**[Merkezi Kimlik Yönetimi Servisi (IDM Service - Identity Management Service)](http://wiki.logo.com.tr/pages/viewpage.action?pageId=65131821)**

Uygulamaların kullanıcı veritabanını tutarak, kullanıcı kayıt ve giriş işlemleri güvenli olarak yönetir.

**Genel Bakış**

Logo PaaS platformunda kullanıcı yönetimi işlemlerini yerine getirir. IDM servisi, kullanıcı arayüzü veya API uçları ile uygulamanıza entegre edilebilir.

IDM servisi ortak kullanıcı havuzu yapısı ile platform servisleri ve uygulamalar arasında tek oturum açma (SSO - Single Sign On) desteği sunar. Kullanıcı oturum kapatma(log out) işleminde kullanıcıyı ister ilgili uygulamadan, isterseniz tüm PaaS uygulamalarından çıkış yaptırabilirsiniz.

Uluslararası Oauth 2.0 protokoküne uygun olarak erişim bileti (access token) ve şifre onayı (password grant) operasyonlarını destekler. Bu protokoI yardımıyla, IDM servisi üzerinden diğer kimlik yönetim sistemlerinde kayıtlı (Google, Facebook ) kullanıcılar ile giriş yapabilirsiniz. IDM servisi, son kullanıcılara ait şifreleri veritabanında şifrelemektedir. Geliştiriciler veya operasyon ekipleri bu şifrelere hiç bir şekilde erişemez. Şifre değiştirme işlemleri son kullanıcı tarafından onay mekanizması ile değiştirilebilir.

**Kullanım Senaryoları**

* Merkezi Kullanıcı Listesini Oluşturma
* Kullanıcı Kayıt İşlemleri
* Kullanıcı Oturum Açma (Login)
* Kullanıcı Oturum Kapatma (Logout)
* Güvenli Şifre Kayıt
* Şifre Sıfırlama
* Excelden Kullanıcı Aktarımı
* Dil Değiştirme
* Kullanıcı Bilgilerini Güncelleme
* Kullanıcı Eşleme
* Şifre Değiştirme Kuralları
* Mail Şablonları
* IDP Sağlayıcısından Kullanıcı Aktarımı

**Kullanım Senaryoları Detaylar**

**Kullanıcı Listesi**

**Test Case1: Kullanıcı Listesine Tıklama**

**Step1: IDM adresine gidilip, geçerli bir kullanıcı adı ve geçerli bir şifre ile oturum açılır.**

**Step2: Anasayfada yer alan Kullanıcı Listesine tıklanır.**

**Step3: Kullanıcı listesi görüntülenir.**

**Test Case2: Kullanıcı Listesi Bütün Kayıtları Görüntüleme**

**Step1: IDM adresine gidilip, geçerli bir kullanıcı adı ve geçerli bir şifre ile oturum açılır.**

**Step2: Anasayfada yer alan Kullanıcı Listesine tıklanır.**

**Step3: Kullanıcı listesindeki bütün kayıtları görüntülemek için ya listenin en altında bulunan sayfa numaralarına tıklanır ya da ok işaretine tıklanır.**

**Step4: Seçilen sayfadaki kullanıcı kayıtları görüntülenir.**

**Test Case3: Kullanıcı Listesini Görüntüleyip Menüye Geri Dönme**

**Step1: IDM adresine gidilip, geçerli bir kullanıcı adı ve geçerli bir şifre ile oturum açılır.**

**Step2: Anasayfada yer alan Kullanıcı Listesine tıklanır.**

**Step3: Sayfanın en alt sağ köşesindeki “Menüye Dön” butonuna tıklanır.**

**Step4: Anasayfaya dönülür.**

**Test Case4: Kullanıcı Listesinde Kullanıcı Adına Göre Arama Yapma**

**Step1: IDM adresine gidilip, geçerli bir kullanıcı adı ve geçerli bir şifre ile oturum açılır.**

**Step2: Anasayfada yer alan Kullanıcı Listesine tıklanır.**

**Step3: Kullanıcı Adı başlığının altındaki arama kutusuna ilgili kullanıcı adı yazılır.**

**Step4: Yazılan kullanıcı adına göre Kullanıcı listesi filtrelenmiş olarak görüntülenir.**

**Test Case5: Kullanıcı Listesinde Epostaya Göre Arama Yapma**

**Step1: IDM adresine gidilip, geçerli bir kullanıcı adı ve geçerli bir şifre ile oturum açılır.**

**Step2: Anasayfada yer alan Kullanıcı Listesine tıklanır.**

**Step3: Eposta başlığının altındaki arama kutusuna ilgili eposta adresi yazılır.**

**Step4: Yazılan eposta adresine göre Kullanıcı listesi filtrelenmiş olarak görüntülenir.**

**Test Case6: Kullanıcı Listesinde İsme Göre Arama Yapma**

**Step1: IDM adresine gidilip, geçerli bir kullanıcı adı ve geçerli bir şifre ile oturum açılır.**

**Step2: Anasayfada yer alan Kullanıcı Listesine tıklanır.**

**Step3: İsim başlığının altındaki arama kutusuna ilgili isim yazılır.**

**Step4: Yazılan isme göre Kullanıcı listesi filtrelenmiş olarak görüntülenir.**

**Test Case7: Kullanıcı Listesinde Soyisme Göre Arama Yapma**

**Step1: IDM adresine gidilip, geçerli bir kullanıcı adı ve geçerli bir şifre ile oturum açılır.**

**Step2: Anasayfada yer alan Kullanıcı Listesine tıklanır.**

**Step3: Soyisim başlığının altındaki arama kutusuna ilgili soyisim yazılır.**

**Step4: Yazılan soyisime göre Kullanıcı listesi filtrelenmiş olarak görüntülenir.**

**Test Case8: Kullanıcı Listesinde Kullanıcıların Aktiflik Durumunu Görüntüleme**

**Step1: IDM adresine gidilip, geçerli bir kullanıcı adı ve geçerli bir şifre ile oturum açılır.**

**Step2: Anasayfada yer alan Kullanıcı Listesine tıklanır.**

**Step3: Aktiflik durumu öğrenilmek istenen Kullanıcının satırı bulunur.**

**Step4: Aktif başlığının altında seçilen kullanıcının aktif ya da pasif olduğu öğrenilir.**

**Test Case9: Kullanıcı Listesinde Seçilmiş Bir Kullanıcıyı Aktive Etme**

**Step1: IDM adresine gidilip, geçerli bir kullanıcı adı ve geçerli bir şifre ile oturum açılır.**

**Step2: Anasayfada yer alan Kullanıcı Listesine tıklanır.**

**Step3: Aktif edilmek istenen kullanıcının satırı bulunur.**

**Step4: Satırın en başındaki check box a tıklanır.**

**Step5: Sayfanın alt kısmında bulunan “Seçili Kullanıcıları Aktive Et” butonuna tıklanır.**

**Step6: “1/1 Kullanıcı Başarı ile güncellendi” mesajı ekranda görülür ve ilgili kullanıcının Aktif başlığı altında “Evet” yazdığı doğrulanmış olur.**

**Test Case10: Kullanıcı Listesinde Seçilmiş Bir Kullanıcıyı Pasife Alma**

**Step1: IDM adresine gidilip, geçerli bir kullanıcı adı ve geçerli bir şifre ile oturum açılır.**

**Step2: Anasayfada yer alan Kullanıcı Listesine tıklanır.**

**Step3: Pasife alınmak istenen kullanıcının satırı bulunur.**

**Step4: Satırın en başındaki check box a tıklanır.**

**Step5: Sayfanın alt kısmında bulunan “Seçili Kullanıcıları Pasife Al” butonuna tıklanır.**

**Step6: “1/1 Kullanıcı Başarı ile güncellendi” mesajı ekranda görülür ve ilgili kullanıcının Aktif başlığı altında “Hayır” yazdığı doğrulanmış olur.**

