Uzak OPC DA Hızlı Başlangıç Rehberi (DCOM)

Kepware Technologies

Remote OPC DA Quick Start Guide (DCOM)

October, 2010

Ref. 02.08'den çevrilmiş ve sadeleştirilmiştir.

06/2017

İçindekiler

1. Giriş 2
2. Kullanıcılar ve Gruplar 2
3. Sunucu Runtime'ı 5
4. DCOM Yapılandırması 6
   4.1. Uygulama Yapılandırması 6
   4.2. Uygulama Kimliğini Yapılandırma (Opsiyonel) 9
   4.3. Sistem Yapılandırması 10
5. Güvenlik Duvarı 12
6. Yerel Güvenlik İlkesi 13
   6.1. Yerel Hesaplar için Paylaşım ve Güvenlik Modeli 13
   6.2. Anonim Kullanıcılara Everyone İzinleri Uygulansın 14
7. Özet 15

1. Giriş

Bu doküman Microsoft Windows XP Service Pack 2 ve sonraki sürümlerde çalışan OPC Sunucu ve İstemci arasında güvenli DCOM haberleşmesini hızlıca sağlayabilmek için gerekli bilgileri içermektedir.

DCOM Nedir?

Dağıtılmış Bileşen Nesne Modeli (**DCOM**), Bileşen Nesne Modelinin (**COM**) genişletilmiş bir sürümüdür. DCOM, farklı bilgisayarlardaki COM Bileşilenlerinin haberleşmesini sağlar. DCOM, bir ağ üzerinden paylaşılabilen standart paketler üretmeyi sağlayan Uzak Prosedür Çağrısı (**RPC**) yöntemini kullanır, böylece yerel makinenin getirdiği sınırlamalar ortadan kaldırılmış olur. DCOM güvenlik açığı oluşturabileceği için işlemler özenle yapılmalı ve sadece gerekli işlemlerle sınırlandırılmalıdır.

OPCEnum Nedir?

OPC Sunucu OPC'ye has bilgilerini registry'de saklar. OPC İstemcilerinin yerel makinede ve uzak makinelerdeki sunucuları bulabilmesi için, bu registry'ye erişim için standart bir yöntem olması gerekir. Bunun için OPC Derneği tarafından OPCEnum isminde bir bileşen sağlanmıştır. OPCEnum genellikle bir OPC Sunucu ile birlikte bilgisayara yüklenen bir program parçacığıdır. Sistem Servisi olarak çalışır ve makinedeki OPC Sunucuların taranmasını ve İstemci uygulamalara listelenmesini sağlar.

2. Kullanıcılar ve Gruplar

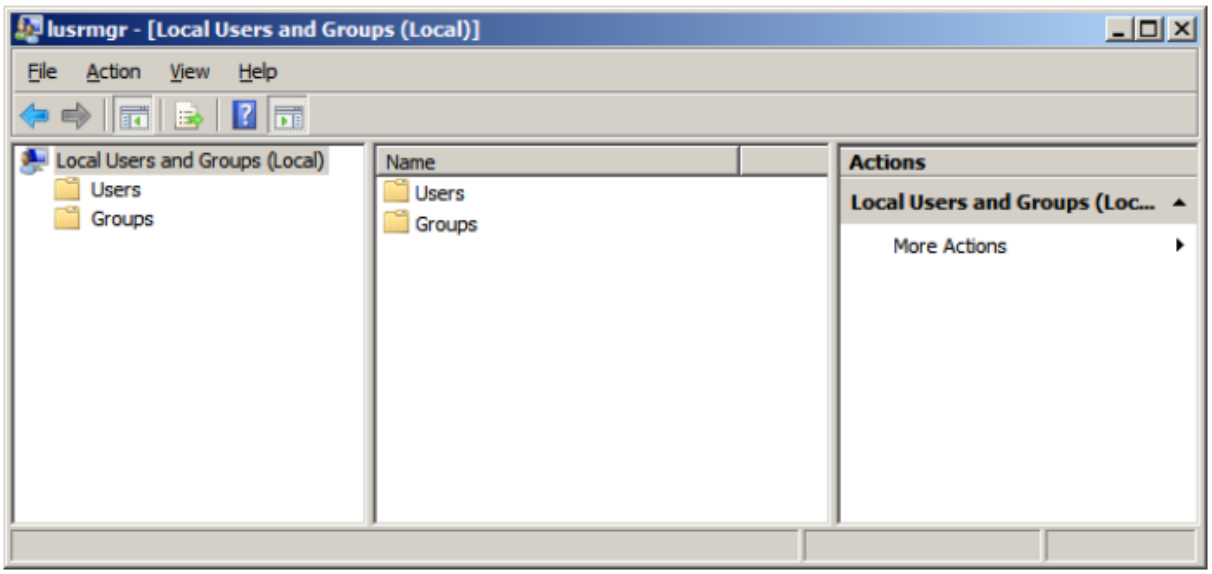
OPC Bağlantısının güvenli olduğundan emin olmak için bu amaca özel kullanıcı ve gruplar oluşturulmalıdır.

Bir **Workgroup** içerisindeki çalışılacaksa, bağlantı yapılacak her bilgisayara elle aynı kullanıcıların oluşturulması gerekir. Kimlik doğrulama için bu kullanıcıların şifrelerin de aynı olmalıdır, boş şifre çoğu zaman geçerli değildir. Yerel Güvenlik İlkelerinde değişikliğe gidilmesi gerekebileceği için, bir Workgroup içerisindeki uzak bağlantı en düşük güvenlikli uzak bağlantı olabilir. Daha fazla bilgi için Yerel Güvenlik İlkelerine göz atabilirsiniz.

