



1. SERVİSLER ve YÖNETİM PANELLERİ

1.1. Giriş

Bu doküman içerisinde Netsis Wings kurulumu ile gelen Servisler ve bu servislerin yönetim panelleri ile ilgili bilgilendirmeyi bulabilirsiniz.

1.2. Servisler

Netsis Wings Kurulumu ile aşağıdaki servislerin kurulumu gerçekleştirilmektedir.

- Logo Netsis Wings Servisi (**Zorunlu**)
- Logo Netsis Wings Broker Servisi (Seçimli)
- Logo Netsis Wings Gateway Servisi (Seçimli)
- Logo Services Agent (Light) (**Zorunlu**)
- Lisans Servisi (**Zorunlu**)

1.2.1. Logo Netsis Wings Servisi

Logo Netsis Wings Servisi web browser ile uygulama arasındaki iletişimi sağlayan bir HTTPS/Websocket sunucusudur. Windows servis olarak kurulur. Sisteme kaydı yapılan ve konfigüre edilen windows uygulamaların çalıştırılması için bu servisin kurulu ve çalışıyor olması gerekmektedir.

Broker ve Gateway servislerinin kurulu olmadığı senaryolarda bütün bağlantıları bu servis karşılar ve cevaplar. Bu senaryo kapsamında gerekli konfigürasyon işlemlerini Ürün kurulum klasörünü altındaki **VUI\bin32\Thinfinity.VirtualUI.Server.exe** 'yi çalıştırarak ya da **Netsis Wings Yönetim Paneli** kısayoluna tıklayarak açabilirsiniz. (Bkz. [Logo Netsis Wings Yönetim Paneli.](#))

1.2.2. Logo Netsis Wings Broker Servisi

Scaling ve Load balancing senaryolarında Logo Netsis Wings Gateway servisi ile birlikte çalışır. Uygulanmak istenen Load Balancing senaryosuna göre (Bkz: [Scaling and Load Balancing](#)) sunucu instance'larını yöneterek, sunucu instancelarının ayakta olup olmadığını kontrol eder. Aynı networkte bulunduğu ve kendisine tanımlanan gatewaylerden gelen istekleri karşılar ve cevaplar.

Bu senaryo kapsamında gerekli konfigürasyon işlemlerini Ürün kurulum klasörünü altındaki **VUI\bin32\Thinfinity.VirtualUI.Broker.exe** 'yi çalıştırarak açabilirsiniz.

1.2.3. Logo Netsis Wings Gateway Servisi

Load balancing senaryolarında en az bir Logo Netsis Wings Gateway servisinin olması gerekmektedir. Logo Netsis Wings Broker servisi ile birlikte çalışır. Gelen bağlantıların ayakta olan sunuculara dağıtılması işlemlerini gerçekleştirir.

Bu senaryo kapsamında gerekli konfigürasyon işlemlerini Ürün kurulum klasörünü altındaki **VUI\bin32\Thinfinity.VirtualUI.Gateway.exe** 'yi çalıştırarak açabilirsiniz.

1.2.4. Logo Services Agent (Light)

Bağlanan istemcilerin kayıt çağrılarını kaydeder ve ilk heartbeat çağrılarında itibaren ilgili haberleşme sürelerini kontrol eder, cevap göndermeyen istemci uygulamasını kapatır.

Windows servis olarak çalışır hale geldikten sonra NAMEDPIPE üzerinden haberleşme kanalını dinler ve kendisine bağlanan istemcinin timeout süresi ile kaydını yapar. İlgili istemcinin gönderdiği ilk heartbeat çağrısından itibaren geçen süreyi hesaplar ve beklenen sürede kendisine yeni bir heartbeat çağrısı gelmemesi durumunda, kayıt olan istemci uygulamasını kapatır.

Netsis Wings kurulumunda ürün exe sini dinleyerek (Örnek : “wingsweb.exe”) ürün exe’sinden timeout süresi boyunca cevap gelmemesi durumunda ürün exe’sini kapatır. Timeout süresi “VUI\bin32\Logo.Web.Client.Registration.exe.Config” dosyasında “WINGS_TIMEOUT” parametresi ile set edilir ve varsayılan değeri 300 saniyedir.

Log seviyesi .config dosyasında bulunur, varsayılan seviye error olarak tanımlanmıştır, loglarını Event Log tarafında varsayılan olarak Servis İzleyisi EventLogSource adı ile loglarını kaydeder.

1.3. Yönetim Panelleri

1.3.1. Netsis Wings Yönetim Paneli

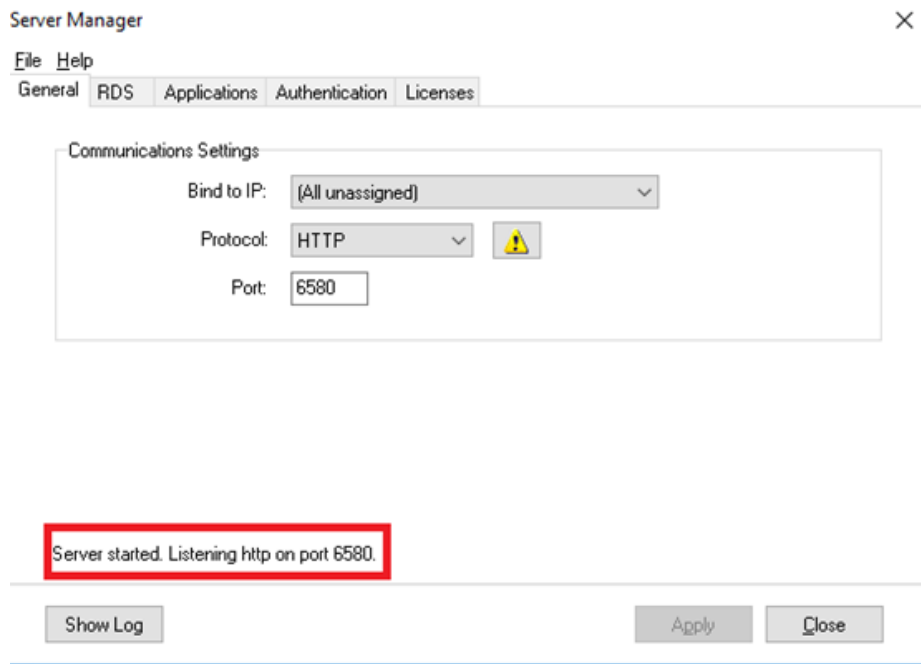
Netsis Wings Yönetim Paneli Logo Netsis Wings Servisinin kurulduğu durumlarda gerekli olan konfigürasyon ayarlarını düzenlemek için kullanılan arayüzdür. Kurulum ile birlikte uygulamanın açılması için gerekli olan konfigürasyon bilgileri ayarlanmış olmakla birlikte herhangi bir sorun durumunda bu arayüz kullanılarak düzenlemeler yapılabilir.

Apply : Bu buton ile yapılan değişiklikler kaydedilir.

Close : Bu buton ile Yönetim paneli ekranı kapatılır.

Show Log : Bu buton ile servis tarafından basılan loglar listelenir.

1.3.1.1. General Tabı






Şekil 1 : Netsis Wings Yönetim Paneli Genel Tabı


Şekil 1 ile gösterilen Yönetim Paneli Genel tabında windows servisin durumunu takip edebilirsiniz (Kırmızı kutu içerisine alınan alan). Servisin ayakta olmaması durumunda görüntü üzerindeki metnin

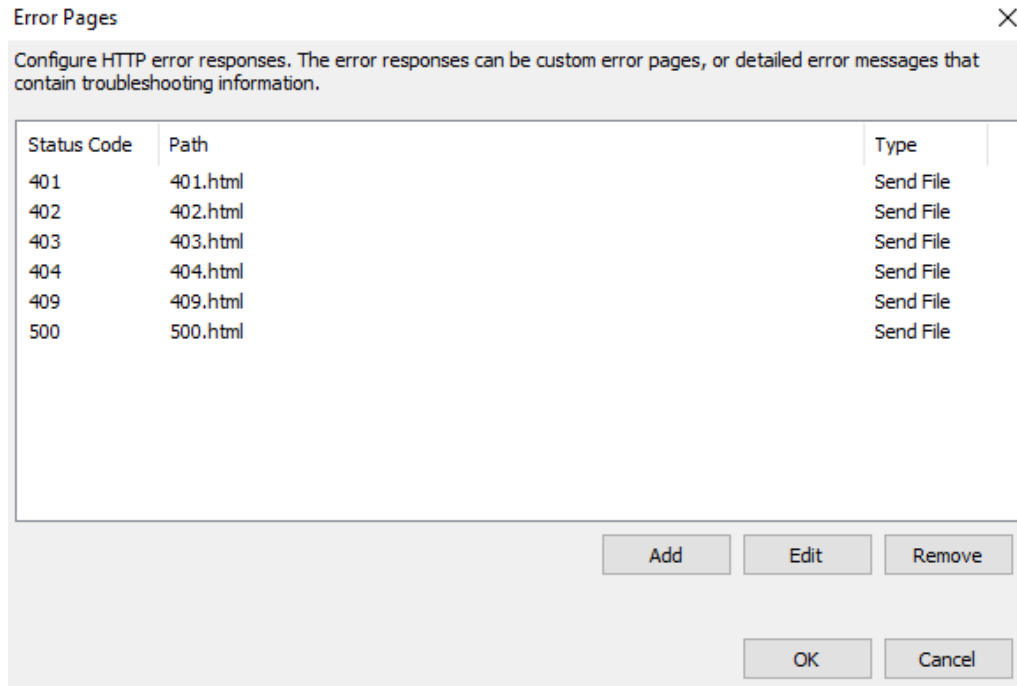
Windows service not running şekline dönüştüğünü göreceksiniz bu durumda Logo Netsis Wings Servisinin çalışır durumda olduğunu kontrol etmeniz gerekmektedir.

