

# NHSmail – TANSync Overview

November 2017

Version 3.0

## Contents

---

<b>1 Purpose of Document</b>	<b>3</b>
<b>2 Overview of Solution</b>	<b>3</b>
<b>3 Non-Functional Specification</b>	<b>5</b>
3.1 Hardware Specification	5
3.2 Software Specification	5
3.3 Security Groups Specification	5
3.4 Service Account Specification	6
3.5 Ports and Traffic Flows	6
3.6 TANSync Attribute Specification	6
<b>4 Glossary of Terms</b>	<b>9</b>

---

# 1 Purpose of Document

NHSmail will introduce a new method for organisations to automatically publish people data (e.g. contact telephone numbers) to the Service. In the past NHSmail has supported three methods of managing people data for the service.

- **Manual data update:** Manually creating, updating and removing people directly within the NHSmail administration portal;
- **Push Connector:** Emailing a comma separated value (.csv) file to [connector.data@nhs.net](mailto:connector.data@nhs.net);
- **Pull Connector:** Setting up NHSmail to retrieve people data directly from a local data source.

NHSmail will continue to support the manual data updates and Push Connector methods. The new publishing service will replace Pull Connectors and will be called the Accenture New Synchronisation (TANSync) Service. The TANSync Service provides a new, standards based interface through which to publish people data. This will make updates to people data timely and faster.

This document provides an overview and a non-functional specification of the TANSync Service and is intended to enable organisations to evaluate the requirements for deployment ahead of receiving the software.

The intended audience for this document is highlighted below:

- End Users
- Training and Business Change Managers
- Local Administrators (LAs)
- IT Managers

## 2 Overview of Solution

### What is TANSync?

TANSync is an Identity Management Solution which enables organisations to synchronise local people data with the NHSmail API. Accenture has created the solution based on Microsoft Identity Manager (MIM) 2016 which is now included as part of the standard Windows Server 2012 R2 license.

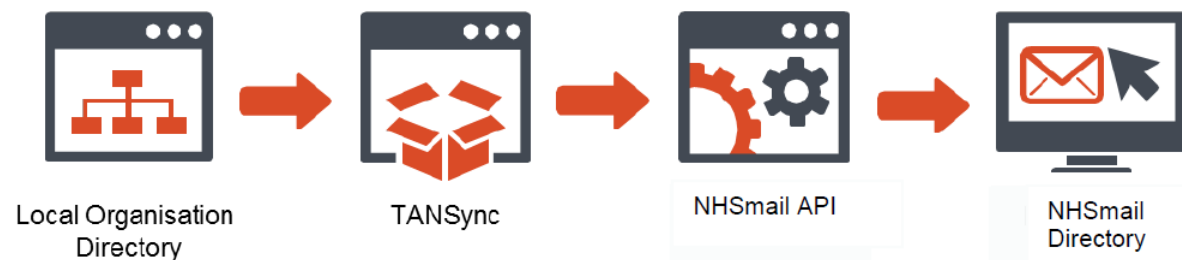
MIM, and its previous versions (Forefront Identity Manager, Identity Lifecycle Manager, Microsoft Identity Integration Server), is a proven technology for managing identity provisioning and is used across thousands of organisations today. TANSync provides a custom connector for MIM and a set of pre-packaged server configurations that will enable you quickly connect an Active Directory or SQL Server based data source to the NHSmail API.

An organisation using a different type of data source can still implement TANSync as out of the box MIM provides connectors for most of the commonly deployed systems. The

connector for the NHSmail API will still be supplied, however pre-packaged MIM configurations for these data sources will not be provided.

The diagram below shows how the service will look once an organisation has installed and connected TANSync to publish their identity data.

## Figure 1: Overview of TANSync



## Who might choose to use TANSync?

The NHSmail Solution will offer a Microsoft Identify Manager (MIM) product that will enable a close integration between an organisations local SQL Server database or Active Directory and NHSmail. The TANSync package facilitates organisations to synchronise local peoples' data using the custom connector for MIM and set pre-packaged server configurations that will allow the organisations data source to connect to the NHSmail API. Organisations may wish to deploy the preconfigured TANSync solution if they:

- Currently rely on a Pull Connector
- Do not have an existing Identity Management Solution;
- Need a temporary solution for connectivity to the NHSmail API (for example, whilst development and testing for their existing Identity Management Solutions).

