

Administrator's Guide for SpeechExec Enterprise Mobile service

Table of Contents

Change history	2
1 Requirements.....	3
2 How to define the location of SEERoot in the IIS web.config file	3
2.1 During installation.....	3
2.2 Modifying the SEERoot manually after installation	3
3 Configuring the web service	5
3.1 How to set up the web service	5
3.2 How to change the user identity for the application pool.....	7
3.3 How to activate Windows Authentication for the service.....	8
3.4 How to set an appropriate value for upload read ahead size	9
3.5 Optional: Using HTTPS for SEEMobile.....	9
3.5.1 Configuration in IIS.....	9
3.5.2 Changing the web.config configuration file of the web service	10
4 Testing the web service	12
4.1 Authentication details for test the web service.....	13
5 Troubleshooting.....	15
5.1 Logging	15
5.2 How to set up the application pool of the web service	16
5.3 How to create a new application pool.....	16

Change history

Document version	Application version	Description
6.0	SEE 6.0	Initial document
6.1	SEE 6.1	Added uploadReadAheadSize configuration section

1 Requirements

SpeechExec Mobile service has the following software requirements:

Warning: Please read the full list of requirements before you start.

Operating system	Windows Server 2008 R2 (64-bit version) or later	
IIS	IIS 7 or later	Make sure that IIS is turned on before installing .NET Framework in order to have a properly installed ASP.NET
Microsoft .NET Framework	Microsoft .NET Framework 4.6.1 or later	

Role and Feature requirements

(example using Windows Server 2016 – Add Roles and Features Wizard):

Roles tab:

- Web Server (IIS) [IIS 7 or later]
 - Security
 - Windows Authentication
 - Application Development
 - .NET Extensibility 4.x
 - ASP .NET 4.x
 - Application Initialization

Features tab:

- .NET Framework 4.x Features
 - WCF Services
 - HTTP Activation

Although the installer of SpeechExec Mobile service installs the web service into IIS, it is the task of the administrator to properly set up IIS.

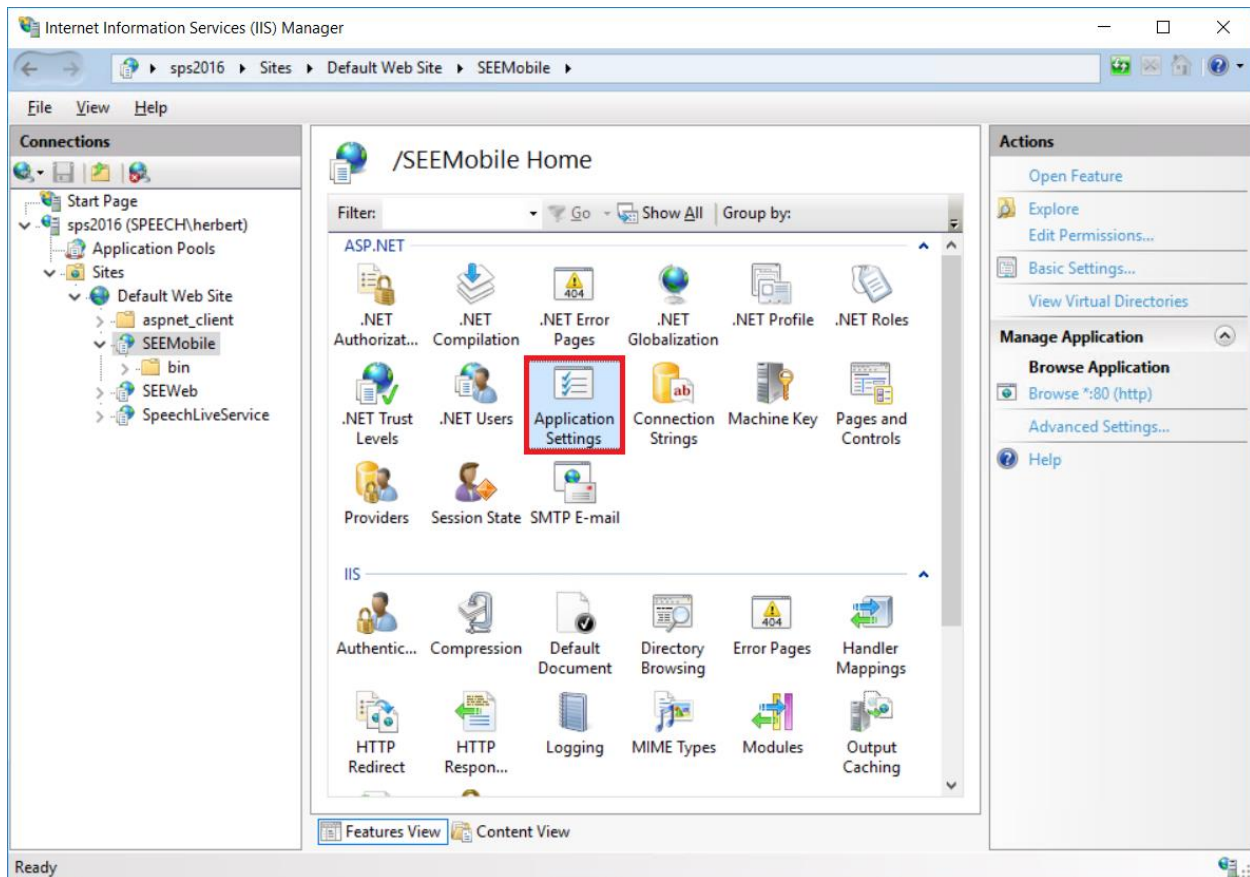
2 How to define the location of SEERoot in the IIS web.config file