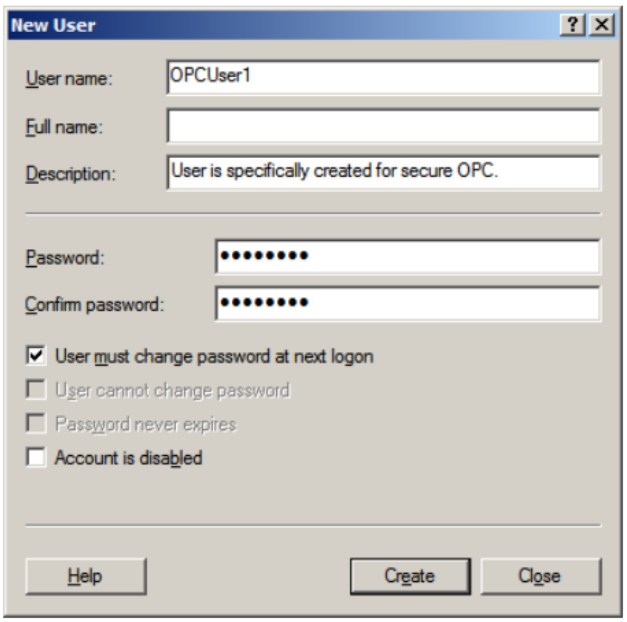
Bir **Domain** içerisinde çalışılacaksa, yerel kullanıcı ve grupların her bir bilgisayara eklenmesine gerek yoktur. Domainler kullanıcı hesap ve güvenlik bilgilerini içeren bir merkezi veri tabanı kullanırlar. Domain içerisindeki değişikliklerin bir ağ yöneticisi tarafından yapılması gerekir. **Domain** ve **Workgroup**'un bir arada olduğu durumlarda yerel kullanıcı hesapları domain bilgisayarına eklenmelidir.

Yerel Kullanıcı Ekleme

Local User and Groups bileşenini çalıştırın. Bileşene **Çalıştır**'a **lusrmgr.msc** yazarak ulaşabilirsiniz.



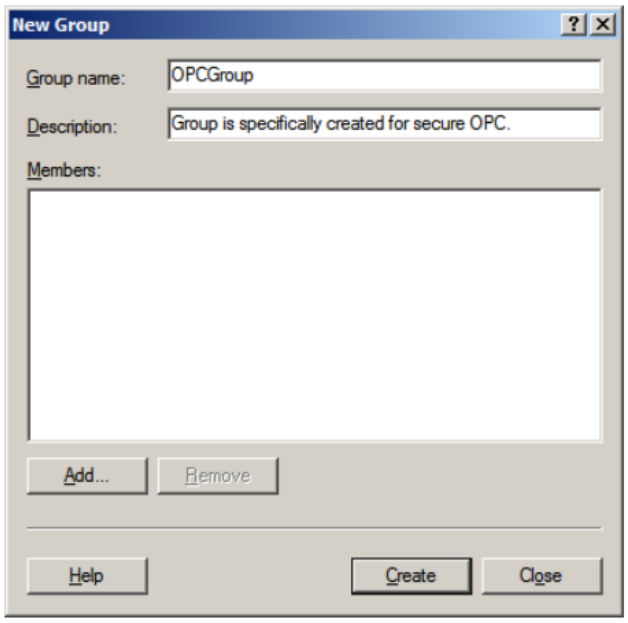
Users klasörüne sağ tıkladıktan sonra **New User**'a tıklayın.



Kullanıcı ismi, şifre, açıklama gibi bilgilerinizi doldurtan sonra, alttaki seçenekleri de isteğinize göre işaretleyin. Daha sonra **Create** butonuyla kullanıcıyı oluşturun.

Yerel Grup Oluşturma

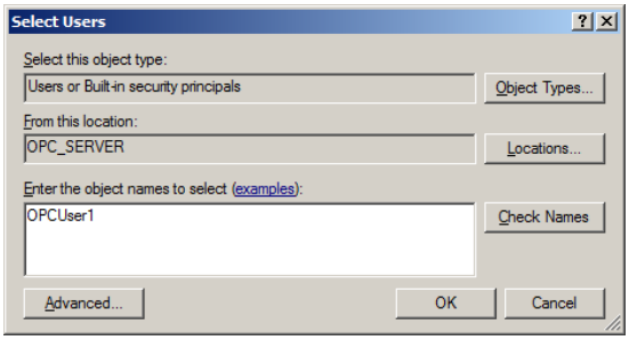
Local User and Groups bileşenini çalıştırın. Bileşene **Çalıştır**'a **lusrmgr.msc** yazarak ulaşabilirsiniz. **Groups** klasörüne sağ tıkladıktan sonra **New Group**'a tıklayın.



Grup ismi ve açıklama kısımlarını doldurduktan sonra **Create** butonuyla grubu oluşturabilirsiniz.

Gruba Kullanıcı Ekleme

Local User and Groups bileşenini çalıştırın. Bileşene **Çalıştır**'a **lusrmgr.msc** yazarak ulaşabilirsiniz. **Groups** klasörüne tıklayın ve listelenen gruplardan kullanıcı eklemek istediğinizi seçin. Sağ tıklayıp çıkan menüden **All Tasks | Add to Group** adımlarını izleyin ve açılan pencerede **Add**'e tıklayın.



Object Types kısmında eklemek istediğiniz kullanıcı tipini belirtin, **Locations** kısmında eklenen kullanıcın konumunu belirtin ve alttaki boş alana kullanıcı adını yazarak ya da **Advanced** seçeneğiyle kullanıcı arayarak eklemek istediğiniz kullanıcıyı giriniz. **Check Names** ve **OK**'e tıklayarak kullanıcı eklemeyi bitiriniz.

