

# **NHSmail Single Sign-on Technical Guidance**

**Integrating Authentication with your  
Application**

October 2018

Version 1

# Contents

---

<b>Introduction</b>	<b>3</b>
<b>Benefits of integrating authentication with your application</b>	<b>3</b>
<b>Supported authentication methods</b>	<b>3</b>
<b>Application authentication process</b>	<b>4</b>
<b>Authentication workflow</b>	<b>5</b>
<b>Further guidance</b>	<b>6</b>

---

## Introduction

This is a guidance document for organisations who would like to enable single NHSmial sign on for other web and desktop applications.

This document is aimed at a technical audience working with the NHSmial supplier to enable Single Sign On (SSO) using a users' NHSmial mail identities (@nhs.net credentials) with your application.

## Benefits of integrating authentication with your application

It is possible to use your normal NHSmial username ([username@nhs.net](#)) and password to authenticate against other web and desktop applications. The requirement is that those applications consume one of the supported authentication methods highlighted in this document.

There are several advantages of implementing SSO for both users and application administrators:

- Users:
  - Replacing many of the current disparate user names and passwords with a single NHSmial credential
  - Users will not be re-prompted for credentials when signing on to multiple applications integrated to NHSmial authentication i.e. OWA, NHSmial Portal, third-party integrated applications etc.
  - Self-service password reset and unlock, along with 24x7 helpdesk support for any NHSmial account issues
- Local Administrators (LAs):
  - Enhances security as users are less likely to write passwords down as they have fewer to remember
  - No need to issue new credentials per application and the account management lifecycle is already managed through existing NHSmial account lifecycle processes
  - Enhanced security processes – Multi-Factor Authentication (MFA), compromised account detection etc.

## Supported authentication methods

The NHSmial ADFS servers supports the following federation protocols:

1. **OAuth 2.0 and OpenID connect** – OAuth 2.0 is the industry-standard protocol for authorization. OAuth 2.0 focuses on client developer simplicity while providing specific authorization flows for web applications, desktop applications, mobile phones, and living room devices.
2. **SAML 2.0** – The Security Assertion Markup Language (SAML) 2.0 is an XML-based framework that allows identity and security information to be shared across security domains. The SAML specification, while primarily targeted at providing cross domain

Web browser single sign-on (SSO), was also designed to be modular and extensible to facilitate use in other contexts.

3. **WS -\* (Federation,Trust,Security)** – WS-Security, WS-Trust, and WS-SecurityPolicy provide a basic model for federation between Identity Providers and Relying Parties. These specifications define mechanisms for codifying claims (assertions) about a requestor as security tokens which can be used to protect and authorize web services requests in accordance with policy. This is not the preferred protocol, so further guidance will not be supplied.

**Note:** Lightweight Directory Access Protocol (LDAP) bind against the NHSmail Active Directory is not supported.

## Application authentication process

If your organisation wishes to implement NHSmail authentication with their Application integrated with nhs.net federation server, please follow the process below.

1. Complete the table below ensuring that all fields are completed.

Requirement	Detail
Application Name	<b>[Insert name]</b> This is the name by which the application is known e.g. EPR 2.1
Redirect / Reply URL	<b>[Insert URL]</b> The URL that NHSmail should redirect the user to after they have authenticated with their authentication code <u>Only for Security Assertion Markup Language (SAML) Apps</u> The reply URL is where the application expects to receive the SAML token. This is also referred to as the Assertion Consumer Service (ACS) URL.
Application Identifier	<b>[Insert identifying value]</b> Value, which uniquely identifies the application for which SSO is being configured. In SAML terminology, it's known as <b>Entity ID</b> .
Federation Metadata (Optional)	<b>[Provide federation metadata]</b> Federation Metadata contains all the parameters required to create Federation Trust. If the Federation metadata is published, Active Directory Federation Services (ADFS) can update trust properties, if any changes happened at App Side.
User Identifier	<b>[Insert name identifier]</b> Name Identifier in SAML. Please specify which attribute to be sent as Name Identifier and SAML claim type.

Additional Claims	<p><b>[Provide expected claim types and attributes]</b></p> <p>Please set out claim Types and Attributes you are expecting.</p>
Target Audience	<p><b>[Provide details of users who are licensed to use the app]</b></p> <p>As there are Multiple NHS organisations using the same authentication platform, determine the users who are licensed to use the app. Any common criteria to define the users will be helpful. Example: Org ID / Department / Job Title</p>
Scope / Purpose of the Application	<p><b>[Provide details on the purpose of this application]</b></p> <p>Define the purpose of application e.g. my application will be used to help users log their working hours per week.</p>
Responsible Organisation	<p><b>[Insert organisation name]</b></p> <p>The organisation that is using the application e.g. NHS Digital</p>
Additional Information	<p><b>[Please add any configuration / security details of which the NHS Digital team should be aware]</b></p> <p><b>Please note: While the local organisation has elected to use NHSmail for authentication, they can at any time revert to using local accounts to control access or use a mix of local and NHSmail accounts as business as usual.</b></p>
Application support details	<p><b>[Insert the contact details for the company that supports the application]</b></p> <p>For example:          Company Name: ACME          Email: <a href="mailto:support@acme.com">support@acme.com</a>          Phone: 001-555-246-1357          Address: 1 Silicon Valley                    San Francisco                    CA, USA</p>

2. Send this information to the [NHSmail helpdesk](#) and a technical contact will be allocated to deal with your request.

## Authentication workflow

1. User accesses the Application
2. Application redirects the user to the NHSmail ADFS servers for authentication
3. The NHSmail ADFS servers prompt the user to enter their NHSmail credentials via the standard sign-in screen. If Multi-Factor Authentication (MFA) is enabled, approval through the chosen authentication method will also be required.



Sign in with your NHSmail account

UserTest@nhs.net

.....

Sign in

This is a private computer

Forgotten Password? [Click here.](#)

4. ADFS authenticates the user and sends an authentication token to the user's device
5. User's device presents the authentication token to the integrated application
6. Application grants/rejects access to the user based on application authorisation rules

**Please note:** NHSmail SSO provides an authentication mechanism only. The responsible organisation is required to determine the application authorisation rules that dictate which users are authorised to access the application.

## Further guidance

[Modern Authentication Using OAuth 2.0 and OpenID Connect](#)

[WS-Fed/Trust](#)

[SAML](#)

[Overview of ADFS](#)