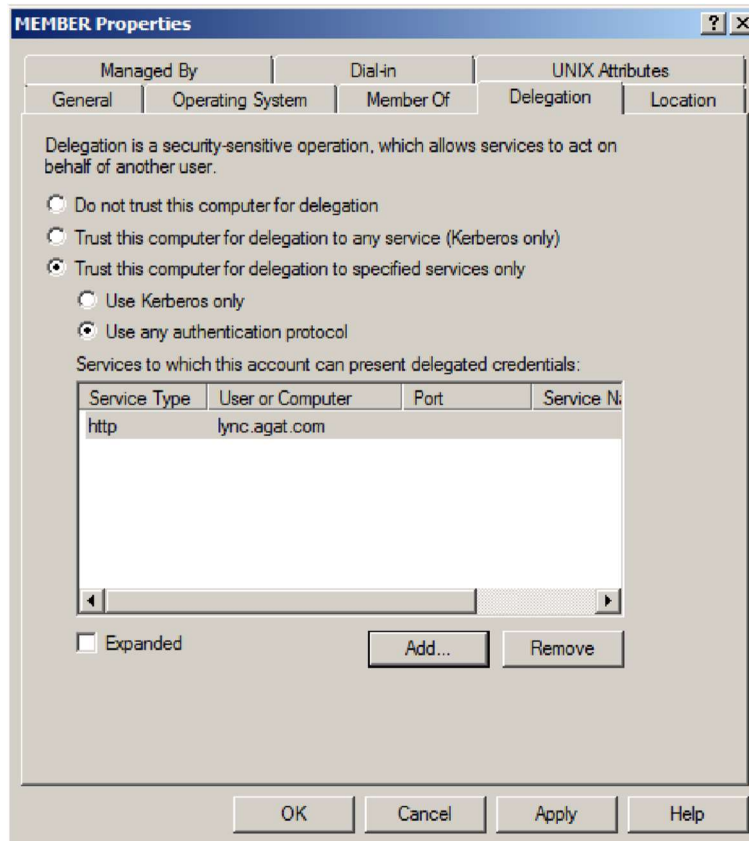


## Installing Authentication Extender server (Dedicated login only)

- 3.1.22 Give the Authentication extender server delegation rights to your Skype for Business External Site HTTP service. Go to Active Directory Users and Computers and enable delegation as show below. Repeat this step for all Skype for Business Director and FE servers as well as Exchange servers that will be used for EWS by Skype for Business.



- 3.1.23 Install Visual C++ 2010 SP1 64 bit redistributable – [vcredist\\_x64.exe](#) (included).
- 3.1.24 [Install .net 3.5 on the server.](#)
- 3.1.25 (Optional) Install [Notepad++](#) for easier text file configuration
- 3.1.26 Copy the “Bastion” and “LogExpert” folder to “C:\Program files” or another location of your choice, from the Authentication Extender package.
- 3.1.27 Run register\_filter.bat script.
- 3.1.28 Configure Bastion.xml (the Bastion configuration file).
- 3.1.29 Configure the SSL certificate for Bastion to use. You may use a pfx file containing both the public and private key, separate certificate and private key, or a certificate installed in the Windows store.

```
<path>cert\DemoServer.crt</path>
<!-- Path to the private key related to this certificate -->
<privateKey>cert\DemoServer.key</privateKey>
<!--Path to intermediate ca bundle file -->
<intermediateCaChain></intermediateCaChain>
<!--
if the private key of the certificate have a password write it here
use Bastion to encrypt the password so it will not be in plain text
command: bastion encrypt "your password"
if you want to leave it in plain text set the encrypted attribute to False
-->
<password encrypted="false">123456</password>
```

- 3.1.30 Configure Bastion to run as “Local System”, to enable delegation.
- 3.1.31 Ensure that the DMZ Bastion server(s) are forwarding traffic to this Authentication Extender Bastion server(s) that is a member of your domain.
- 3.1.32 Configure a channel that publishes HTTP/HTTPS traffic to your Skype for Business External site in Bastion.xml.

```
<channel name="Skype" listener="Skype_Listener">
  <!--for which hosts this channel will apply-->
  <externalHosts>
    <host>*</host>
  </externalHosts>
  <!--Where to publish connections on this channel -->
  <publish>
    <host>FE1.internal-pool.local</host>
    <port>8080</port>
    <sslPort>4443</sslPort>
    <convertTo>keep</convertTo>
  </publish>
  <filters>
    <filter>Skype\AuthConsumer</filter>
    <filter>Skype\KCD</filter>
  </filters>
</channel>
```

- 3.1.33 **Configure AuthConsumer.xml with the path to your certificate (no private key needed). You can use the included certificate (in the Bastion folder) for testing purposes and replace with your own certificate once the system is up and running. Save the changes.**

Make these changes to AuthConsumer.xml in all filter subdirectories.

```
<signerCerts>
  <cert path="signing.crt" />
</signerCerts>
```

- 3.1.34 **Configure KCD.xml with the SPN of your Skype for Business external site, as defined in step 1.**

