Guideline to secure Datatal Flexi server

Summary

Datatal Flexi is a communication platform that helps with your company´s telephony. Datatal Flexi uses several interfaces to communicate with other systems and some of them might be targeted for hacking attempts. This guide will help you to better secure you Flexi system.
Datatal cannot guarantee that Flexi won't be hacked by following these steps and Datatal take no responsibility if this would happen.

This document will focus on secure interfaces that Datatal Flexi uses. This document best applies to Flexi release 5.9 or higher.

This document is a guideline how to enhance security, in addition to this there are other ways to improve the security around the Flexi-platform. We recommend that you to read this document throughout before implementing any changes.

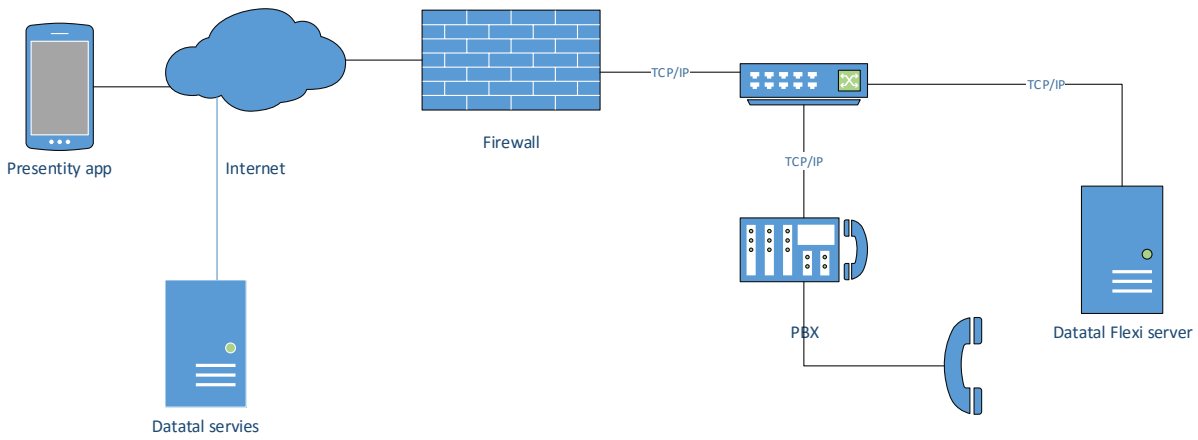
Summary checklist

1. Strong NT-account administrator password
2. Activate Windows update, update at least every month
3. Firewall
4. Antivirus
5. Valid Web SSL certificate
6. Block /admin from external access, look at IP and domain restriction
7. DNS
8. Use both IPv4 and IPv6
9. Use only https

Table of content

Technical overview

This is a basic setup.



Interfaces between Datatal Flexi server and PBX depends on the PBX brand. All integration between Datatal Flexi and PBX brands use SIP (Session Initiated Protocol) for VoIP functionality. For CTI (Computer Telephony Interface) Flexi uses, TAPI, CSTA3, MiTai or Mitel OIP Corba.

Description	Protocol	Port	Access
SIP – VoIP functionality	TCP/UDP	5060	Internal. Flexi <-> PBX
RTP – Audio stream protocol	UDP	40000-50000	Internal. Flexi <-> PBX
TAPI – Avaya IP office	TCP and UDP	50797	Internal. Flexi <-> PBX
TFTP – Avaya IP office	UDP	69	Internal. Flexi <-> PBX
TAPI - Panasonic NS1000	TCP and UDP	33333	Internal. Flexi <-> PBX
CSTA3 – Mitel Mx-one	HTTP	80	Internal. Flexi <-> PBX
MiTai ICP	TCP	Unknown	Internal. Flexi <-> PBX
Mitel OIP Corba	TCP	2809	Internal. Flexi <-> OIPsrv
Web interfaces	HTTP/HTTPS	443	External. Flexi <-> app/web
Datatal Telephony manager	TCP	9692	External. Flexi <-> app/web
Datatal Active state	TCP	13404	External. Flexi <-> operator
Datatal Exchange connector	TCP	13317	Internal. Flexi <-> Exchange server
Datatal license server	HTTPS	443 to IPv4 82.115.148.0/24 IPv6 2a01:650:28:5::255:0/112	External. Flexi <-> services.datatal.se
Datatal Voice manger	HTTPS	443 to IPv4 82.115.148.0/24 IPv6 2a01:650:28:5::255:0/112	External. Flexi <-> services.datatal.se

Windows security

Securing the Windows operating system is the most important part. If unauthorized users gets control of Windows, there are some test tools and other functions that could be abused.

Here is a checklist of actions;

1. Datatal supports the use of a virtual environment, either vmware or Hyper-V. All of Datatal´s internal testing and development is done on server applications in a virtual environment.
2. Activate windows update, we always test Flexi with the latest Windows patches. It can be set to download automatically but should be installed and rebooted under supervision. Basic testing of Flexi after a Windows update is recomended.
    a. Test the use of basic functionality for each product, for example;
        i. Flexi Tid, book a call and call it back
        ii. Flexi Presentity, divert a user and call diverted user
        iii. Flexi CC, call a queue and verify that the call gets transferred to an agent
3. Antivirus software installed
4. Local firewall installed and configured. Port and application name is listed in the beginning of this document
5. Continuous Backup of Flexi root folder, it includes voicemail, database and registry. Default C:\Flexi
6. Disk, it´s recommended to have 2 partitions, C: and D:. During the installation phase install all Flexi components and Flexi root under D:. Remember that SQL server express and Flexi Database will be stored under C: by default, also that Windows update tend to consume a lot of disk space over time. It´s rather complicated to expand C: drive even in virtual environment. A typical Flexi installation should not take more than a total of 20 GB. Use thin provisioning in the virtual environment to save disk space on data storage.

Secure Connection

For secure connection https must be activated in IIS, from the release 5.11.1 https gets activated by default for the Flexi websites.

Presentity App

In the Flexi Presentity mobile application, there is a setting that activates *Secure connection*, this means that HTTPS will be used to communicate with the Flexi Presentity server. This setting is next to server id in the app.

Presentity Operator

Same as in the Flexi Presentity mobile app, there is a checkbox to activate secure connection. This will ensure the use of https for communication with the server.

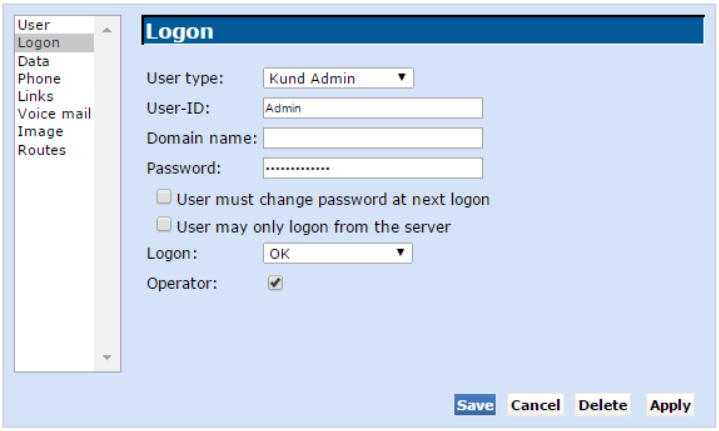
Other Web applications

All other web interfaces can be accessed using https. Such as Flexi Tid user web, Admital Web, Presentity Web.