**Kullanıcı Oturum Açma (Login)**

**Test Case1: Başarılı Oturum Açma**

**Step1: IDM adresine gidilir.**

**Step2: Geçerli bir kullanıcı adı ve şifre girilir.**

**Step3: “Giriş” butonuna tıklanır.**

**Step4: Başarıyla oturum açılır ve anasayfa ekranda gösterilir.**

**Test Case2: Başarısız Oturum Açma – Kullanıcı Adı**

**Step1: IDM adresine gidilir.**

**Step2: Geçersiz bir kullanıcı adı ve geçerli bir şifre girilip, “Giriş” butonuna tıklanır.**

**Step3: “Kullanıcı adı ya da şifre hatalı” mesajı ekranda gösterilir.**

**Step4: Kullanıcı anasayfaya yönlendirilmez ve login ekranında kalır.**

**Test Case3: Başarısız Oturum Açma – Şifre**

**Step1: IDM adresine gidilir.**

**Step2: Geçerli bir kullanıcı adı ve geçersiz bir şifre girilip, “Giriş” butonuna tıklanır.**

**Step3: “Kullanıcı adı ya da şifre hatalı” mesajı ekranda gösterilir.**

**Step4: Kullanıcı anasayfaya yönlendirilmez ve login ekranında kalır.**

**Kullanıcı Oturum Kapatma (Logout)**

**Test Case: Oturum Kapatma**

**Step1: IDM adresine gidilip, geçerli bir kullanıcı adı ve geçerli bir şifre ile oturum açılır.**

**Step2: Anasayfada yer alan “Çıkış” a tıklanır.**

**Step3: Oturum kapatma işlemi başarıyla gerçekleşir ve login ekranına dönülür.**

**Güvenli Şifre Kayıt**

**Test Case: Beni Hatırla Özelliği ile Şifre Kaydetme**

**Step1: IDM adresine gidilir.**

**Step2: Geçerli bir kullanıcı adı ve şifre girilir.**

**Step3: Şifre alanının altındaki “Beni Hatırla” check box ına tıklanır. Böylece kullanıcı adı girilince, şifre girmeden otomatik olarak şifre alanı doldurulmuş olur.**

**Step4: “Giriş” butonuna tıklanır.**

**Şifre Sıfırlama**

**Test Case1: Şifre Sıfırlama – Kullanıcı Adı**

**Step1: IDM adresine gidilir.**

**Step2: Giriş butonunun altındaki, “Şifremi Unuttum” a tıklanır.**

**Step3: Geçerli bir kullanıcı adı girilir.**

**Step4: “Şifremi Sıfırla” butonuna tıklanır.**

**Step5: “Hata: Kullanıcı adı ve eposta girilmelidir” mesajı ekranda gösterilir.**

**Test Case2: Şifre Sıfırlama – Eposta**

**Step1: IDM adresine gidilir.**

**Step2: Giriş butonunun altındaki, “Şifremi Unuttum” a tıklanır.**

**Step3: Geçerli bir eposta adresi girilir.**

**Step4: “Şifremi Sıfırla” butonuna tıklanır.**

**Step5: “Hata: Kullanıcı adı ve eposta girilmelidir” mesajı ekranda gösterilir.**

**Test Case3: Şifre Sıfırlama – Kullanıcı Adı & Eposta**

**Step1: IDM adresine gidilir.**

**Step2: Giriş butonunun altındaki, “Şifremi Unuttum” a tıklanır.**

**Step3: Geçerli bir kullanıcı adı ve eposta adresi girilir.**

**Step4: “Şifremi Sıfırla” butonuna tıklanır.**

**Step5: “Şifre sıfırlama bağlantısı e-posta adresinize gönderildi. Lütfen e-posta adresinizi control ediniz.” mesajı ekranda gösterilir.**

**Test Case4: Şifre Sıfırlama Oturum Açma Sayfasına Geri Dönme**

**Step1: IDM adresine gidilir.**

**Step2: Giriş butonunun altındaki, “Şifremi Unuttum” a tıklanır.**

**Step3: “Geri Dön” butonuna tıklanır.**

**Step4: Kullanıcı, Oturum Açma ekranına yönlendirilir.**

**Excelden Kullanıcı Aktarımı**

**Test Case1: Excelden Kullanıcı Aktarma**

**Step1: IDM adresine gidilip, geçerli bir kullanıcı adı ve geçerli bir şifre ile oturum açılır.**

**Step2: Anasayfada yer alan Kullanıcıları İçeri Al (Excel) e tıklanır.**

**Step3: “Kullanıcı aktarımı için bir \*.xlsx dosyası seçin” yazısının altında tıklanır ve yüklenmesi istenilen dosya seçilir.**