Communication Settings alanında aşağıdaki değerlerin girilmesi beklenmektedir :

Bind to IP	'All unassigned' seçeneği ile bütün mevcut IP adresleri ile gelen bağlantıların servis tarafından karşılanmasını sağlar. Özel bir IP adresi girilir ise sadece bu IP adresi üzerinden gelen istekler cevaplanır.
Protocol	Http ve Https protokolleri arasında yapılan tercih bu kısımda belirtilir. Varsayılan olarak Http portu üzerinden yayın yapılmaktadır.
	Protocol bilgisinin yanında yer alan bu buton ile Http varsayılan hatalarının yönlendirileceği hata sayfalarının değiştirilebileceği Hata Sayfası ekranına geçiş yapılır. (Bkz. Hata Sayfası Ekranı)
	Protocol olarak Https seçildiği durumda görünür.Https için kullanılacak olan SSL sertifikası tanımının yapıldığı SSL Sertifikası ekranını açar. (Bkz SSL Sertifikası Ekranı)
	Protocol olarak Https seçili olduğu durumlarda ve Broker ve Gateway servislerinin kullanılmadığı senaryolarda kullanılır. Https Güvenlik Ayarları ekranını açar. (Bkz Https Güvenlik Ayarları Ekranı)
Port	Logo Netsis Wings Servisinin hangi porttan dinleme yaptığını gösterir.Varsayılan olarak 6580 portundan dinleme gerçekleştirir.

1.3.1.1.1. Hata Sayfası Ekranı

General tabında yer alan  butonuna basarak bu ekrana ulaşabilirsiniz.



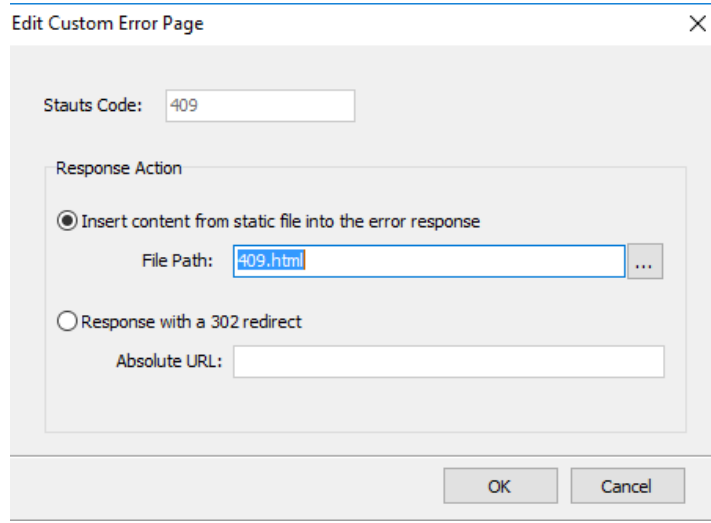
Şekil 2 : Hata Sayfaları Ekranı

Varsayılan olarak ürün kurulumunun altında yer alan "VUI\web" altındaki hata sayıları kullanılmaktadır.

Listede yer alan alanlar ve tanımları :

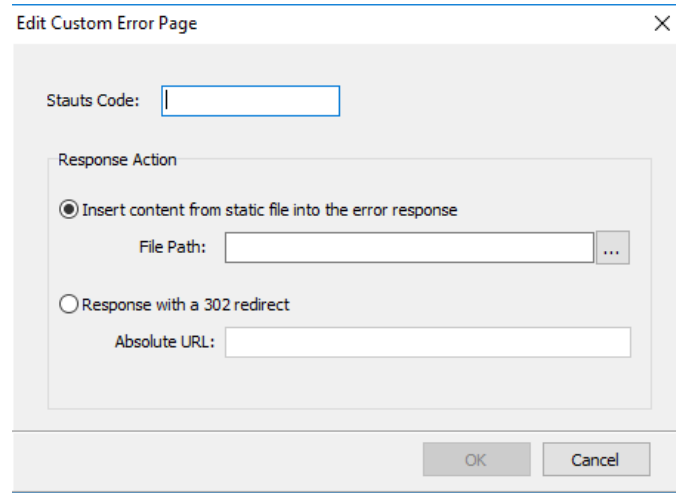
Status Code	Http cevabının durumunu bildiren sayısal kod alanı.
Path	Hatalı Html cevabı için gösterilecek olan sayfa adresi
Type	Send file : Fiziksel olarak sunucuda bulunan bir sayfanın disk üzerindeki adresi girilerek yapılmış bir tanım olduğunu belirtir. Redirect : Yönlendirme yapılacak olan sayfanın URL adresi girilerek yapılmış bir tanım olduğunu belirtir.

Edit : Edit listede seçili olan kaydın güncellenmesi için Özel Hata Sayfası Düzenleme Ekranı açılır. Seçili olan Status Code için yeni sayfa tanımlamak için kullanılır. (Bkz [Hata Sayfası Tanımlama Ekranı](#))



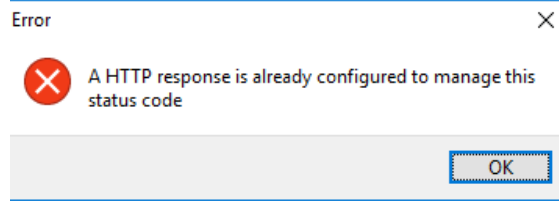
Şekil 3 : Hata Sayfası Güncelleme Ekranı

Add : Yeni bir hata sayfası tanımı girmek için kullanılır. Mevcut Status Code tanımları için ekleme yapılamaz. (Bkz [Hata Sayfası Tanımlama Ekranı](#))



Şekil 4 : Hata Sayfası Ekleme Ekranı

Mevcut status code tanımları için ekleme yapılmaya çalışıldığında aşağıdaki hata ekranı ile karşılaşılacaktır.



Şekil 5 : Mevcut Status Code Hatası

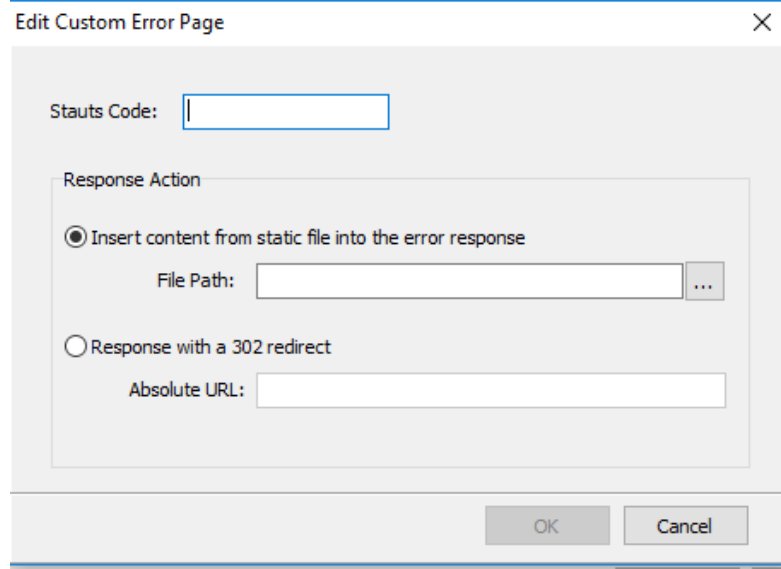
Delete : Seçili olan Hata sayfası tanımını siler.

OK : Yapılan değişiklikleri kayıt ederek ekranı kapatır.

Cancel : Yapılan değişiklikleri gözardı ederek ekranı kapatır.

1.3.1.1.1.1. Hata Sayfası Tanımlama Ekranı

Bu sayfada hata kodları için sayfa tanımlamaları ve güncellemeler yapılır.



Şekil 6 : Hata Sayfası Tanımlama Ekranı

Status Code : Http cevabının durumunu bildiren sayısal kod alanı.


File Path : Fiziksel bir sayfa tanımlanacağı zaman aktif hale gelir ve disk üzerinden fiziksel sayfanın seçilmesini sağlar. Hata sayfası tanımının tipi **send file** olur.

Absolute URL : Başka bir Url e yönlendirme yapılacağı zaman ilgili Url bilgisinin girilmesini sağlar. Hata sayfası tanımının tipi **Redirect** olur.

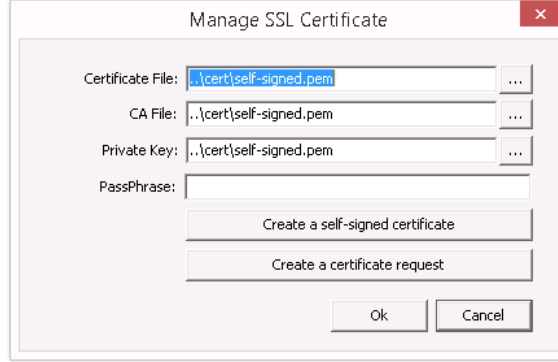
OK : Yapılan değişiklikleri kayıt ederek ekranı kapatır.

Cancel : Yapılan değişiklikleri gözardı ederek ekranı kapatır.

1.3.1.1.2. SSL Sertifikası Ekranı

General tabında Protocol olarak Https seçildiği durumda  butonuna basarak bu ekrana ulaşabilirsiniz. Varsayılan olarak Thinfinity VirtualUI sertifikası ürün kurulumu ile birlikte gelmektedir. Bu sertifikayı ürün kurulumunda “VUI\cert\” klasörü altında bulabilirsiniz.

Bu sertifikayı kullanmak istediğiniz zaman aşağıdaki ekran görüntüsü gibi bilgileri doldurup kaydetmeniz yeterli olacaktır.



The dialog box titled "Manage SSL Certificate" contains the following fields and buttons:

- Certificate File: ..\cert\self-signed.pem
- CA File: ..\cert\self-signed.pem
- Private Key: ..\cert\self-signed.pem
- PassPhrase: (empty)
- Buttons: "Create a self-signed certificate", "Create a certificate request", "Ok", "Cancel"

Şekil 7 : SSL Sertifikası Ekranı

Kendi Sertifikanızı tanımlamak için bu ekranda aşağıdaki bilgileri girmeniz gerekmektedir.

Certificate File	Sertifika dosyasının adresi
CA File	Tanımsız bir sertifika otoritesi tarafından yayımlanmış sertifikalar için CA sertifikasının adresi girilmelidir.
Private Key	Sertifika Private Key adresi
PassPhrase	Private Key oluşturulurken şifre kullanılmış ise bu şifre bilgisi bu alana girilmelidir.

