Fendix Media Ltd

Segmented Advertising System Process and Data Capture Overview

System Version 5.0

Revision History

- 07 Jan 2019: Draft
- 14 Jan 2019: Initial Release
- 18 Jan 2019: Added Glossary of Terms

Introduction

The purpose of this document is to describe how the segmented advertising system delivers targeted adverts using data based on either the user's Electronic Staff Record (ESR) or based on a user's Active Directory (AD) group membership. It also explains what information is transmitted to Fendix Media's servers and how this is used and stored.

Although primarily intended to answer commonly asked questions from IT teams, this guide will also be of interest to those with governance considerations regarding the transmission and use of an organisations' data.

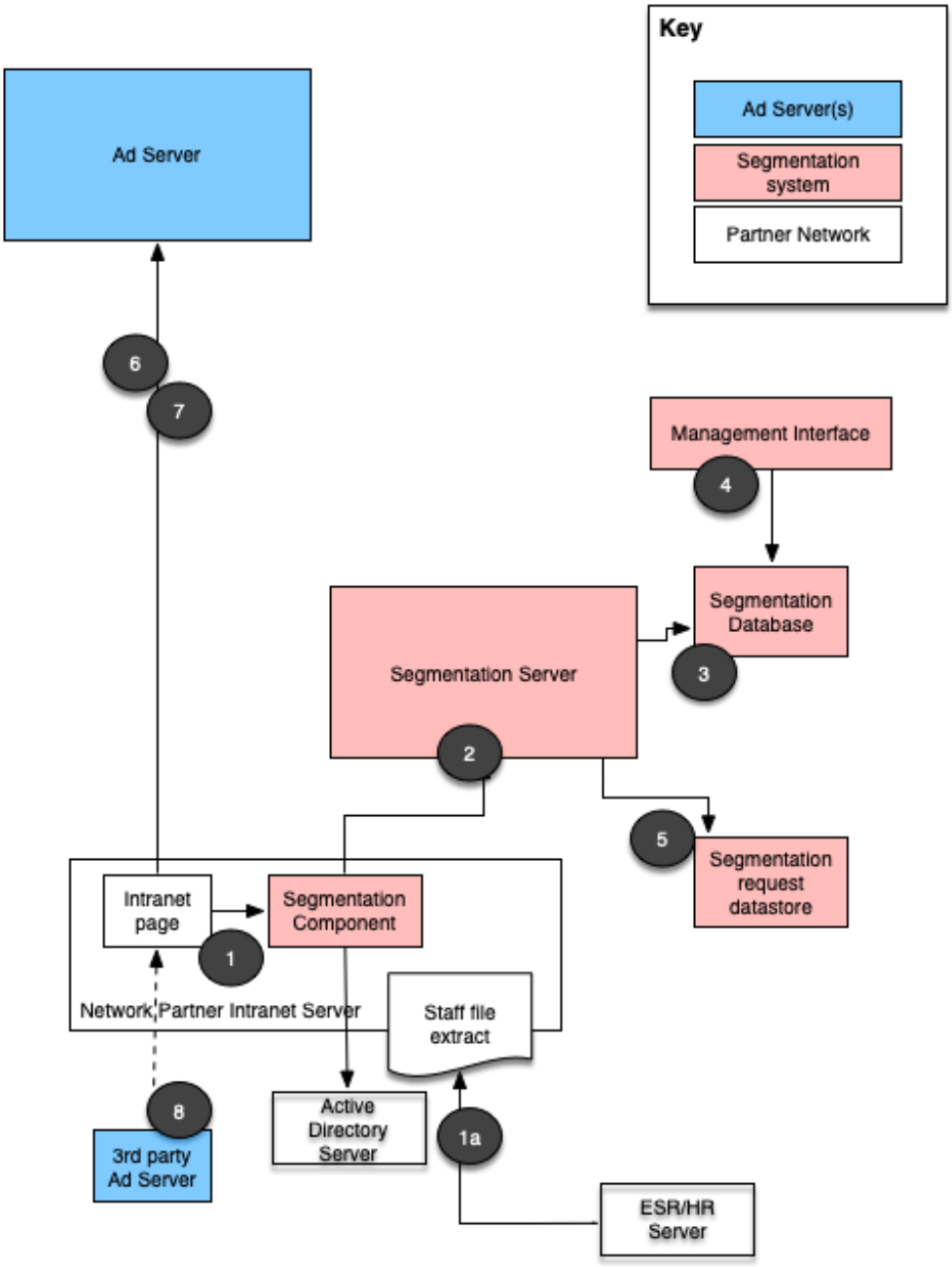
Glossary Of Terms

*

- Network Partner (or Partner): NHS Trust or Health Board receiving intranet advertising from Fendix Media
- Segmentation: The assignment of relevant advertising keywords to an intranet user based on their clinical or professional specialisms

Process Overview

The following diagram provides a simplified schematic of the various stages of the segmentation process.



1. A small script tag embedded on the network partner's Intranet pages calls through to the Fendix Segmentation Component. This component is installed on a Microsoft web server residing on the Trust network (IIS) with Windows Authentication enabled - this authentication method allows the component to obtain the Windows username of the user viewing the Intranet page.

