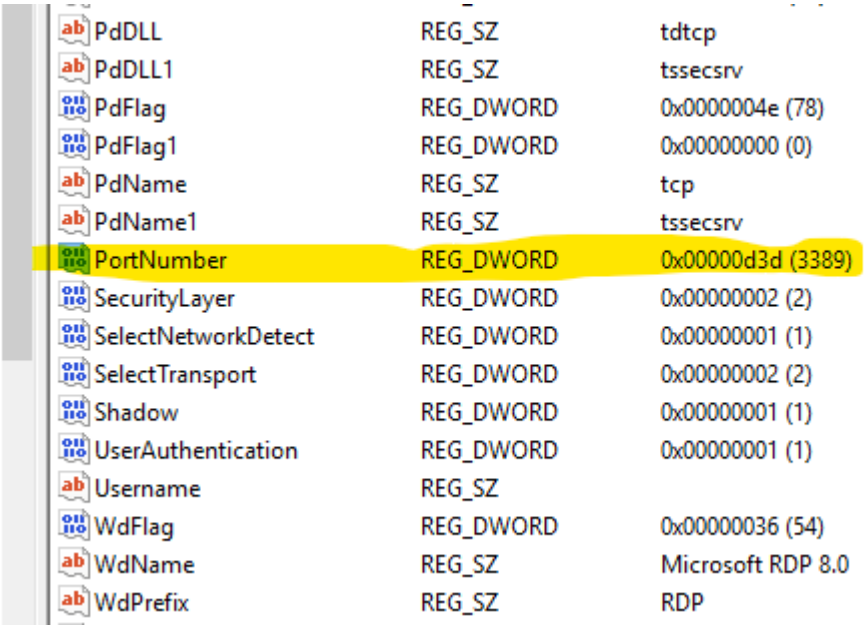
Varsayılan Uzak Masaüstü (RDP) Portu Değiştirme



Uzak masaüstü uygulaması Microsoft tarafından geliştirilen faydalı bir uygulama olsa da güvenliği tam sağlanamazsa ciddi bir güvenlik açığına sebep olmaktadır. Bu güvenlik açığının sebeplerinden biri RDP protokolünün varsayılan portunun herkes tarafından biliniyor olmasıdır. Bu güvenlik açığına bir nebze de olsa alınabilecek önlemlerden akla ilk geleni RDP portunun değiştirilmesidir.

RDP portunu değiştirmek için:

- Kayıt Defteri Düzenleyicisini (regedit) açın
- **HKEY_LOCAL_MACHINE\System\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp\PortNumber**



PdDLL	REG_SZ	tdtcp
PdDLL1	REG_SZ	tssecsrv
PdFlag	REG_DWORD	0x0000004e (78)
PdFlag1	REG_DWORD	0x00000000 (0)
PdName	REG_SZ	tcp
PdName1	REG_SZ	tssecsrv
PortNumber	REG_DWORD	0x00000d3d (3389)
SecurityLayer	REG_DWORD	0x00000002 (2)
SelectNetworkDetect	REG_DWORD	0x00000001 (1)
SelectTransport	REG_DWORD	0x00000002 (2)
Shadow	REG_DWORD	0x00000001 (1)
UserAuthentication	REG_DWORD	0x00000001 (1)
Username	REG_SZ	
WdFlag	REG_DWORD	0x00000036 (54)
WdName	REG_SZ	Microsoft RDP 8.0
WdPrefix	REG_SZ	RDP

RDP Port Numarası

- İşaretlenen PortNumber değerini istenen ve başkası tarafından tahmin edilemeyecek bir değer ile değiştirin
- Kayıt Defteri Düzenleyicisini kapatın
- Bilgisayarı yeniden başlatın

Bu işlemlerden sonra bilgisayarınıza RDP ile bağlantı sağlarken artık girdiğimiz güncel port numarası üzerinden gidebilirsiniz.

Yönetici İznine (UAC) Takılan Program Sorunu

Çalışırken bazı programlar görünürde yönetici iznini gerektirecek her hangi bir işlem yapmamalarına rağmen yönetici izni istemektedirler. Özellikle bilgi güvenliği noktasında prosedürler yürüten firmalarda da kullanıcı bilgisayarı üzerinde yönetici olmadığından uygulamayı çalıştırmakta başarısız olmaktadır.

Programın yönetici izni istemesinin temelinde yatan neden, çalışırken ya sistem ayarlarına müdahale ediyor olması yada sistem dosyalarında işlem yapmaya çalışmasıdır. Burada sistem dosyaları sözü aklı karıştırmasın. Program "Program Files" varsayılan klasörüne yüklendiğinde kendi dosyaları da "Program Files" klasörünün özelliği gereği Windows tarafından sistem dosyası olarak işaretlenmektedir ve bu dosyalar üzerinde işlem yapabilmek için yönetici izni gerekmektedir.