**Step4: Sol alt köşede yer alan “Yükle” butonuna tıklanır.**

**Test Case2: Excelden Kullanıcı Aktarma Menüye Geri Dönme**

**Step1: IDM adresine gidilip, geçerli bir kullanıcı adı ve geçerli bir şifre ile oturum açılır.**

**Step2: Anasayfada yer alan Kullanıcıları İçeri Al (Excel) e tıklanır.**

**Step3: Sağ alt köşedeki “Menüye Dön” butonuna tıklanır.**

**Step4: Kullanıcı, anasayfaya yönlendirilir.**

**Dil Değiştirme**

**Test Case: Dil Değiştirme**

**Step1: IDM adresine gidilir.**

**Step2: Logo ambleminin aşağısında yer alan ve üstünde “Türkçe” yazan combobox a tıklanır.**

**Step3: “English” seçilir.**

**Step4: Oturum Açma sayfasının tamamının ingilizce olarak gösterildiği doğrulanır.**

**Kullanıcı Bilgilerini Güncelleme**

**Kullanıcı Eşleme**

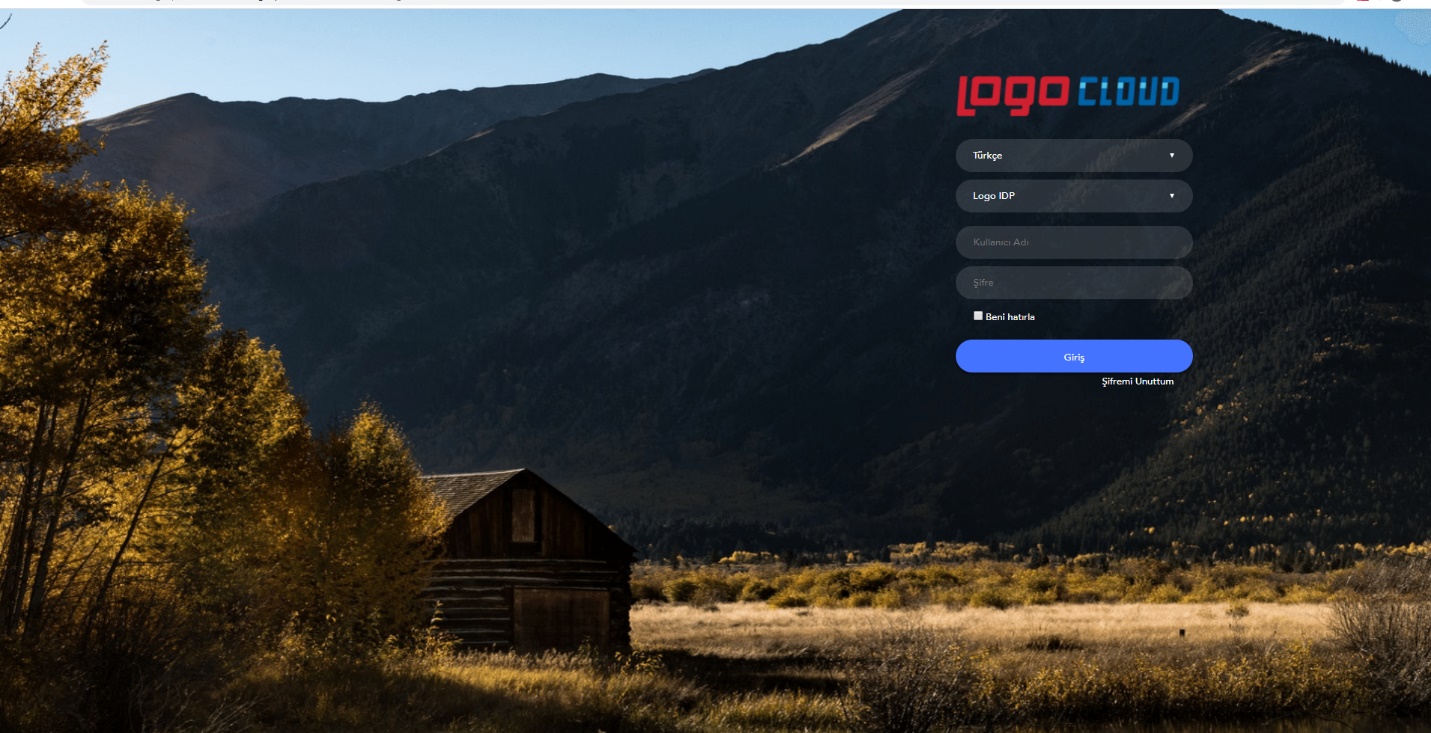
**Şifre Değiştirme Kuralları**

**Mail Şablonları**

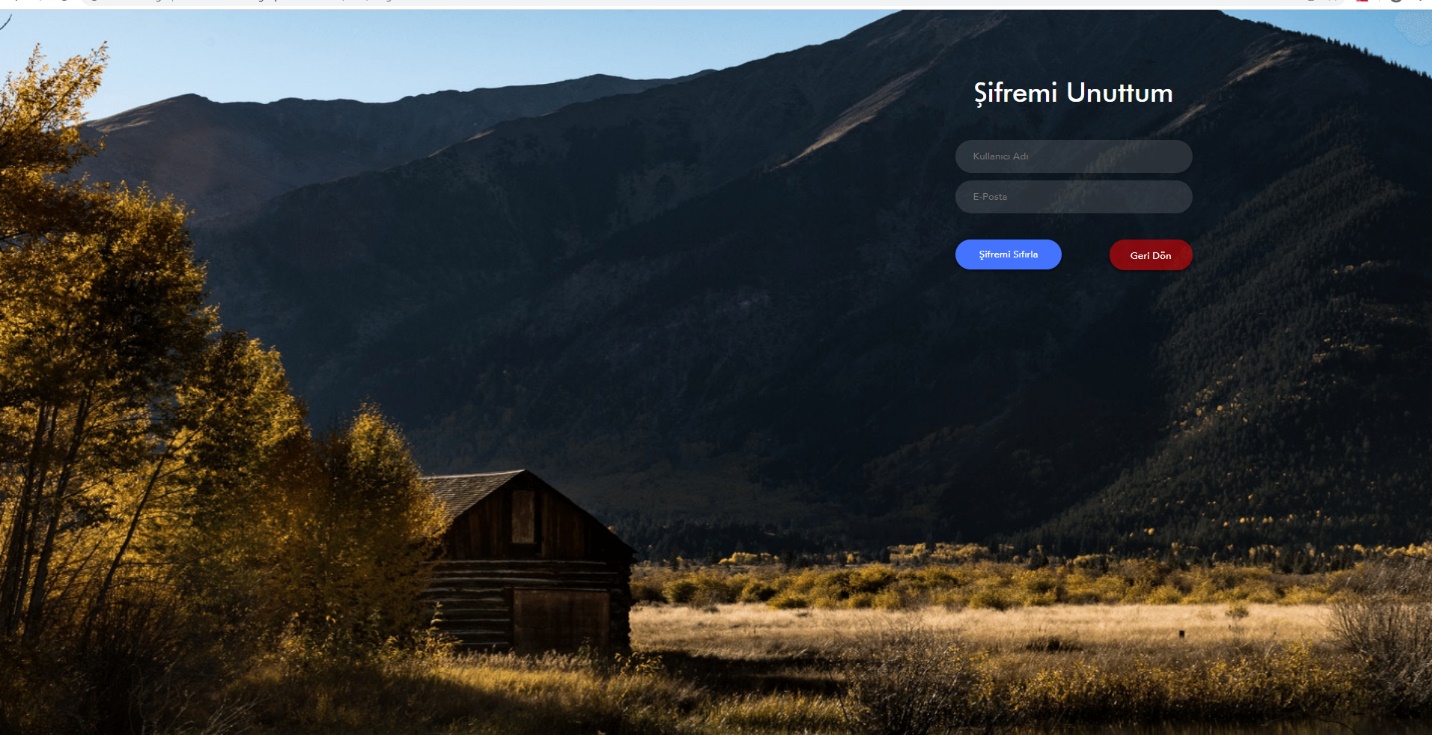
**IDP Sağlayıcısından Kullanıcı Aktarımı**