Accounts

A first step to secure a Flexi installation is to set strong passwords for the NT-account of Windows Server, at least 10 characters with both digits and special characters. It is the single most important account!

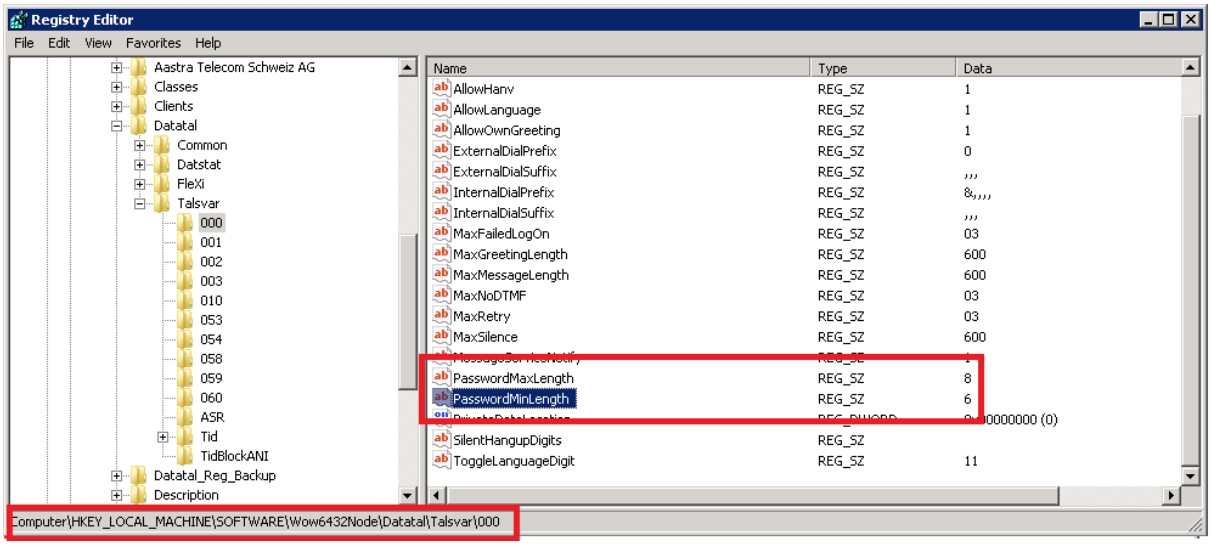
Second, secure the default system admin accounts for Flexi. There are 2 default accounts for Flexi, sysop and admin. Sysop account can only log into Flexi administration from the local server. Admin account password is required to be changed from default when Flexi gets installed or upgraded. These accounts can be used to logon to Flexi Server https://<SERVERIP/FQDN>/admin go to user and click on customer admin account. Go to Logon and set credentials.



The setting *User may only logon from server* means that this account can only be used on the local server. By default, it is only the Sysop account that has this feature activated. Password length is recommended to be at least 10 characters long.

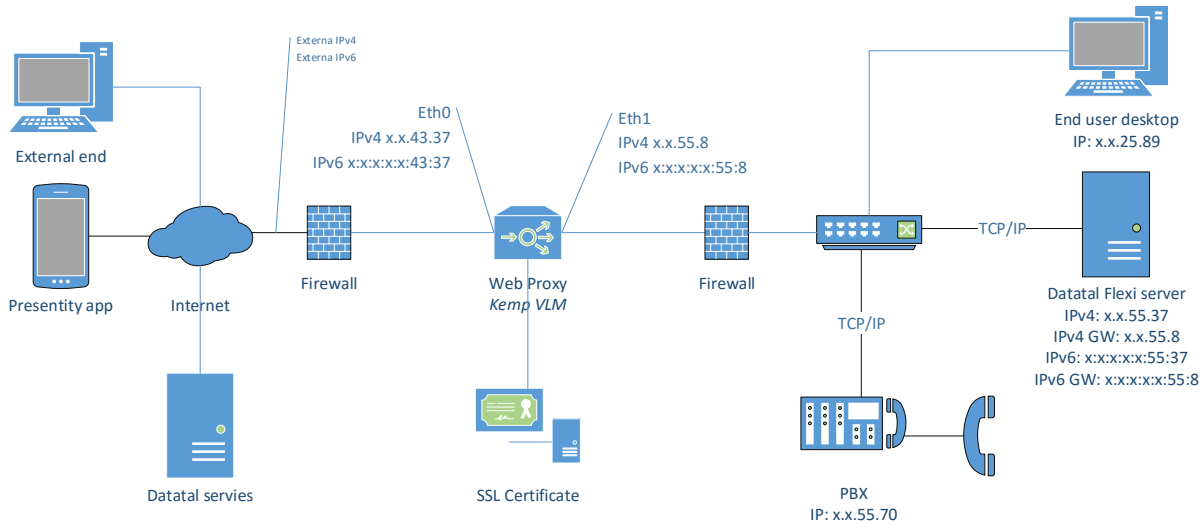
All Flexi users that has a User-Id and password will be able to log into Admital web, but only as a user. By default, user privilege cannot access any settings.

For Flexi users that uses Presentity functionality, such as Presentity app or voicemail. All new Presentity users will receive 0000 as default pin code. **Pin code should be changed to something else ASAP**. By default pin code is limited to 4 digits, this can be extended. Recommended is 6-8 digits but this can be hard for end users to remember. Pin code must be digits because users can call into the system and use the dial pad to log into Flexi. **To change min/max pin code length, edit these registry entries.**



Datatal Flexi and Kemp VLM

It´s recommended to have a web proxy between the Flexi server and the internet. Datatal recommends Kemp VLM, it can be deployed as a virtual appliance. Below is an example setup. For installation and system configuration for the Kemp VLM please consult Kemp documentation. It is also **strongly** recommended to get a public certificate from an SSL Certificate Provider. Datatal recommend GlobalSign



Datatal Flexi supports IPv6, if IPv6 is to be used for Presentity mobile application or other Flexi Web application this must be configured in the Web proxy as well.