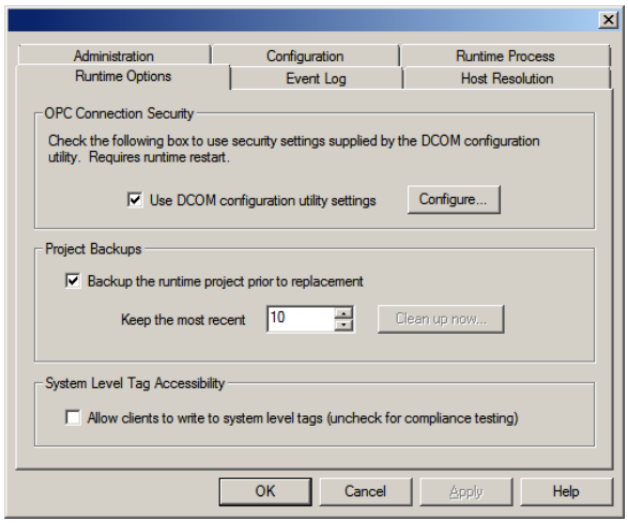
3. Sunucu Runtime'ı

DCOM Ayarları yapılandırılmadan önce hem güvenlik düzeyi hem de sunucunun işlem modu gözden geçirilmelidir. En yüksek güvenlik seviyesini sağlamak için uygun ayarlar seçilmelidir. Her mod değişiminde DCOM Ayarları sıfırlandığı için bu ayarlar DCOM yapılandırma öncesi belirlenmelidir. Detaylı bilgi için sunucunun yardım dosyasına göz atınız.

OPC Bağlantı Güvenliği

En yüksek güvenlik seviyesi için DCOM Runtime ayarlarında aktif edilmelidir. Bu seçenek varsayın olarak aktiftir. Bu seçenek DCOM Ayarlarının uygulandığından ve kullanıcı kimlik denetiminin gerçekleştiğinden emin olmanızı sağlar. Bu seçeneği pasif hale getirmeniz tavsiye edilmez.

Sistem çubuğundaki **Administration** ikonuna sağ tıklayın ve **Settings**'i seçin. **Administration** ikonu gözükmüyorsa **Başlat** aracılığıyla da ulaşabilirsiniz. Açılan pencereden **Runtime Options** sekmesini açın ve **Use DCOM configuration utility settings** seçeneğinin aktif olduğundan emin olun. Pasif durumda ise, aktif hale getirdikten sonra **Apply** ve **OK** adımlarını izleyin, Runtime'ın yeniden başlatılması istenirse yeniden başlatın.



İşlem Modu

Sunucu Runtime'ı ayrıca Interactive moduyle bir kullanıcı bilgileri altında çalışabilmektedir. Bu ayar varsayılan olarak Sistem Servisidir. Birkaç durum için Interactive modun kullanılması gerekebilir. Modlar arası geçiş için sunucunuzun yardım dosyasına göz atınız. *Bu geçişlerin DCOM ayarlarını sıfırlayacağını unutmayınız.*

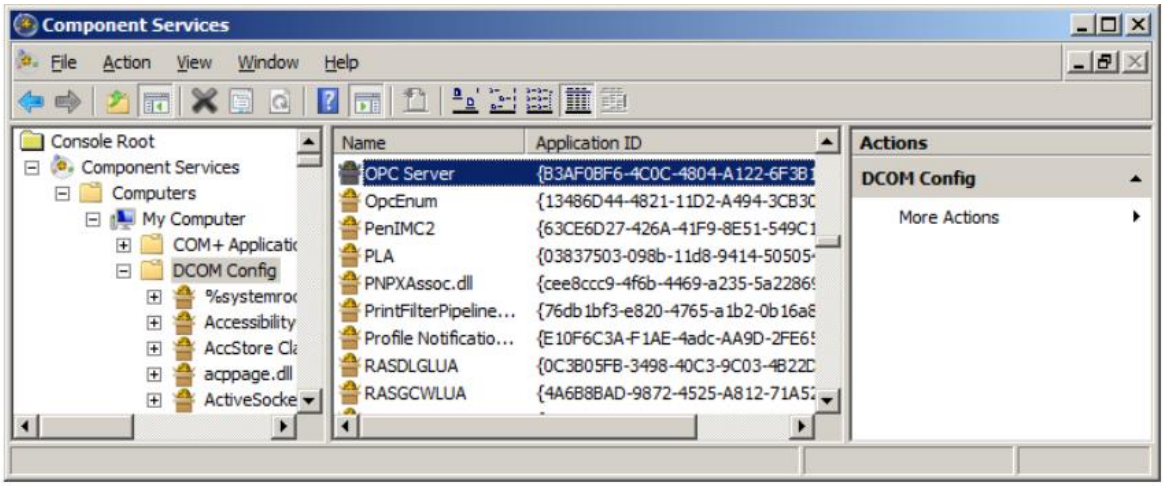
Uzak OPC Haberleşmesi için en tahmin edilebilir sonuçları Sistem Servisi modu vermektedir. Bu modda Runtime sistem başladığında başlayacak, herhangi bir kullanıcı girişine gerek duymayacaktır. Interactive modun kullanımı ek DCOM Ayarları gerektirmedir. Bu ek ayarlardan kaçınmak ve kimlik denetimini geçebilmek için en kısa yol, her iki bilgisayarda da bu DCOM Ayarının yapılandırıldığı kullanıcı ile oturum açmak olacaktır.

4. DCOM Yapılandırması

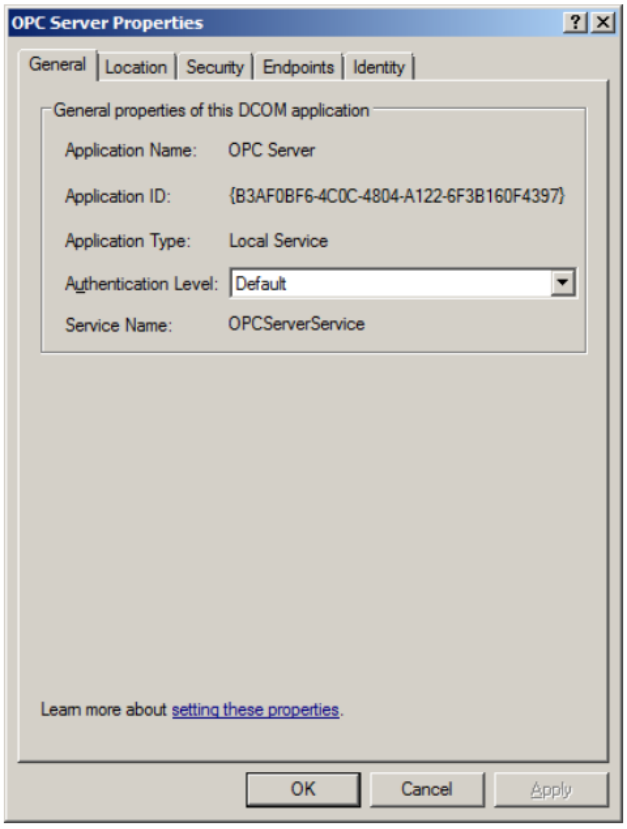
Uzak bağlantı yapılacak OPC Sunucu ve İstemci uygulamaların bulunduğu bilgisayarların her ikisinde uygulama ve sistem düzeyinden DCOM Ayarlarının yapılandırılması gereklidir. Bu yapılandırmaların işlenmesi için ayrıca bilgisayarlar yeniden başlatılmalıdır.