Organisations that currently use their own Identity Management solutions such as Novel and Oracle, will need to set up an additional agent to connect to their Identity Management manually, to enable the organisations to use TANSync to communicate with NHSmail.

## How is TANSync deployed?

Organisations wishing to deploy the TANSync solution as a replacement to their existing Pull Connectors will need to provision a basic server in their environment and deploy the TANSync solution using the pre-packaged MIM configurations Accenture will provide.

This solution has been designed to enable a simple installation process for organisations with an Active Directory or SQL Server-based Pull Connector. This should enable the organisation to self-install the solution with minimal support by phone and email from the Accenture NHSmail Team. Where required, the NHSmail supplier (Accenture) is able to provide additional support on an individual basis for organisations deploying TANSync. This will be available as a charged service to the local organisation.

## What are the next steps for deploying TANSync?

The rest of this document provides a non-functional specification for the TANSync solution to allow organisations to evaluate the requirements for deployment ahead of receiving the software. This will be followed by more complete installation instructions and demonstrations of the solution for interested organisations.

## 3 Non-Functional Specification

### 3.1 Hardware Specification

The table below outlines the hardware specification required to deploy TANSync:

Site	Requirement	Operating System	Minimum System Specification	Quantity
<b>Local Organisation Premises</b>	MIM Synchronisation Server	Microsoft Windows 2012 R2	4 Core 8GB RAM 100GB disk 1Gbps network	1

An existing Windows Server 2012 R2 can be used for this, there is no need to set up a dedicated instance for TANSync.

### 3.2 Software Specification

The following software will need to be installed on the TANSync MIM Synchronisation Server for each of the organisations:

Requirement	Description	Quantity
<b>Windows Server 2012 R2 Licenses</b>	All Physical Servers require licensing	1
<b>Microsoft Identity Manager 2016</b>	Server license covered by the Operating System.	1
<b>SQL Server 2008 R2 SP3</b>	MIM support SQL Server 2008 R2 SP3 and above. All Physical Servers require licensing	1*
<b>.Net Framework 3.5</b>	Install as a feature onto Server 2012	1

An existing remote SQL server instance can be used. Where organisations have an existing SQL server meeting the above requirement Accenture recommends utilising it for TANSync as opposed to purchasing a new SQL license.

### 3.3 Security Groups Specification

The following security groups are required to complete the installation of the MIM solution. It is recommended to have security groups created in Active Directory, however it is also acceptable to create them locally on the MIM server.

Site	Requirement	Description	Quantity
NHS Organisation Site	MIMSyncAdmins	MIM synchronization administrator group	1
NHS Organisation Site	MIMSyncOperators	MIM synchronization operator group	1
NHS Organisation Site	MIMSyncJoiners	MIM synchronization joiner group	1
NHS Organisation Site	MIMSyncBrowse	MIM synchronization browse group	1
NHS Organisation Site	MIMSyncPasswordSet	MIM synchronization password set group	1

### 3.4 Service Account Specification

Installation of a MIM server will require the following service accounts to be created either prior to, or as part of the install:

Site	Requirement	Description	Quantity
NHS Organisation Site	Svc_MIMSynchService	MIM synchronization service will use this account for running the service	1
NHS Organisation Site with AD as data source	Svc_MIMADMA	MIM Active Directory management agent will use this account for running Import, Export and Synchronization run profiles	1
NHS Organisation Site with SQL as data source	Svc_MIMSQLMA	MIM SQL management agent will use this account for running Import, Export and Synchronization run profiles	1
Portal	TANSync_Account for each of the NHS Organisations	TANSyncMA will use this account for running Import, Export and Synchronization run profiles. The account is organisation-specific and will have the role assigned, which will provide access only to the identities of the specified Organisation.	1

### 3.5 Ports and Traffic Flows

TANSync communicates with the NHSmail API over encrypted TCP port 443 and uses outbound connections only. This is much more secure and does not require an organisation to expose their internal network to the NHSmail service.