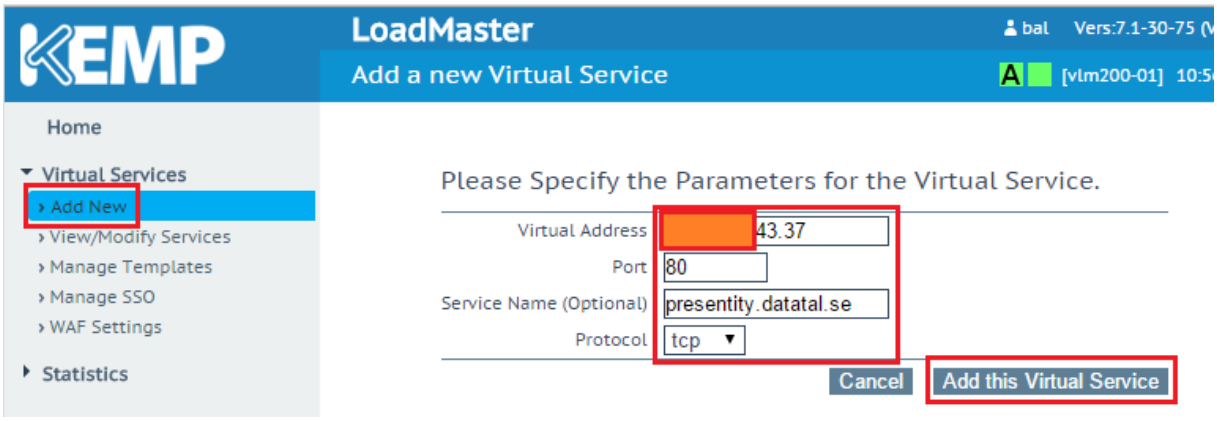
On the Flexi server, the default gateway must be set to web proxy server, but you should add some specific alternative route for internal usage. Do this before you change the default GW on the server. In this example End user desktop cannot communicate directly to server. Use route add command on the Flexi server.

Example, change the x:es to correct numbers. Both for IPv4 and IPv6

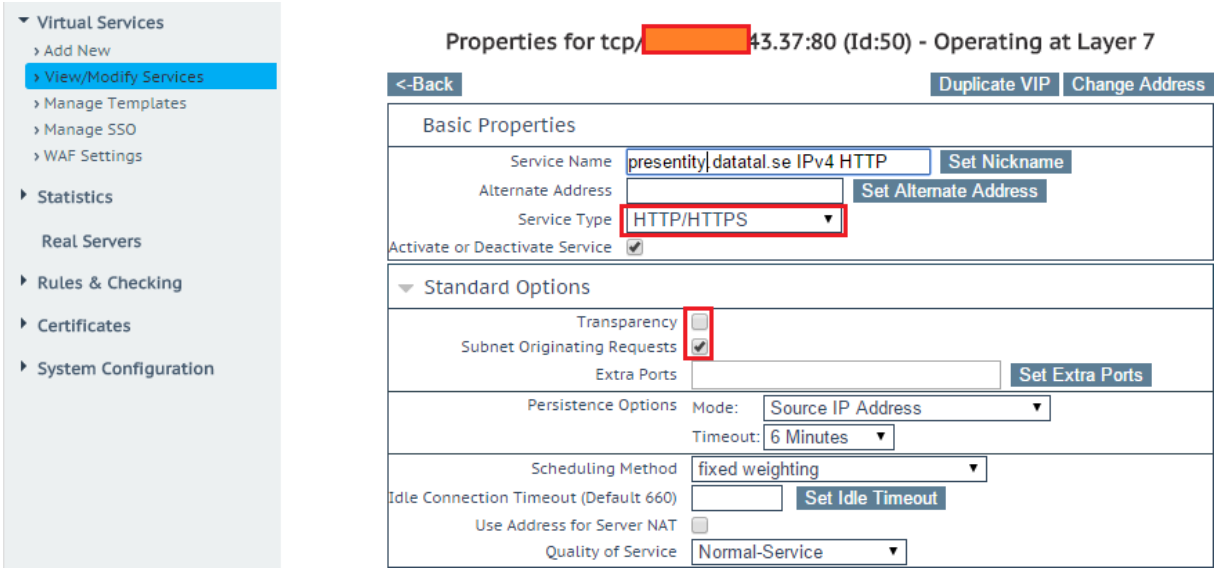
Route –p ADD x.x.25.0 MASK 255.255.255.0 x.x.25.<Real GW IP>

Setup Kemp VLM with HTTP

Create a new Virtual Service and set DMZ IP and Port 80

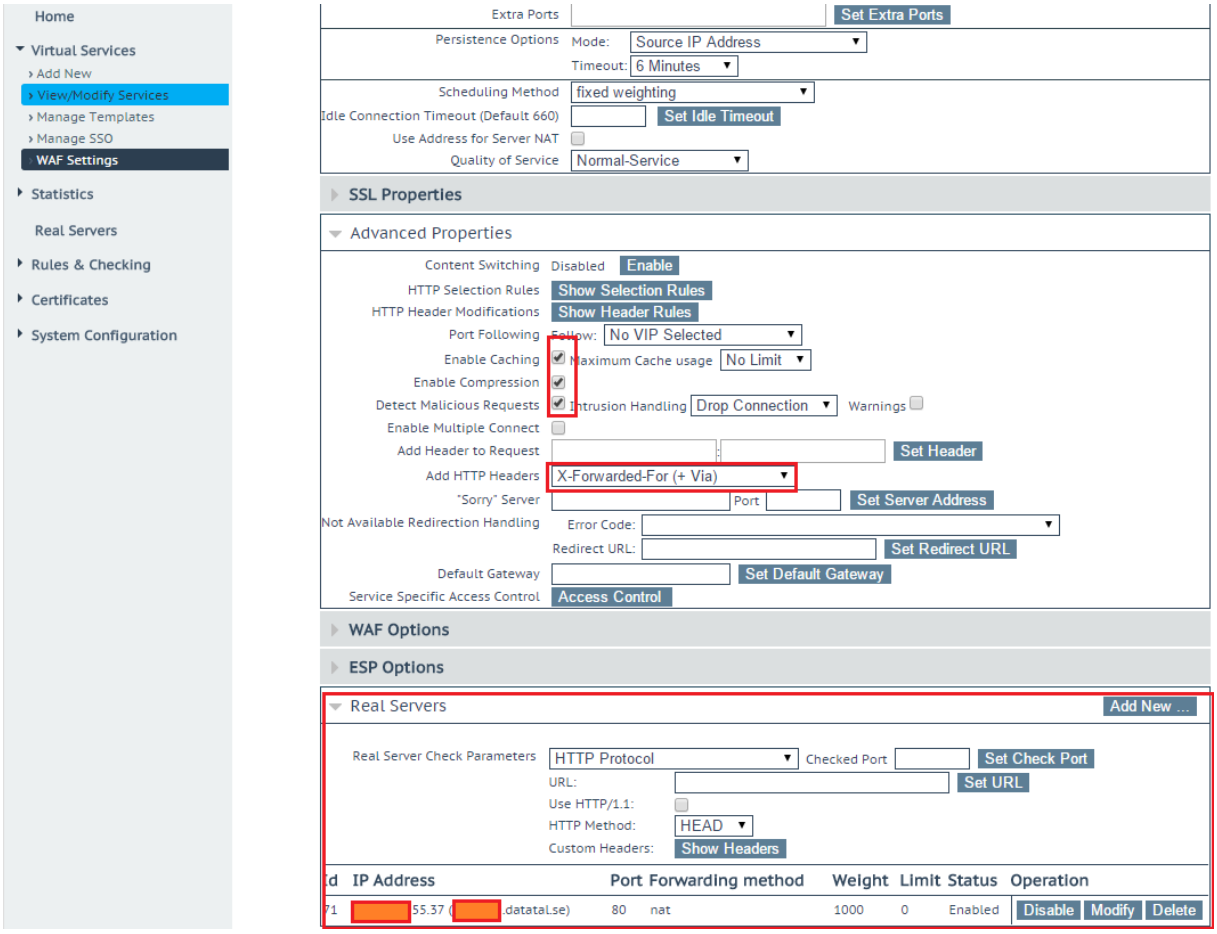


Service Type, must be HTTP/HTTPS



Enable feature caching, compression and detect malicious requests. Important to also set Add Http Headers to X-forwarded-For(+Via). This enables that the Flexi server can get the originated IP address on HTTP request.