Çözüm olarak karşımıza iki seçenek çıkmaktadır;

- Kullanıcıya yerel yönetici haklarını vermek ki bu özellikle bilgisayar noktasında tecrübesi olmayan kullanıcılar tarafında ayrı bir güvenlik açığına sebep olmaktadır.
- Diğer bir seçeneğimiz de programın kurulum yolunu değiştirmektir. Örneğin C:\ diski altında oluşturacağımız bir klasörü kurulum yolu olarak verirsek, oluşturduğumuz bu klasör sistem klasörü olmadığından uygulamamız da sıkıntısız çalışacaktır.

Domain Yapısındaki Grupları Client Local Gruplara Ekleme

Domain yapılarında yapılan işlemlerden biri de kullanıcılardan local adminlik dediğimiz yönetici haklarının alınmasıdır. Bu işlemi yapmada ki amaç, kullanıcının bilgisayarı amacı dışında kullanmasına engel olmaktır. Bu işlemi yaparken de, özellikle bilgi işlem departmanının local admine atanması gerekmektedir. Bu atamayı yapmanın çeşitli yolları olmaktadır;

- Bilgi teknolojileri departmanının hepsini, Domain Admins grubuna dahil etmek: Bu seçenek güvenlik tehlikesini client bazından çıkarıp direk bütün yapı seviyesine çıkarır. Departmanda yer alan özellikle stajyer ve yeteri bilgiye sahip olmayan yeni çalışanların oluşturacağı güvenlik tehdidi göz ardı edilemez. Bu seçenek kabulümüz değil dolayısıyla
- Her kurulan yeni client bilgisayara, kurulumdan sonra BT departmanındaki bütün kişileri elle yöneticiler grubuna eklemek. Bu yönteminde dezavantajları: Kişileri tek tek eklerken kişiler unutulabilir, departman değiştiren kişiler bilgisayarlarda yönetici olarak kalmaya devam edecek…
- BT departmanı için domain yapısında bir grup oluşturup departman kişileri bu gruba üye edilir. Bu işlemden sonra Group Policy üzerinden oluşturulan bu grup clientlara otomatik olarak yönetici grubuna eklenir. Bu işlem için gereken group policy kuralı aşağıdaki gbidir.

Kuralın sol tarafında yer alan “Group” başlığı clientlara

eklenecek olan domain üzerinde tanımlı olan gruptur. SORHAN burada domain adını temsil etmektedir. HelpDesk de BT departmanı grubudur. Sağ tarafta yer alan “Member of” başlığı da grubun client tarafında nereye ekleneceğini ifade eder. BUILTIN ifadesi client makineyi ifade eder ve sabittir. Administrators ifadesi de clent makine üzerinde tanımlı Administrators grubunu ifade eder.

GP Üzerinden Herkese Güncelleme Yetkisi Verme

Bilişim sistemlerinin en önemli konularının başında sistemin güvenliğidir. Konu güvenlik olunca da makinelerde yetkilendirme devreye giriyor. Her şirkette olması gereken yetki kısıtlarından biri de bilgisayarlarda local adminliklerin olmaması kuralıdır. Kullanıcılardan local admin yetkileri alındıktan sonra ortaya bir sıkıntı daha çıkmaktadır: o da güncellemeleri yüklemek için kullanıcılardan yönetici izni istemek…

Güncelleme yüklenmeyince sistem açıklarını kapatan güncellemeler sisteme yüklenmemektedir.

Çözümümüz şu olacak: Group policy üzerinden bütün kullanıcılara güncelleme yükleme izni vermemiz gerekmektedir. İlgili GP ve gerekli değeri aşağıdaki resimdeki gibidir.

SAP Şifre Karmaşıklığı Zorlama

Her veri barındıran sistemin olmazsa olmazı güvenlik ve güvenliğin akla ilk geleni şifreler ve en önemli konu şifre karmaşıklığı. Şifre karmaşıklığının önemi üzerine ne kadar kullanıcıya uyarıda bulsanız da gene de kullanacakları şifre 123456, qwerty, qazws gibi basit şifreler oluyor. Bu noktada bilgi işlem departmanına düşen iş şifre karmaşıklığını kullanıcının insafına bırakmayıp sistem parametrelerini ayarlamaktır.

SAP'de şifre karmaşıklığı RZ10 sistem parametreleri ekranında aşağıdaki şekilde ayarlanmaktadır. Burada dikkat edilmesi gereken nokta değişikliğin devreye girmesi için sistemin yeniden başlatılması gerekmektedir.

