Cyberoam
A SOPHOS Company

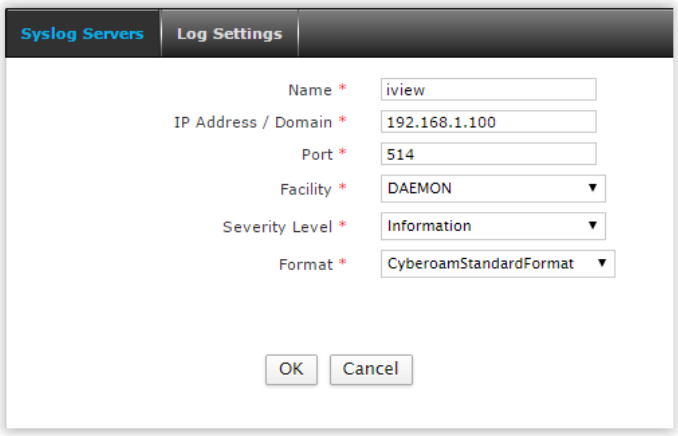
Harici Iview Kurulum

DMZ
Bilişim Teknolojileri

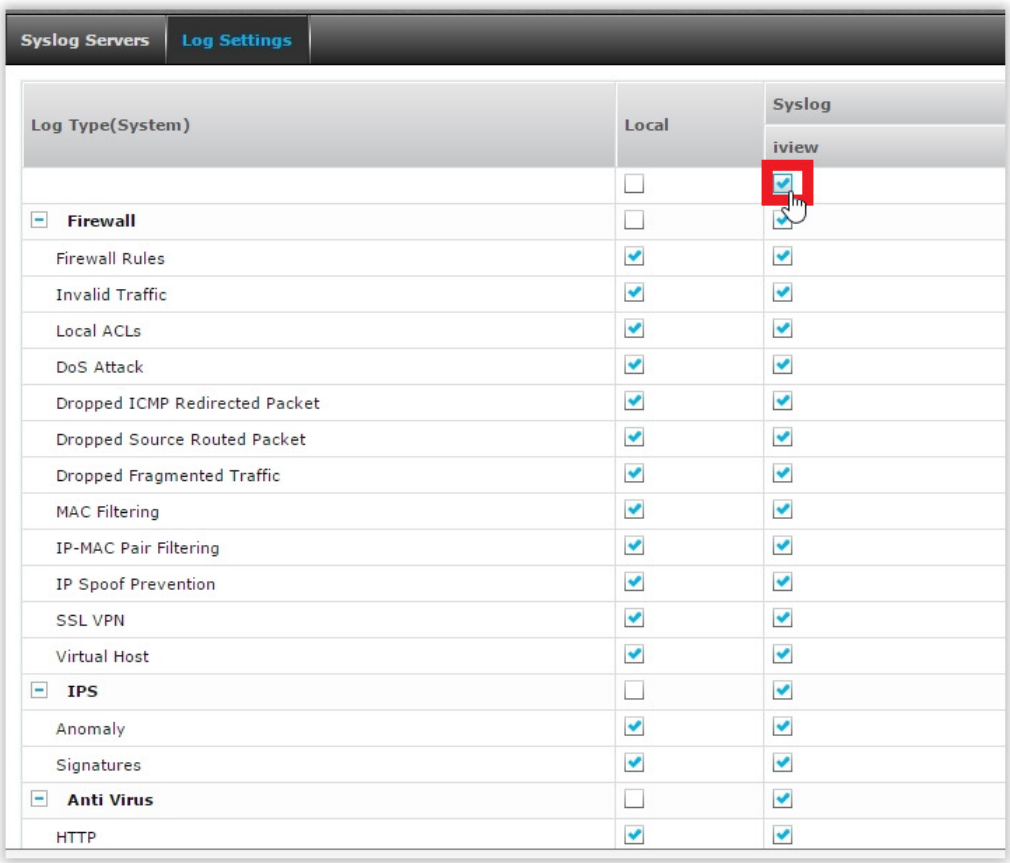
+90 (216) 688 77 33 (PBX)
destek@dmzbilisim.com
www.dmzbilisim.com

Cyberoam'a harici iview tanımlama:

Cyberoam arayüzüne bağlanarak menüdeki Log&Reports bölümünden Configuration bölümüne giriniz.
Syslog Servers sekmesinden add yaparak kurulumu yapacağımız sistemin ip' sini (örnek resimde 192.168.1.100 olarak verilmiştir ancak bu kısma iview yazılımını kuracağınız sistemin ip adresini girmelisiniz) ve ayarları yapılandırınız.