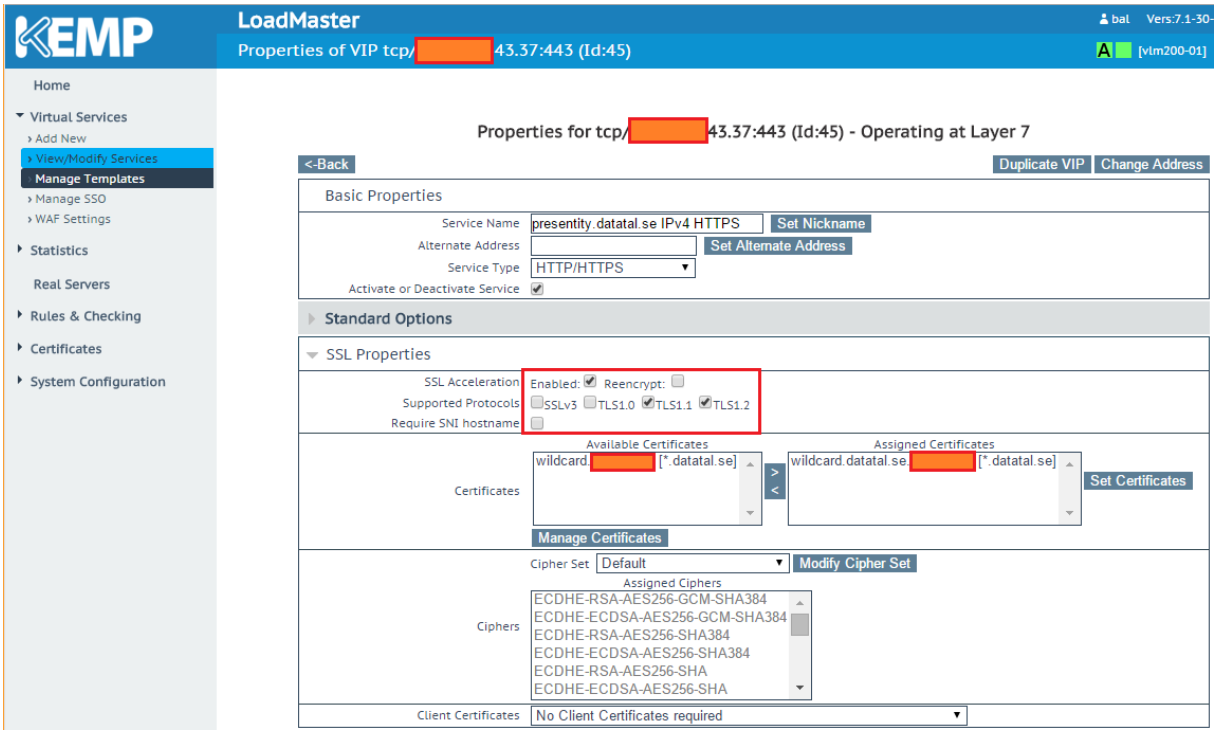
Also add a Real server (Flexi server)

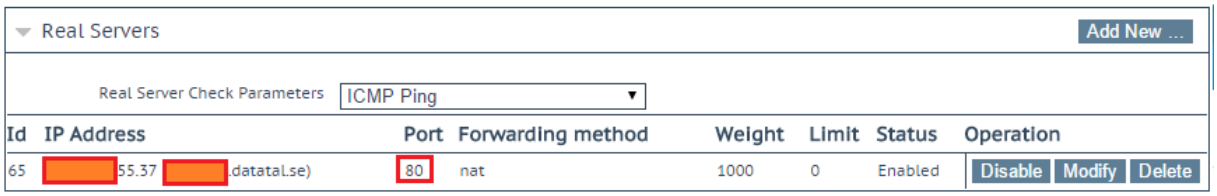


Setup Kemp VLM with HTTPS

Same setup but uses 443 for port and some additional settings under SSL Properties

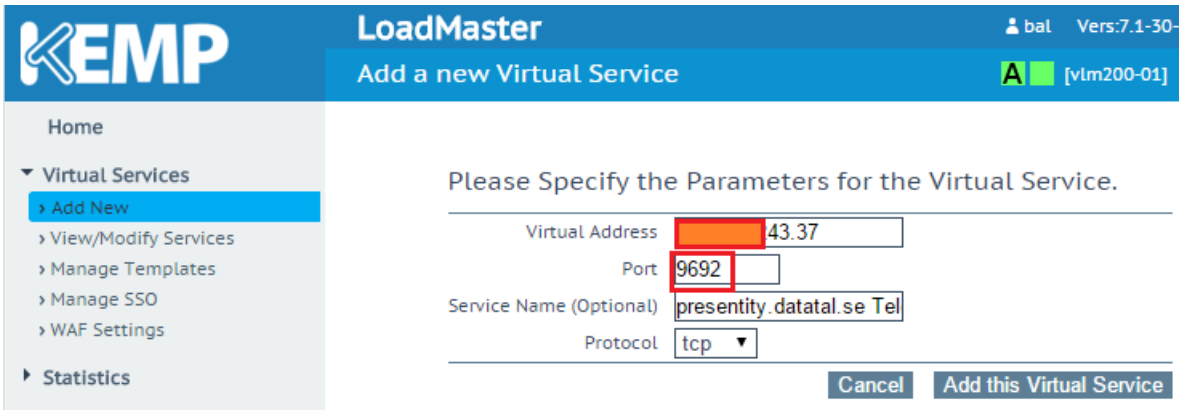
In this setup wse use a wildcard certificate.



