Fendix Media Ltd

Segmented Advertising System

New System Installation and Configuration Guide

System Version 5.0.0

Revision History

1. 14 December 2018: *Initial Draft*
2. 07 January 2019: *Release*
3. 15 February 2019 *Amended*
4. 25 July 2019 *Amended*

Introduction

This document describes the installation and configuration process for the Network Partner hosted components of the Fendix Media segmented advertising 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 advert impressions to Intranet users. There are two methods by which this can be done:

1. Active directory group-based segmentation

1. A query is made to the Trust's Active Directory (AD) server to obtain a list of AD groups for which the current user is a member.
2. The group list is then encoded and sent to the Fendix segmentation server.
3. On the segmentation server, AD group names are cross referenced to a list of keywords that advertisers use to target their advertising to (for example an AD group "Geriatric Nurses" might be mapped to the keywords 'Elderly Care' and 'nurses'). Along with the list of AD groups, a hash of the username may also be sent to the segmentation server. A hash is a non-reversible encoding of the username, this allows statistical data to be gathered about the number of unique people who have matched to ad keywords, without allowing the identification of individuals.
4. Once the complete list of groups has been cross referenced, an ad request script containing the keywords is returned to the user’s browser, this is then executed to request a relevant advert from our ad servers.

2. Electronic Staff Record based segmentation

For this approach, data from the NHS Electronic Staff Record (ESR) system (or equivalent HR system) is used to allow allocation of relevant ad keywords based on a user's job role and department information.

The process is similar to that of the AD based method, however instead of obtaining a list of active directory security groups to match to keywords, a CSV extract file is generated from the ESR system containing email, job title and department information for each system user. A corresponding extract is made from AD with samUSERNMAME and email. These two files are then merged together via a supplied PowerShell Script. The logged in user is then matched in the merged file and the job title and department are extracted to be matched to advertising keywords. Usernames are hashed in the same way as for the AD method and this, along with the job title and department info is transferred to the segmentation server (real names are 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.

With both of these mechanisms, no trust information is ever released from the Fendix Media infrastructure or passed to advertisers. Only keyword lists and request statistics are available to advertisers.

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 2008R2 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 ad system is to display adverts 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, either from Active Directory or from the ESR data file generated by the Trust. This is determined by configuration options detailed in this document. The information is used to determine keywords for advert targeting, allowing a request to be made to the Fendix Media advertising servers for an appropriately targeted advert.

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

Preparing the ESR Data File

This step is only required if using the ESR rather than the Active Directory group segmentation method

The ESR staff data file is a simple csv format file generated from the Trust/Health Board's ESR (or other HR) system. This needs to contain a means of identifying relevant users and information to allow identification of role specialisms. The required format is **email,job title,department** with no spacing (just the comma separator) between fields.

This file should be named ESRExtract.csv (here is an example)

EmailAddress,JobTitle,Department
joe.bloggs@TestTrust.nhs,Surgeon,Cardiac
sam.smith@TestTrust.nhs,Physio,Physio
mary.moon@TestTrust.nhs,Nurse,Accident and Emergency

NOTE: IF your system does not use your email address as your logon username, please contact us.

Once generated, the datafile should be placed in a directory accessible to the IIS worker process.

The data file is loaded into memory when the segmentation application starts. If an updated datafile is produced (we recommend regenerating the datafile every month) the application should be restarted.

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. This should not be modified unless advised directly by Fendix Media to do so.

- **TrustURN**: The unique identification code for your organisation. 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.

- **AdOrientation**:Specifies the default type of advert to deliver. If your ads are normally horizontal banners, specify **leaderboard.** If your ads are vertical banners, specify **skyscraper**

- **NoSegmentationForMobileDevices**: If set to true, the system will attempt to identify from the request headers to identify 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 recieved from a referrer that does not match the pattern set in AuthURI, no segmentation is performed, and a non-segmented request returned instead

- **HashType**: Specifies the hashing algorithm that is used to encode the username for anonymity before it is transferred to Fendix Media. Allowed values are **MD5, SHA256, SHA512.** If not specified, system defaults to MD5. Once set and live this setting should not be changed as it would affect stats collection

- **salt**: An optional salting string that is appended to usernames prior to hashing to give extra complexity and thus privacy. If set this string should not be communicated to Fendix Media and should not be changed as it would affect stats collection.