2.1 During installation

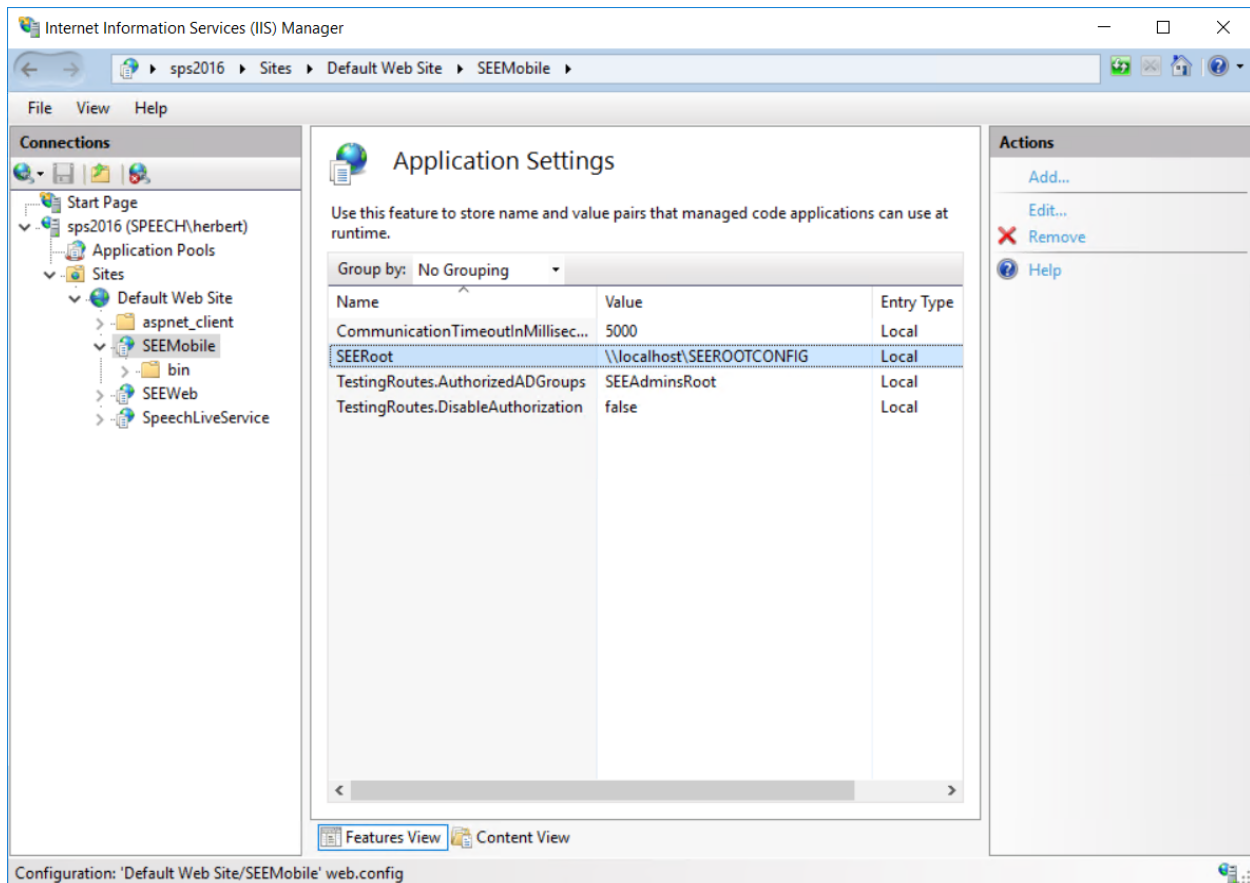
During installation the SEERoot configuration folder must be selected and cannot be modified by the installer later, only manual modification is supported.