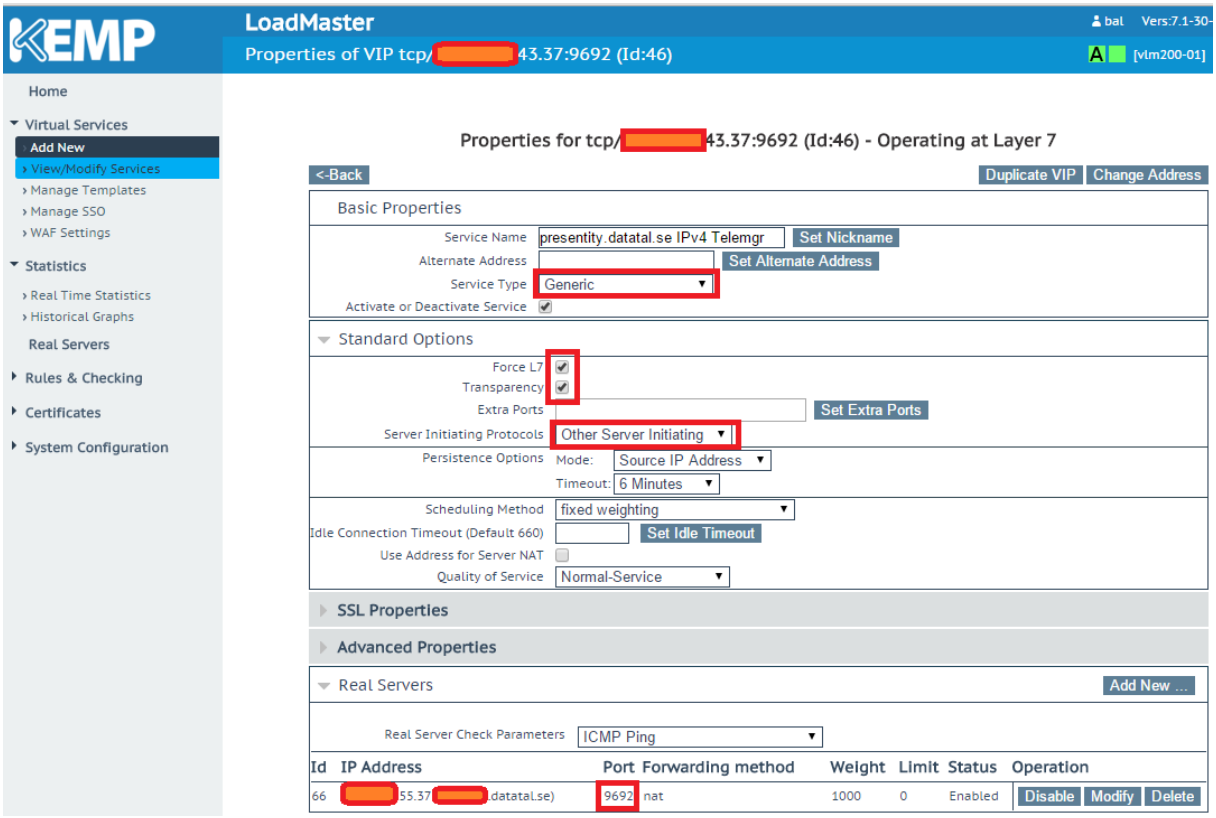


Setup Kemp VLM with Telephony manager port

Port is 9692

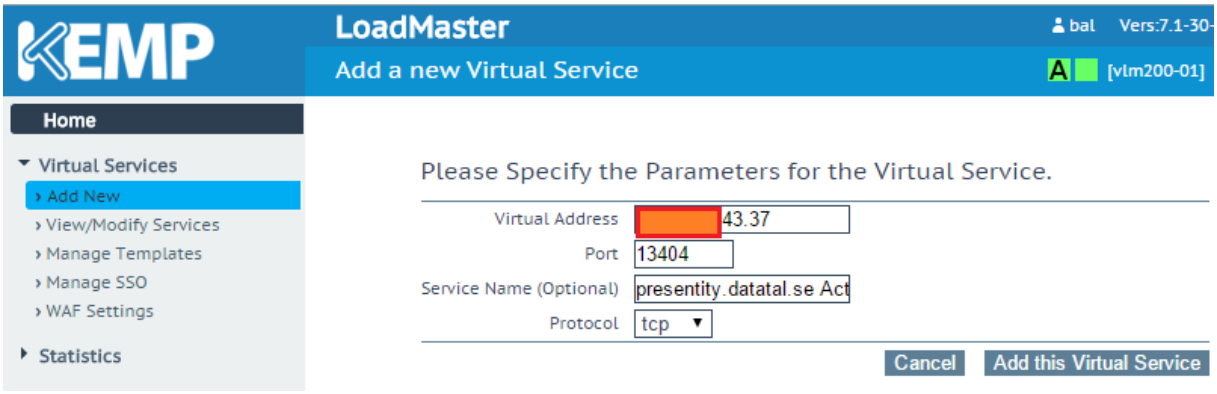


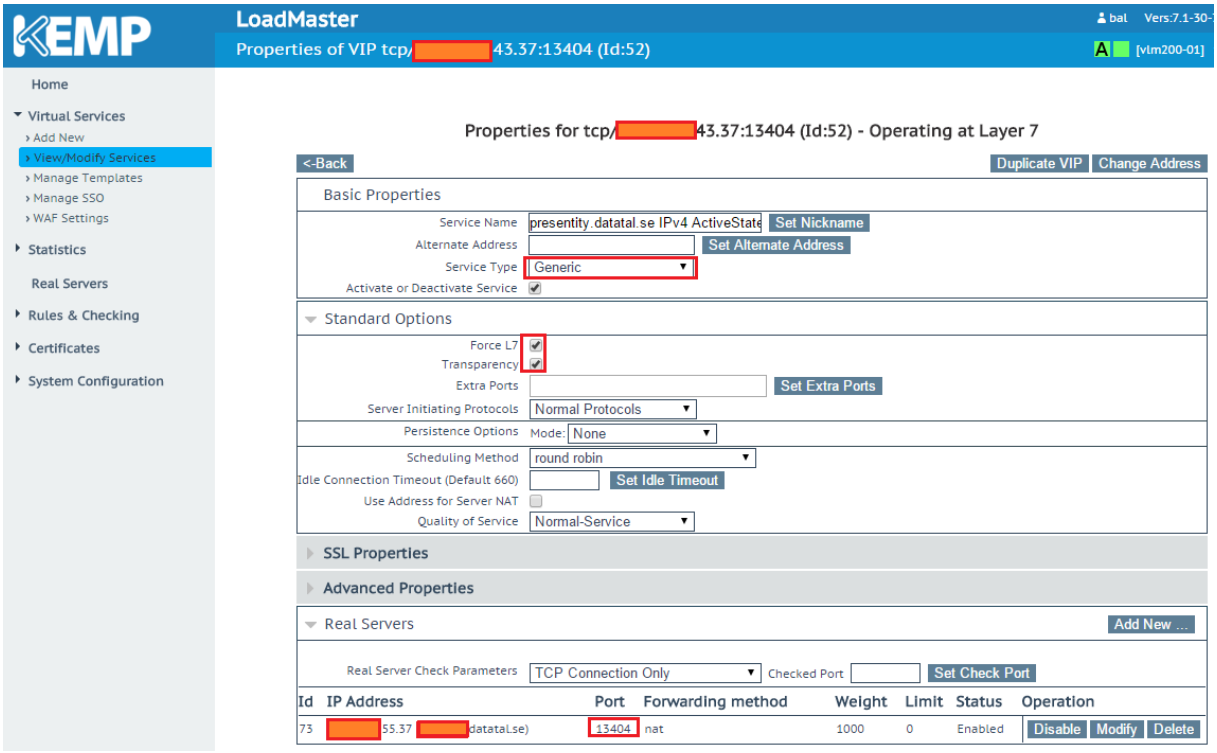
Service Type is set to Generic



Setup Kemp VLM with Active State port

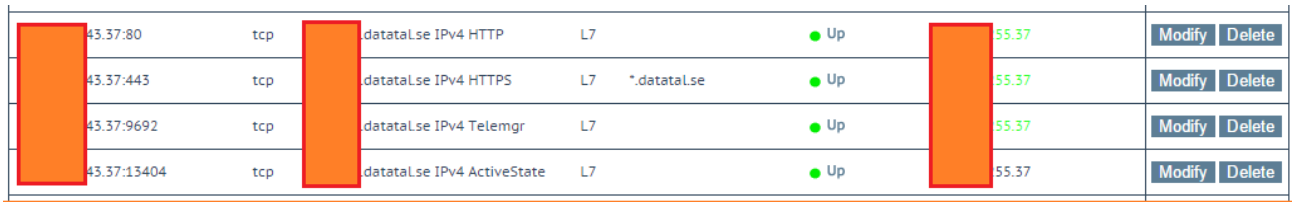
If a Presentity operator is present and should be able to access Presentity server externally. It´s required to setup Active State port 13404 TCP