RZ10 transection koduna giriş yapılır ve aşağıda yer alan parametreler isteye göre düzenlenir.

Parametre Adı	Değer	Açıklama
login/min_password_diff	3	Son üç şifre ile aynı şifre kullanılamaz

login/min_password_digits	1	En az bir rakam bulunmalı
login/min_password_lowercase	1	En az bir küçük harf bulunmalı
login/min_password_uppercase	1	En az bir büyük harf bulunmalı

NOT: Sahada aktif kullanılan el terminallerinde parametre değişikliği sonrasında sıkıntı yaşamamak adına işlem öncesinde el terminallerinde kullanılan şifreleri yeni politikaya göre düzenlemeye gidebilirsiniz.

Cisco Cihazlara Giriş Şifresi Verme

Network cihazlarında olmazsa olmazımız güvenliktir, güvenliğin ilk adımı da şifrelerdir. Cisco cihazlarında kullanılan çeşitli şifreler bulunmaktadır.

- Console Şifresi
  Cihaza console üzerinden bağlantı sırasında istenen şifredir. User Moda giriş için kullanılır. Console şifresi tanımlamak için yazılması gereken kodlar aşağıdaki gibidir.

Komut	Açıklama
CihazYeniAdi(config)#line console 0	console konfigurasyon ekranına giriş yapar
CihazYeniAdi(config-line)#password Password	Giriş için şifreyi “Password” olarak belirler

CihazYeniAdi(config-line)#login	Şifreyi aktifleştirir, login komutu girilmezse şifre aktifleşmeyecektir.
CihazYeniAdi(config-line)#exit	çıkış yapar

- Ayrıcalıklı EXEC modu Şifresi
  Kullanıcı modundan enable komutu ile ayrıcalıklı moda geçiş için kullanılacak olan şifredir. password ve secret olmak üzere iki türü bulunmaktadır.

  - password şifresi
    Ayrıcalıklı moddan ayrıcalıklı moda geçişte kullanılır. Konfigurasyon dosyasında düz metin olarak tutulur. Ayarlamak için aşağıdaki kodları yazmak gerekmektedir. Aktifleştirme için login komutu şart değildir.

    Daha önceki adımda User şifresini belirlediğimiz için user moda girişte öncelikli olarak şifreyi istiyor.

    CihazYeniAdi(config)#enable password 123456 : Şifreyi 123456 olarak belirler.

  - secret şifresi
    password şifresi ile aynı işlemi yapar ancak konfigurasyon dosyasında şifreli olarak tutulur. Ayarlamak için "CihazYeniAdi(config)#enable password 123456" komutunda password yerine secret kelimesi yazılır.
    Password ve secret beraber etkinleştirilirse secret baskın çıkar.
    CihazYeniAdi(config)#enable secret 123456

Şifreler ayarlanıp show running-config komutu ile çalışan konfigurasyon dosyası gösterildiğinda:

CihazYeniAdi#show running-config
Building configuration…

```
Current configuration : 1141 bytes
!
version 12.2
no service timestamps log datetime msec
no service timestamps debug datetime msec
no service password-encryption
!
hostname CihazYeniAdi
!
enable secret 5 $1$mERr$H7PDxl7VYMqaD3id4jJVK/
enable password 123456
…..
```

Görüldüğü gibi password ve secret ikisi de 123456 olarak ayarlanmasına rağmen secret şifrelenmiş olarak görünüyor.

- Telnet (VTY) Şifresi
  Cihaza telnet bağlantısı yapılırken sorulacak olan şifredir. Telnet şifresi yapılandırılmamış bir cihaza kesinlikle telnet bağlantısı yapılamaz. Telnet şifresi yapılandırmak için gerekli olan kodlar aşağıdaki gibidir:

Yapılan bütün bu işlemler RAM üzerinde tutulmaktadır. yapılandırılan şifrelerin kalıcı hale gelmesi için ayarların ROM üzerine kaydedilmesi gerekmektedir. Bunun için gerekli olan kod aşağıdadır.

Kali Linux Kullanıcı Şifresi

Değiştirme

Kali Linux üzerinde kullanıcı şifresi değiştirmek için;

- Root şifresi değiştirme

1. Terminalde **passwd** yazarak Enter'a basın

2. Yeni şifreyi yazıp Enter'a basın ardından şifreyi doğrulamak için tekrar yazıp Enter'a basın.

- Root dışında bir kullanıcının şifresini değiştirme

1. Terminalde **passwd kullaniciAdi** yazıp Enter'a basın.

2. Yeni şifreyi yazıp Enter'a basın ardından şifreyi doğrulamak için tekrar yazıp Enter'a basın.