2.2 Modifying the SEERoot manually after installation

If you want to change the path of the SEERoot configuration folder after the installation, open the IIS Manager, select the **SEEMobile** node and double click **Application Settings**:



Double click "SEERoot" to change the path of the SEERoot configuration folder:



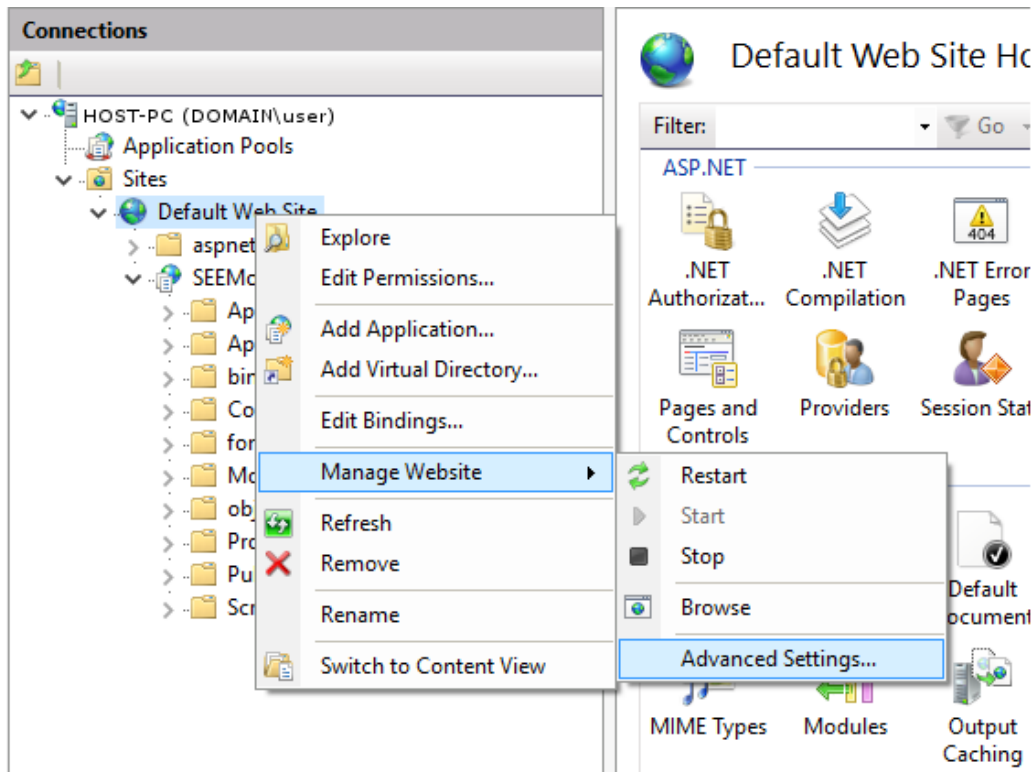
3 Configuring the web service

3.1 How to set up the web service

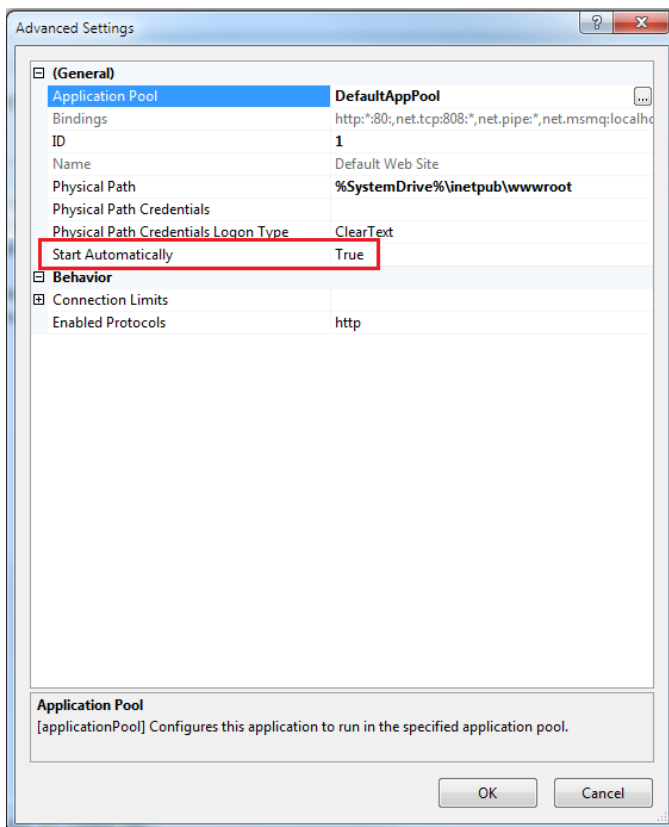
To set up the web service to start automatically, do the following:

Older IIS versions (earlier than version 8):

1. Right-click on **Default Web Site** and select **Manage Web Site > Advanced settings...**



2. Set Start Automatically to True.



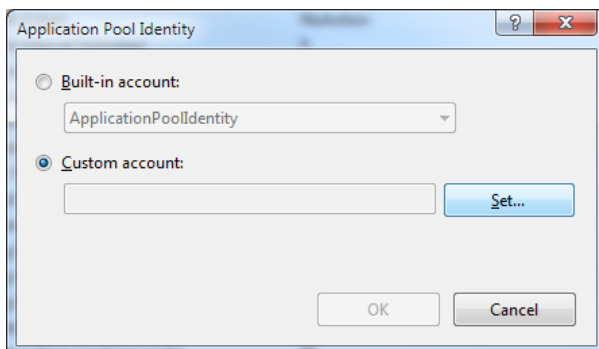
Newer IIS versions (8 or later):

