NHSmail Same Sign On

Onboarding Guide

October 2022

Version 7.4

Contents

1 Overview

1.1 Intended audience

This document is intended for organisations that are implementing the Same Sign On solution for those using NHSmail as its primary email service. It details the end-to-end process for implementing the solution, including the installation of a user synchronisation solution as a pre-requisite and the Same Sign On tool. It provides a step-by-step guide which readers are encouraged to use as a checklist for reference during the onboarding process.

This guide focuses on the implementation of technical pre-requisites, such as TANSync and Local Active Directory (Local AD) integration, and then on the installation of the tool. Where necessary, it includes links to accompanying documentation to facilitate the onboarding process. For example, the installation process for TANSync is detailed in a separate guide.

Readers are expected to have a comprehensive understanding of the installation of Microsoft products and experience working with identity solutions such as Identity Lifecycle Manager (ILM), Forefront Identity Manager (FIM) or Microsoft Identity Manager (MIM).

2 Executive Summary

This section introduces the Same Sign On product, outlining its capabilities, key benefits and a high-level solution overview.

2.1 Same Sign on solution

NHSmail currently provides collaboration, directory and identity services to 1.7 million users within the NHS. It is used by around 11,000 NHS organisations as a collaboration solution, providing Exchange Online and Office 365 services.

The majority of NHS organisations operate a local directory service which is used for their desktop/laptop estate and for integration with local applications. Almost all of these are based on Microsoft Active Directory with no unique domain name.

Currently, these directories are typically standalone and do not have any link to other directories within the NHS, i.e., no trust relationships or shared forests. This means that users must manage two separate passwords, one for NHSmail to access their mailbox, and one for their local AD to log into their workstation. This causes a high volume of password reset tickets to organisations' local service desks.

The Same Sign On solution will provide simpler password management for users by enabling the bi-directional synchronisation of passwords between NHSmail and organisations' local ADs.

The Same Sign On solution will:

- Allow the same password to be used to access local workstations, NHSmail services, applications using NHSmail single sign on and Azure Active Directory
- Ensure the application of a single Password Policy for both NHSmail and Local AD

- Align password expiry dates between NHSmail and Local AD The Same Sign On solution will not:
- Have any impact on Microsoft Office 365 nor will it work directly with Microsoft Office 365
- Support multiple organisations sharing one AD Domain

3 Key Benefits

 **Reduce overhead on password management for users** – users currently face the challenge of managing multiple different passwords, with different complexity requirements and expiry times

 **Reduce overhead on service desk to support password reset** – having a single password, common to NHSmail and organisations' Local ADs will simplify password management. The Same Sign On solution is likely to reduce password reset requests to an organisation's helpdesk and NHSmail Local Administrators.

 **Unified Password Policy across the two services** – The NHSmail Password Policy is intended to reduce the risk of passwords being compromised and improve cyber security. The Same Sign On solution allows organisations' Local ADs to benefit from this same policy.

4 Solution overview

The automated synchronisation of passwords between NHSmail and organisations' Local ADs entails that:

- Passwords that are changed on NHSmail platform are securely sent to the Local ADs and can then be used to log on to local desktops/laptops and applications
- Passwords that are changed on the Local ADs are securely sent to NHSmail and can then be used to log on to NHSmail services

All NHSmail accounts within organisations that onboard the Single Sign On will be covered by the solution, including inactive NHSmail accounts.

NHSmail accounts that no longer belong to an organisation will not be covered by the solution, for example leavers or permanently deleted accounts.

The below high-level diagram describes the flows for capturing password changes in either the NHSmail Portal or Local ADs, and then writing password changes securely in the other system.