4.1. Uygulama Yapılandırması

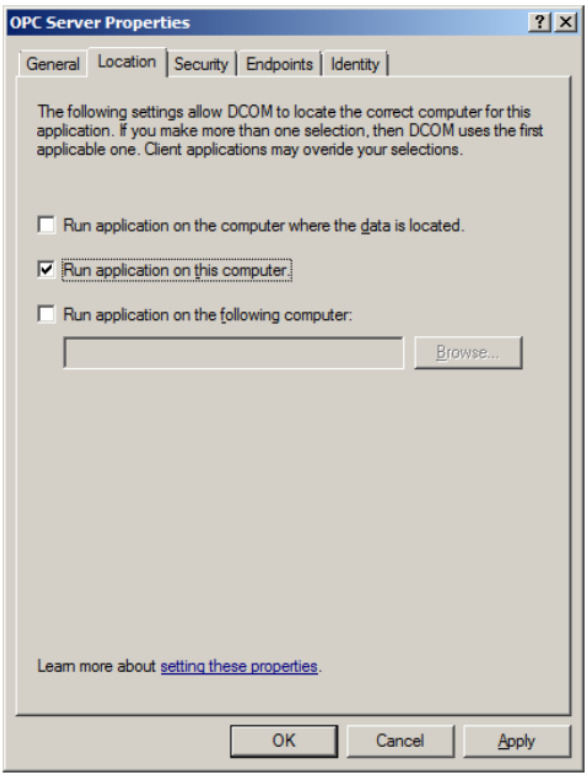
Component Services bileşenini çalıştırın. Bileşene **Çalıştır**'a **dcomcnfg** yazarak ulaşabilirsiniz. **Console Root, Component Services, Computers, My Computer** sekmelerini genişleterek **DCOM Config** klasörünü bulun.



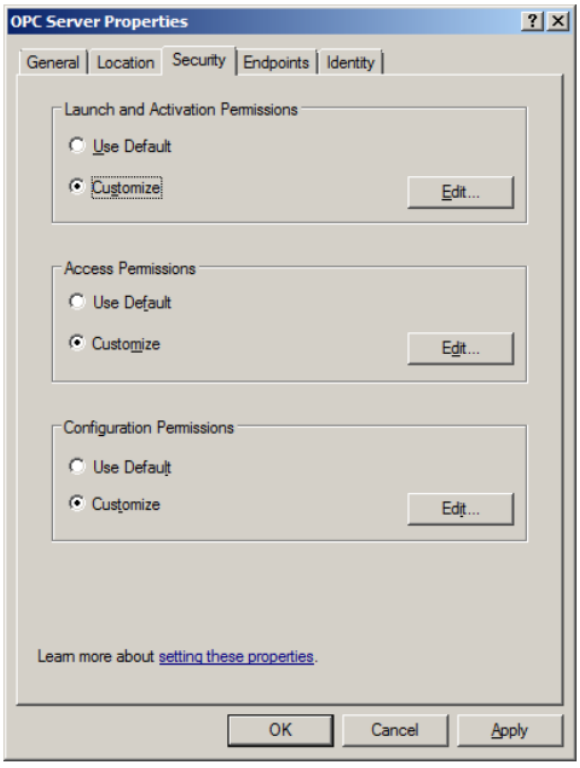
Gelen listeden OPC Sunucunuzu tespit edin. Örnek olarak yukarıdaki resimde "OPC Server" gösterilmiştir. Uygulamayı sağ tıklayın ve **Properties**'i seçin. Açılan pencerede **General** sekmesinde **Authentication Level**'i **None** yapın.



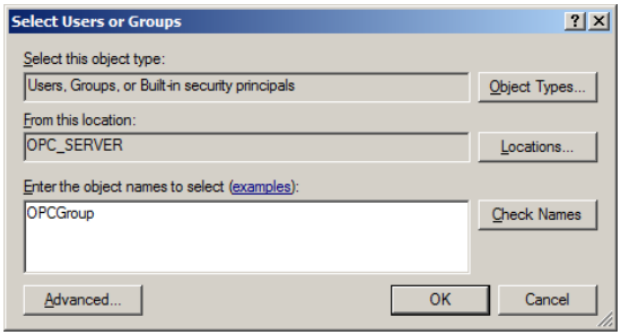
Location sekmesinde **Run application on this computer** sekmesinin aktif olduğundan emin olun.