1. In IIS Manager, click the computer name on the **Connection** pane.
2. Switch to **Features View** if the view is not active.
3. Double-click **Configuration Editor** in the **Management** section of the **Features View**.
4. Click the down-arrow for the **Section** field, expand system.applicationhost, and then click application pools.
5. Click **(Collection)** and then click ellipses (...) next to the field that shows the count.
6. In the **Collection Editor**, select the application pool for which you want to configure the startMode attribute.
7. In the **Properties** window at the bottom, set the following values:
 - autoStart attribute to **true**
 - startMode attribute to **AlwaysRunning**

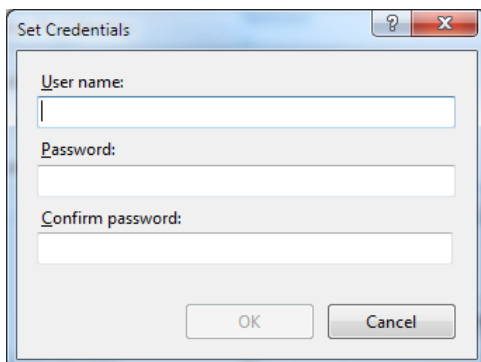
3.2 How to change the user identity for the application pool

To change the user identity of the application pool newly created by the application setup, follow the instructions below:

1. On the **Application Pools** panel in IIS, right-click on the **SEWebServicesAppPool** item and select **Advanced Settings...**
2. In the **Advanced Settings** dialog, select **Identity** and click **Browse (...)**.
3. In the **Application Pool Identity** dialog, check **Custom account** and click **Set**.



4. In the **Set Credentials** dialog, enter your user identity credentials and click **OK**.



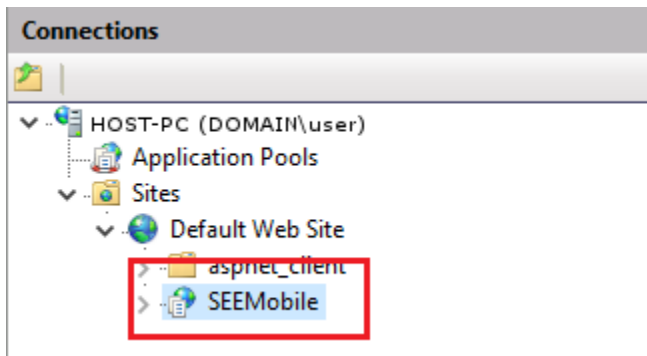
NOTE: the user has to have read and write permissions for the **SEERoot** configuration, finished dictation and archive folders)

For information on how to create an application pool, see [Optional: How to create a new application pool](#).

