Fendix Media Ltd

Segmented Message System

New System Installation and Configuration Guide

System Version 6.7

Revision History

1. 29 January 2020: *Initial Draft*
2. 12 March 2020: *added Occupation to ESR List*
3. 12 May 2020: *Edited to include ESR Remote only.*
4. 27 July 2020: *Edited to include Opt Out Code.*

Introduction

This document describes the installation and configuration process for the Network Partner hosted components of the Fendix Media segmented messaging system.

This document is intended for those Network Partners who are installing this version of the segmentation system onto a server for the first time.

If you have any questions regarding the implementation or testing procedure, please contact support@fendixmedia.co.uk or contact your Network Account Manager

Overview of System Behaviour and the

Segmentation Process

The purpose of the segmentation system is to enable Fendix Media to deliver relevant messages to Intranet users.

1. Data from the NHS Electronic Staff Record (ESR) system is used to allow allocation of relevant keywords based on a user's job role, occupation, and area of work information. This ESR file is held on our IG Compliant secure server with no User Identifiable data.
2. On the segmentation server, job role, occupation, and area of work are cross referenced to a list of keywords that are used to target the relevant messages to (for example job role "Geriatric Nurse" might be mapped to the keywords 'Elderly Care' and 'nurses').
3. Once the job role, occupation, and area of work has been cross referenced, a request script containing the keywords is returned to the user’s browser, this is then executed to request a relevant message from our servers.

The users email address is encrypted and securely transferred to the segmentation server (***identifiable information is never transferred outside of the Trust network***).

To perform this match, it is necessary for the email field to be populated in the active directory userPrincipalName field, or mail field, if this is not the case in your installation please contact us.

No trust information is ever released from the Fendix Media infrastructure. Only keyword lists and request statistics are available to clients.

Minimum System Requirements

Windows Server 2003 running Internet Information Server 6 as part of a Windows domain.

.Net Framework v4.5.2

Recommended system Requirements

Windows Server 2019 or higher running Internet Information Server 7 or higher as part of a Windows domain.

.Net Framework v4.5.2 or higher

New System Installation

The purpose of the segmented messaging system is to display messages on your intranet that are relevant to individual users. To do this, a small IIS web application is installed which performs a look up of relevant user information from the ESR data file hosted by us. The information is used to determine keywords for message targeting, allowing a request to be made to the Fendix Media servers for an appropriately targeted message.

The segmentation service should be installed on a separate IIS web site to your main intranet site. If your intranet site is hosted on an IIS server, it is possible to install the service on a new site on the same server, listening on an unused port.

> The decision as to whether to install on the same server as your intranet should be based on the performance of your server, volume of intranet traffic and internal IT policy. The segmentation service should however be installed on a server on the same domain.

Once the new web site is created in IIS, the web components, as supplied in the zip file accompanying this document should be copied into the root folder of the newly created website

> If you have received the zip file as an e-mail attachment, it is likely that Windows will have marked the file (and its file contents) as 'blocked'. Files in this state may be prevented from executing in IIS, dependant on security configuration. Prior to unzipping, remove any block by right-clicking on the zip file and clicking the 'Unblock' button if it is present.

Authentication

The segmentation system consists of a main root directory and a sub-directory entitled 'Auth'

The root directory of the new site should be configured with 'anonymous authentication' enabled.

The Auth directory should be configured with 'windows authentication - enabled' all other authentication options (including anonymous) should be set to disabled for this directory.

> Note: It is necessary that the windows authentication role be installed on the server

Server Configuration Options

Within the web.config file in the server application, the following settings may be set within the appSettings section:

- **Serve**: Instructs the system whether or not to deliver ad code to the intranet page, this allows ad serving to be stopped without needing to remove html tags from intranet pages (e.g. when scheduled maintenance of the Fendix infrastructure is taking place, or when internet connectivity is lost). Valid values are: **true** - ads are served. **false** - ads are not delivered to the browser

- **SegmentationServer**: The location of the Fendix key wording service. Usually //code.fendixmedia.net. This should not be modified unless advised directly by Fendix Media to do so.

- **TrustURN**: The unique identification code for your organisation. i.e. “T001” This will be supplied by Fendix Media.

- **ADServer**: Location of your Active Directory server. This can normally be left blank and the segmentation service will use auto discovery to identify the AD server. If it is necessary to specify the server, ensure that the server location is prefixed with 'LDAP://' followed by the fully qualified URL of the domain controller.