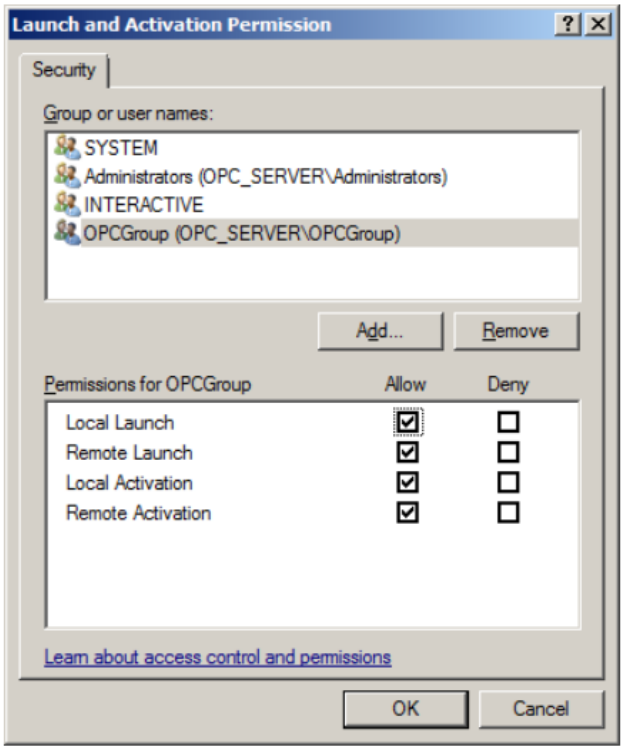
Security sekmesinde uygulama için kullanıcı yetkilendirmeleri verilir. Sistem düzeyinden DCOM Ayarları yapılandırılmışsa ya da yapılandırılacaksa **Launch and Activation Permissions** ve **Access Permissions** ayarları **Use default** olarak seçilebilir. Sadece uygulama düzeyinden yapılandırma yapılacak ise bu iki ayar ve her durumda **Configuration Permissions** ayarı **Customize** seçilmeli ve **Edit**'e tıklayarak kullanıcılar tanımlanmalıdır.



Edit penceresinde **Add**'e tıklanarak DCOM Yapılandırması için ayrılmış kullanıcı ya da gruplar ile birlikte **Administrator, Anonymous Logon, Everyone, Interactive, Network, Service, System** kullanıcıları eklenmelidir. Bu seçimler açılan pencereden **Advanced**'e tıklanarak topluca seçilebilir.



Kullanıcı ve grupların ekleme işlemlerinden sonra bu kullanıcıların her birinin izinlerinde **Allow** seçeneği işaretlenmelidir.



Her üç seçenek için de gerekli ayarlamalar yapıldıktan sonra **OK** denilerek işlem tamamlanır. Bu yapılan ayarların işlenmesi için bilgisayarların yeniden başlatılması gerekmektedir.

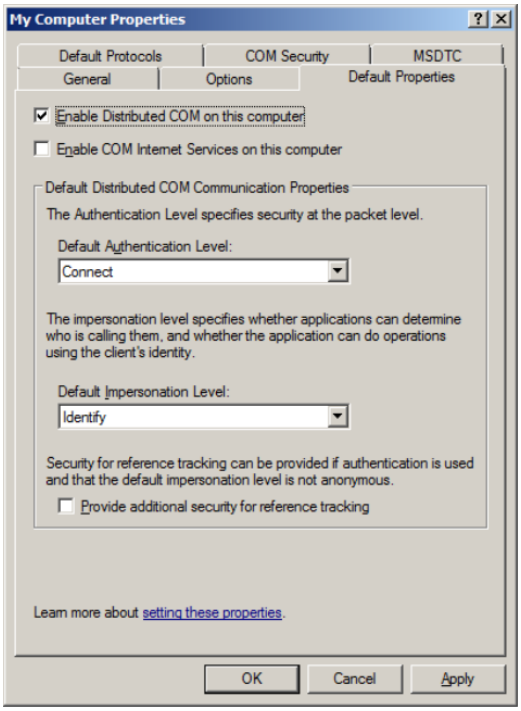
4.2. Uygulama Kimliğini Yapılandırma (Opsiyonel)

İşlem modunun Interactive olduğu durumlarda, sunucunun bulunduğu bilgisayarda birden fazla kullanıcı girişi olacaksa ya da bilgisayar DCOM izinleri verilmemiş bir kullanıcı tarafından kullanılacaksa **Identity** ayarı OPC Sunucu ve İstemci uygulamalar için yapılandırılmalıdır. Identity sekmesinde seçilecek **This user** seçeneği, uygulamanın bu kullanıcı kimliği ile çalıştırılmasını sağlar. Belirtilen kullanıcın oturum açmış olması gerek duyulmamaktadır. Bu kullanıcı ayrıca Administrators grubuna dahil olmalıdır.

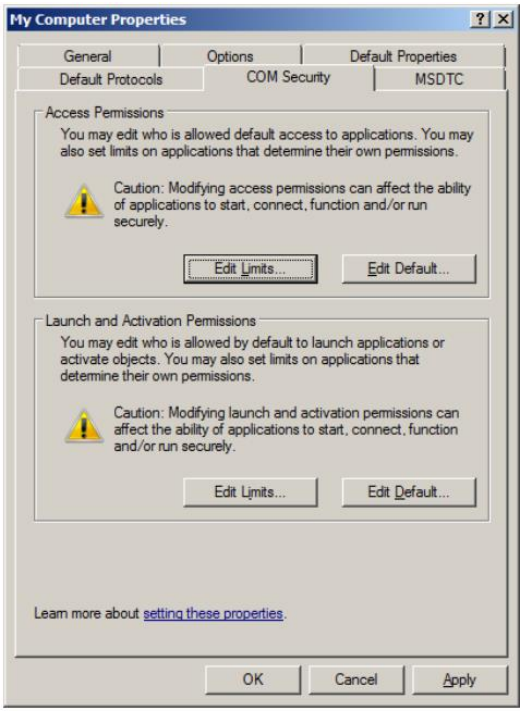
Yapılandırma işlemi için **Component Services** bileşenini çalıştırın. Bileşene **Çalıştır**'a **dcomcnfg** yazarak ulaşabilirsiniz. **Console Root, Component Services, Computers, My Computer** sekmelerini genişleterek **DCOM Config** klasörünü bulun. Bu klasör içerisinden DCOM yapılandırması yapılacak OPC Sunucu ya da İstemci uygulamaları bulun. Sağ tıklayarak **Properties** menüsünü açın. **Identity** sekmesinde **This user** seçeneğini ve DCOM ayarları yapılandırılmış olan kullanıcın bilgilerini giriniz.