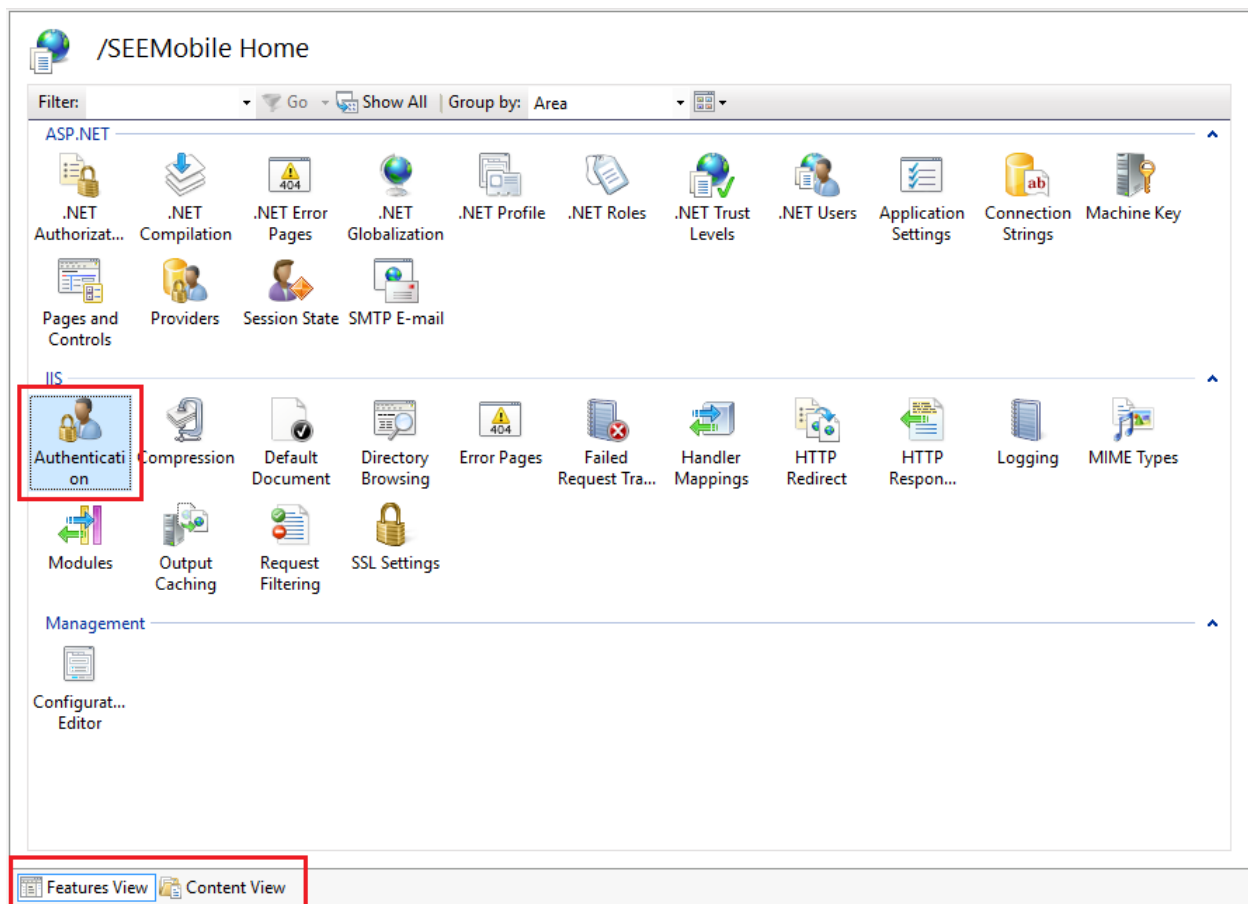
3.3 How to activate Windows Authentication for the service

To enable Windows Authentication, do the following:

1. In the **Connections** panel on the left, select the **Sites > SEEMobile** web service.

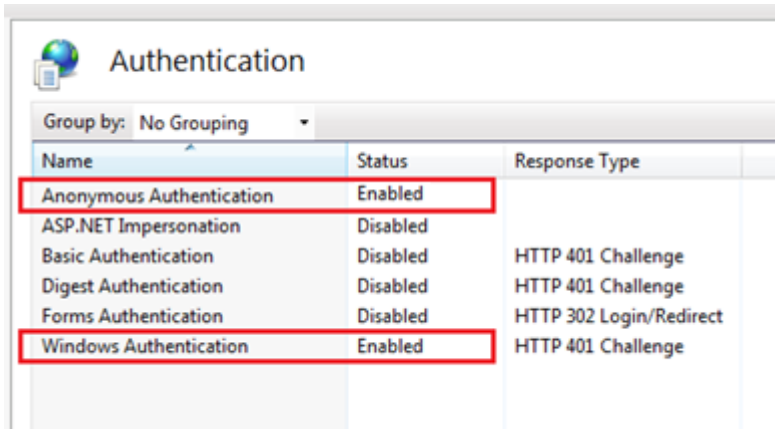


2. Select the **Features View** at the bottom of the panel.
3. Double-click on **Authentication** in the **IIS** section of the panel.



4. In the **Authentication** panel, do the following:

- Right-click **Anonymous Authentication** and select **Enabled**.
- Right-click **Windows Authentication** and select **Enabled**.



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

3.4 How to set an appropriate value for upload read ahead size

The Philips Voice Recorder mobile app uploads dictation files in about 400KB parts, however, certain IIS installations have smaller upload limits, resulting in failing dictation uploads.

Follow the steps below to make sure that dictation files can be uploaded to Mobile Service without IIS rejecting it.

1. Open IIS Manager and select “**SEEMobile**” on the left side
2. Open **Configuration Editor** located in the middle panel under **Management**
3. On the top of the window, locate the 2 dropdown lists labeled **Section** and **From**
4. Set the **Section** dropdown to: “**system.webServer/serverRuntime**”
5. Set the **From** dropdown to: “**ApplicationHost.config**”
6. In the available setting list, locate the setting named “**uploadReadAheadSize**”
7. If the value is lower than “**10485760**” (approx. 10 Mb), set the value to “**10485760**”, otherwise leave it unchanged
8. Press **Apply** in the top right corner
9. Recycle the application pool used by “**SEEMobile**”

3.5 Optional: Using HTTPS for SEEMobile

In order to use SEEMobile with HTTPS, you need to set the following settings:

3.5.1 Configuration in IIS

1. In IIS Manager select the **Default Web Site** (or the one containing SEEMobile) node on the **Connections** panel.
2. On the **Actions** panel (on the right) select **Bindings...**
3. Click **Add**.
4. Select **https** from the **Type** combo box.
5. Select an SSL certificate from the **SSL certificate** combo box.
6. Click **OK**.
7. To properly apply the new settings, a host computer restart is recommended.