Source	Destination	Protocol	Port	Direction
TANSync Server	NHSmail API	IP (TCP)	443	Outbound Initiated

### 3.6 TANSync Attribute Specification

The following attributes are currently supported on the NHSmail API. Local organisations can map their local data source attributes to these in a wide variety of configurations. Local organisations will be able to tailor their MIM attribute flows for TANSync to their local individual needs.

The 'Write Capability' column indicates whether local organisations can write data from their local data source to the NHSmal. The 'Mandatory' column indicates whether an attribute is required to be provided for the successful publication of data to NHSmal.

Attribute Name	Mandatory	Leave Blank	Data Type	Description
ClinicalRoleMultiValued			string	User Clinical Role (multivalued attribute)
ClinicalSpecialityMultiValued			string	User Clinical Specialty (multivalued attribute)
DisplayName		Yes	string	User display name. This is automatically generated if null. (Portal has its own format, it is best to let this be generated)
Email			string	Email address.  If known please give the value. This allows successful joins on objects during Initial Synchronization Cycle.  If left blank this will be auto generated.
EmailSize			string	Email box size.  Auto generated to have value of 4 if left blank. (4GB)
EmailType		Yes	string	Email type will be auto generated with value "user".  Please leave this blank for auto generation.
ExternalSynclId			string	Anchor attribute this attribute should be mapped to a unique attribute which should not change once set. This allow successful joins on objects during Initial Synchronization Cycle.  If left blank, this will be automatically generated.
Fax			string	Fax number

Attribute Name	Mandatory	Leave Blank	Data Type	Description
<b>FirstName</b>	Yes		string	User first name
<b>ID</b>		Yes	string	User ID in the portal. This value is auto generated during provisioning of the user into the Portal.
JobTitle			string	User job title
<b>LastName</b>	Yes		string	User last name
MobilePhone			string	Mobile phone number
Notes			string	Notes
OfficePhone			string	Office telephone number
<b>Organisation</b>	Yes		string	Organisation code
OrganisationUnit			string	Organisation Unit code: A code of Department within the Organisation.  If left blank if not known and this will be auto generated to have the same code as Organisation
Pager			string	Pager number
Status		Yes	string	User account status. (Pending, Active, Deleted...). The value comes from the portal. User account status
Subscriptions		Yes	string	User Portal subscription ID. (comma separated multiple values)  This value is auto generated if left blank. By default this is 1.
Title			string	Personal Title (Mr, Mrs, Lord...)
UserPrincipalName			string	Portal User Principal Name This is automatically generated



Attribute Name	Mandatory	Leave Blank	Data Type	Description
WorkAreaMultiValued			string	User work area (Multivalued attribute)

## 4 Glossary of Terms

Term	Abbreviation	Description
<b>Active Directory</b>	AD	AD is the Microsoft directory service providing the authentication and authorisation for users of an application.
<b>Application Programmatic Interface</b>	API	An API provides a set of routines and protocols that provide the foundations for interaction between different applications and application components.
<b>Microsoft Identity Manager</b>	MIM	MIM provides is an identity and access management solution. Predecessors of MIM include, Forefront Identity Manager (FIM), Identity Lifecycle Manager (ILM) and Microsoft Identity Integration Server (MIIS).
<b>Pull Connector</b>	Not Applicable	A Pull Connector enables synchronisation between a local organisation data source and the NHSmail Directory by automatically initiating requests for the data from NHSmail to the local data source.
<b>Push Connector</b>	Not Applicable	A Push Connector enables synchronisation between a local organisation data source and the NHSmail Directory through the manual submission of data files from a local organisation.
<b>SQL Server</b>	SQL	A SQL Server is a relational database management system for which the primary function is to store and retrieve data for other applications. For example, user contact data.
<b>The Accenture New Synchronisation Service</b>	TANSync	TANSync is an Identity Management Solution providing integration between local data sources and the NHSmail API.
<b>Transmission Control Protocol</b>	TCP	TCP is the network protocol enabling two hosts to establish a connection and exchange data.