**Kullanıcı Arayüzü**

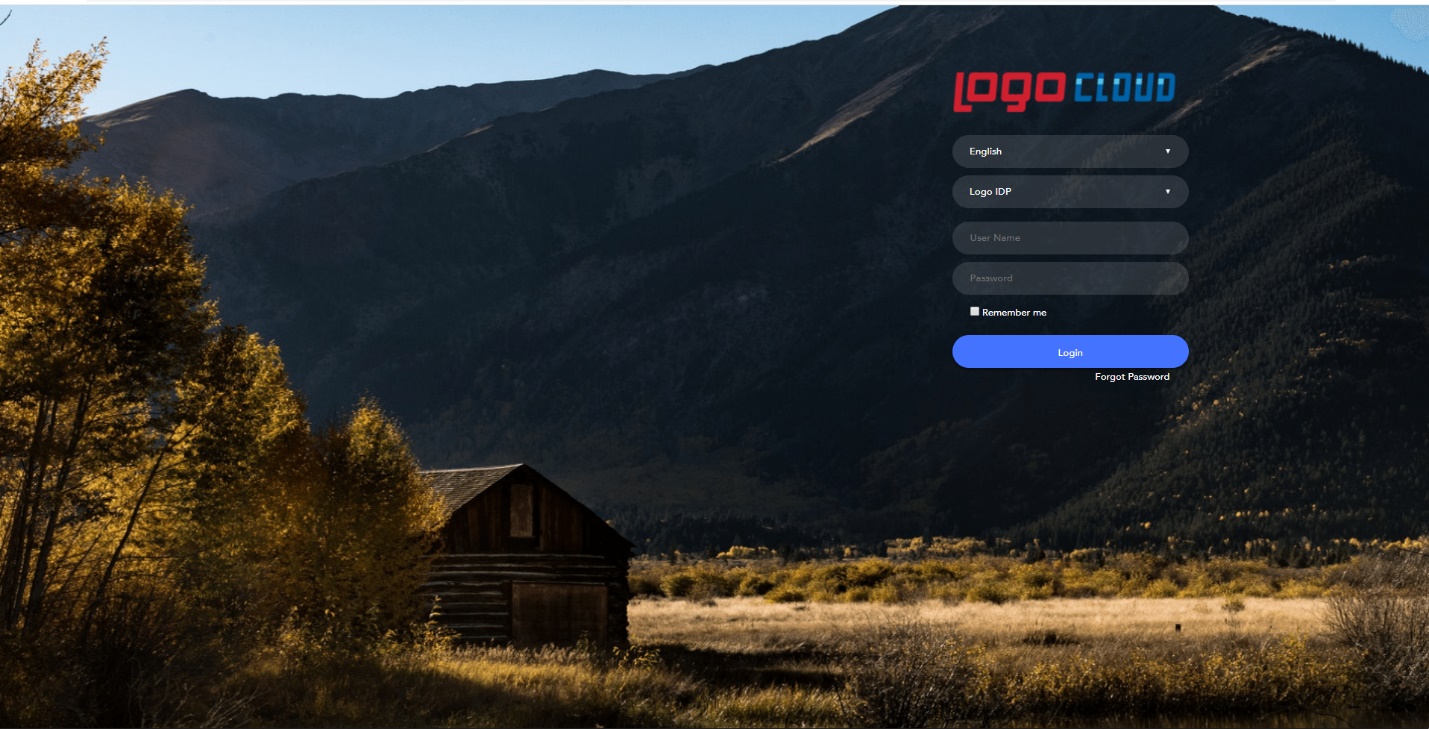
**Kullanıcı Oturum Açma**



**Şifremi Unuttum**



**Dil Değiştirme**



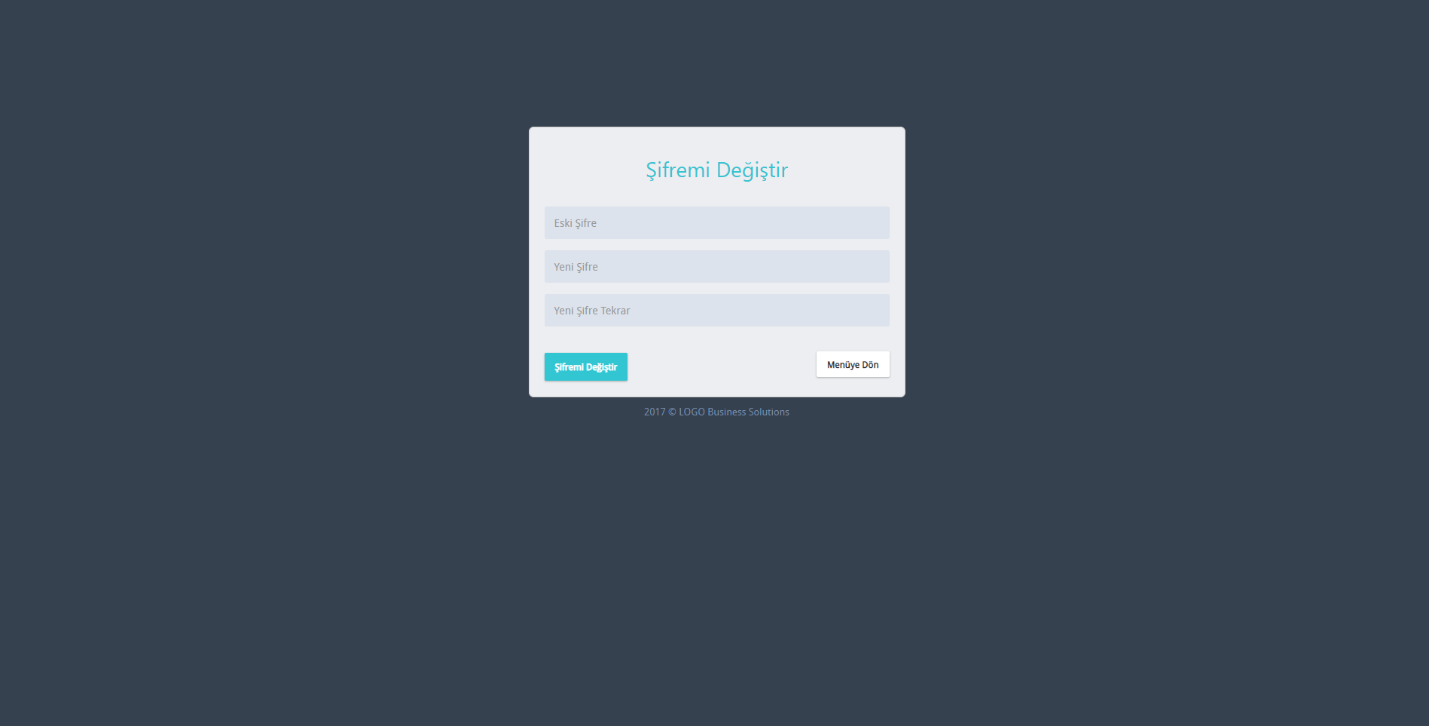
**Ana Sayfa**



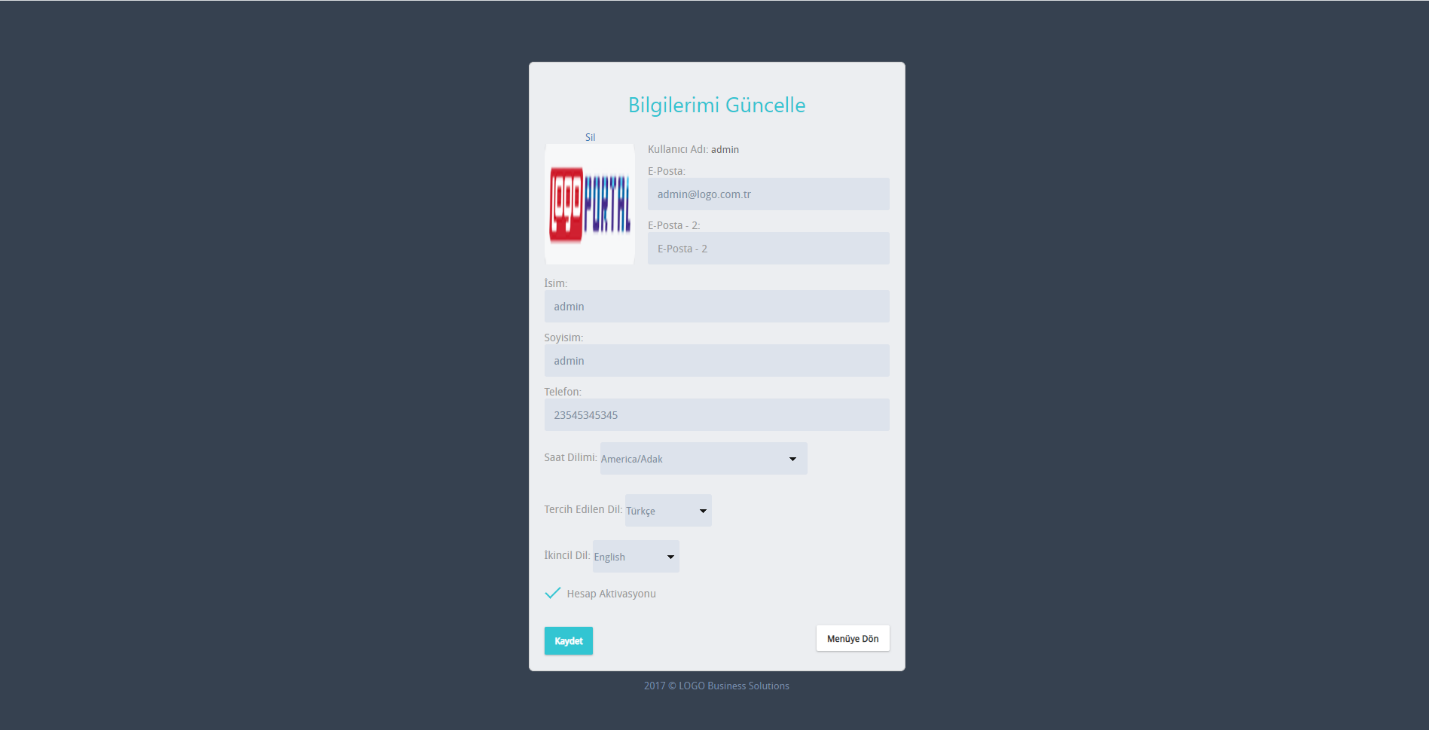