Create a self-signed certificate

Self Signed bir sertifika oluşturup bu sertifikayı kullanmak istiyorsanız Create a self-signed certificate butonuna tıklayarak açılan ekranda aşağıdaki bilgileri girmeniz gerekmektedir. Geçerli bir sertifika otoritesi olmayacağı için browser tarafından uyarı verilir.



The dialog box titled "Create self-signed certificate and private key" contains the following fields and buttons:

- Country Code: (dropdown)
- State: (text box)
- Locality: (text box)
- Organization: (text box)
- Organizational Unit: (text box)
- Common Name: (text box)
- E-Mail address: (text box)
- Bits: (dropdown) >= 512
- Text: "Certificate and private key are written to the same file. Private key will not be password protected."
- Buttons: "Create", "Close"

Şekil 8 : Create Self Signed Certificate Ekranı

Country Code	ISO 3166 standartlarındaki iki karakterlik ülke kodu
State	Organizasyonun bulunduğu il adı (kısaltılmamış tam isim)
Locality	Organizasyonun bulunduğu semt (Kısaltılmamış tam isim)
Organization	Firmanın resmi ünvanı
Organizational Unit	Organizasyon içindeki farklı birimleri ayırmak için kullanılır
Common Name	Sertifikayı kullanmayı düşündüğünüz sunucu ve domain adı (wings.logo.com.tr) ya da Url bilgisi
E-Mail Address	Firma eposta adresi
Bits	2048 büyüklüğünde anahtar kullanılması tavsiye edilir.

Gerekli bilgiler tanımlandıktan sonra **Create** butonuna basılarak sertifikanın kaydedileği klasörü seçmemiz istenecek. Varsayılan klasör olarak **"VUI\Cert"** klasörü açılır. Bu işlem başarılı bir şekilde yapıldıktan sonra artık bu sertifika kullanılıyor olacak.

Close : butonu ile işlemi kaydetmeden ekranı kapatabilirsiniz.

Create a Certificate Request

Geçerli bir sertifika otoritesinden (VeriSign vs.) sertifika almak için kullanılır.



Şekil 9 : Create a Certificate Request Ekranı


Country Code	ISO 3166 standartlarındaki iki karakterlik ülke kodu
State	Organizasyonun bulunduğu il adı (kısaltılmamış tam isim)
Locality	Organizasyonun bulunduğu semt (Kısaltılmamış tam isim)
Organization	Firmanın resmi ünvanı
Organizational Unit	Organizasyon içindeki farklı birimleri ayırmak için kullanılır
Common Name	Sertifikayı kullanmayı düşündüğünüz sunucu ve domain adı (wings.logo.com.tr) ya da Url bilgisi
E-Mail Address	Firma eposta adresi
Bits	2048 büyüklüğünde anahtar kullanılması tavsiye edilir.

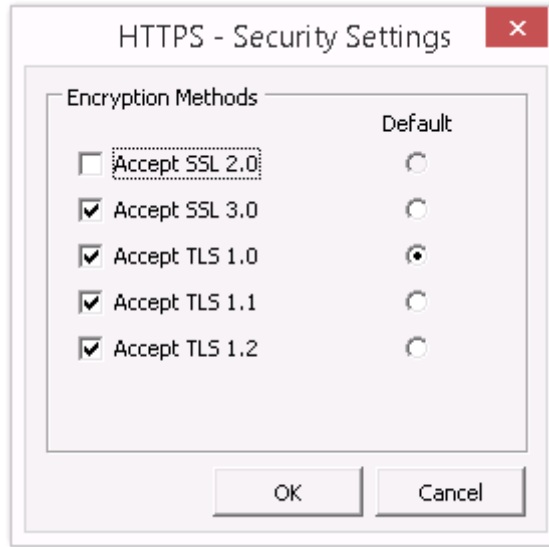
Gerekli bilgiler tanımlandıktan sonra **Create** butonuna basılınca sistem iki dosya üretecektir. Öncelikle Private Key dosyasını bir klasöre kaydetmeniz istenecek, sonrasında istek dosyasını bir klasöre kaydetmeniz istenecek. Oluşturulan istek dosyasını Sertifika otoritesine göndererek sertifika temini sağlanır. Bu dosyalar Sertifika tanımlama ekranından tanımlanarak bu sertifikaların kullanılması sağlanır.

Close butonu ile işlemi kaydetmeden ekranı kapatabilirsiniz.

1.3.1.1.3. Https Güvenlik Ayarları Ekranı

General tabında Protocol olarak Https seçildiği ve Broker ve Gateway servislerinin kullanılmadığı

senaryolarda  butonuna basarak bu ekrana ulaşabilirsiniz.

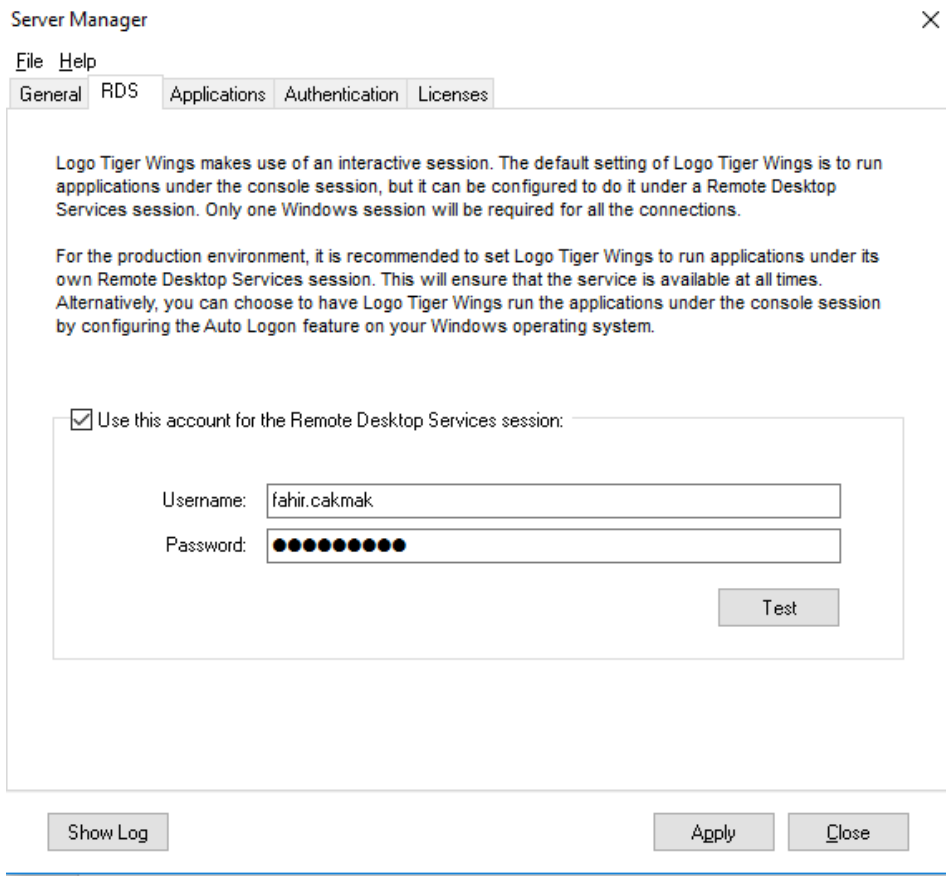


Şekil 10 : Https Güvenlik Ayarları Ekranı

Encryption Methods	Desteklenmesini istediğiniz Https encryption metodları seçebilirsiniz.
Default	Varsayılan Encryption metodu işaretlenir, varsayılan encryption metodunun desteklenmediği browserlarda diğer encryption metodlarına bakılır.

1.3.1.2. RDS Tabı

Uygulamalar interactive kullanıcı heabı altında çalıştırılır, eğer kurulum yapılan sunucu üzerinde interactive kullanıcı yok ise uygulamalar açılmaz. Remote Desktop ile session açılan bir sunucuda uygulamaları çalıştırmak için RDS tabında bu alanın doldurulması gerekmektedir.



Şekil 11 : RDS Tabı

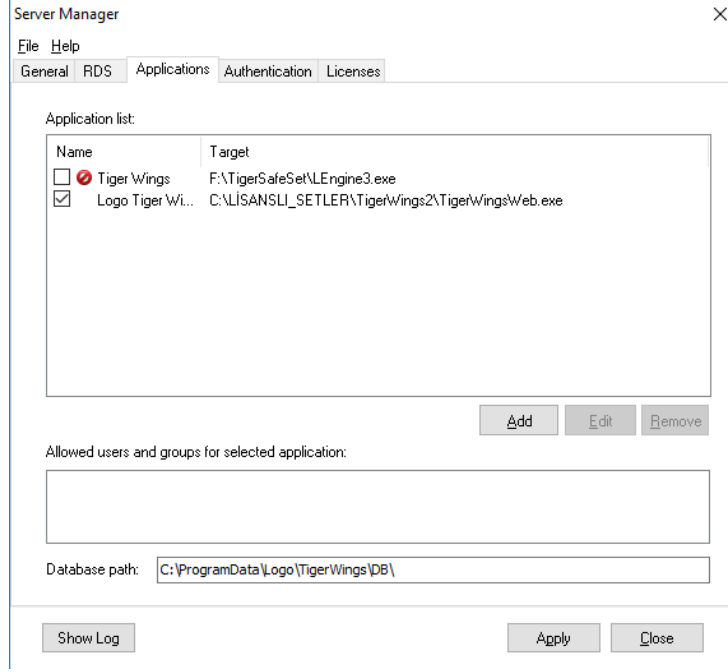
Use this account for the Remote Desktop Services session	Uygulamaların girilen Remote Desktop Service sessionı altında çalışması sağlanır.
Username	Remote Desktop Service sessionı kullanıcı adı
Password	Remote Desktop Service sessionı kullanıcı şifresi
Test	Girilen kullanıcı bilgilerini kontrol eder

1.3.1.3. Applications Tabı

Çalıştırılacak olan uygulama tanımlarının yapıldığı alandır. Bu tanımlama ile uygulama web sunucunda yayınlanmaya başlayacaktır. Yayımlanan uygulamaya erişmek için girmiş olduğunuz uygulama bilgilerine göre aşağıdaki URL formatını web browserında yazmak yeterli olacaktır.

http:\\{local-ip}:{port}\\{virtualpath}

Örnek : http:\\localhost:6580\\Wings



Şekil 12 : Application Tabı

Application List	Tanımlanmış olan uygulamaların listesini gösterir. Sağ tarafta yer alan checkbox seçimi ile uygulama aktif pasif yapılabilir. Name : Uyguklamanın Adı Target : Uygulamanın çalıştırılabilir dosyası (WebLink tipindeki uygulamalar için web adresi)
Add	Yeni uygulama ekleme ekranını açar (bkz: Uygulama Detay Ekranı)
Edit	Seçili olan uygulama tanımının güncellenmesini sağlar. (bkz: Uygulama Detay Ekranı)
Allowed Users and Groups for selected profile	Seçili uygulama için yetkili olan kullanıcı ve grupları gösterir.
Database path	Uygulama için servis tarafından kullanılan veritabanı bilgilerinin tutulacağı klasör.