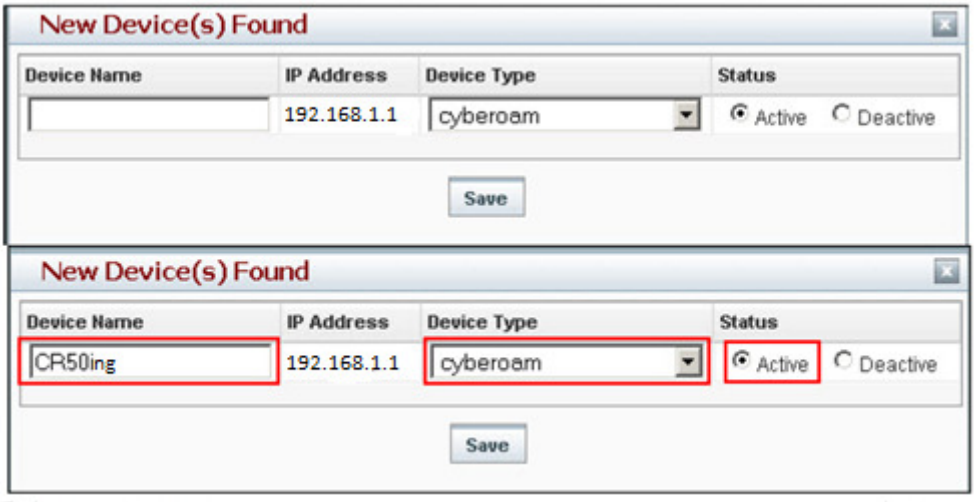
Cyberoam arayüzünden menüdeki Log&Reports bölümünden Configuration bölümü altında
Log Settings bölümünden eklemiş olduğumuz iview isminin altındaki(örnek resim için iview) tüm kutucukları işarteleyip uygulayınız.



System olarak Windows 7/XP/2003/2008 tercih edilebilir.
Iview setup dosyasını aşağıdaki linkten indirebilirsiniz.

http://www.cyberoam-iview.org/downloadiview.html

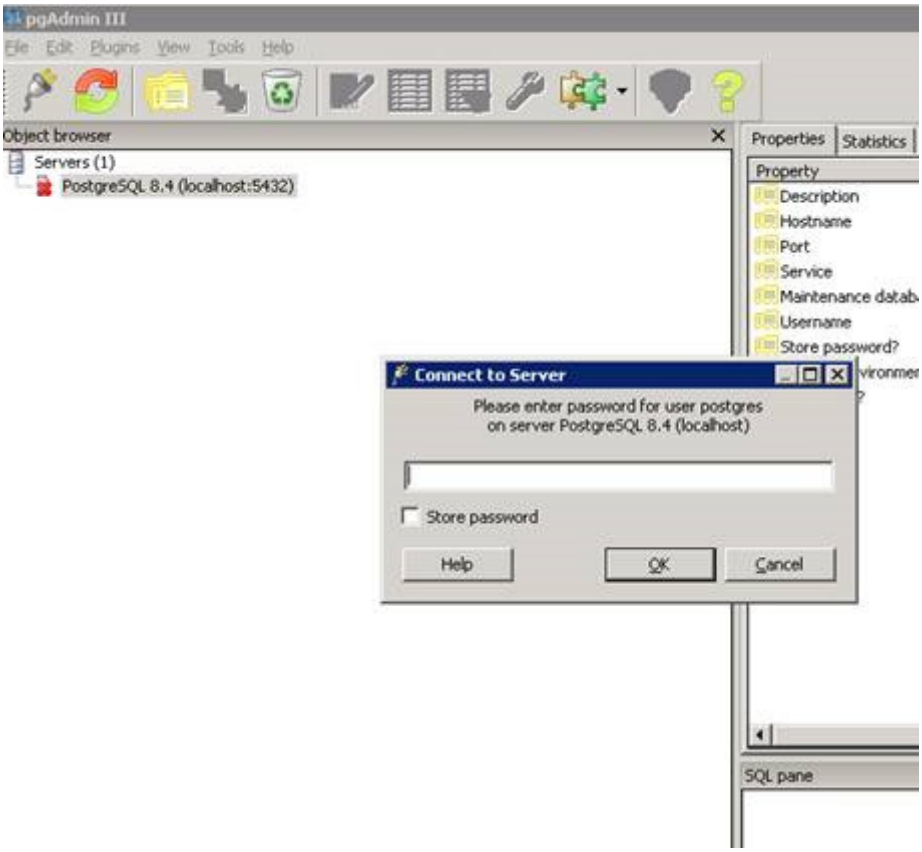
Kurulum sonrası "http://ip adres:8000" (http://localhost:8000) adresinden login oluyoruz
Önümüze gelen ekrandan cihaz ismini yazıp cihaz türüne Cyberoam seçip kaydediyoruz.