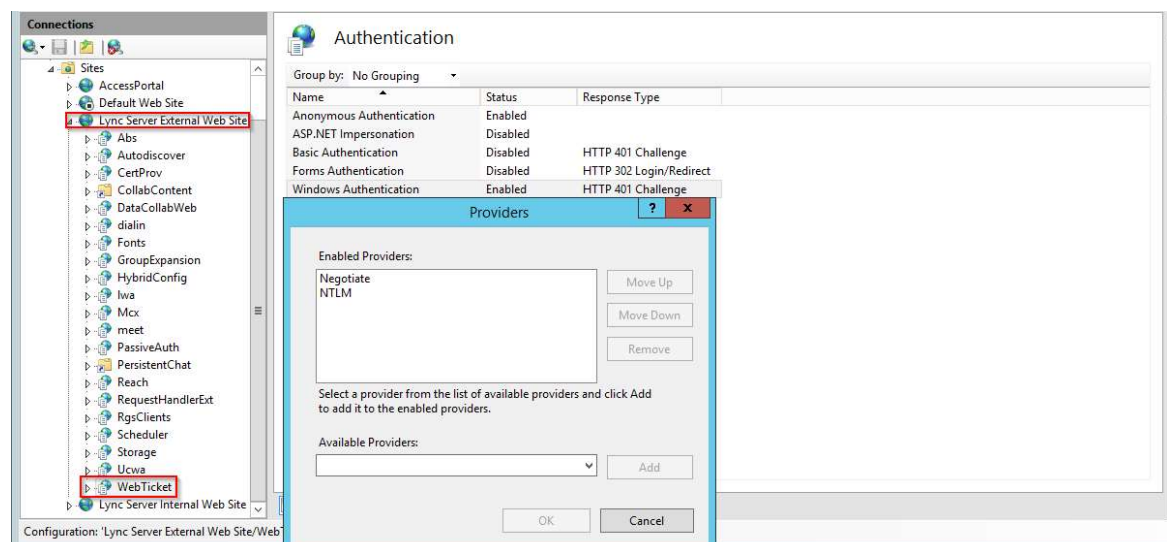
In each channel folder there needs to be a copy of KCD.xml, which will need to be configured according to the SPN of the SfB or Exchange server. This cannot be a pool SPN.

*This entry will be different for each channel.*

```
<target spn='http/YourSfBServer-FE1.company.local' />
<target spn='http/YourSfBServer-FE2.company.local' />
<target spn='http/ExchangeServer1.company.local' />
```

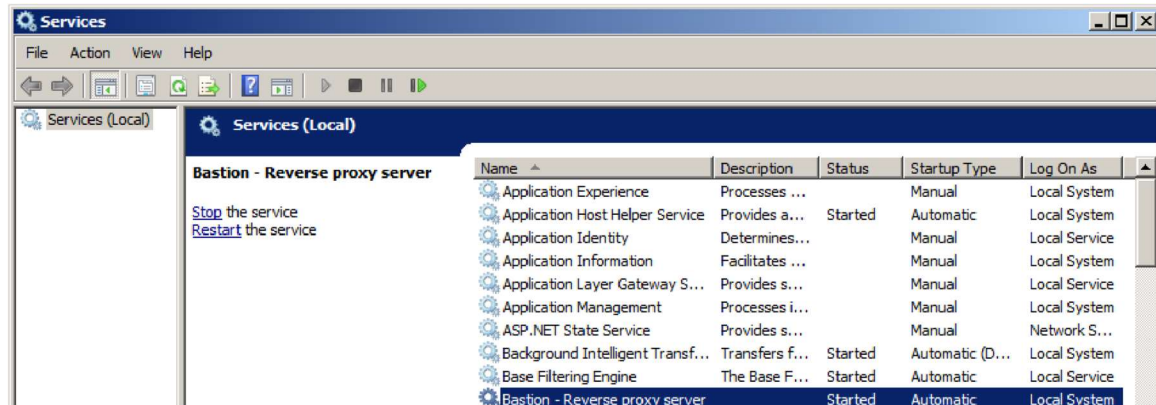
- 3.1.35 **Configure the WebTicket application in the Skype for Business Server External Web Site to support Negotiate Authentication.**

- 3.1.36 **Steps: IIS -> Skype for Business Server External Website -> WebTicket (application) -> Authentication -> Windows Authentication -> Providers... -> Choose "Negotiate" from the list of available providers -> Add.**



3.1.37 Install Bastion as a service by running the command “Bastion install” from a command prompt running at the location of the folder. “Bastion remove” unregisters Bastion as a service.

3.1.38 Ensure Bastion is running as Local System.



## 4 Calendar support for dedicated Login scenario

When Lync Access Control is configured to support the use of dedicated credentials, EWS traffic will need to also go through the Authentication extender.

- 4.1.1 Configure the *EWS* application in the Skype for Business Server External Web Site to support *Negotiate* Authentication, as well as the Autodiscover application.
- 4.1.2 Steps: IIS -> Default Website -> EWS (application) -> Authentication -> Windows Authentication -> Providers... -> Choose “Negotiate” from the list of available providers -> Add.

**Connections**

- Start Page
- DC (AGINT\meird)
  - Application Pools
  - Sites
    - Default Web Site
      - aspnet\_client
      - Autodiscover
      - ecp
      - EWS
      - Microsoft-Server-A
      - OAB
      - owa
      - PowerShell
      - Rpc
      - Exchange Back End

**Authentication**

Group by: No Grouping

Name	Status	Response Type
Anonymous Authentication	Enabled	
ASP.NET Impersonation	Disabled	
Basic Authentication	Disabled	HTTP 401 Challenge
Digest Authentication	Disabled	HTTP 401 Challenge
Forms Authentication	Disabled	HTTP 302 Login/Redirect
Windows Authentication	Enabled	HTTP 401 Challenge

**Providers**

Enabled Providers:

- Negotiate
- NTLM

Move Up

Move Down

Remove

Select a provider from the list of available providers and click Add to add it to the enabled providers.

Available Providers:

▼ Add

OK Cancel