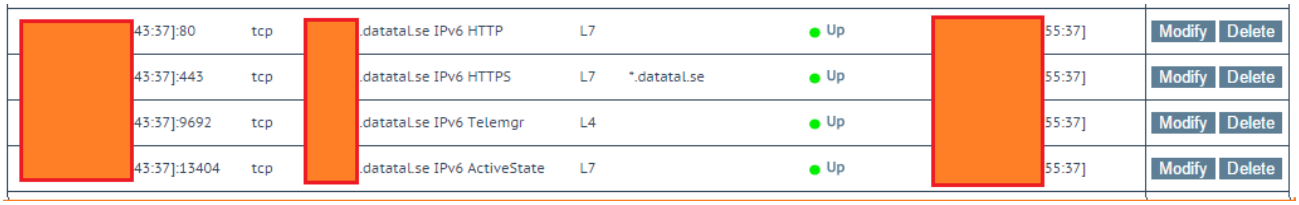


Overview

IPv4

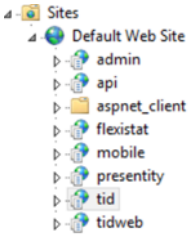


Repeat this step 1-4 to add IPv6 as well.



Internet Information Service settings

Datatal Flexi uses several virtual applications. These application's is created by Flexi server setup. Below is a summary of these virtual applications



/admin

Admital Web, administration web for Flexi. Here an administrator can login and configure user and system settings. Site is coded in PHP

/api

A REST api, it´s primary usage is for Flexi Presentity Operators. But it can also be accessed by 3rd party via a license. .NET 3.5.1 website

/flexistat

Extended statistics website, can only be accessed within Admital Web. .NET 4.5 website

/mobile

Presentity mobile applications primary communication API, is an XML based API. This site must be accessible for external users if the Presentity mobile application should work at all. This also creates a ticket for other APIs, such as Telephony Manager Port 9692. Site is coded in PHP

/Presentity

Presentity main web site, it´s for the end users. Within this site a user can listen to voicemails, set presence state and have a basic overview of their colleague's telephony states. .NET 3.5.1 website

/tid

FlexiTid main web site, it´s for the end users that uses FlexiTid. From this site a user can call booked calls, answer queued call and listen to voicemails. Site is coded in PHP

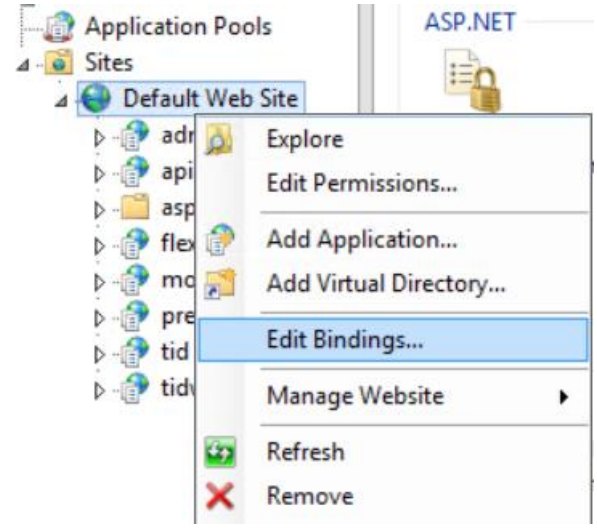
/tidweb

Flexi Tid external booking site. From this a customer can book a time to be called by agents in FlexiTid. This site should be accessible from internet if FlexiTid and this feature is requested. Site is coded in PHP

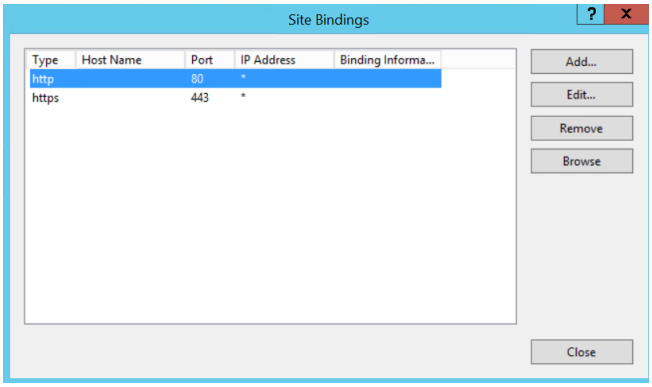
Site Bindings

Bind port to correct host name

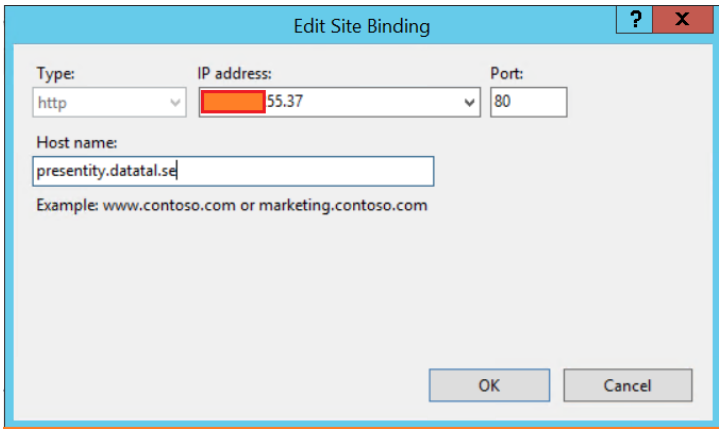
Edit Bindings



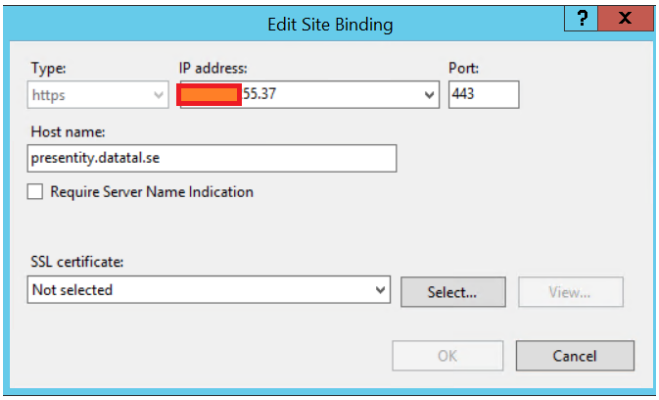
Edit http



Set correct IP to bind and set correct FQDN



Same procedure for HTTPS, but this step requires a SSL Certificate, this could be a self-signed but it's recommended to get a valid form a SSL Certificate Provider.