- **SegmentationMethod**:Specifies whether to use active directory groups or personnel data file to perform segmentation. Valid values are **ESR** or **AD**

- **ESRRoute**: The URL of the ESR segmentation service - either fully qualified or relative to the route segmentation page.

- **ADRoute**: The URL of the Active Directory segmentation service - either fully qualified or relative to the route segmentation page.

- **ADFallBack**: Specifies whether or not the system should try and use the AD group method if it is unsuccessful with the ESR method. Default value is **false**.

ESR specific settings

These configuration settings are specifically for the ESR datafile based segmentation method. For AD segmentation they do not need to be set.

- **preHashedUserName**: Specifies whether the username stored in the ESR data file has already been hashed or if it is in clear text. If **true** the user name should be hashed with same algorithm and salt as specified in HashType and salt. This option is only relevant if ESRUseRealNames is **false**.

- **roleFields**: a comma separated list of numbers specifying which fields in the ESR data file contain information for ad targeting. This list is zero based (thus for a file containing forename,surname,job title,department. The relevant values would be 2,3)

- **forenameField**:Specifies which field in the ESR data file specifies the user forename. Field numbers are zero based. This setting is only relevant if ESRUseRealNames is true

- **surnameField**:Specifies which field in the ESR data file specifies the user surname. Field numbers are zero based. This setting is only relevant if ESRUseRealNames is true

- **usernameField**:Specifies which field in the ESR data file specifies the windows username. Field numbers are zero based. This setting is only relevant if ESRUseRealNames is false

- **includeDomain**:Specifies whether the username field contains just the actual username (false) or the windows domain/username (true). This setting is only relevant if ESRUseRealNames is false

- **userDataFile**:The fully qualified windows filename containing the ESR data

AD specific settings

These configuration settings are specifically for the ESR datafile based segmentation method.

- **LstOU**: Specifies whether to use organisational unit to segment users rather than security groups (this is a less precise mechanism than security groups so is not recommended unless your organisation does not use security groups). Valid values are: **true** - use OU, **false** (default)- use security groups

- **FullOU**: Specifies whether to return full OU path (**true**) or just the parent OU unit name (**false**). This setting is only relevant if LstOU is true. Default value for this setting is true.

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 ads.

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 campaigns (or other non-targeted campaigns) running at your trust You should see an advert banner image at the bottom of the page.

For more in depth testing, the AD and ESR services can be tested individually by calling them directly, the standard urls for these are as follows:

ESR Method: `http://localhost:25500/Auth/ESRSegmentation.ashx`

AD Group Method: `http://localhost:25500/Auth/ADSegmentation.ashx`

These can be called with an additional ?debug=true querystring appended - if the system is installed correctly, debugging information will be displayed.

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 ads, a simple tag needs to be inserted into your intranet pages. This takes the form of an inline `<script>` tag which calls the segmentation.ashx page on the web site configured in the previous section.

This tag should be placed at the location at which you wish the ad to display (normally at the top of the page in the case of Leaderboard ads). 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 id="fendix"></div>

<script type="text/javascript">
// jQuery used as an example of delaying until load.
$(function() {
// Build url params and make the ad call
var adparam = ((window.location.toString().indexOf("?") > -1) ?
"http://servername.domain.nhs.uk:25500/Auth/ESRSegmentation.ashx"+"?"
+window.location.toString().split('?')[1] :
"http://servername.domain.nhs.uk:25500/Auth/ESRSegmentation.ashx");
postscribe('#fendix', '<script src='+adparam+'><\/script>');
  });
</script>
```

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 an ad in the default orientation as specified in the *AdOrientation* parameter (see Server configuration). To specify an orientation, add a querystring parameter 'AOr' to the end of the URL. Either AOr='leaderboard' or AOr ='skyscraper' will be accepted.

You must also ensure that both jquery and postscribe are loaded on the page:

```
<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>
```

Asynchronous Ad Loading

The default loading behaviour for ads 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 that 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 ads in the background while the rest of the page loads.

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