3.5.2 Changing the web.config configuration file of the web service

Change the following part of the configuration by undoing the comments (<!-- -->) on the "MobileServiceBindingHttps" related part and commenting out the "MobileServiceBindingHttp" part.

Default configuration after installation (with HTTP non secure version enabled):

```

<services>
  <service name="EMS.Web.SELiveBroker"
    behaviorConfiguration="MobileServiceServiceBehavior">
    <endpoint contract="SELive.SELiveBroker.Service.ISELiveBroker"
      binding="wsHttpBinding"
      address="SELiveBrokerServiceAddress"
      bindingConfiguration="MobileServiceBindingHttp">
    </endpoint>
    <!--<endpoint contract="SELive.SELiveBroker.Service.ISELiveBroker"
      binding="wsHttpBinding" address="SELiveBrokerServiceAddress"
      bindingConfiguration="MobileServiceBindingHttps" />-->
    </service>
  <service name="EMS.Web.WebDriveServer"
    behaviorConfiguration="MobileServiceServiceBehavior" >
    <endpoint contract="SpExec.WebDrive.WebRole.Service.ISELiveService"
      binding="wsHttpBinding"
      address="SELiveServiceAddress"
      bindingConfiguration="MobileServiceBindingHttp">
    </endpoint>

    <!--<endpoint contract="SpExec.WebDrive.WebRole.Service.ISELiveService"
      binding="wsHttpBinding"
      address="SELiveServiceAddress"
      bindingConfiguration="MobileServiceBindingHttps" />-->
    </service>
</services>

```

Configuration after HTTPS modifications (Commenting out HTTP and enabling HTTPS):

```

<services>
  <service name="EMS.Web.SELiveBroker"
    behaviorConfiguration="MobileServiceServiceBehavior">
    <!--<endpoint contract="SELive.SELiveBroker.Service.ISELiveBroker"
      binding="wsHttpBinding"
      address="SELiveBrokerServiceAddress"
      bindingConfiguration="MobileServiceBindingHttp" />-->
    <endpoint contract="SELive.SELiveBroker.Service.ISELiveBroker"
      binding="wsHttpBinding"
      address="SELiveBrokerServiceAddress"
      bindingConfiguration="MobileServiceBindingHttps">
    </endpoint>
  </service>
  <service name="EMS.Web.WebDriveServer"
    behaviorConfiguration="MobileServiceServiceBehavior" >
    <!--<endpoint contract="SpExec.WebDrive.WebRole.Service.ISELiveService"
      binding="wsHttpBinding"
      address="SELiveServiceAddress"
      bindingConfiguration="MobileServiceBindingHttp" />-->
    <endpoint contract="SpExec.WebDrive.WebRole.Service.ISELiveService"
      binding="wsHttpBinding"
      address="SELiveServiceAddress"
      bindingConfiguration="MobileServiceBindingHttps">
    </endpoint>
  </service>
</services>

```

4 Testing the web service

Mobile service provides a dedicated testing interface:

`<url_of_web_service>/test/testconfig`

For example, if the web service is running on the local computer, the URL looks like the following:

<http://localhost/SEEMobile/test/testconfig>

To limit user access to the URL, opening this URL by default requires the following:

- an authenticated Active Directory user session on the calling (browser) side
- the calling user must be the member of the `SEAdminsRoot` Active Directory security group

The test process validates the servers' configuration settings and returns a JSON array of validation steps. Each validation step consists of a StepID, a StepResult and a StepExplanation.

Returned response codes can be the following:

- 401 (Unauthorized), if the current user cannot be authenticated by the web service
- 566, if any of the validation steps failed
- 200 (OK), if all validation steps passed

Please make sure that Mobile service is 'Enabled' and has a compatible License Server configured in Enterprise Manager before attempting a test!

To turn on Mobile Service:

- Open Enterprise Manager -> System Administration -> Groups and users -> Mobile service settings (panel) and enable Mobile Service.
- Add a supported License Server (with a compatible license loaded) in the "License Settings..." window (accessible from the same panel).

If the above conditions are not met, the test will fail at "020_SEELicenseServerAddressFoundInConfig".

Validation steps:

StepID	Explanation
001_SEERootFoundInConfig	SEERoot value must be found in web.config
005_SEERootExists	The folder specified by the SEERoot value exists.
010_SEERootStructureCorrect	The service must be able to read from and write to SEERoot.
020_SEELicenseServerAddressFoundInConfig	License server address found in SEERoot configuration
025_SEELicenseServerPortFoundInConfig	License server port found in SEERoot configuration
030_SEELicenseServerCanConnect	Can connect to License server with the given address and port in the SEERoot configuration

Please note that the response content is always returned in English.