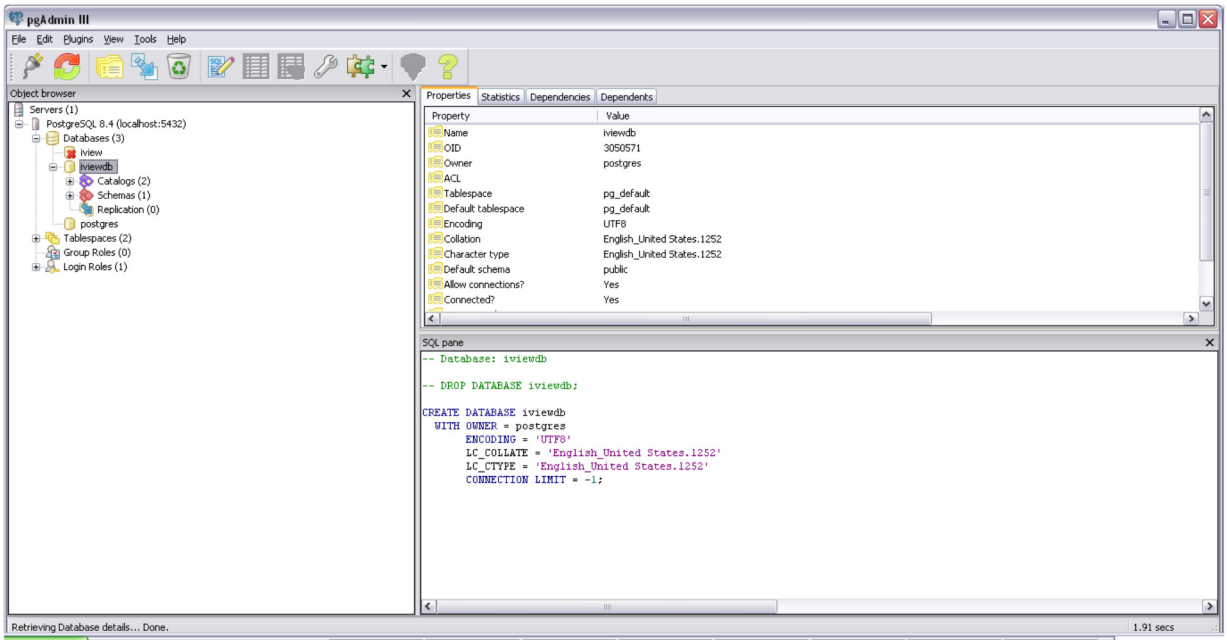
sonra iview'in 5651 ile ilgili loglarını ayrı bir klasöre toplamasını sağlamak için aşağıdaki adımları izlemeniz gerekmektedir..

iView ile 5651 uyumluluğu hk.