1.3.1.3.1. Uygulama Detay Ekranı

Uygulama ekleme yada güncelleme işlemleri bu ekran üzerinden gerçekleştirilir.

Logo Tiger Wings Application Profiles Editor

Name:

Virtual Path:

Home Page:

Access Key:

Icon: Application Web Link

Default application Visible

General | Credentials | Permissions

Program path and file name:

Arguments:

Start in the following folder:

Resolution:

Browser rules file:

Reconnection timeout: seconds

Şekil 13 : Uygulama Detay Ekranı

Name	Uygulama Adı
Virtual Path	Her uygulama için tekil bir adres oluşturabilmek için bu değer kullanılır, daha önce kullanılmamış bir değer olması gerekir. Uygulama erişim adresine eklenir. Ör : http://localhost/Wings
Home Page	Karşılama Sayfa Adresi (Netsis Wings için ürün altında yer alan web klasöründeki index.html seçilmelidir.)
Access Key	Uygulama için yaratılan tekil değer (Id bilgisi)
Icon	Uygulama için icon seçme alanıdır, seçilen icon birden fazla uygulama olduğunda uygulama adresi girilmeden (http://localhost:6580) açıldığında karşımıza çıkacak olan uygulama listesinde uygulama tanımını göstermede kullanılıacaktır.
Application/Web Link	Web Link seçildiğinde bu uygulama Web Hyperlink olarak davranacaktır, Netsis Wings için Application seçimi yapılmalıdır.
Default Application	Varsayılan uygulama olarak seçilen uygulama, uygulama adı urlde girilmedende ulaşılabilir olacaktır (http://localhost:6580 ile Netsis Wings uygulaması açılabilir olacaktır.)

1.3.1.3.1.1. General Tabı

General | Credentials | Permissions

Program path and file name:

Arguments:

Start in the following folder:

Resolution:

Browser rules file:

Reconnection timeout: seconds

Şekil 14 : Uygulama Detay Ekranı – General Tabı

Program path and file name	Uygulamanın çalıştırılabilir(exe) dosyasının tam adresi.
Arguments	Uygulamaya gönderilecek olan parametre değeri/ değerleri.
Start in the following folder	İçerik kalsörü.
Resolution	Seçili olan listeden uygun çözünürlük ayarı seçilebilir. Netsis Wings için kullanılan varsayılan değer Fit To Browser window.
Browser rules file	Remote Desktop çözünürlük ayarlarını tanımlayan dosyanın adresi
Idle Timeout	Uygulama kapatıldıktan sonra exe dosyasının ne kadar sonra kill edileceğini gösterir. Bu süre zarfında uygulama session bilgisi açık kalır. 0 verilmesi durumunda uygulama kapatılır kapatılmaz exe öldürülür.

1.3.1.3.1.2. Credentials Tabı

Uygulamanın hangi interaktif kullanıcı hesabı altında çalışacağını belirler.

General | Credentials | Permissions

Credentials:

Use the authenticated credentials

Use these credentials:

User name:

Password:

Şekil 15 : Uygulama Detay Ekranı – Credentials Tabı

Use the Authenticated Credentials	Permissions tabında tanımlanan kullanıcılar arasından browserda girilen kullanıcı bilgisini kullanmak için bu seçenek işaretlenir. Kullanıcı bağlı değilse bağlantı sağlanır.
Use these credentials	Bilgileri girilen kullanıcı hesabı ile bilgisayara bağlanılır ve uygulama çalıştırılır.

1.3.1.3.1.3. Permissions Tabı

General | Credentials | **Permissions**

Allow anonymous access

Group or user names:

Add Remove

Şekil 16 : Uygulama Detay Ekranı – Permissions Tabı

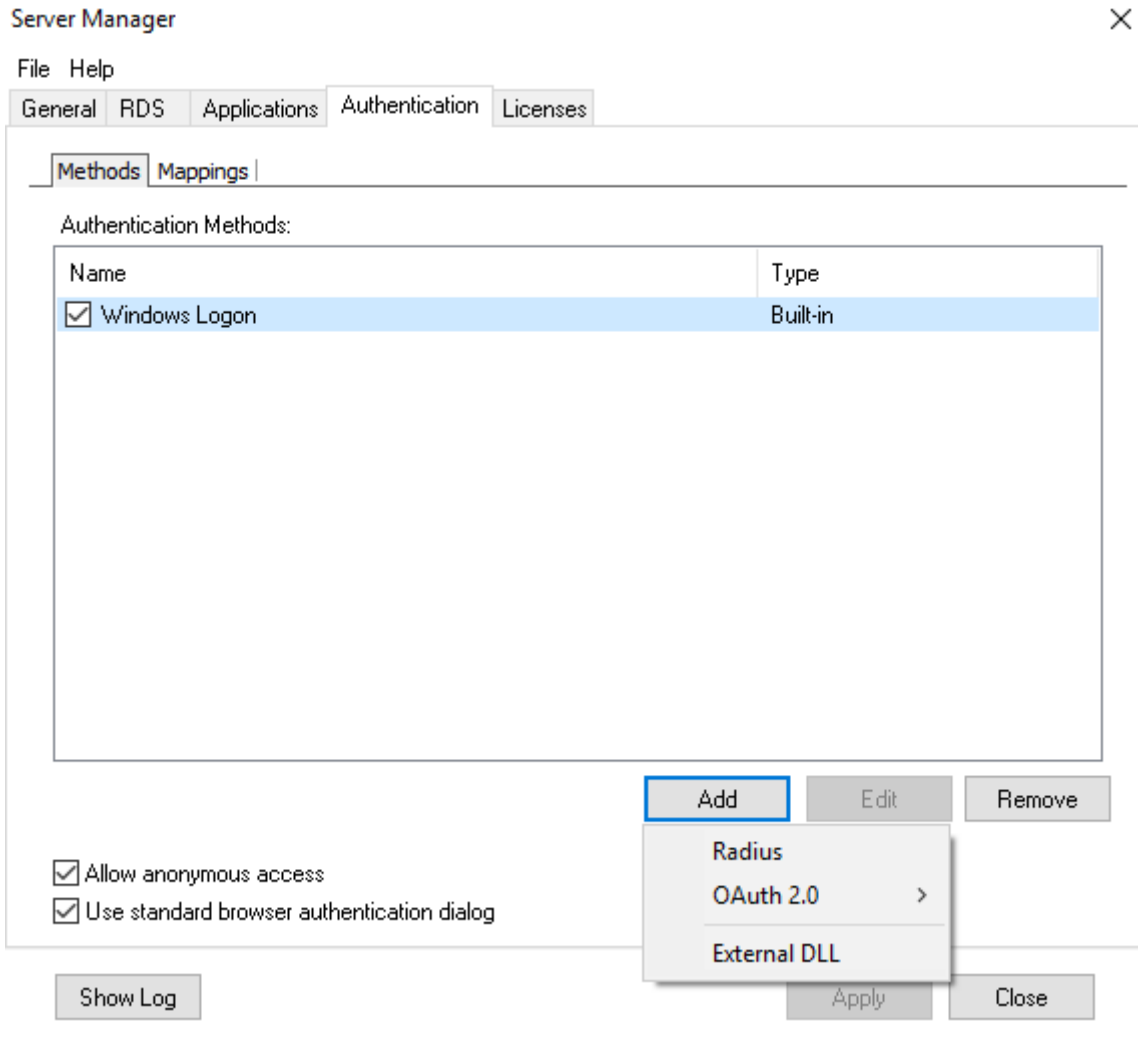
Bu uygulamaya erişebilecek olan kullanıcı listesi.

Allow anonymous access	Herhangi bir login işlemi olmadan uygulamanın çalışmasını sağlar. Yani herkese açık olur.
Add	Allow anonymous access seçili değil ise uygulamaya login olup kullanabilecek olan yetkili kullanıcıları seçmemizi sağlar.
Remove	Daha önce eklenmiş olan bir hesabın yetkisini kaldırmamızı sağlar.

1.3.1.4. Authentication Tabı

Authentication yönteminin belirlendiği alandır.