4.3. Sistem Yapılandırması

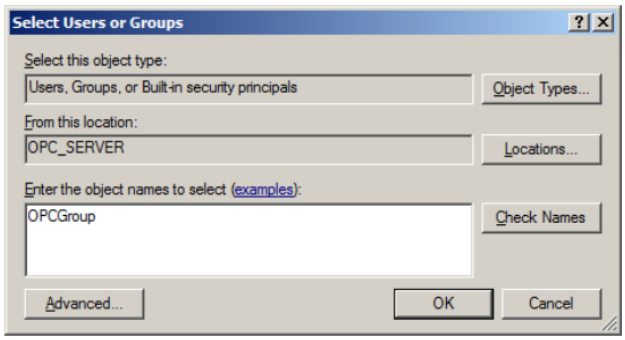
Component Services bileşenini çalıştırın. Bileşene **Çalıştır**'a **dcomcnfg** yazarak ulaşabilirsiniz. **Console Root, Component Services, Computers** sekmelerini genişleterek **My Computer**'ı bulun. Sağ tıklayarak **Properties**'i açın. **Default Properties** sekmesinde bulunan **Default Authentication Level** seçeneğini **None** ve **Default Impersonation Level** seçeneğini **Anonymous** seçiniz.



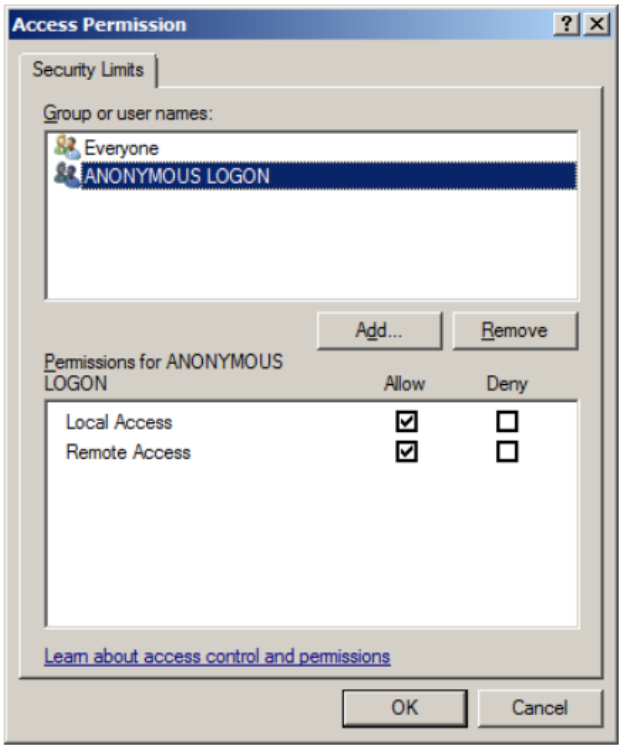
Daha sonra **COM Security** sekmesine geçiniz. **Access Permissions** ve **Launch and Activation Permissions** bölümlerindeki her bir **Edit Limits** ve **Edit Default** seçeneklerini bir sonraki adımda gösterildiği şekilde düzenleyiniz.



Edit seçeneklerinde **Add**'e tıklanarak DCOM Yapılandırması için ayrılmış kullanıcı ya da gruplar ile birlikte **Administrator, Anonymous Logon, Everyone, Interactive, Network, Service, System** kullanıcıları eklenmelidir. Bu seçimler açılan pencereden **Advanced**'e tıklanarak topluca seçilebilir.



Kullanıcı seçimleri yapıldıktan sonra **OK**'e basılır ve her bir kullanıcı için izinler **Allow** seçenekleri işaretlenerek verilir.



Her birinde gerekli ayarlamalar yapıldıktan sonra **OK** denilerek işlem tamamlanır. Bu yapılan ayarların işlenmesi için bilgisayarların yeniden başlatılması gerekmektedir.

5. Güvenlik Duvarı

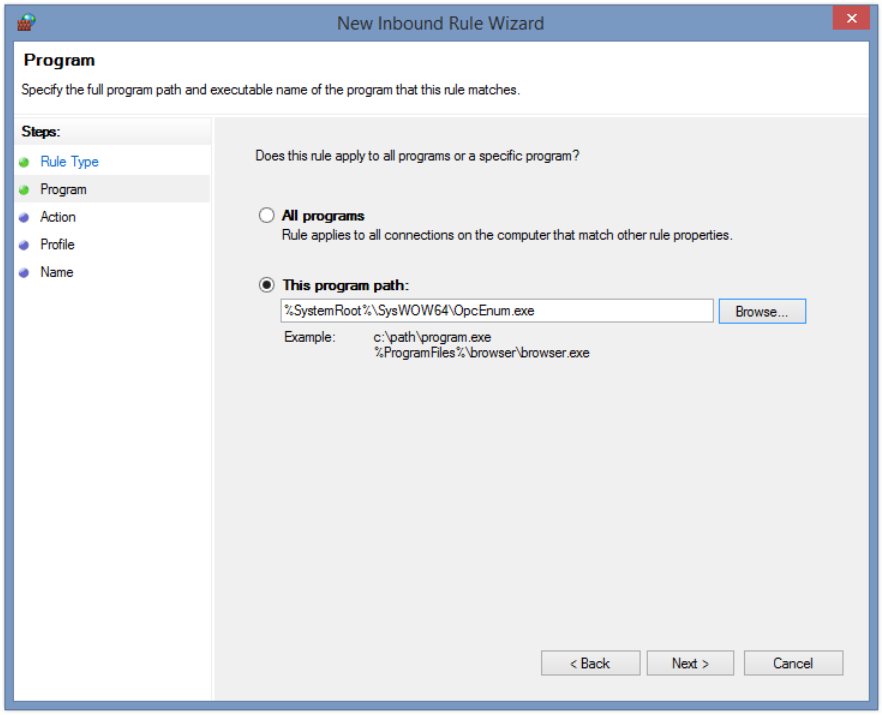
Çoğu durumda DCOM Ayarları yapılandırılmadan önce güvenlik duvarının kapatılması ve bağlantı sağlandıktan sonra eski ayarlara dönülmesi ve gerekli izinlerin sağlanması gerekmektedir.