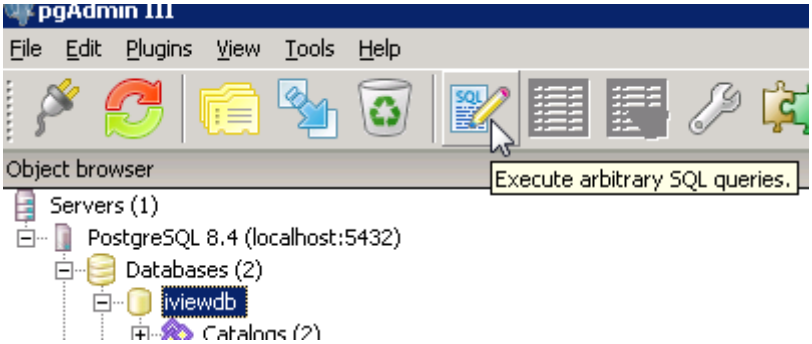
1- iView windows Servisini durdurunuz.
2- Postgres programının kurulu olduğu C:\iView\PostgreSQL\8.4\bin dizinine gidiniz.
3- pgAdmin3.exe çalıştırınız.
4- PostgresSQL8.4 SQL iki sefer tıklayınız.
5- Şifre isteyecektir, şifre bölümünü boş bırakıp enter yapınız.



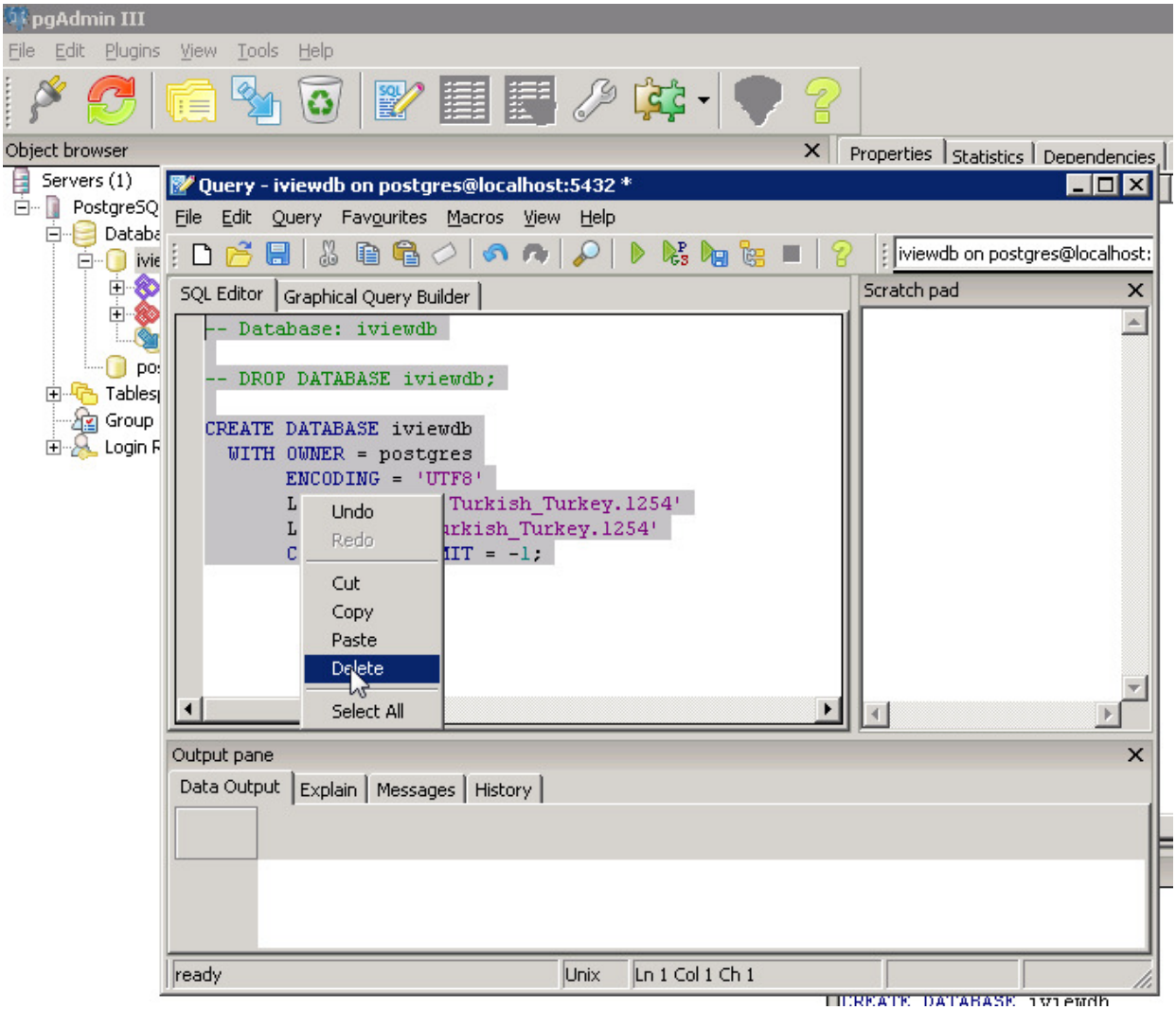
6- Databases tıklayın ve iViewDB açılacaktır.