1.3.1.4.1. Methods Tab

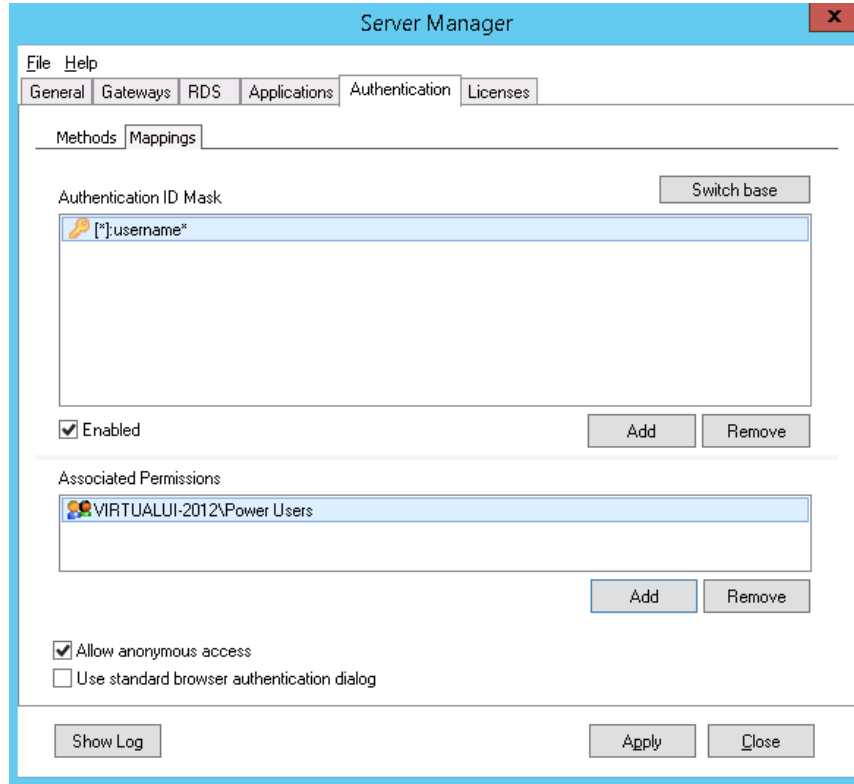


Şekil 17 :Authentication Tabı – Methods Tabı

Authentication Methods	Tanımlı authentication yöntemlerinin listelendiği alandır. Sol taraftaki checkbox ile seçili authentication metodu aktif/pasif yapılabilir. Name : Authentication yönteminin adı Type : Authentication yönteminin tipi
Add	Yeni bir authentication yöntemi eklemek için kullanılır. Tıklandığında eklenebilecek authentication yöntemleri açılır.
Edit	Seçili authentication yöntemini güncellemek için kullanılır.
Remove	Seçili authentication yöntemini silmekte kullanılır.
Allow anonymous access	İşaretlendiğinde kullanıcılar anonymous access olarak tanımlanmış olan uygulamalara erişebilirler.
Use standart browser authentication dialog	Seçili olduğunda browserın login dilogu kullanılır seçili değilse Virtual Uı in web login ekranı kullanılır.

1.3.1.4.2. Mappings Tab

Windows logon dışındaki diğer authentication yöntemlerindeki kullanıcıların Windows Active Directory kullanıcıları ile eşleştirilmesini sağlar. Bu eşleştirme ile kullanıcıların uygulamalara erişimleri sağlanır.



Şekil 18 : Authentication Tabı – Methods Tabı

Switch Base	Authentication Id Mask ve Associated Permission listesinin görünüm sıralarını değiştirir.
Authentication Id Mask	Authentication Id Mask listesini gösterir. Authentication Id bilgisi yada bir maskeleme ile kayıt girişi sağlanır.Kullanıcı adının belli karakteri girilerek * wildcardı kullanılarak maskeleme yapılabilir.
Associated Permissions	AuthenticationId mask ile ilişkilendirilen Active Directory Kullanıcı/gruplarını listeler.
Enabled	Authentication Id Mask sadece üst tarafta gösterilirken görünür.Seçili authentication Id Mask bilgisini aktif/pasif yapar.
Add	Yeni bir Authentication Id mask ya da Active Directory User/group ekleme işlemini yapar.
Remove	Üst tarafında yer alan listeden Authentication Id Mask yada Active Directory Kullanıcısı/Grubu silme işlemini gerçekleştirir.

1.3.1.4.3. Radius Authentication Yöntemi

Authentication yöntemi olarak Radius seçildiğinde aşağıdaki ekranda bazı tanımlamaların girilmesi gerekmektedir.

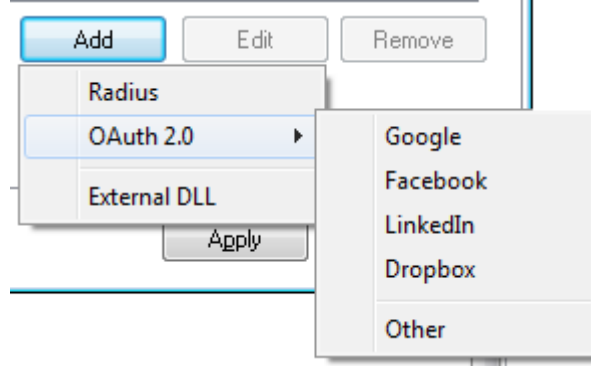
The screenshot shows a dialog box titled "Authentication Method Settings". The "Name" field contains "Radius". Below this is a "Server" tab. Under the "Server" tab, the "Server IP" field is set to "127.0.0.1", the "Port" field is set to "1812", the "Shared Secret" field is empty, and the "Authentication Type" dropdown menu is set to "PAP". There is a "Test Configuration" button and "Ok" and "Cancel" buttons at the bottom of the dialog.

Şekil 19 : Radius Authentication Method

Name	Authentication yönteminin adı
Server IP	Radius Sunucu Ip si
Port	Radius Port
Shared Secret	Radius Shared Secret
Authentication Type	Authentication Tip seçimi yapılır
Test Configuration	Radius sunucusuna bağlanıp test etmek için kullanılır.

1.3.1.4.4. Oauth 2.0 Authentication Yöntemi

Oauth 2 Authentication Yöntemi tanımı yapmak için kullanılır.



Şekil 20 : Oauth Authentication Method List

Önden tanımlı Oauth 2 sunucuları için (Google, Facebook, LinkedIn, Dropbox) aşağıdaki ekrandaki bilgileri girmek gerekmektedir.

General Tabı

Authentication Method Settings

Name:

Virtual Path:

General **Server**

Client ID:

Client Secret:

Ok Cancel

Şekil 21 : Oauth Authentication Method Tanımı

Name	Authentication yöntemini adı
Virtual Path	Bu authentication yöntemini kullanacak olan uygulamanın virtual path bilgisi
Client ID	Authentication Provider Client Id bilgisi
Client Secret	Authentication Provider Client Secret Bilgisi

Server Tabı

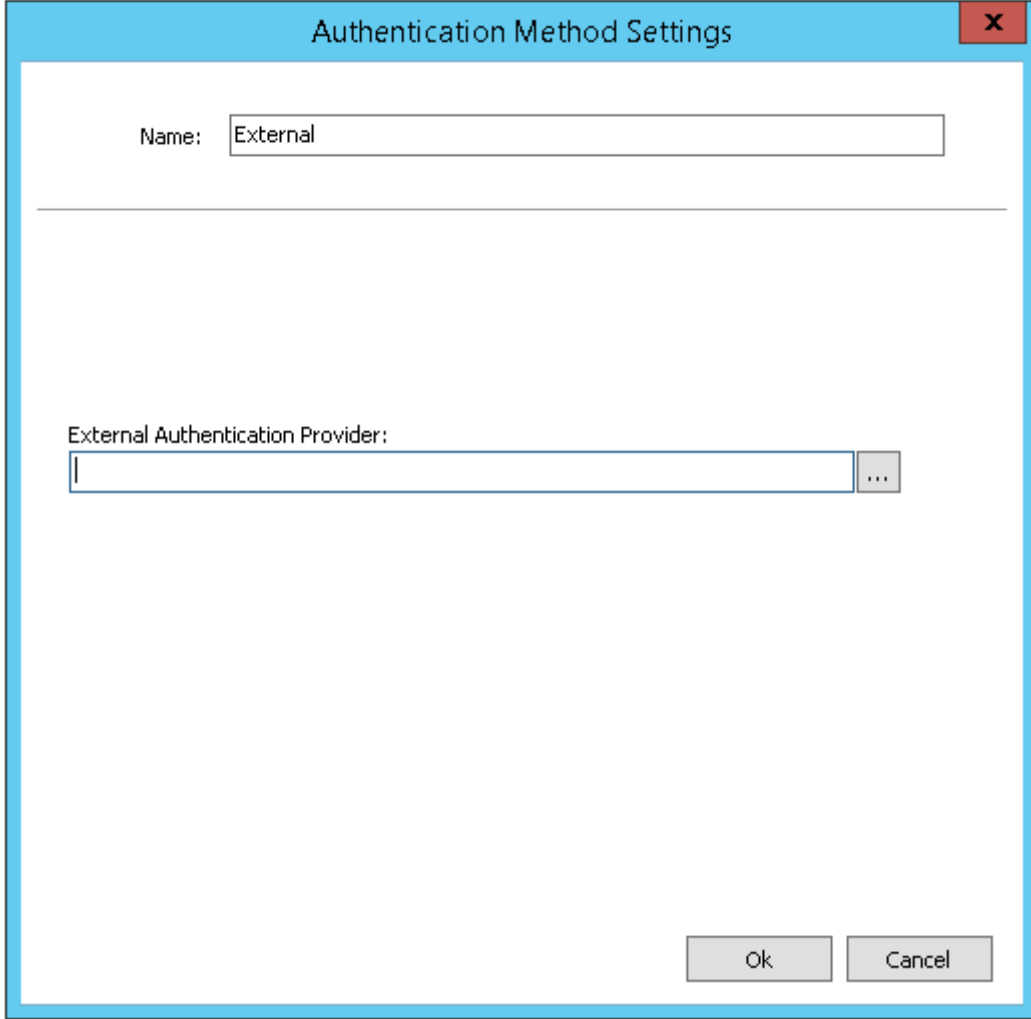
The screenshot shows a dialog box titled 'Authentication Method Settings' with a close button (X) in the top right corner. The dialog is divided into two tabs: 'General' and 'Server'. The 'Server' tab is active. At the top, there are two input fields: 'Name' with the value 'Google' and 'Virtual Path' with the value 'google'. Below these, there are two sub-tabs: 'General' and 'Server'. The 'Server' sub-tab contains several input fields: 'Authorization URL' with the value 'https://accounts.google.com/o/oauth2/auth', 'Authorization parameters' (empty), 'Token Validation Server URL' with the value 'https://accounts.google.com/o/oauth2/token', 'Profile information server URL' with the value 'https://www.googleapis.com/oauth2/v1/userinfo', and 'Login username value in returned JSON' with the value 'email'. At the bottom right of the dialog, there are two buttons: 'Ok' and 'Cancel'.