**Çıkış**



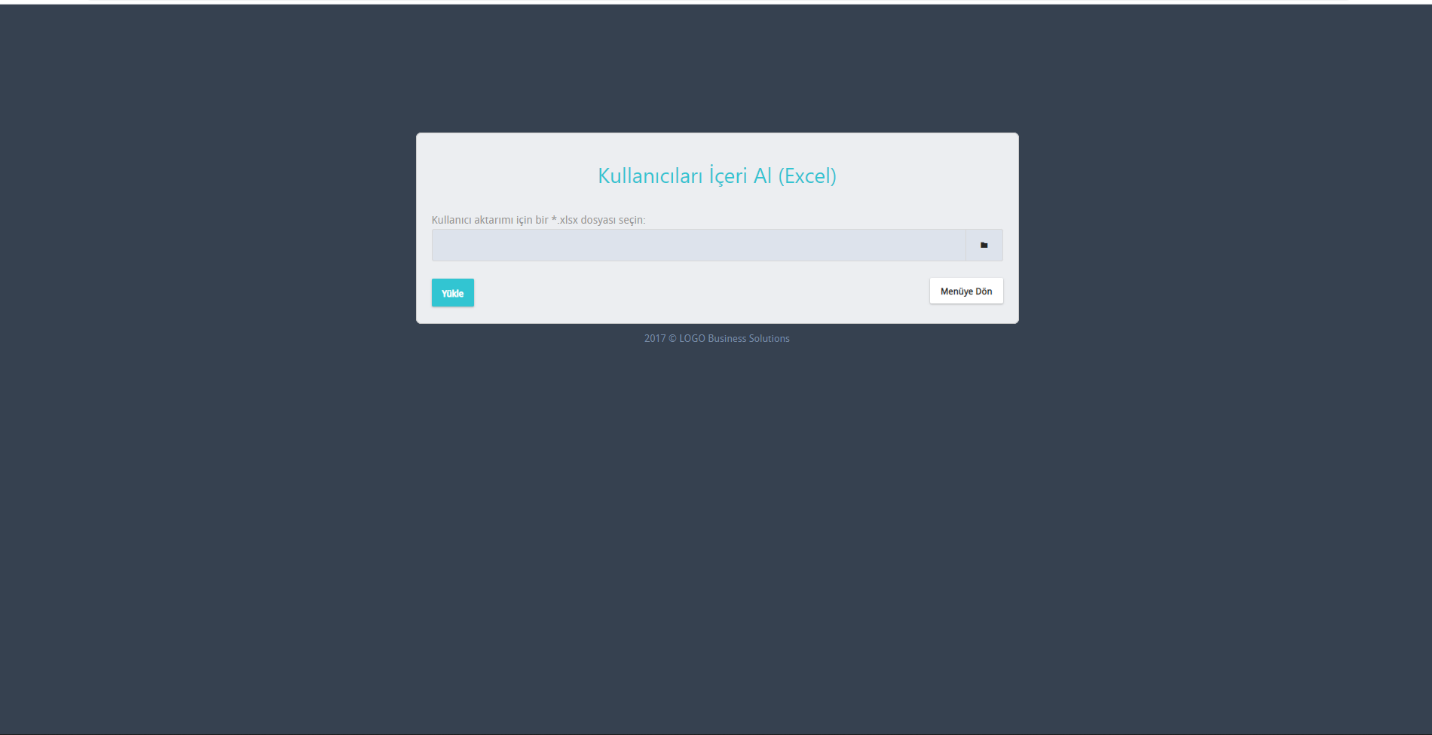
**Şifre Değiştir**



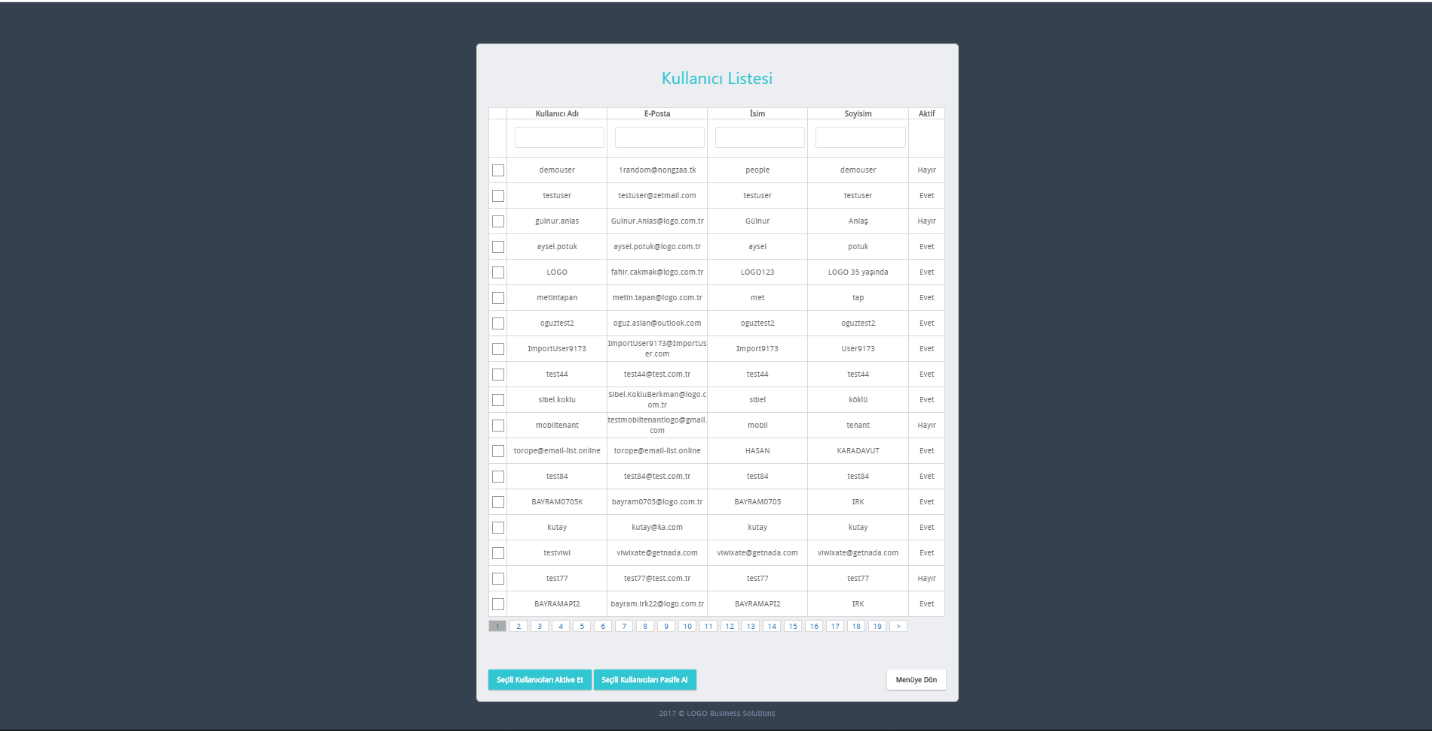
**Bilgilerimi Güncelle**



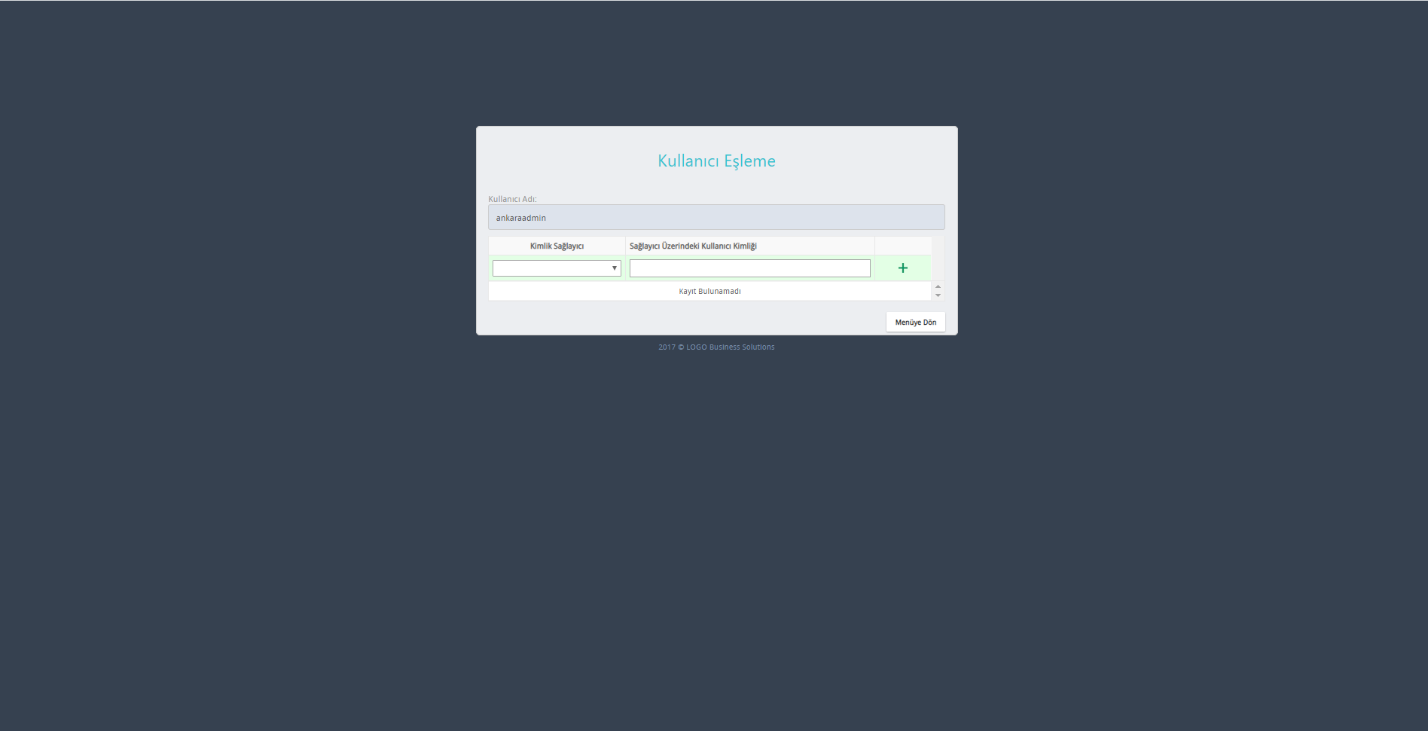
