NHSMail Single Sign-on Technical Guidance

Integrating Authentication with your Application

January 2022
Version 3.0

Contents

Introduction

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

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

Benefits of integrating authentication with your application

It is possible to use your normal NHSmail 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 usernames and passwords with a single NHSmail credential
  - Users will not be re-prompted for credentials when signing on to multiple applications integrated to NHSmail authentication, for example Outlook Web Application (OWA), the NHSmail Portal, third-party integrated applications etc.
  - Self-service password reset and unlock, along with 24x7 helpdesk support for any NHSmail 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 NHSmail account lifecycle processes
  - Enhanced security processes – Multi-Factor Authentication (MFA), compromised account detection etc.

Supported authentication methods

The NHSmail Active Directory Federation Services (ADFS) servers support the following federation protocols:

1. **OAuth 2.0 and OpenID connect –** OAuth 2.0 is the industry-standard protocol for authorisation. OAuth 2.0 focuses on client developer simplicity while providing specific authorisation 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 SSO, was also designed to be modular and extensible to facilitate use in other contexts. Before raising the form with the SAML information, please clarify that your application is compatible with ADFS. ADFS is our identity provider we use for standardised relying party configuration. If the application you want to integrate with SSO is only compatible with Azure, please use the following process - https://support.nhs.net/knowledge-base/servicenow-request-process-for-stores/
3. **SAML 2.0 WS -* (Federation, Trust, Security) –** WS-Security, WS-Trust and WS-Security Policy 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 authorise 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.

please specify which type of SSO setup is being configured:

SAML 2.0 □

SAML 2.0 WS -*□

oAuth□

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.

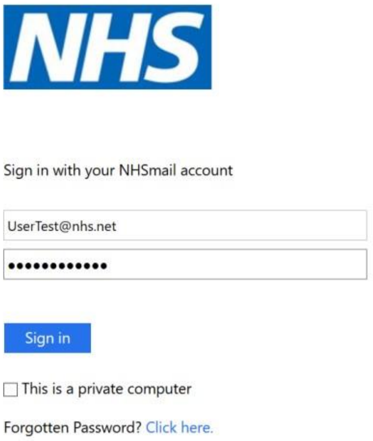
Requirement	Detail
Application Name	[*Insert name*] This is the name by which the application is known e.g. EPR 2.1
Redirect / Reply URL	[*Insert URL*] The URL that NHSmail should redirect the user to after they have authenticated with their authentication code. Only for Security Assertion Markup Language (SAML) Apps 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. Can the user also please specify if the reply URL is a SAML Assertion Consumer or WS-Federation endpoint, as this will avoid potential conflicts during the setup.
Application Identifier	[*Insert identifying value*] Value which uniquely identifies the application for which SSO is being configured. In SAML terminology, it's known as **Entity ID.**
Federation Metadata	[*Provide federation metadata*] 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. If your application can produce a metadata file, please attach this file/the URL of the metadata and this will allow us to create a consistent relying party with all relevant data required. Metadata is only required if it is a SAML application.
User Identifier	[*Insert name identifier*] Name Identifier in SAML. Please specify which attribute to be sent as Name Identifier and SAML claim type.

Additional Claims	[*Provide expected claim types and attributes*] Please set out claim Types and Attributes you are expecting. The attributes that are available are shown below so please specify which ones you would like to see as claims in the SSO token. • Display Name • UPN • Primary Mail Address • ODS Code
Target Audience	[*Provide details of users who are licensed to use the app*] 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. Ideally to best target the users, the ODS Code of the org the users are under would be best to provide to enable us to ensure the correct users have access.
Scope / Purpose of the Application	[*Provide details on the purpose of this application*] Define the purpose of application e.g. my application will be used to help users log their working hours per week.
Responsible Organisation	[*Insert organisation name*] The organisation that is using the application e.g. NHS Digital. This must be an open organisation that exists in Portal (status is not closed). Please provide the organisation name and organisation ODS Code exactly as displayed in Portal.
Additional Information	[*Please add any configuration / security details of which the NHS Digital team should be aware of*] **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.**
Application support details	[*Insert the contact details for the company that supports the application*] For example: Company Name: ACME Email: support@acme.com Phone: 001-555-246-1357 Address: 1 Silicon Valley San Francisco CA, USA

2. Send this information to the NHSmail helpdesk and a technical contact will be allocated to deal with your request.
3. Once the application has been created through our Request For Change process, SAML metadata will be supplied in the ServiceNow ticket which will be required to be configured on the application identifier

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

••••••••••••

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.

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.

Token Lifetime

NHSmail ADFS Replying Parties are configured to have a default token lifetime of one hour. Token issuance requires that the token requestor has been authenticated by AD FS and has authorisation to request a token. When a user is authenticated by AD FS an authentication cookie is written to the client to provide an SSO period, and subsequent requests to AD FS utilise this SSO period (authentication cookie). The configured SSO lifetime period for this is 8 hours with the “This is a private computer” setting selected by the end user.

Multi Factor Authentication

When configuring an application within our Identity Provider, each app is configured with a default access control of “Permit everyone and require MFA for specific group”. This group mentioned is the Azure MFA security group which is used for all users who require MFA. By default, each application will prompt a user for MFA if they are part of this group. If they don’t require MFA (Standard user account), the app won’t prompt them for 2FA as we don’t expect every user to have MFA set up.

We have also created a custom access control policy to allow applications to be requested to only allow users under a certain ODS codes to be authenticated, alongside being part of the MFA group or not.

Further guidance

WS-Fed/Trust

SAML

Overview of ADFS