Şekil 22 : Oauth Authentication Method Tanımı – Server Tabı

Authorization URL	Authorization isteğinin yapılacağı adres
Authorization Parameters	Authorization Url için extra parametreler
Token Validation Server URL	Token Validation Server URL
Profile Information Server URL	Information Server URL
Login username value in returned JSON	Username bilgisinin döneceği JSON alanının adı

1.3.1.4.5. External DLL Authentication Yöntemi

Sadece external dll bilgisinin ayarlanması yeterli olacaktır.

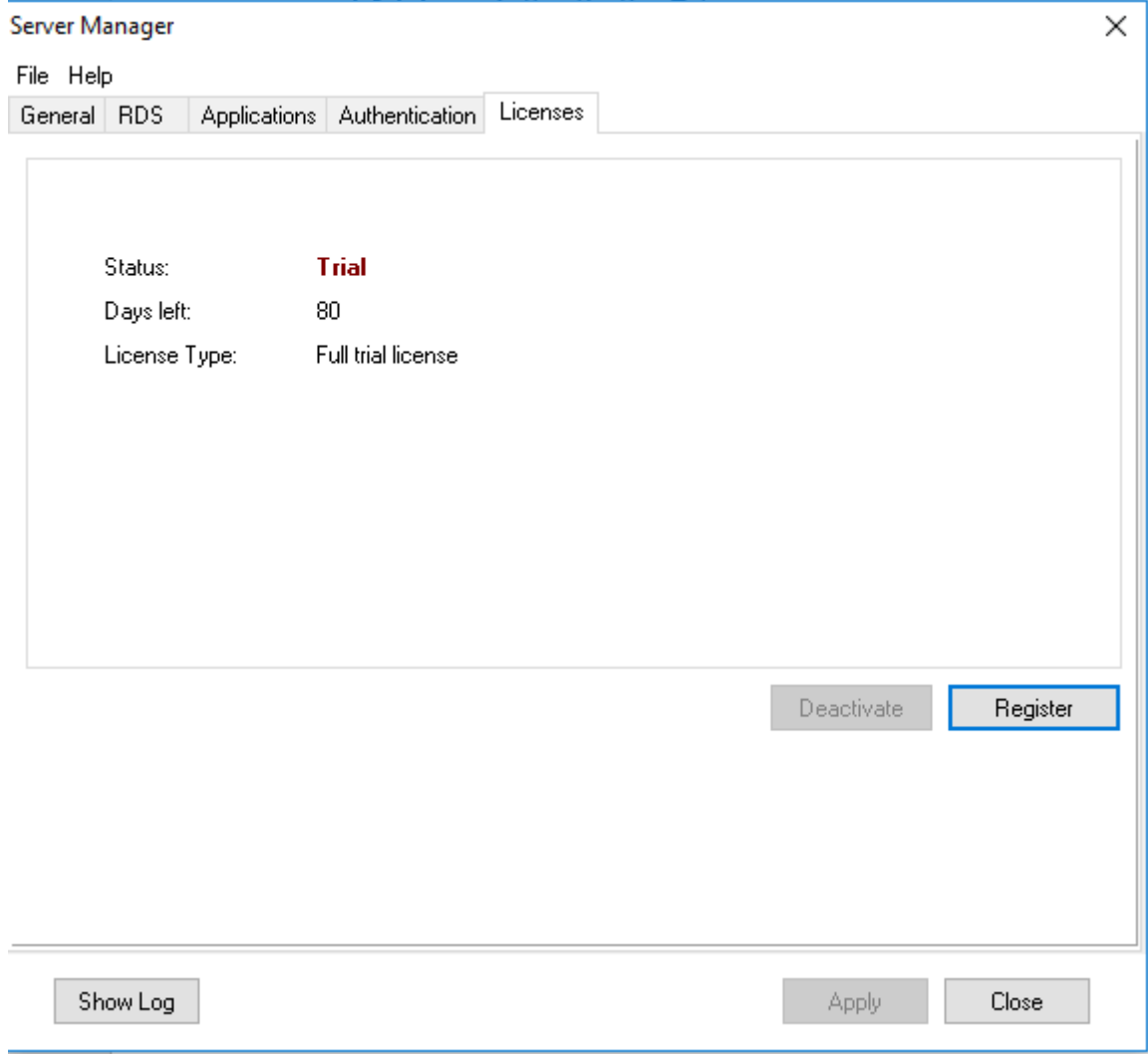


The image shows a dialog box titled "Authentication Method Settings". The dialog has a blue header bar with the title and a red close button. The main content area is white. At the top, there is a label "Name:" followed by a text input field containing the word "External". Below this is a horizontal line. Further down, there is a label "External Authentication Provider:" followed by a text input field that is currently empty. To the right of this input field is a small grey button with three dots. At the bottom right of the dialog, there are two buttons: "Ok" and "Cancel".

Şekil 23 : External Authentication Yöntemi Tanımlama Ekranı

1.3.1.5. Licenses Tabı

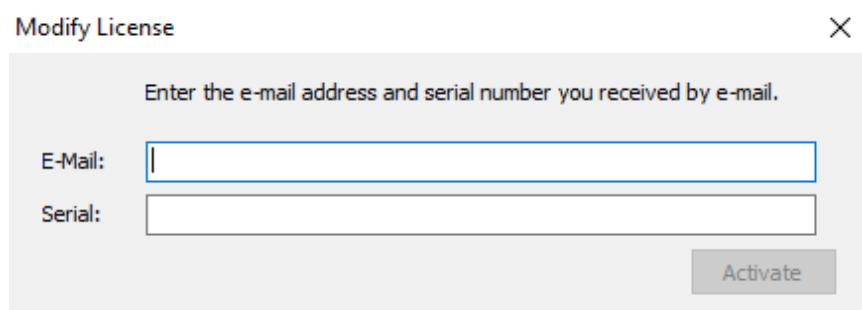
Lisans bilgisinin görüntülediği ekrandır. Kullanıcın sahip olduğu lisansın durumu gösterilir.



Şekil 24 : Lisans Tabı

Deactivate : Mevcut kurulu olan lisans bilgisi sunucudan kaldırılır.

Register : Yeni lisans bilgisi tanımlama ekranını açar.



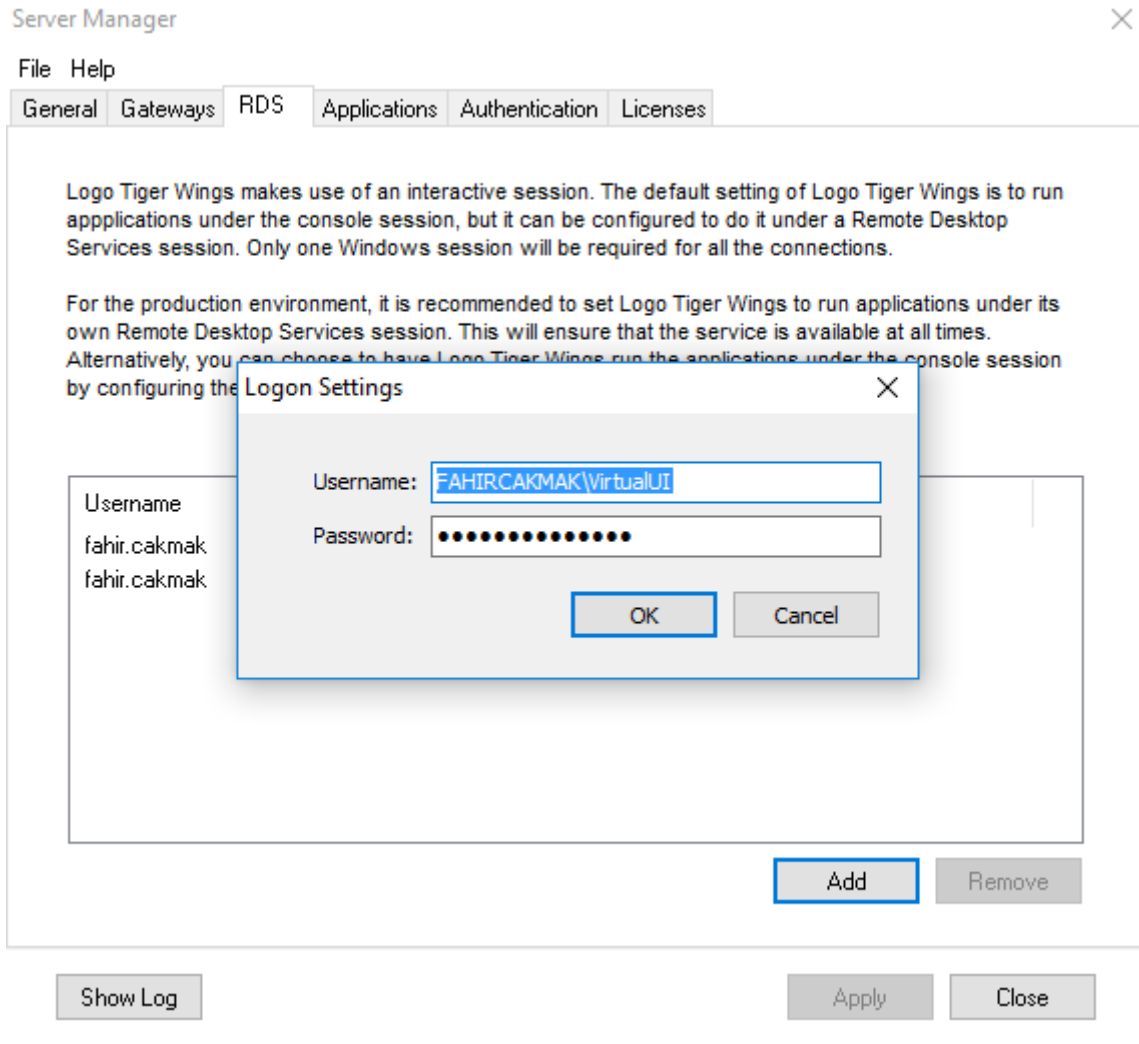
Şekil 25 : Register License Ekranı

Bu ekranda E-Mail adresi alanı Müşteri Numarası Serial alanına üretilen serial key bilgisi girilerek Lisans kaydı gerçekleştirilir.