**Kullanıcıları İçeri Al (excel)**



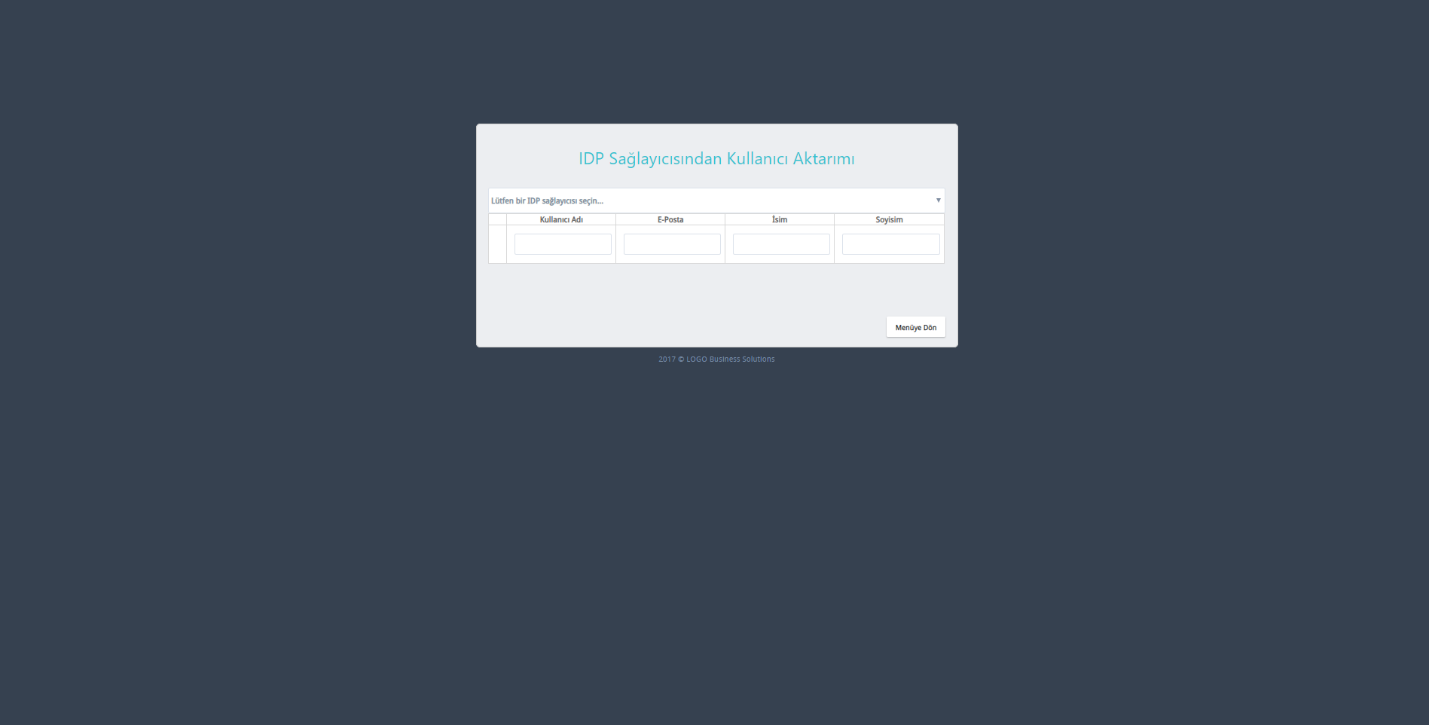
**Kullanıcı Listesi**



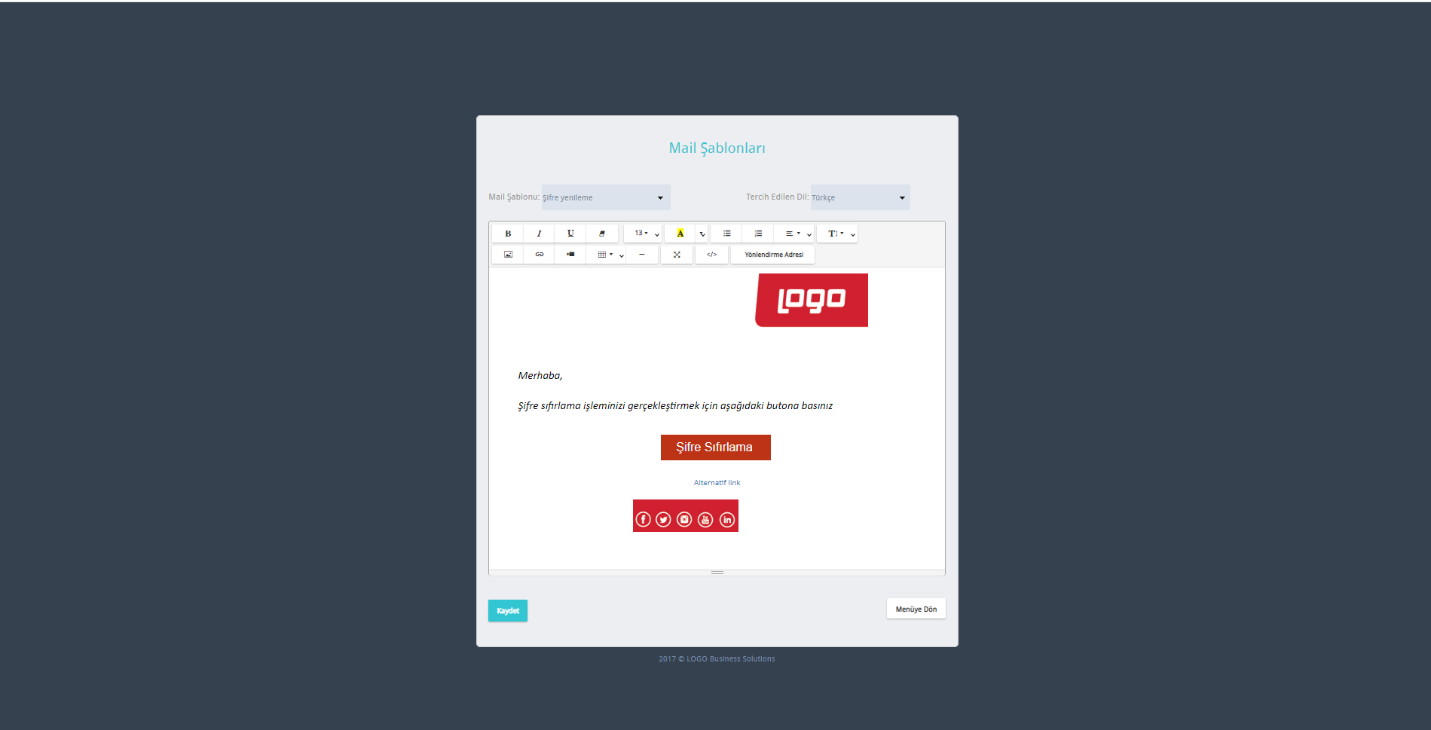
**Kullanıcı Eşleme**



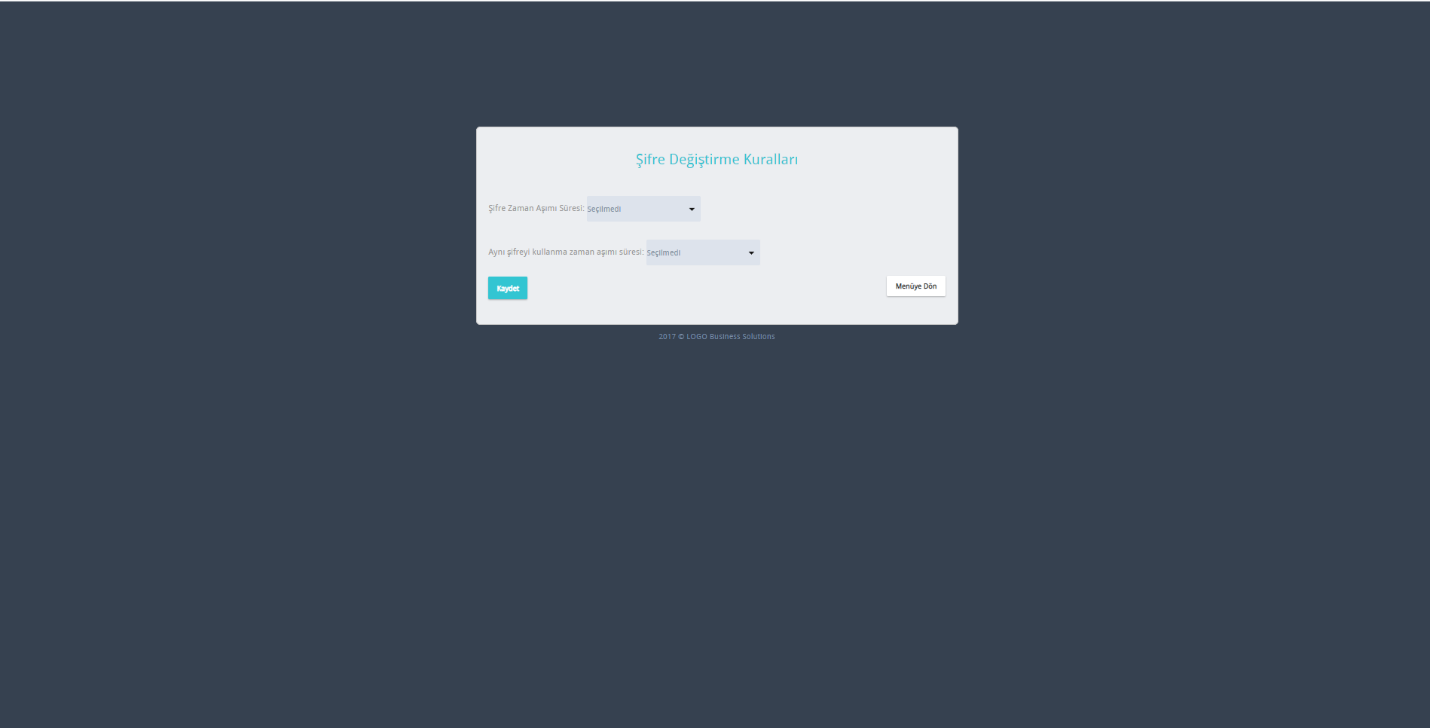
**IDP Sağlayıcısından Kullanıcı Aktarımı**