- **NoSegmentationForMobileDevices**: If set to true, the system will attempt to identify from the request headers if the request has been made from a mobile device (phone or tablet) and if so, not attempt to perform a segmentation lookup.
- **AuthURI**: A pattern specifying the base URL on which authenticated users access the intranet - if external, non-authenticated users, access on a different base URL (e.g. some network partners offer external access on a different port). If a request is received from a referrer that does not match the pattern set in AuthURI, no segmentation is performed, and a non-segmented request returned instead
- **SegmentationMethod**: Should be set to REMOTE to perform segmentation. Valid values are NONE or **REMOTE**
- **ADMatchFieldName:** Should be left blank if the users log in using their nhs email address, otherwise the name of the field where the nhs email address is stored, usually “mail”.
- **OptOut**: put location and name of opt out list i.e. "C:\inetpub\wwwroot\optoutlist.txt" This file must be accessible to this IIS web application and consist of just the users login name, one on each line the name stored must match the username the opted out user uses to log in to the intranet.

Testing the Server Installation

Once the server components have been installed, either from scratch or in addition to a previous version, the installation should be tested before intranet pages are configured to serve messages.

To perform an initial test, on the local server, open a web browser on the server and point to the testpage.htm file.

`http://localhost:25500/testpage.htm`

If you have installed the segmentation service on a different port, you should modify the URL accordingly.

If you currently have active house messages (or other non-targeted messages) running at your trust You should see a banner image at the bottom of the page.

When it is installed and running please run the file `http://localhost:25500/Auth/LDAPTest.aspx`, and it should show whether your AD server is visible to our system so we can serve segmented messages.

Once debug information is displaying successfully, proceed to the next section 'Intranet Configuration'

In the event of problems occurring during testing, please contact us at support@fendixmedia.co.uk.

Intranet Configuration

In order to display message banners, a simple tag needs to be inserted into **all** of your intranet pages. This takes the form of an inline `<script>` tag which calls the segmentation.ashx application on the IIS site configured in the previous section.

This tag should be placed at the location at which you wish the message banner to display (normally at the top of the page in the case of Leaderboard banners). We recommend wrapping the script tag inside a `<div>`, `<span>` or other tag as appropriate.

The form of the script tag is as follows:

```
<div><script
src="http://servername.domain.nhs.uk:25500/segmentation.ashx">
</script></div>
```

servername.domain.nhs.uk should be replaced by the fully qualified path of the IIS server where you have installed the segmentation website.

If you have installed the segmentation website on a port other than 25500,

this should be edited as appropriate

The standard tag will display a message banner in the default orientation as specified in the *AdOrientation* parameter (see Server configuration). To specify a different orientation, add a querystring parameter 'AOr' to the end of the URL: (Do not do this without Fendix co-ordination as we may not have the appropriate banner available).

```
<div><script
src="http://servername.domain.nhs.uk:25500/segmentation.ashx?
AOr=leaderboard"></script></div>
```

The above tag specifies a horizontal 'leaderboard' message banner.

```
<div><script
src="http://servername.domain.nhs.uk:25500/segmentation.ashx?
AOr=skyscraper"></script></div>
```

The above tag specifies a vertical 'skyscraper' message banner.

Asynchronous Loading

The default loading behaviour for banners is to load synchronously at the point that the script tag is executed. In most circumstances this does not impact page load adversely (typically the whole ad loading process should take less than 0.2 seconds)

In some circumstances page load times may be affected by slow network connections or other access issues. If this is found to be the case, it is possible to use the open source 'Post Scribe' JavaScript library to asynchronously load banners in the background while the rest of the page loads.

This requires the jQuery and postscribe libraries to be installed and would look like this

```
<script src="https://code.jquery.com/jquery-1.10.2.js"></script>

<script
src="https://cdnjs.cloudflare.com/ajax/libs/postscribe/2.0.8/postscribe
.min.js">

</script>
```

And the actual script on the page would be like this:

```
<div id="fendix"></div>

<script type="text/javascript">

  $(function() {

    // Build url params and make the server call

 var adparam = ((window.location.toString().indexOf("?") > -1) ?
“http://servername.domain.nhs.uk:25500/segmentation.ashx”+"?"+window.lo
cation.toString().split('?')[1] :
"http://servername.domain.nhs.uk:25500/segmentation.ashx");

    postscribe('#fendix', '<script src='+adparam+'><\/script>');

  });
```

If you require assistance with the implementation of the Post Scribe library, please contact support@fendixmedia.co.uk