4.1 High-Level Design

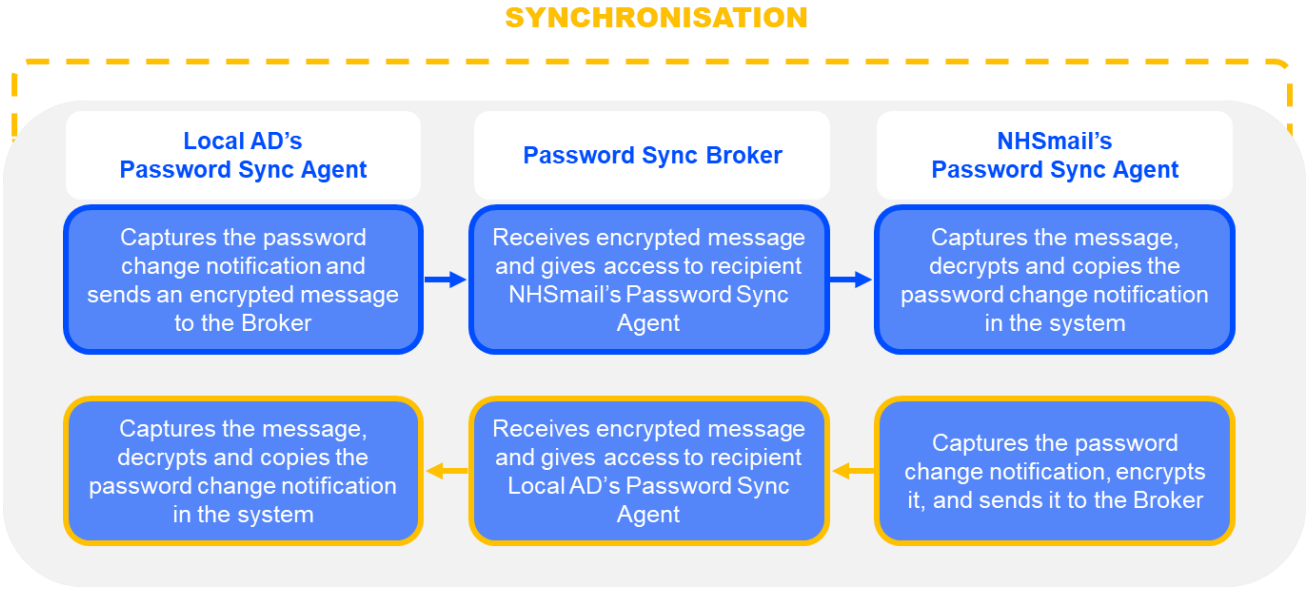


Figure 1: Overview of the solution – Synchronisation of Password from NHSmail to Local AD, and from Local AD to NHSmail

All data exchanged as part of the process will be via encrypted connections in line with the agreed encryption ciphers.

The Same Sign On solution will leverage the following components to ensure the secure synchronisation of passwords between NHSmail and Local ADs:

- **TANSync version or an equivalent identity matching solution** will synchronise user details between the NHSmail portal and organisations' Local AD. This is an important prerequisite so that NHSmail email addresses can be written to the local organisations' ADs to identify users that require a change of password. This is possible once the email address is the same in NHSmail and Local AD.
- **Password Sync Agents** are applications that will be located in NHSmail and Local ADs, performing a dual function of:
- Capturing password change notifications from either the NHSmail platform or the local organisation, encrypting and signing password change messages to send to the Password Sync Broker
- Receiving password change messages from the Password Sync Broker, verifying and decrypting the message, then setting the password to the correct user account in either NHSmail or an organisation's local ADs. This is identifiable through the NHSmail email address

- **Password Sync Broker** is a component implemented on Microsoft Azure. The purpose of this component is to:
- Receive messages from the NHSmail Password Sync Agent and distribute the message to the correct local Password Sync Agent
- Receive messages from the local organisation's Password Sync Agent and forward this to the NHSmail Password Sync Agent
- Microsoft Azure offers high availability, load balancing and scalability for the Password Sync Broker. Hence, this component is scalable to handle a large number of messages. It also is highly available and resilient to network or agent downtime, by queueing messages which can be retrieved when an endpoint comes back online
- The synchronisation happens near real-time

Important Note: Same Sign On can currently only be configured for one ODS ode per AD domain. If your organisation has multiple ODS codes, only one can be chosen to be used for this solution.

Important Note: If your organisation has additional LSA protection enabled on your domain controllers, currently password synchronisation will only occur from NHSmail to the local AD and not bi-directionally.