**Mail Şablonları**



**Şifre Değiştirme Kuralları**



**Teknik Özellikler**

* Oauth 2.0 standardı

**API Dokümantasyonu**

* Swagger UI: <http://dev-linux.logo-paas.com:5100/api-docs/>

**IDM Yönetici Paneli**

* Swagger UI: <http://dev-linux.logo-paas.com:5100/idmweb/>

**IDM Konfigurasyon Paneli**

* Swagger UI: [http://dev-linux.logo-paas.com:5100/settings/ui/](http://dev-linux.logo-paas.com:5100/api-docs/)

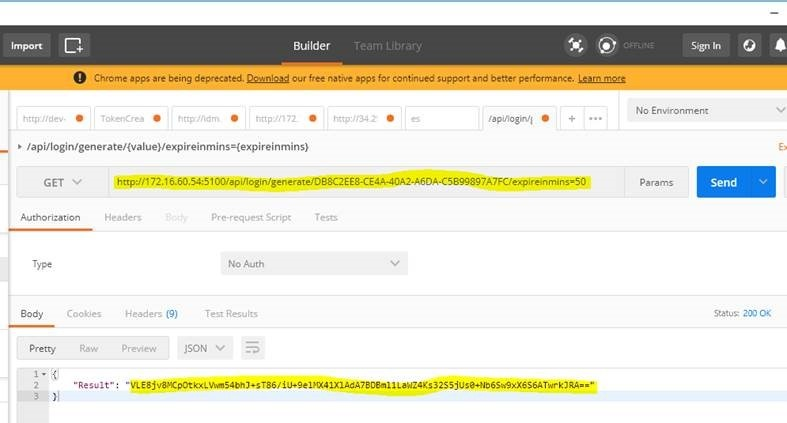
**İlişkili Platform Servisleri**

* RBMS:MsSQL veya PostgreSQL
* NoSQL (multiple instance çalışma durumunda session storage olarak): MongoDB
* Apache Kafka
* CloudControl Servis

**IDM’e Uygulama Kaydetme**

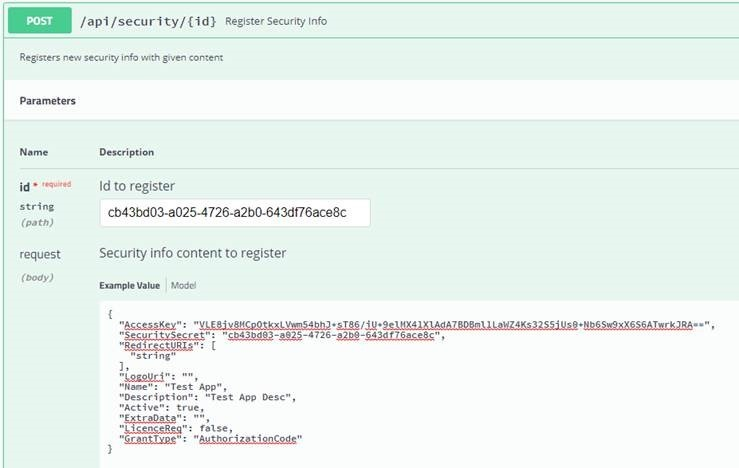
**1-** IDM sistemine yeni bir uygulama kaydetmek için öncelikle, aşağıdaki adrese çağrı yapılarak geçici erişim anahtarı alınmalıdır. Üretilen geçici anahtar **expireinmins** süresi kadar geçerli olacaktır.

[http://idmadresi/api/login/generate/DB8C2EE8-CE4A-40A2-A6DA-C5B99897A7FC/expireinmins=50](http://localhost:5100/api/login/generate/DB8C2EE8-CE4A-40A2-A6DA-C5B99897A7FC/expireinmins=50)

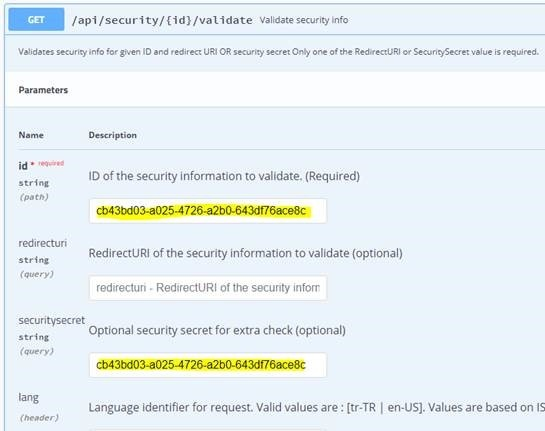


**2-** IDM Swagger UI üzerinden **/api/security/{id}** ucu ile yeni uygulamanın bilgileri kaydedilebilir.

* Id ve SecuritySecret parametrelerine sırasıyla, yeni uygulama için random olarak oluşturulan SecurityId ve SecuritySecret bilgisi girilecektir.
* AccessKey parametresine ise bir önceki adımda elde edilen geçici erişim kodu verilmelidir.
* GrantType parametresi; yeni uygulama IDM'den response\_type=token formatı ile browser üzerinden token alacaksa (tek aşamada), "Implicit" olarak girilmelidir.



**3-** Kaydedilen uygulama IDM Swagger UI üzerinden **/api/security/{id}/validate**ucu ile doğrulanabilir.





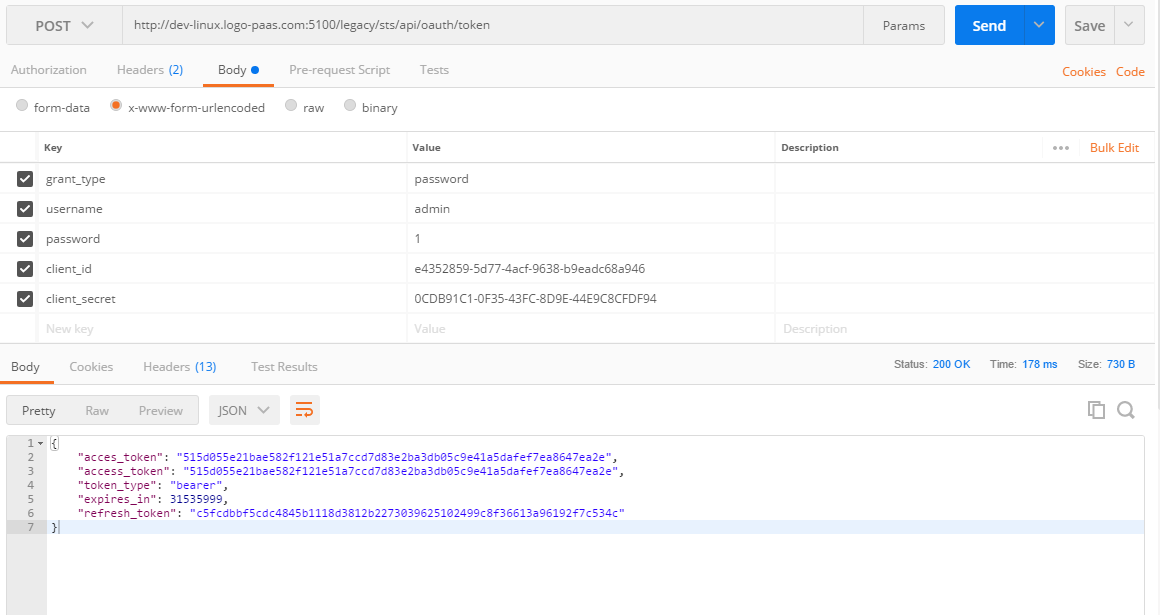
**IDM’e Kullanarak Access Token Alma**

Uygulama kaydı yapıldıktan sonra IDM sistemi üzerinden access token 3 farklı şekilde alınabilir.