Example response result when the 1st step passed, but the 2nd step failed:

```
[
  {
    "StepID": "001_SEERootFoundInConfig",
    "StepResult": "SUCCESS",
    "StepDescription": "SEERoot value is found in web.config"
  },
  {
    "StepID": "005_SEERootExists",
    "StepResult": "FAIL",
    "StepDescription": "The folder specified by the SEERoot value does not exist"
  }
]
```

Example response result when all steps are passed:

```
[
  {
    "StepID": "001_SEERootFoundInConfig",
    "StepResult": "SUCCESS",
    "StepDescription": "SEERoot value is found in web.config"
  },
  {
    "StepID": "005_SEERootExists",
    "StepResult": "SUCCESS",
    "StepDescription": "The folder specified by the SEERoot value exists (D:\\seeroot)"
  },
  {
    "StepID": "010_SEERootStructureCorrect",
    "StepResult": "SUCCESS",
    "StepDescription": "The structure of SEERoot is correct (it has all required sub-folders and required .config files)"
  },
  {
    "StepID": "020_SEELicenseServerAddressFoundInConfig",
    "StepResult": "SUCCESS",
    "StepDescription": "Valid License Server address in configuration"
  },
  {
    "StepID": "025_SEELicenseServerPortFoundInConfig",
    "StepResult": "SUCCESS",
    "StepDescription": "Valid License Server port in configuration"
  },
  {
    "StepID": "030_SEELicenseServerCanConnect",
    "StepResult": "SUCCESS",
    "StepDescription": "License Server connection successful"
  }
]
```

4.1 Authentication details for test the web service

Important: The /test/testconfig URL should only be accessible for administrators, and only for testing purposes.

For diagnostics purposes, access control can be re-configured using the following `web.config` settings:

```
<add key="TestingRoutes.AuthorizedADGroups"
      value="%GROUPLIST%" />
<add key="TestingRoutes.DisableAuthorization"
      value="false" />
```

By setting the value of `TestingRoutes.DisableAuthorization` to “true”, access to the `/test/testconfig` URL becomes **totally unrestricted**, i.e. **ANY** user can call it **WITHOUT authentication**.

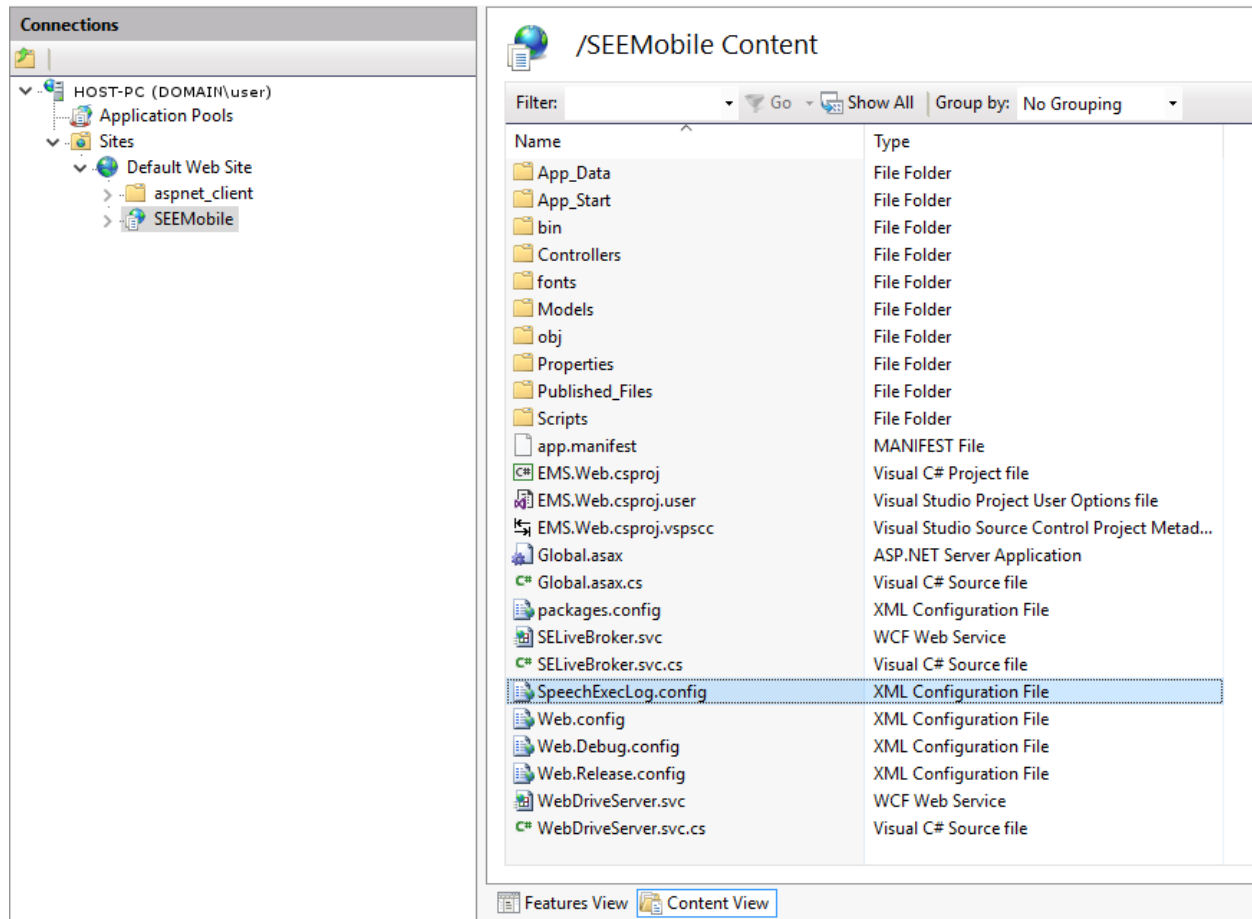
Access to the `/test/testconfig` URL can be restricted to members of certain Active Directory security groups by listing the allowed groups in the value of `TestingRoutes.AuthorizedADGroups`.

