Fendix Media Ltd

Segmented Content Serving System

System Update and Configuration Guide

System Version 5.6.0.2

Revision History

1. 26 November 2019: *Initial Draft*

Introduction

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

This document is intended for those Network Partners who are updating their current IIS installation or 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

Reason for Update of Segmentation Process

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

We have been forced to change the server used to deliver content to the Trust Network by our current supplier withdrawing from the UK Market.

In order to deliver content to the trust network a script is embedded on each page of the intranet where content is to be displayed.

Older installations for trusts with no segmentation have a script which calls the content server directly.

Some segmented trusts have older versions of our segmentation component, which calls the current content server.

The latest version of our segmentation component calls our own segmentation server for more focussed keyword mapping and the content server script including the keywords is passed back by our segmentation server to the page.

In order to change over to the new content server, we require all trusts to be brought up to date by installing our latest segmentation component.

The new component will allow us to switch each trust over to the new content server by making a change to our internal database in a controlled manner with minimal interruption to serving of contents.

Minimum System Requirements

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

.Net Framework v4.5.2 or higher

Recommended system Requirements

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

.Net Framework v4.5.2 or higher

New System Installation

The purpose of the segmented content delivery system is to display content on your intranet that is 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 system. This is determined by configuration options detailed in this document. The information is used to determine keywords for content targeting, allowing a request to be made to the Fendix Media servers for appropriately targeted content.

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 (or available on our download page: https://www.fendixmedia.co.uk/downloads/)

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 content to the intranet page, this allows content 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** - content served. **false** - content 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**: Leave this at **leaderboard**.

- **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 received 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 the ESR system to perform segmentation.
  Valid values are **ESR** or **AD** or **REMOTE.**

- **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**. **Note**: this setting can only be used by Trusts that are transitioning from the AD to ESR method. and are therefore already set up on our system with AD groups keyword mapping.

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 segmentation. This list is zero

based (thus for a file containing email,job role,area of work. The relevant values would be 1,2)

- **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 AD 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 content.

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 content 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 content.

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 content, 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 content to display (normally at the top of the page). 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

If you or your third party supplier require assistance with the implementation of the script, please contact support@fendixmedia.co.uk

Asynchronous Loading

The default loading behaviour for content 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 content 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 content 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