Windows Güvenlik Duvarı Nedir?

Windows Güvenlik Duvarı, Microsoft Windows masaüstü ve sunucu yayınlarıyla birlikte gelen güvenlik duvarı servisidir. Windows XP Service Pack 2'ye kadar Internet Connection Firewall olarak adlandırılan bu servisin amacı, beklenmeyen ya da istisnalar içinde bulunmayan internet trafiğini kesmektir. Güvenlik duvarı yönetimi hem OPC Sunucunun hem İstemcinin bulunduğu bilgisayarda yapılmalıdır.

Program İzinleri

Çalıştır'a **firewall.cpl** yazarak **Windows Firewall**'u açın. Hem Inbound Rules hem de Outbound Rules için yeni bir kural ekleyin. **Rule Type** olarak **Program**'ı seçin.

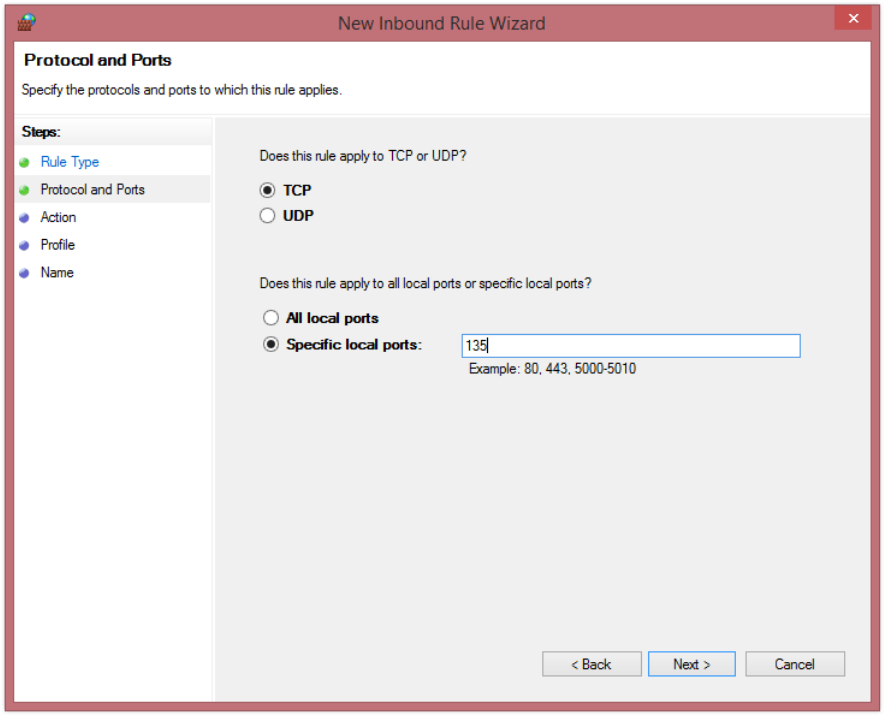


Daha sonra program yolu olarak C:\Windows\System32\ veya C:\Windows\SysWOW64\ klasörü altında bulunan **OPCEnum.exe** programını seçin. **Action** adımında **Allow the connection** seçimiyle ilerleyip, **Profile** adımında bağlantının sağlandığı ağın bulunduğu profili ya da tüm profilleri seçerek en son adımda bu kural için bir isim vererek OPCEnum.exe için izin işlemlerini sonlandırın.

Aynı işlemleri bilgisayarda bulunan OPC Sunucu ya da İstemci uygulaması için, o uygulamanın program yolunu belirterek yineleyin.

Port İzinleri

Çalıştır'a **firewall.cpl** yazarak **Windows Firewall**'u açın. Hem Inbound Rules hem de Outbound Rules için yeni bir kural ekleyin. **Rule Type** olarak **Port**'u seçin.



Daha sonra **Protocol and Ports** kısmında **TCP**'yi seçin ve **Specific local ports** kısmına 135 giriniz. **Action** adımında **Allow the connection** seçimiyle ilerleyip, **Profile** adımında bağlantının sağlandığı ağın bulunduğu profili ya da tüm profilleri seçerek en son adımda bu kural için bir isim vererek 135 Portu için izin işlemlerini sonlandırın.

6. Yerel Güvenlik İlkesi

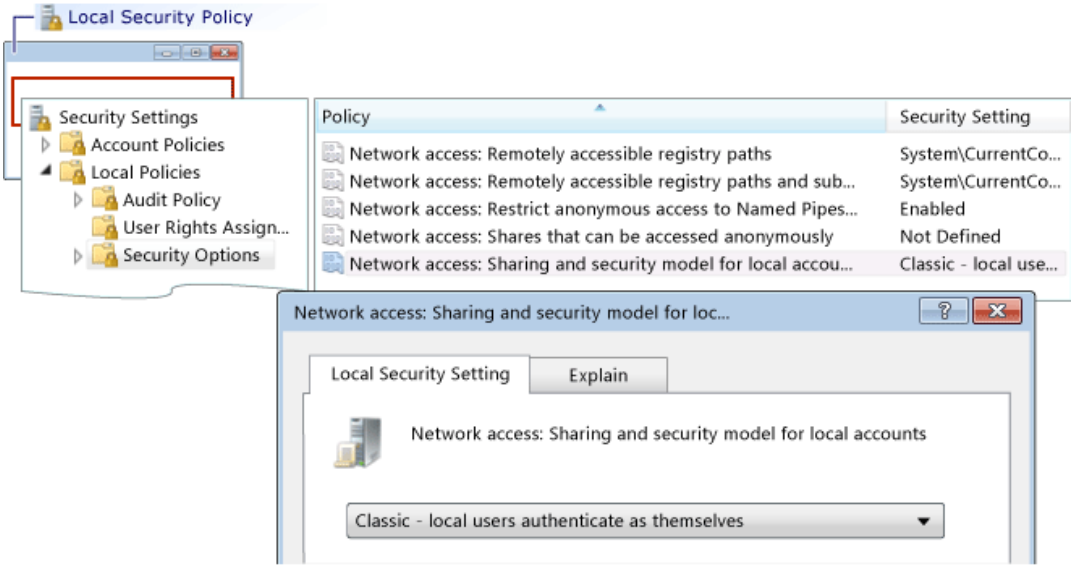
Uzak bilgisayarlar arsında sağlıklı bir haberleşme için **Yerel Güvenlik İlkesi**nin düzenlenmesi gerekebilir. Bu ayarlar güvenlik açığı oluşturabileceği için sadece gerekli durumlarda değiştirilmelidir. Çoğu durumda sunucu bilgisayarı kimlik denetimi sağlamak, istemci bilgisayar ise sunuculara göz atabilmek için bu ayarlara gereksinim duyar.

