Fendix Media Ltd Segmented Messaging System Process and Data Capture Overview

System Version 6.7

Revision History

12 May 2020: Initial Issue

Introduction

The purpose of this document is to describe how the segmented messaging system delivers targeted messages using data based on the user's Electronic Staff Record (ESR). 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.

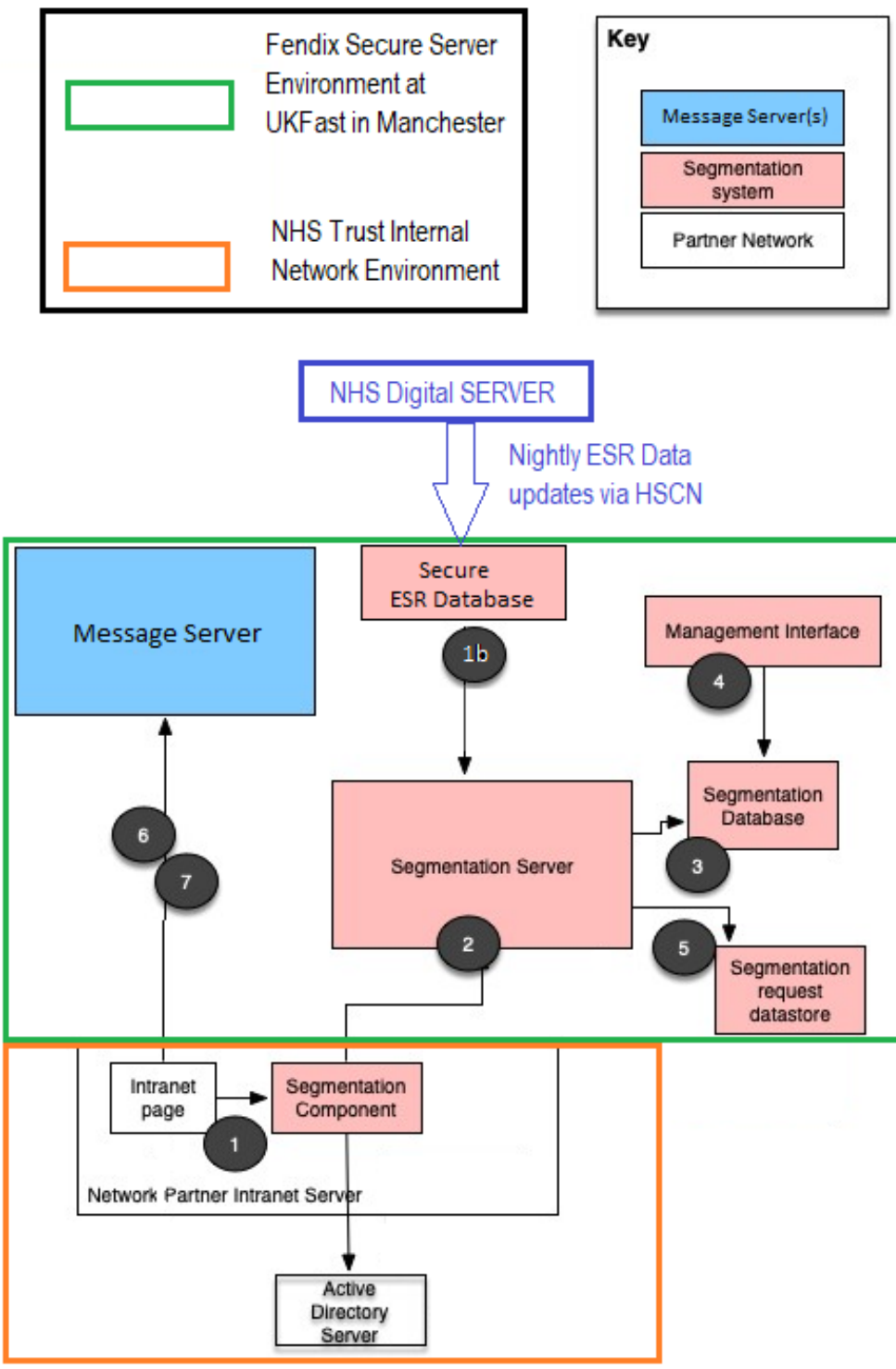
Glossary of Terms

Network Partner (or Partner): NHS Trust or Health Board receiving intranet messaging banners from Fendix Media

Segmentation: The assignment of relevant 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.


Fendix Secure Server Environment at UKFast in Manchester
NHS Trust Internal Network Environment
Key
Message Server(s)
Segmentation system
Partner Network
NHS Digital SERVER
Nightly ESR Data updates via HSCN
Message Server
Secure ESR Database
1b
Management Interface
4
Segmentation Database
3
Segmentation Server
2
5
Segmentation request datastore
6
7
Intranet page
1
Segmentation Component
Network Partner Intranet Server
Active Directory Server

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.

    a The Secure Hash of the email address is sent to the Fendix Segmentation Server and job role, occupation and area of work, will be looked up on the Fendix media secure ESR extract database provided by NHS Digital directly to our servers via the HSCN.