1.3.2. Netsis Wings Broker Yönetim Paneli

Scaling ve Load balancing senaryolarında yapılan kurulumlarda konfigürasyon yönetim işini Netsis Wings Yönetim panelinden devir alır. Ekranlarda Netsis Wings Yönetim Panelindeki tablolar ve anlatılan bilgiler aynen geçerli olup RDS tabında çoklu RDS account girme farklılığı vardır. Netsis Wings Yönetim Panelinde olmayan ve scaling ve load balancing senaryolarında gerekli olan Gateways tabı bulunmaktadır.

1.3.2.1. RDS Tabı

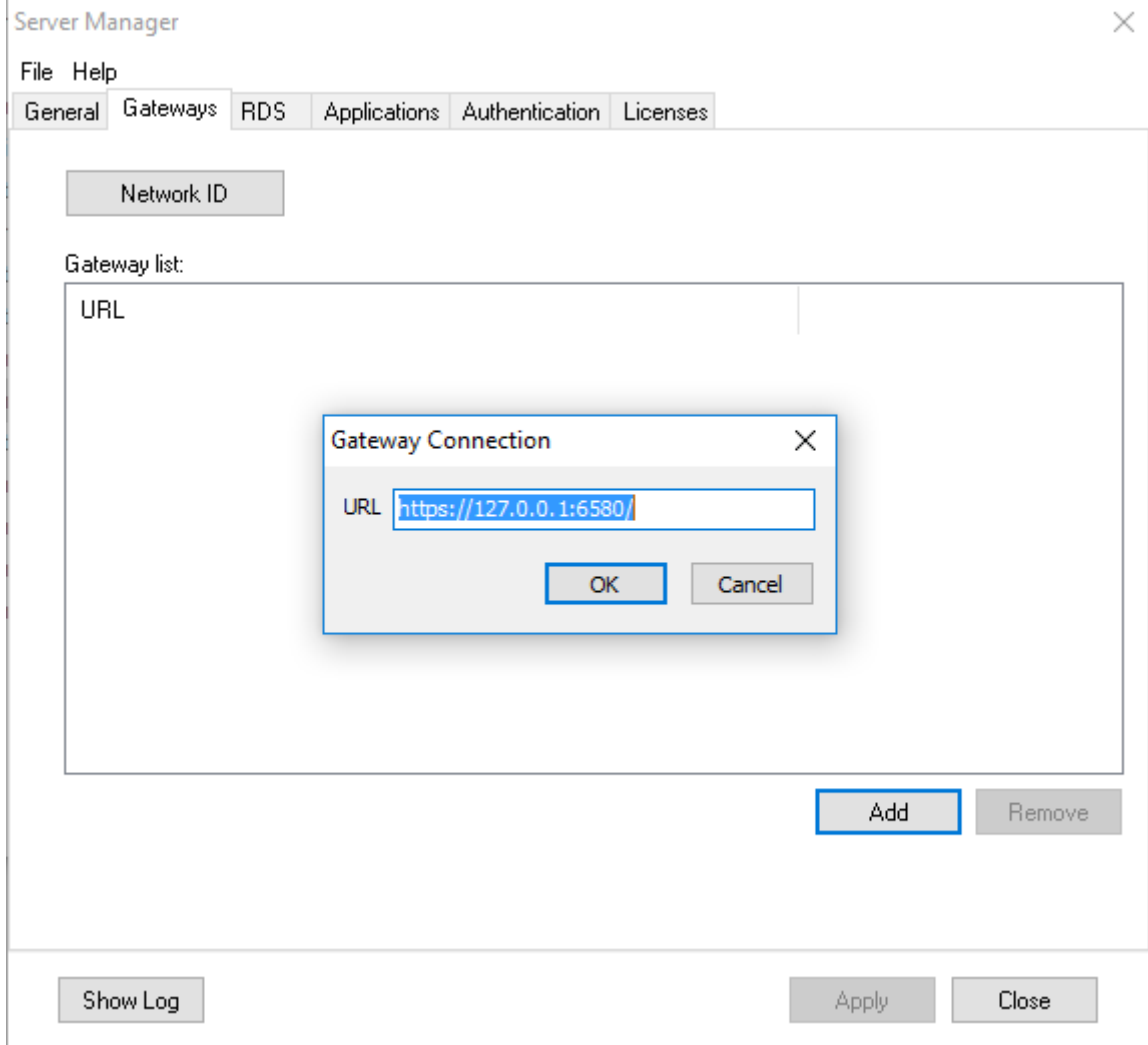


Şekil 26 : Broker Yönetim Paneli- RDS Tabı

Bu alanda mevcut kullanıcı hesaplarını ekleyebileceğiniz gibi işletim sisteminde tanımlı olmayan kullanıcı hesaplarını da ekleyebilirsiniz. İşletim sisteminde olmayan hesaplar otomatik olarak işletim sistemi kullanıcı hesaplarına eklenecektir. Kullanıcı hesapları admin yetkilerine sahip olmalıdır. Bu özelliği kullanabilmek için Servis RD Session Host Role Servisinin yüklü olduğu bir Windows sunucuya kurulu olmalıdır.

Tek bir bilgisayardan daha fazla bağlantıya cevap verebilmek için her RDS sessionı farklı uygulama instancelarını işler. (Bkz : [Scaling ve Load Balancing](#))

1.3.2.2. Gateways Tabı



Şekil 27 : Broker Yönetim Ekranı – Gateways Tabı

Network Id'si eşleşen ve gateway adresi bu alanda tanımlanmış olan gatewaylerden gönderilecek olan istekler işlenip sadece bunlara cevap verilir.

1.3.3. Netsis Wings Gateway Yönetim Paneli

Netsis Wings Gateway Yönetim Paneli load balancing senaryolarında kullanılacak olan Logo Netsis Wings Gateway Servisinin yönetim panelidir. Gateway konfigürasyon ayarları bu panel üzerinden gerçekleştirilmektedir. Tasarlanan sistemde bir adet Gateway düşünülüyor ise bu kısımda girilecek olan IP ve port bilgileri bizim gateway bağlantı bilgilerimiz olacaktır. Eğer birden fazla gateway bulduran bir mimari işletilecek ise DNS sunucusuna bu IP nin girilerek DNS sunucusunun bağlantıları bu gatewaylere yönlendirilmesi sağlanmalıdır. Aynı zamanda aynı mimari içerisinde yer alan bütün gateway ve broker sunucularının aynı network Id yi paylaşıyor olması gerekmektedir.

Apply : Bu buton ile yapılan deęişiklikler kaydedilir.

Close : Bu buton ile Yönetim paneli ekranı kapatılır.

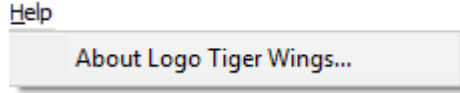
File Menüsü



Şekil 28 : File Menüsü

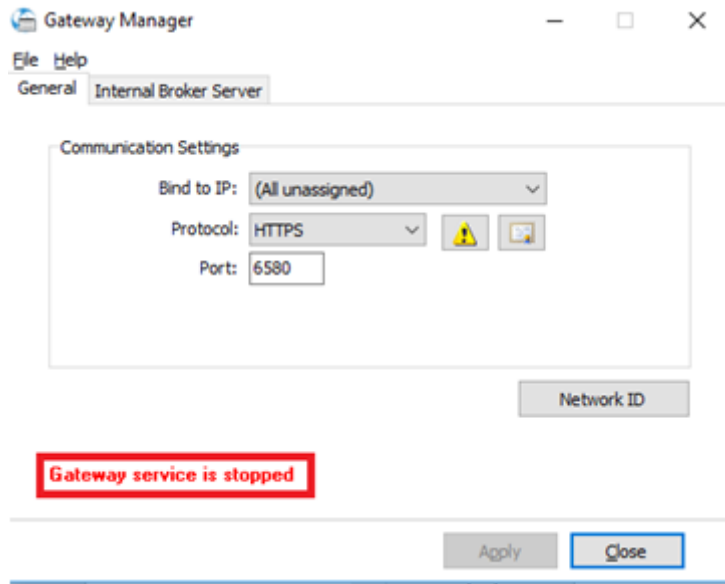
Save	Sistem ayarlarında yapılan deęişiklikleri kaydeder.
Close	Netsis Wings Gateway yönetim panelini kapatır.

Help Menüsü :



Şekil 29 : Help Menüsü



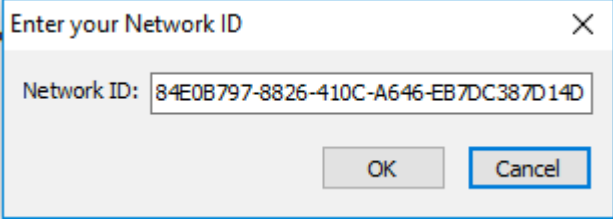
1.3.3.1. General Tabı



Şekil 30 : Netsis Wings Gateway Yönetim Paneli

Şekil 1 ile gösterilen Yönetim Paneli Genel tabında windows servisin durumunu takip edebilirsiniz (Kırmızı kutu içerisine alınan alan). Servisin ayakta olmaması durumunda Logo Netsis Wings Gateway Servisinin çalışır durumda olduğunu kontrol etmeniz gerekmektedir.