6.1. Yerel Hesaplar için Paylaşım ve Güvenlik Modeli

Bu ayar yerel kullanıcıların nasıl konumlandırılacağını belirler. **Klasik** seçili iken, uzaktan oturum açmalar, yereldeki aynı isme ve şifreye sahip oturum ile aynı seviyeye konumlandırılacaktır. **Sadece misafir** seçili iken, ağ oturum açmaları Misafir hesapları ile aynı seviyede konumlandırılacaktır.

OPC Sunucu bilgisayarında bu ayar **Classic** olarak seçilmelidir. İstemci tarafından alınan (HR=80070005) hata kodu bu ayarların düzenlenmesini işaret eder.

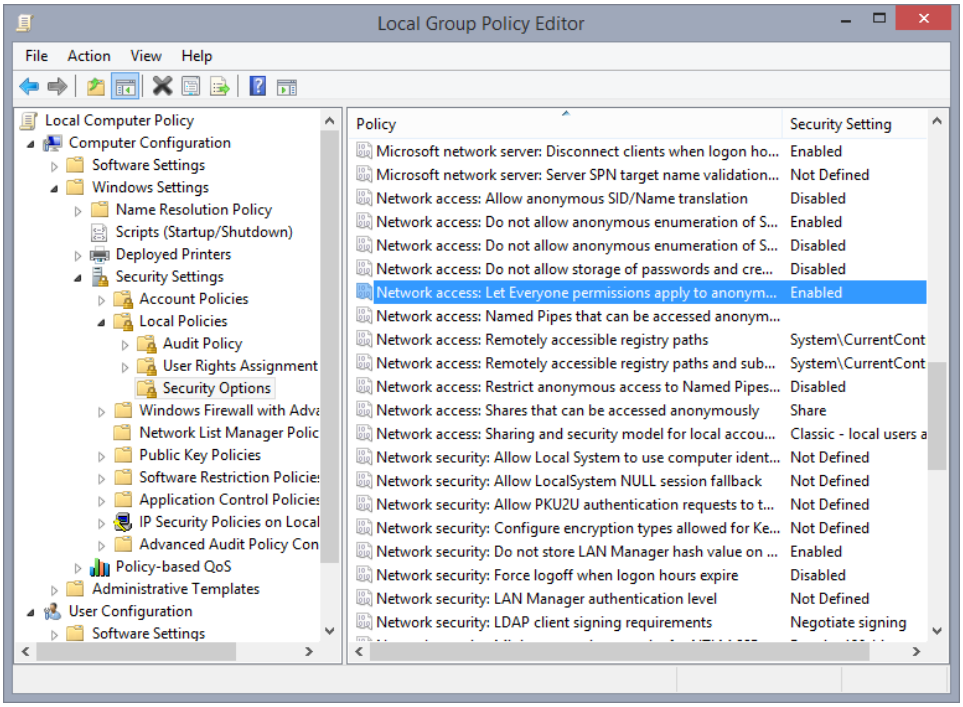
Yerel Güvenlik İlkelerine **Çalıştır**'a **secpol.msc** yazarak ulaşabilirsiniz. **Güvenlik Ayarları, Yerel İlkeler** sekmelerini genişleterek **Güvenlik Seçenekleri**'ni bulun. Burada Ağ Erişimi ile birlikte bulunan ilkeyi bulun ve ayarı **Klasik** yapınız.



6.2. Anonim Kullanıcılara Everyone İzinleri Uygulansın

Bu ayar anonim kullanıcılara ek izinleri verilmesini düzenler. Bu seçenek **Devre Dışı** ise Everyone kullanıcı için tanımlanan izinler anonim kullanıcılara uygulanmaz. Bu seçenek **Etkin** ise **Everyone** grubuna tanımlanan tüm izinler anonim kullanıcılara da tanımlanır. Everyone izinlerinin sadece istemci bilgisayarında düzenlenmesi gerekmektedir. DCOM Ayarları yapılandırıldığı halde bir İstemci uygulaması sunucuya ulaşamıyorsa bu ayar düzenlenmelidir.

Yerel Güvenlik İlkelerine **Çalıştır**'a **secpol.msc** yazarak ulaşabilirsiniz. **Güvenlik Ayarları, Yerel İlkeler** sekmelerini genişleterek **Güvenlik Seçenekleri**'ni bulun. Burada Ağ Erişimi ile birlikte bulunan ilkeyi bulun ve ayarı **Etkin** yapınız.



7. Özet

OPC protokol gereği uzak haberleşmelerde DCOM kullandığı için bu ayarların düzgün yapılması ciddi önem taşımaktadır. Kullanıcıların bu dokümandaki yönergeleri takip ederek güvenli bir haberleşme sağlayabilirler. Daha fazla bilgi için, http://www.opcfoundation.org/ adresini izleyerek OPC Derneğinin destek dokümanlarını inceleyebilirsiniz.