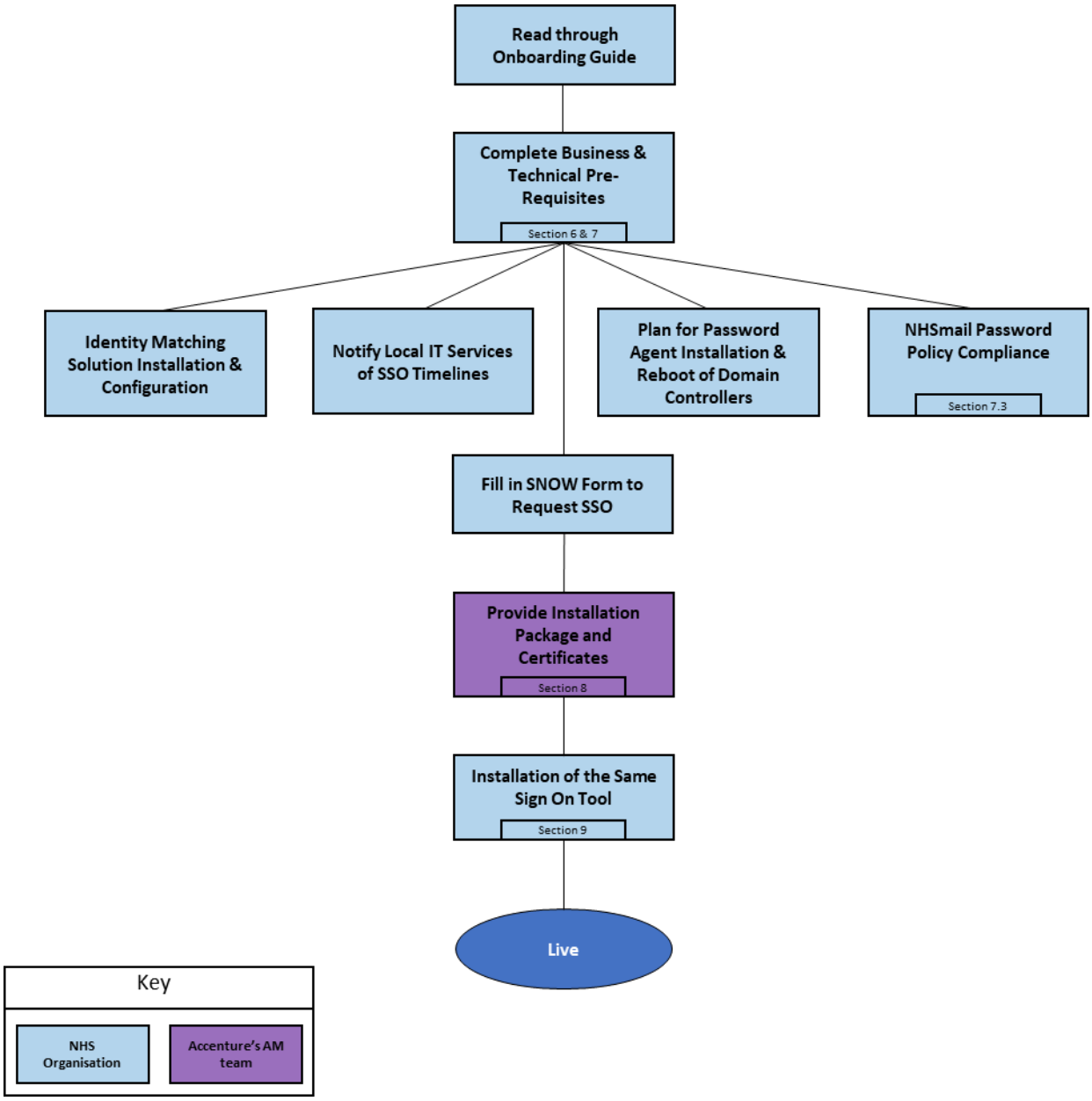
5 Onboarding Overview

5.1 Pre-Onboarding Checklist

There is a pre-onboarding checklist in the appendix which can be used to ensure all tasks are completed ahead of filling the SNOW form to request Same Sign On.

5.2 Onboarding Steps

The diagram below outlines the steps that organisations will follow to complete onboarding of the Same Sign On solution.



The timeline for Onboarding the Same Sign On solution will depend on organisations' ensuring the fulfilment of business readiness and technical pre-requisites, as detailed in Section 6 and Section 7 of this Onboarding guide.