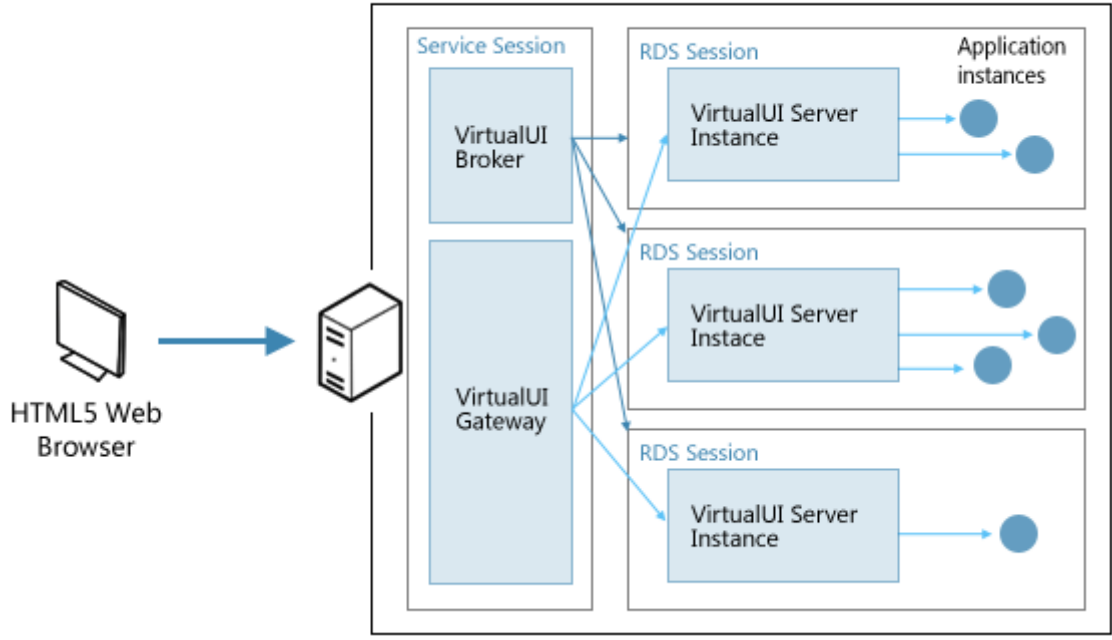
Communication Settings alanında aşağıdaki değerlerin girilmesi beklenmektedir :

Bind to IP	'All unassigned' seçeneği ile bütün mevcut IP adresleri ile gelen bağlantıların servis tarafından karşılanmasını sağlar. Özel bir IP adresi girilir ise sadece bu IP adresi üzerinden gelen istekler cevaplanır.
Protocol	Http ve Https protokolleri arasında yapılan tercih bu kısımda belirtilir. Varsayılan olarak Http portu üzerinden yayın yapılmaktadır.
	Protocol bilgisinin yanında yer alan bu buton ile Http varsayılan hatalarının yönlendirileceği hata sayfalarının değiştirilebileceği Hata Sayfası ekranına geçiş yapılır. (Bkz. Hata Sayfası Ekranı)
	Protocol olarak Https seçildiği durumda görünür.Https için kullanılacak olan SSL sertifikası tanımının yapıldığı SSL Sertifikası ekranını açar. (Bkz SSL Sertifikası Ekranı)
Port	Logo Netsis Wings Gateway Servisinin hangi porttan dinleme yaptığını gösterir.Varsayılan olarak 6580 portundan dinleme gerçekleştirir.
Network Id	İlgili Logo Netsis Wings Gateway kurulumunu tanımlar. (Id bilgisi). Kaynaklarını bu gateway ile paylaşmak isteyen Netsis Wings Broker kurulumları bu Network Id bilgisini tanımlamalıdır. Varsayılan olarak restgele bir string değer atanır, daha tanımlayıcı bir değerle değiştirilebilir. 

1.4. Scaling and Load Balancing

1.4.1. Tek Sunucu Çoklu Hesap

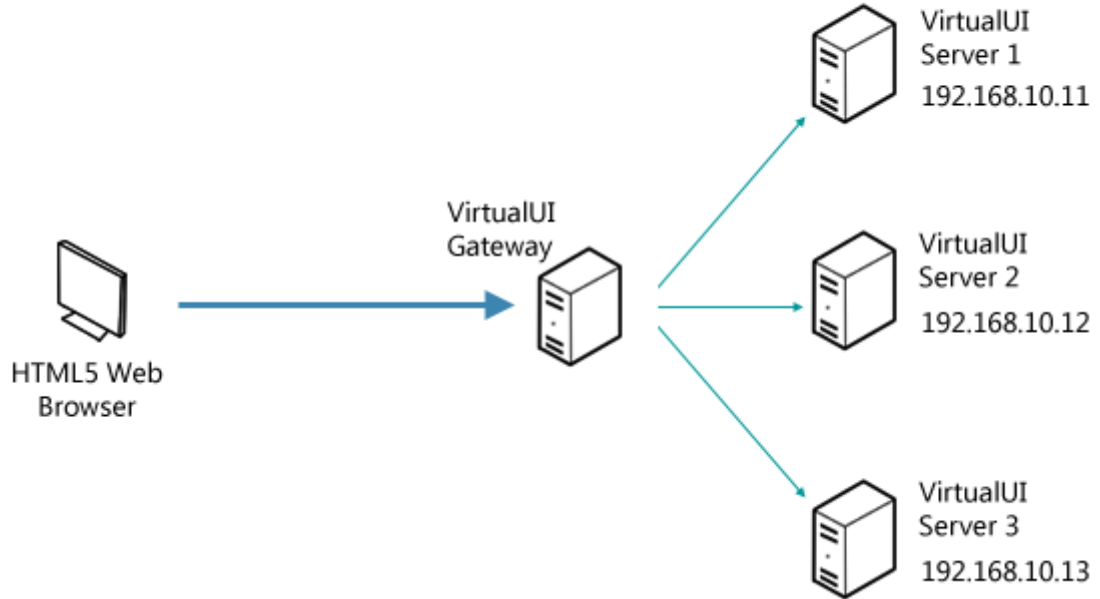
Tek bir sunucu üzerinde Çoklu RDS Hesapları ile farklı sunucu instanceları oluşturularak, farklı uygulama instancelarının ayrı ayrı sunucu instanceları tarafından ele alınması sağlanabilir. Oluşturulan bu sunucu instanceları Logo Netsis Wings Broker Servis tarafından yönetilir, instanceın sağlıklı bir şekilde çalışır durumda olduğu kontrollerini yaparak, uygulama instancelarının sunucu instancelarına dağıtılması işini Logo Netsis Wings Gateway Servis ile birlikte çalışarak halleder.



Şekil 31 : Tek Sunucu Çoklu Hesap Senaryosu

1.4.2. Çoklu Sunucu ile Load Balancing

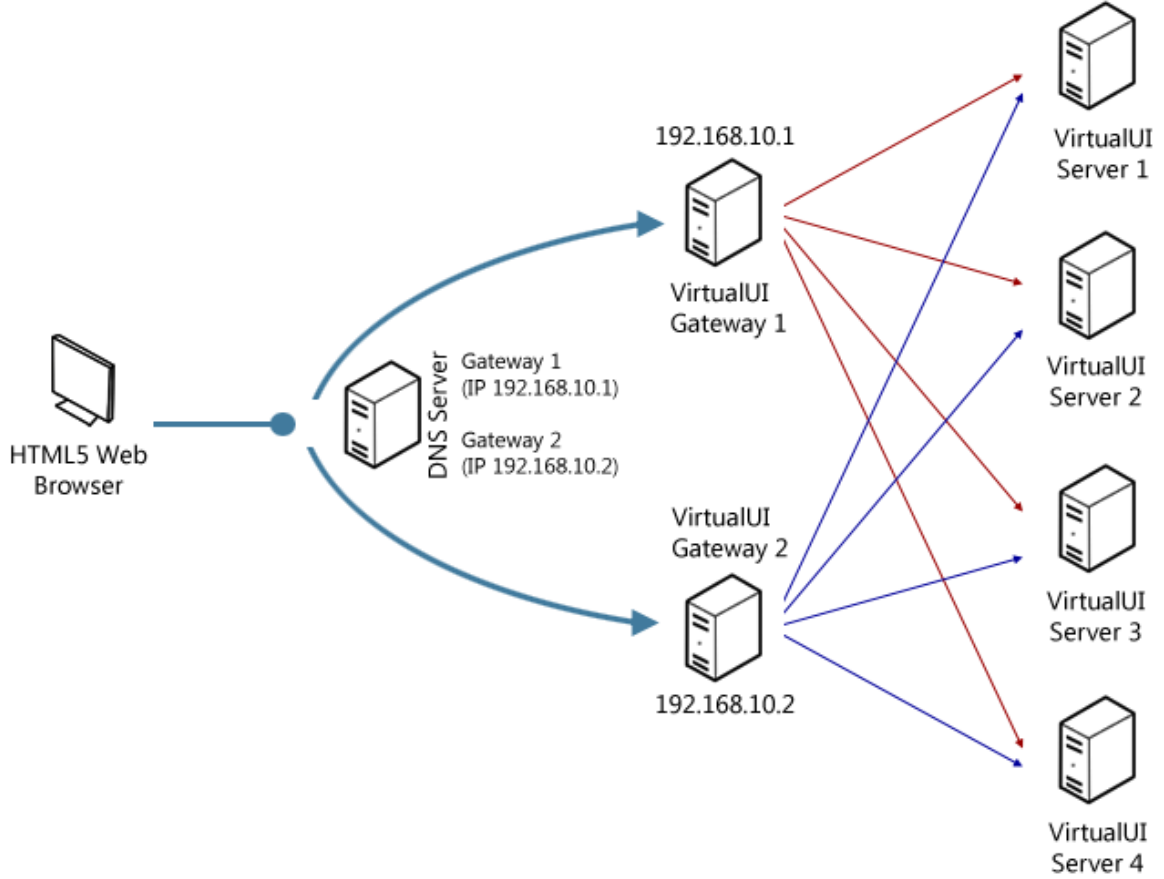
Bu senaryoda tek bir Logo Netsis Wings Gateway Servisi bağlantıları farklı sunuculara dağıtır.



Şekil 32 : Çoklu Sunucu ile Load Balancing Senaryosu

1.4.3. Çoklu Gateway ve Sunucu ile Load Balancing

Bu senaryoda dış kaynaklı bir DNS sunucusu farklı Gateway servislerine load balancing yapar.



Şekil 33 : Çoklu Gateway ve Sunucu ile Load Balancing Senaryosu

1.4.4. Çoklu RDS Hesabı ve Çoklu Sunucu ile Load Balancing

Bu senaryo Tek Sunucu Çoklu Hesap senaryosu ve Çoklu sunucu ile Load balancing senaryolarının birleştirilerek kullanılması ile gerçekleştirilir.