PHP settings

In C:\Windows\php.ini change these settings.

```
expose_php = Off
```

Create a separate Website for External web

It's also possible create a new Website for the sites for External use only. To only expose those end user virtual applications, use these commands to create a separate website for external web connections and the separated virtual application. When you have created this new virtual application you may change in the web proxy to use the 8080 port instead of 80 on the real server. Same with https, 443 to 4443.

Create app pool for external usage.

%windir%\SysWoW64\InetSrv\AppCmd.exe add apppool /name:DatatalExternalTidExternal /managedRunTimeVersion:v2.0 /managedPipelineMode:Integrated /enable32BitAppOnWin64:true

%windir%\SysWoW64\InetSrv\AppCmd.exe add apppool /name:DatatalExternalPresentity /managedRunTimeVersion:v2.0 /managedPipelineMode:Integrated /enable32BitAppOnWin64:true

%windir%\SysWoW64\InetSrv\AppCmd.exe add apppool /name:DatatalExternalMobile /managedRunTimeVersion:v2.0 /managedPipelineMode:Integrated /enable32BitAppOnWin64:true

%windir%\SysWoW64\InetSrv\AppCmd.exe add apppool /name:DatatalExternalAPI /managedRunTimeVersion:v2.0 /managedPipelineMode:Integrated /enable32BitAppOnWin64:true

Create a new website for external connections

%windir%\SysWoW64\InetSrv\appcmd add site /name:DatatalExternal /bindings:http/:8080:,https/*:4443: /physicalPath:"C:\inetpub\wwwroot"*

Notice that you also need to assign a SSL certificate to 4443 port, otherwise it will not work. This site binds on http 8080 and https 4443

Create Virtual applications for external connections

Note that the /physicalPath parameter maybe must be changed, this is the default path

%windir%\SysWoW64\InetSrv\appcmd add app /site.name:DatatalExternal /path:/mobile /physicalPath:"C:\Program Files (x86)\Datatal\FleXi\WWW\Mobile Web"

%windir%\SysWoW64\InetSrv\appcmd add app /site.name:DatatalExternal /path:/tidweb /physicalPath:"C:\Program Files (x86)\Datatal\FleXi\WWW\tidexternal"

%windir%\SysWoW64\InetSrv\appcmd add app /site.name:DatatalExternal /path:/presentity /physicalPath:"C:\Program Files (x86)\Datatal\FleXi\WWW\presentity web"

%windir%\SysWoW64\InetSrv\appcmd add app /site.name:DatatalExternal /path:/api /physicalPath:"C:\Program Files (x86)\Datatal\FleXi\WWW\web api"

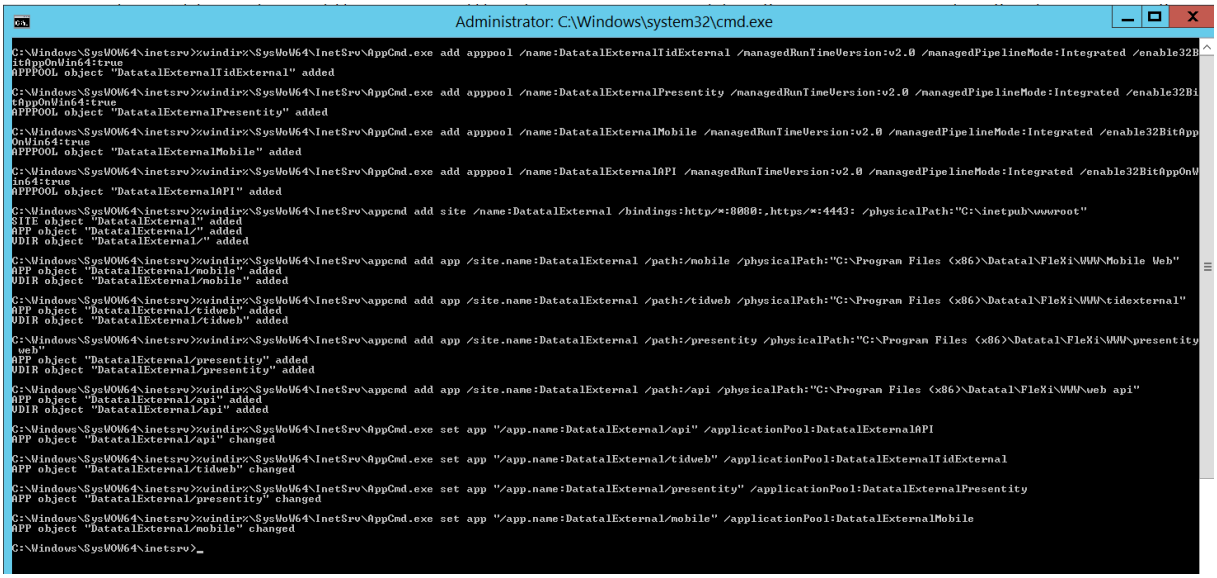
Set correct app pools

%windir%\SysWoW64\InetSrv\AppCmd.exe set app "/app.name:DatatalExternal/api" /applicationPool:DatatalExternalAPI

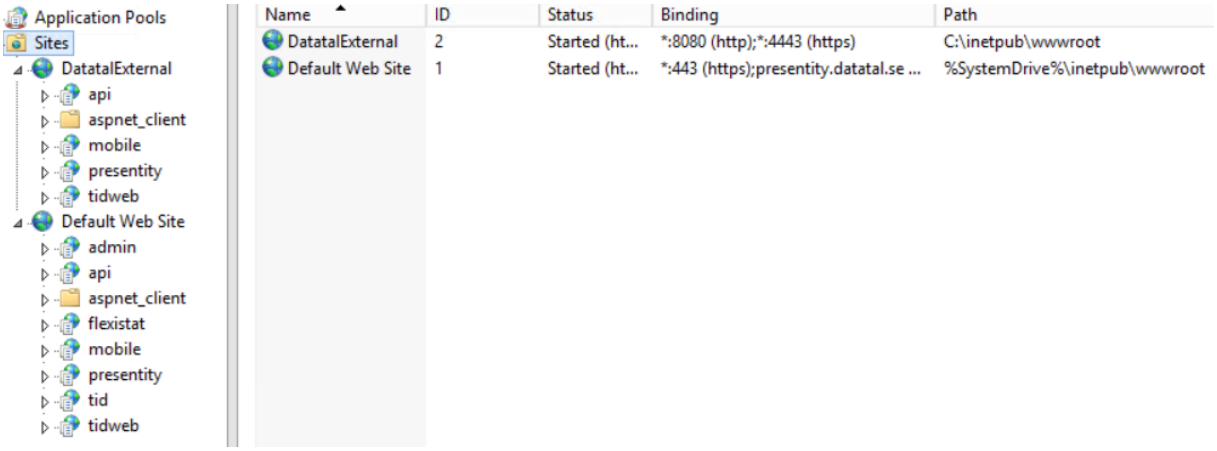
%windir%\SysWoW64\InetSrv\AppCmd.exe set app "/app.name:DatatalExternal/tidweb" /applicationPool:DatatalExternalTidExternal