Multiple groups can be specified by separating the Active Directory group names with a comma (,).

5 Troubleshooting

5.1 Logging

The name of the log configuration file is **SpeechExecLog.config**. It is located in the root folder of the **SEEMobile** service (visible in **Content View**).



It is the IIS administrator's responsibility to manually edit the SpeechExecLog.config file and specify correct configuration values.

The default path of the log file is:

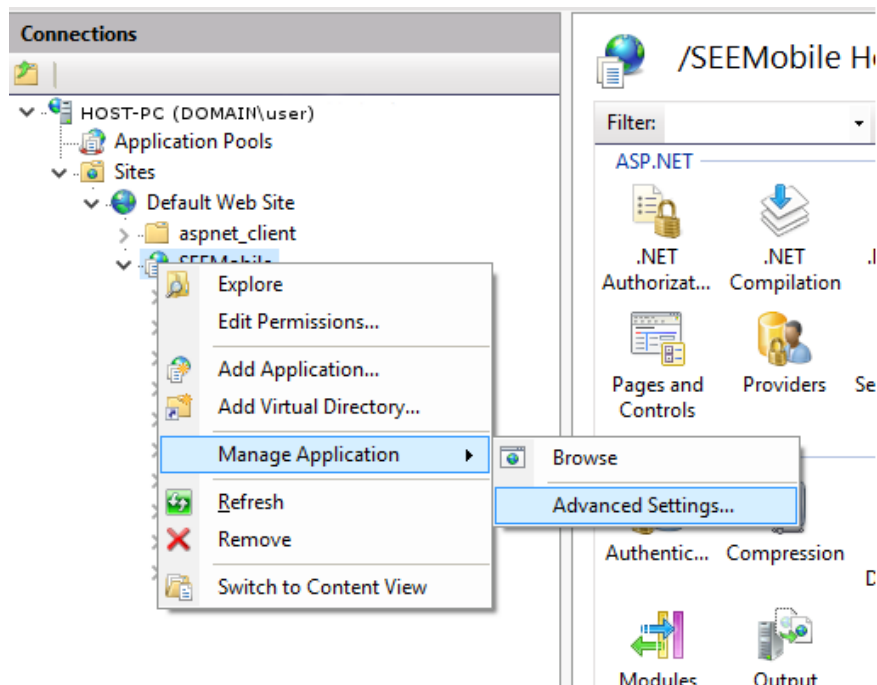
```
<param name="File" value="c:/SEEMobileServiceLogFolder/SEEMobileService.log" />
```

The default maximum size of the log file is:

```
<param name="MaximumFileSize" value="1000MB" />
```

5.2 How to set up the application pool of the web service

1. In the **Connections** panel on the left, select the **Sites > SEEMobile** web service.
2. Right-click on the web service, and click **Manage Application > Advanced settings...**



3. In the **Advanced Settings** dialog, select **Application Pool** and click on **Browse (...)**.
4. In the **Select Application Pool** dialog, select **SEWebServicesAppPool**, and click **OK**.

5.3 How to create a new application pool

Application pools allow isolating one web application from another, even if they are running on the same server. This way, if there is an error in one app, it will not take down other applications.

Additionally, applications pools allow specifying different levels of security (for example, file access security) for different apps.

The installer of the web service will by default create a new application pool and assign the web service to the pool.

If a new application pool need be created, follow the instructions below:

1. Open the Internet Information Services (IIS) Manager.
2. Select **Application Pools** from the **Connections** panel on the left. Right-click on the **Application Pools** panel and select **Add Application Pool...**
3. Enter a name for your new application pool, such as **SEWebServicesAppPool**.
4. In the **.NET CLR version** list, select :
 - o .NET CLR Version v4.0.30319
5. Make sure the **Start application pool immediately** checkbox is selected.

6. Click **OK** to create and start the application pool.