The end-to-end process to adopt the Same Sign On solution can be summarised as follows:

1. Ensure you have read through the onboarding guide thoroughly.
2. If the organisation has more than one ODS code, choose which ODS code they want to implement the Same Sign On solution for
3. Complete business and technical pre-requisites for onboarding Same Sign On:

- ✦ Installing and configuring TANSync (as detailed in Section 7.1 to Section 7.2 of this Onboarding guide) or equivalent identity matching solution
- ✦ Aligning local AD Password Policy with that of NHSmail
- ✦ Notifying local IT Service Desk of the timelines to install the Same Sign On Solution and send out relevant communications
- ✦ Planning for the installation of the password agents and the subsequent rebooting of the Domain Controllers

4. Fill in ServiceNow (SNOW) form to request Same Sign On through the Support Site
5. Organisation receives the installation package and certificates to install the Same Sign On tool
6. The Same Sign On solution is live

6 Business Readiness

The Onboarding process of the Same Sign On solution will begin by fulfilling business readiness, followed by completion of technical pre-requisites, as detailed in Section 7 of this Onboarding guide.

The Same Sign On solution onboarding process requires sufficient investment of resource. To ensure a successful onboarding experience, organisations are required to make the following preparations:

- **Capacity:** Same Sign On solution requires IT representatives to meet all pre-requisites and complete installation activities. The identity matching solution used (such as TANSync 2.0) should be supported similarly to any other IT infrastructure. To mitigate problems effectively, organisations are advised to upskill more than one person with the knowledge to support the identity matching solution used.
- **Service Desk:** Organisations should inform their Service Desk teams about Same Sign On solution onboarding due to the potential for increased contact from users following Go-Live

7 Technical Pre-requisites:

The Same Sign On solution requires IT colleagues to update their local Password Policy to align with that of NHSmail, and to successfully install an identity matching solution such as TANSync. Other identity matching solutions besides TANSync are accepted as part of the onboarding process, however, it is important to note that where organisations choose to use

an alternative identity matching tool, any issues with regards to the tool should be dealt with through the organisation's IT support.

7.1 TANSync

TANSync solutions are NHSmail Identity Management Solutions that give organisations the ability to synchronise local data with NHSmail using NHSmail Portal APIs. The solutions are based on Microsoft Identity Manager (MIM) 2016.

TANSync enables the matching of identities between NHSmail and Local AD, and organisations are required to monitor that the solution is functioning correctly prior to the activation of the Same Sign On solution tool.

- Organisations that **already have TANSync installed** can progress to Section 7.2 of this Onboarding guide
- Organisations that **do not have TANSync installed please refer to** NHSmail Support Site **for TANSync installation guides** Relevant links:
- TANSync Deployment Guide – NHSmail Support
- TANSync Overview – NHSmail Support
- TANSync Webinar – NHSmail Support

Important Note: Organisations are advised to run two instances of TANSync 2.0 in failover mode to ensure the continuous working of the Same Sign On solution.

Requirement: It is important that local organisation's AD user objects' mail attribute value matches with their @nhs.net email address.

7.2 Compliance with NHSmail Password Policy

Once an identity matching solution is installed, configured and running, organisations should align the Local AD Password Policy with the NHSmail Password Policy. Organisations are required to follow the Password Change guidance to ensure the Password Policy of the Local AD complies with the NHSmail Password Policy.

The NHSmail Password Policy requires that a password meets the following criteria:

- Minimum length: 10 characters ***without*** requiring mix of character types
- Maximum Age: 365 days
- Not matching previous 4 passwords
- Not detected as a common password
- Not detected as a breached password

- Not containing a banned substring

Organisations are required to implement the NHSmail Password Policy in their Local ADs. The implementation and enforcement of the Password Policy should be accounted for in the effort required for organisations to onboard the Same Sign On solution.

Important Note: Even with password policy compliance, there may be occasions in which password synchronisation does not occur because a password is used which is in the password history of either the local AD or NHSmail.This could occur in the example where a user sets their password on NHSmail which has been in their local AD password history. Therefore, if a user's password is accepted but it is not synchronised, they should be made aware by the Local Admin that this may be due to their password history on either NHSmail or Local AD. They should then be asked to change their password again to one which has not been used on either the Local AD or NHSmail account.