7- Alt resimdeki SQL Button tıklayınız.

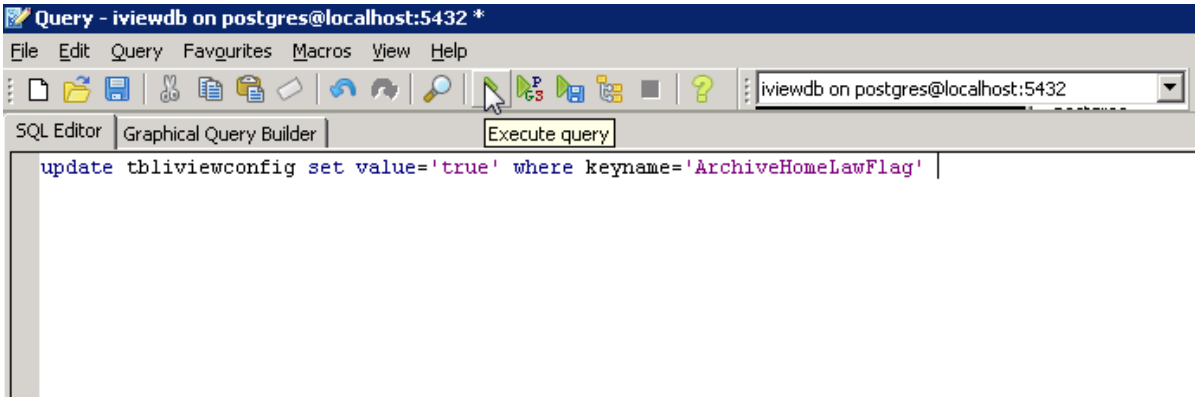


8- Önünüze gelen alan içeriği seçip siliniz.



9- Sildiğiniz alana **update tbliviewconfig set value='true' where keyname='ArchiveHomeLawFlag'** yazıp sorguyu çalıştırınız.

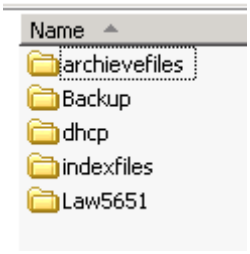
10- Query menüsüne gidip Execute çalıştırınız.



11- Çıkış ekranında "**Query returned successfully: 1 row affected, 0 ms execution time**" yazısını göreceksiniz.

12- iview yüklü olduğu klasörü açınız. Bu klasör içindeki archives klasörünü kopyalayarak aynı klasöre yapıştırınız. Aynı klasöre yapıştırdığınızda yeni klasör archives(copy) adında gelecektir. Öncelikle kopyaladığınız arcihves klasörünün adını değiştirerek archives_old yapınız. Sonrasında yeni kopyaladığınız arcihes(copy) klasörünün adını değiştirerek archives yapınız. Bu işlem klasör yetkilendirmesi için yaptığımız bir işlemdir. Klasör yetkilendirmesini alt klasörlerde tek tek yapmaktan daha kolay olduğu için kopyalama yöntemi ile anlatılmıştır.

13- Daha sonra iView servisini çalıştırınız.
14- Sonra 10-15 dakika sonra arşiv klasörüne gidin ve LAW5651 klasörünün oluştuğunu ve logların burada yer aldığını göreceksiniz.



15- Logların imzalanması için Zamanbaz programını kurarak oluşan Law5651 klasörünü seçiniz. Bu adımlar için Zamanbaz kurulum dokümanımızı takip edebilirsiniz.