   1(A) If segmenting is to be done using ESR data, an extract file containing the role data for each user is generated from the ESR system and placed on the web server. This is used as the data source for segmentation.

   Once the Windows logon name is obtained, user information is obtained: either by a list of Active Directory security groups for which the user is a member (the Active Directory Method), or by looking up the relevant user record in the Staff extract file (the ESR method) - to do this the forename and surname is extracted from the user's AD record and this name is then located in the extract file (this happens within the partner network and forename/surname data is not transferred to Fendix Media).

2. Once the targeting info has been obtained, it is encoded using Base64 encoding and transmitted to a web service on the Fendix segmentation server (code.fendixmedia.net), along with a one way hash of the username(in either MD5, SHA256 or SHA512 format).

3. The segmentation server checks the list of supplied information against a lookup table in the segmentation database which matches fields from the segmentation datafile to advertising keywords. This list is performed for each field to obtain an aggregate list of keywords pertinent to the user.

   Once the list is complete, the segmentation server generates a small JavaScript tag specifying a call to the Fendix Ad Server containing the relevant keywords.

4. If a field value is encountered that is not already present in the segmentation database it can be stored for later keywording using the Management interface, which allows designated Fendix staff to maintain keyword groupings for Network Partners.

5. For statistical purposes a record of each segmentation request is stored containing the following information:

   - Date/time of request
   - Network Partner unique reference number (URN)
   - User Hash
   - Keyword list

6. Once the relevant ad invocation code is passed back to the Segmentation Component, it is then returned to the Intranet page on the user's browser, where it is executed resulting in a call to the Fendix Ad Server to request an appropriate advert.

7. The advert code is returned to the user's browser where it is executed and displayed.

8. For some campaigns, ad content may be served from a partner advertising agency's ad server infrastructure. In these cases, the ad code delivered in (7) instructs the browser where to obtain the ad content from.

Summary of data transfer

This section details which data is passed outside of the Network Partner network and what it is used for. Some explanatory notes are also provided to assist non technical readers who may not be familiar with specific terminology.

The following information is sent to the segmentation server:

Trust Unique code: This is the 4 character code which identifies each trust and is supplied by Fendix Media.

Segmentation Field List: The full list of relevant segmentation data for a user (typically this might be job title and department if the ESR method is being used or list of Active Directory groups where the AD method is used). These are used by the segmentation server to match to advertising keywords via a look up mechanism.

Field values and name-keyword mappings are stored in the main segmentation database. No user specific information is stored in this database.

Username Hash: A hash is a one way mathematical function that encodes a piece of data in a consistent way, but such that it is not possible to decode the message to view the original content. By using a hash of the username, it is possible for Fendix Media to gain insight into the number of unique users that match to each ad keyword whilst ensuring that it is not possible to identify actual people. The system supports three hashing algorithms, MD5, SHA256 and SHA512 - this is configured at installation time and can be chosen by Trust.

Key datastores

There are three key datastores that form the Fendix ad-serving infrastructure, the segmentation database, the core ad server(s) and the analytics database. Each resides on separate servers with no linkages between them.

Segmentation database: Stores lists of segmentation field values for each trust along with keyword mappings. No user specific data is stored, nor is individual ad request data stored in this database. Access to the segmentation database is allowed via the segmentation API servers (these run as a cluster of servers for availability and performance) and the Fendix Management Interface application server.

Analytics database: this is a document store which records a log of every

segmented ad request, this log records the following data:

- Date/time of request
- Network Partner unique reference number (URN)
- User Hash
- Keyword list

From this data, analytical information such as the number of ad requests containing particular keywords and the number of unique individuals who match a given keyword can be deduced. This information is of interest to advertisers for assessing potential reach of an advertising campaign. It also allows Fendix Media to assess trends. None of the raw data is available to advertisers

Access to the analytics database is only possible from the segmentation servers (these only perform writes to the database), with read access only possible from within the Fendix media office network.

Ad Servers: The core advertising servers are where actual ad content is delivered from, these are run as a managed service by the system developers and function completely independently of the segmentation infrastructure.

No Trust data is ever communicated to the ad servers.

Administrative access

Administrative access to all servers in the Fendix segmentation infrastructure is by secure SSH session using public/private key access. Private keys are only available to Fendix system administrators and where applicable, access is only permissible from IP addresses within the Fendix network.

Information dissemination

Advertisers are able to select the broad specialism keywords that they wish to target their ads for serving to (e.g. doctors, procurement, cardiac). They are able to choose these from a pre-defined list. For example, Macmillan Cancer Support recently ran a campaign to inform healthcare professionals of the support information available to patients. They wanted to target this campaign to nurses, cancer and palliative care. The only information that is supplied to advertisers is the number of ad impressions served against the chosen keywords (if they request this level of granularity, typically an advertiser is only given a report of the number of impressions served and the number of clicks generated)

At no point do advertisers have access to actual Trust data, nor how they are mapped to specialism keywords. Advertisers are also not advised as to how many items are mapped to a keyword, nor how many users match a specific field value.