%windir%\SysWoW64\InetSrv\AppCmd.exe set app "/app.name:DatatalExternal/presentity" /applicationPool:DatatalExternalPresentity

%windir%\SysWoW64\InetSrv\AppCmd.exe set app "/app.name:DatatalExternal/mobile" /applicationPool:DatatalExternalMobile



In the IIS manager interface



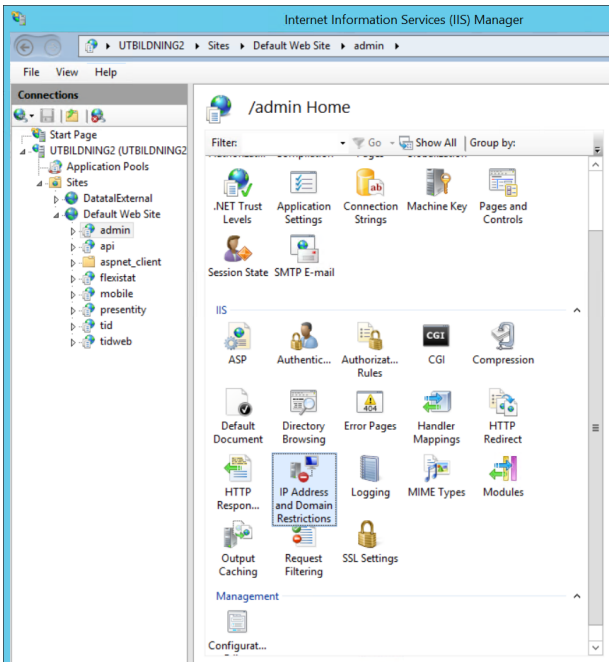
IP Address and Domain Restrictions

Internet information service has an IP address filer function. With this it is also possible to restrict access to some virtual applications. First you must add additional Webserver feature for IP address and domain Restrictions.

To install this, run this command in terminal as administrator

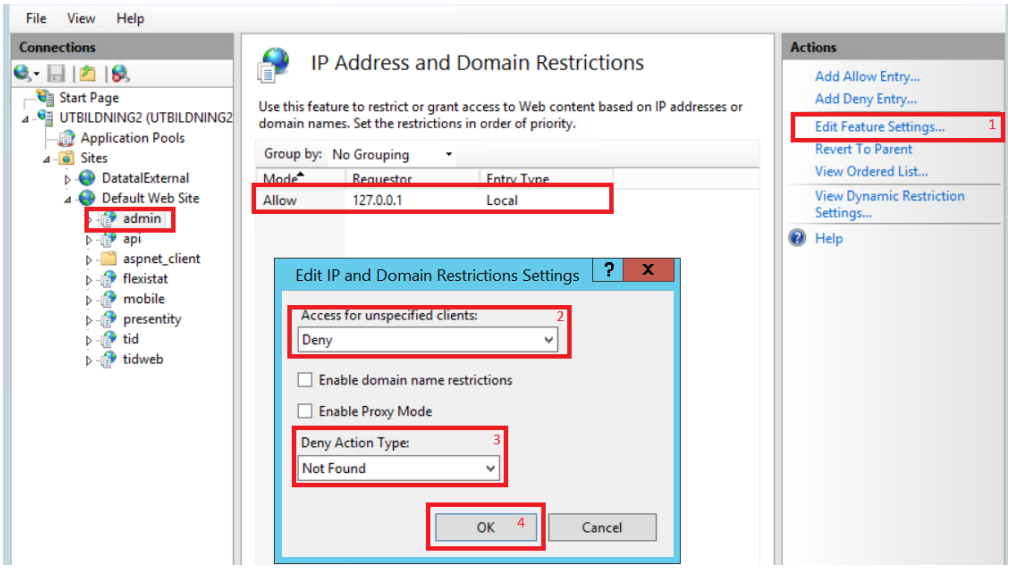
dism /Online /Enable-Feature /FeatureName:IIS-IPSecurity /all /norestart /quiet

After, go into IIS manager, under each virtual application there is a new feature



From here you can narrow down to single IP or set ranges of IP that can access this specific virtual application. Consult the help file to get this right, and test!

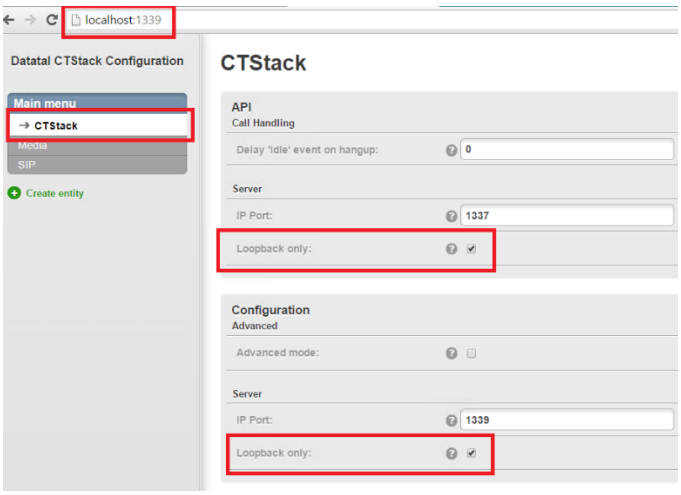
With these settings it is only possible to access /admin from local server.



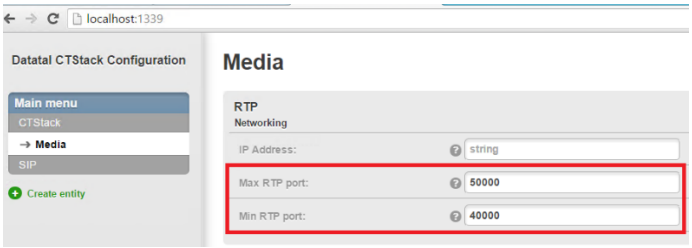
Secure Datatal CTStack

Datatal CTStack handles the SIP communication with the PBX. To access the configuration for CTStack, browse to http://localhost:1339 on the Flexi Server. To configure standard settings for each PBX, consult the documentation. Datatal CTStack doesn´t support SIP over TLS, SIPS, SRTP.

First verify that the CTStack´s API only can be accessed from local server.



As standard SIP uses RTP to transfer audio stream. By default it uses a large range of ports and are configured under Media. RTP uses UDP.



Bindings and Security, by default Datatal CTStack will bind port 5060 first IP-address at installation. If IP address is an alternative IP or is changed during implementation, this setting must be edited. For security settings, if PBX require a login for outgoing call. It can be provided here; most PBX only uses IP-address for secure measure.