### **1- Rest çağrısı ile backend üzerinden token alma**

Uygulama backendi üzerinden IDM UI'a yönlendirme yapmaksızın access token almak için aşağıdaki çağrı yapılabilir.

* Client\_id ve secret için ilgili uygulamanın bilgileri kullanılmalıdır.
* grant\_type=password parametresi sabit olarak gönderilmelidir.



### **2- SecuritySecret kullanılmadan redirecturi kontrolü ile IDM login ekranı kullanılarak access token alma**

Security secret'ın kullanılamadığı ve sadece front-end kodun bulunduğu ortamlarda IDM üzerinden token almak için, aşağıdaki adres formatında bold ile yazılan kısımlar değiştirilerek IDM login ekranına yönlendirme yapılması sağlanabilir.

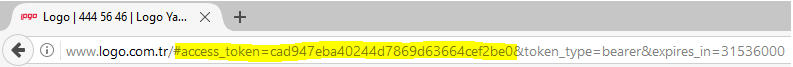
Bu yöntem redirecturi konfigurasyonu gerektirdiği için ihtiyaç olmadıkça kullanılmamalıdır. Bunun yerine bir sonraki başlıkta anlatılan 3. yöntem önerilmektedir.

[http://**idmadresi**/connect/authorize?client\_id=**securityid**&scope=vendorExtensions&response\_type=token&redirect\_uri=**urlencoded\_redirecturi**](http://idmadresi/connect/authorize?client_id=securityid&scope=vendorExtensions&response_type=token&redirect_uri=urlencodedredirecturi)

**Örnek**:  <http://stg-idm.vyapari-mumbai.com/connect/authorize>?client\_id=ca3ca995-3b1e-4e01-81e1-1f226686a3f7&scope=vendorExtensions&response\_type=token&redirect\_uri=http%3A%2F%[2Fw](http://2fstg-dashboard.vyapari-mumbai.com/)ww.logo.com.tr%2F

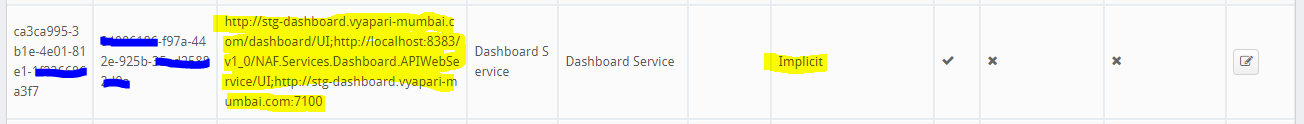


Giriş yapıldıktan sonra IDM redirect uri'de belirtilen adrese browser'ı yönlendirecek ve url fragment formatında access token'ı url'e ekleyecektir.



**Not:**Bu yöntemin kullanılabilmesi için uygulama kaydı yapılırken GrantType: "Implicit" olarak belirlenmeli ve RedirectUri bölümü doldurulmalıdır. IDM api'leri üzerinden bu bilgiler değiştirilebileceği gibi, AuthorizationWeb UI uygulama güvenliği menüsü üzerinden ilgili uygulama için bu bilgiler güncellenebilir.

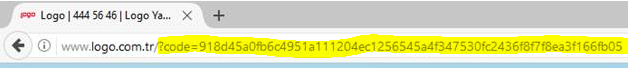




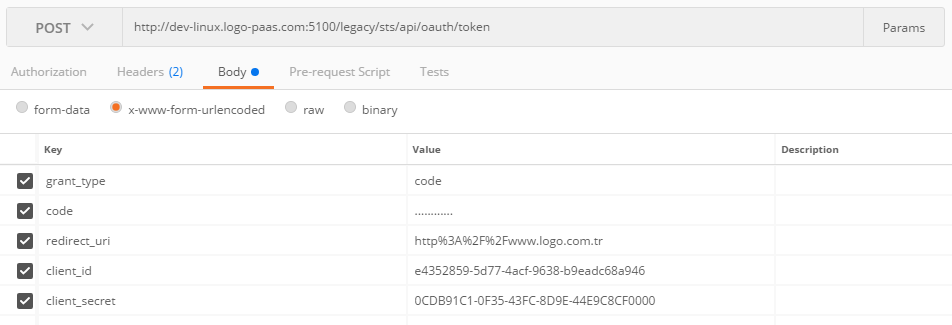
### **3- SecuritySecret ile IDM login ekranı kullanılarak (2 aşamalı) access token alma**

IDM kullanımında Single Signon operasyonları için önerilen yöntemdir. 2 aşamalı olarak çalışmaktadır;

* İlk aşamada bir önceki yöntemde olduğu gibi browser üzerinden IDM'e yönlendirme yapılır. (Aşağıda bold olarak belirtilen alanlar değiştirilmelidir)  
    
  [http://**idmadresi**/connect/authorize/callback?client\_id=**securityid**&scope=offline\_access&response\_type=code&redirect\_uri=**u**](http://stg-idm.vyapari-mumbai.com/connect/authorize/callback?client_id=e172fe44-8a84-4759-aceb-0b65c6d35e19&scope=offline_access&response_type=code&redirect_uri=http%3A%2F%2Fstg-services-b.vyapari-mumbai.com%2Fauthorizationweb%2FHome%2FMenu)**rlencoded\_redirecturi**  
   **Örnek:**[**http://stg-idm.vyapari-mumbai.com/connect/authorize/callback?client\_id=e172fe44-8a84-4759-aceb-0b65c6d35e19&scope=offline\_access&response\_type=code&redirect\_uri=http%3A%2F%2Fwww.logo.com.tr%2F**](http://stg-idm.vyapari-mumbai.com/connect/authorize/callback?client_id=e172fe44-8a84-4759-aceb-0b65c6d35e19&scope=offline_access&response_type=code&redirect_uri=http%3A%2F%2Fstg-services-b.vyapari-mumbai.com%2Fauthorizationweb%2FHome%2FMenu)
* Giriş yapıldıktan sonra browser, redirect uri de belirtilen adrese geçici kod içeren bir query string parametresi ("code") ile geri yönlendirilir.



* İkinci aşamada uygulama gelen "code" bilgisini alıp backend'de IDM'e bu bilgiyi ileterek asıl access token'ı alır. Redirect uri olarak ilk çağrıda gönderilen adres aynı şekilde post body'de parametre olarak iletilmelidir.



**Not:**Bu yöntemin kullanılabilmesi için uygulama kaydı yapılırken GrantType: "AuthorizationCode" (default değer) olarak belirtilmiş olmalıdır. RedirectUri verilmesine gerek yoktur.

**IDM’den Logout Olma**

IDM login ekranı kullanılarak alınan access token'ların invalide edilmesi ve Single Sign On oturumunun düşürülmesi için idm'in logout ucu aşağıdaki şekilde çağrılmalıdır.

* Bu çağrı yapıldığında aktif kullanıcı için yaratılan bütün token'lar invalide edilmekte ve IDM login arayüzü üzerinden açılmış olan (başka bir uygulamadan idm'e yönlendirme yapıldığında önceden açılmış bir oturum varsa tekrar kullanıcı adı ve şifre sorulmasını engelleyen) oturum sonlandırılır.
* Logout işleminden sonra aşağıda urlencoded\_redirect\_uri olarak belirtilen adrese yönlendirme yapılır.

[http://**idmadresi**/account/logout?redirect\_uri=**urlencoded\_redirecturi**&forcesignout=True&appid=**s**](http://stg-idm.vyapari-mumbai.com/account/logout?redirect_uri=http://stg-services-b.vyapari-mumbai.com/authorizationweb/Home/Menu&forcesignout=True&appid=e172fe44-8a84-4759-aceb-0b65c6d35e19)**ecurityid**

**Örnek**: <http://stg-idm.vyapari-mumbai.com/account/logout?redirect_uri=http://stg-services-b.vyapari-mumbai.com/authorizationweb/Home/Menu&forcesignout=True&appid=e172fe44-8a84-4759-aceb-0b65c6d35e19>