2. 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 messaging keywords. This list is performed for each field to obtain an aggregate list of keywords relevant to the user.

    Once the list is complete, the segmentation server generates a small JavaScript tag specifying a call to the Fendix Message Server containing the relevant keywords.
    The incoming targeting data received from the trust is destroyed at this time.

3. The management interface is used by Fendix Staff to manage the system as required.

4. 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)
    - Keyword list

5. Once the relevant message 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 Message Server to request an appropriate display message.
6. The message display code is returned to the user's browser where it is executed and displayed.

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 which is hosted in the UK on a Fendix contracted secure cloud service in the secure Public Sector hosting centre at UKFast in Manchester.

Trust Unique code: This is the 4-character code which identifies each trust and is supplied by Fendix Media. **e.g.** ***"T034"***

A secure Hash of the user's email address. This is used by the segmentation server to match message keywords via a look up mechanism.

e.g.
80078ca28176e808a42491ee834fc3d02d9d305ea5fff31979a6b7fc843abb6d00a54da7ff38659b4c1b5a56ba4b4312def4684a5947f180cf5f4c9a1d1f6611 (Hash of email address)

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

A secure Hash of the user's email address is sent and the job role, occupation and area of work, will be looked up on the Fendix media secure ESR extract database provided by NHS Digital directly to our servers via the HSCN. 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 secure Hash of the user's email address, it is possible for Fendix Media to match the incoming Hash to the Hash stored in the database whilst ensuring that it is not possible to identify actual people. The system uses the secure SHA512 hash with a unique salt for each email address by adding the data before the @ sign to the end of the email before hashing.

Key datastores

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

These are hosted in the secure Public Sector hosting centre at UKFast in Manchester.

Segmentation database: Stores lists of segmentation field values along with keyword mappings. No user specific data is stored, nor is individual message 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.

Core message server. This only stores admin data such as project data indicating which Trusts and keywords should be served which creative banner message, and statistical data recording what creative banner message was served when and where to.

Analytics database: This is a document store which records a log of every segmented message request, this log records the following data:

- Date/time of request - **e.g.** ***"2019-10-01 00:00:00.231Z"***
- Network Partner unique reference number (URN) - **e.g.** ***"T034"***
- Keyword list - **e.g.** ***emergency, general_medicine***

From this data, analytical information such as the number of message requests containing particular keywords can be deduced. This information is of interest for assessing potential reach of a particular service. It also allows Fendix Media to assess trends. None of the raw data is available to clients

Access to the analytics database is only possible from the segmentation servers (these only perform writes to the database), with read access only possible by Fendix Media Staff.

Message Server: The core messaging server is where actual message content is delivered from, this is also hosted in the secure Public Sector hosting centre at UKFast in Manchester.

No personal identifiable data is ever communicated to the messaging 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 registered to the Fendix network.

Information dissemination

Clients are able to select the broad specialism keywords that they wish to target their messaging 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 service to inform healthcare professionals of the support information available to patients. They wanted to target this service to nurses, cancer and palliative care. Another example is a Biogen service that provides free medical education to a neurology audience. The only information that is supplied to clients is the number of message impressions served against the chosen keywords (if they request this level of granularity, typically a client is only given a report of the number of impressions served and the number of clicks generated)

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

Issues that may prevent the system from working or only partially working

If the on page <script> tag is correctly formed, the only other issues that prevent the system working properly are related to network access and permissions.

ISSUE: **NO Banner Showing**

Each page which should display a banner should have a <script> tag which calls our internal segmentation server which is running on the trusts internal network. If the intranet page cannot reach our segmentation app due to network routing or permission issues, no banner will appear.

Normally fixed by network port and permission settings

If our internal segmentation app cannot access our external segmentation server due to network routing or permission issues, no banner will appear.

Normally fixed by whitelisting **.fendixmedia.net*

If our external segmentation server sends the correct script back to the intranet, but no banner appears this indicates that the intranet cannot access the message server.

Normally fixed by whitelisting **.fendixmedia.net*

ISSUE: **Only Generic Banner Showing, no Segmented messages being delivered**

If the page script can reach our segmentation app, but we cannot identify the user, because our segmentation app cannot reach your AD server, you will only get generic banners showing.

Normally fixed by network port and permission settings

If the page script can reach our segmentation app, but we cannot identify the user, because they are not logged on to your AD network, you will only get generic banners showing.

System is working as designed

If our segmentation app sends correct details to our external segmentation server and no keywords match those groups, or there are matching keywords but there are no services running that match those keywords, you will only get generic banners showing.

System is working as designed