For further information please visit the Password Policy guidance.

Please refer to the Appendix section of this Onboarding guide for a detailed view of the different password change scenarios and the outcomes that result from running the Same Sign On solution.

7.3 Networking prerequisites

The servers will need to have network connectivity to the following endpoints via network port 443. Organisation should consult with their networking team.

https://passwordsyncbroker-prod.azurewebsites.net

https://api.pwnedpasswords.com

https://s3.eu-west-2.amazonaws.com/battlecatstuff/Config-prod.json

8 Preparing for installation

Once Sections 6 and 7 of this Onboarding guide are completed, organisations should fill in the SNOW form on the Support Site to receive the installation package and begin the installation of the Same Sign On tool. Please note that organisations are required to make sure PowerShell is installed on their servers to allow execution of the installation script.

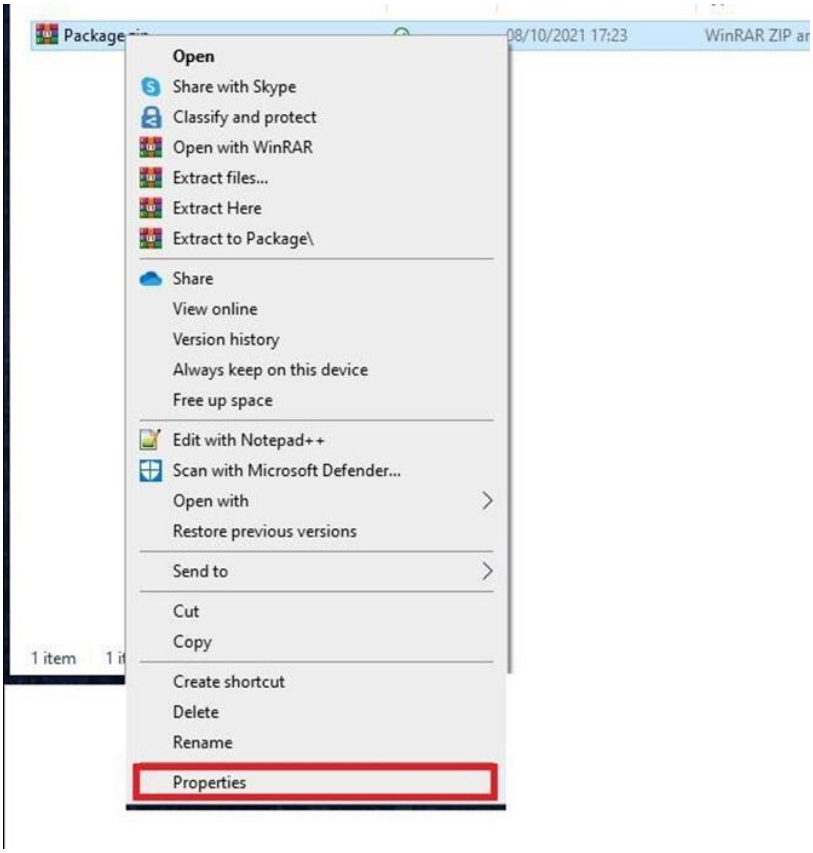
Organisations should plan the installation carefully as the installation of the tool requires the restart of the Domain Controllers. Users will not be able to log in during the restart. Please refer to **Section 9** for further recommendations on the installation of the solution.

Once the tool is deployed, organisations should communicate the Same Sign On change to users. Once guidance and trial of the tool is completed any additional support required will be managed through the NHSmail Service Desk (helpdesk@nhs.net).

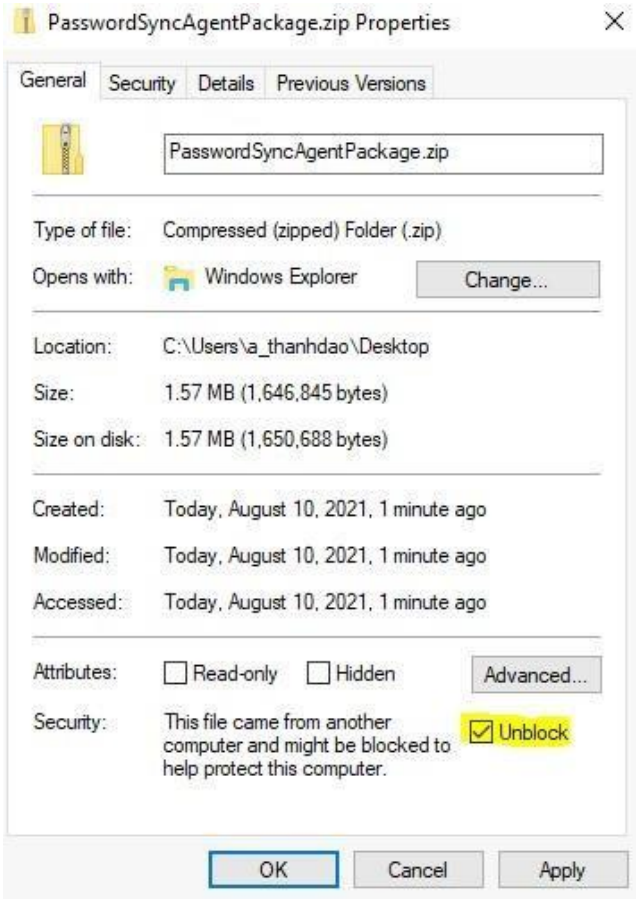
8.1 Installation package

1. Prior to the installation of the tool, organisations are required to unblock the password synchronisation package zip files. This will allow the binaries to run on the targeted machine. **Please note**: not all version of windows server requires this step.

- Right click on the zip file, select Properties



- Tick the **Unblock box** as per screen shot below to unblock the binaries

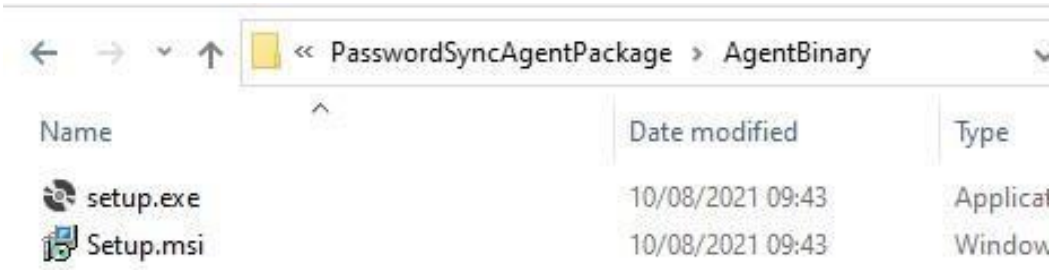


2. Organisations are required to ensure that all the necessary components required to configure the Password Sync Agents are available in the **C:\PasswordSyncAgentPackage** folder. The screenshot below shows the top-level folder structure:

3. Below is a summary of each folder and its contents:

- **Certificate**: Contains certificates used to configure the agents

- **AgentBinary**: Component installation files



9 Installation of the tool

Recommendations:

- The first deployment of the Password Agent will require the rebooting the Domain Controller (DC) machines. Organisations are advised to plan the rebooting of the DCs in phases rather than all at the same time.
- Organisations are advised to deploy the agents in read-only mode first, and to begin the configuration change of the agents when all DCs have been rebooted.
  - This can be done by changing the value of configuration item SendMessage to False in configuration file PasswordCheckerService.exe.config (update the configuration file with “SendMessage: False”)

```
<add key="SendMessage" value="False" />
```

  - The values should be changed back to True once the users have been communicated and the Password Sync Agents deployed successfully Detailed steps to install and configure the environment can be found below.

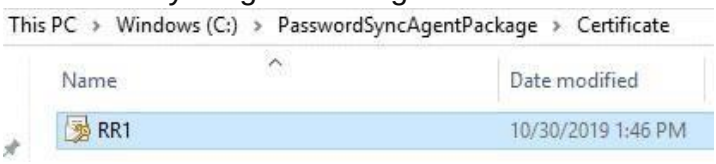
9.1 Installation of the certificate

Organisations will be provided with a certificate in the installation package. This will be used for authenticating to the Password Sync Broker, signing of the message with its public key, and decryption of the received messages with its private key.

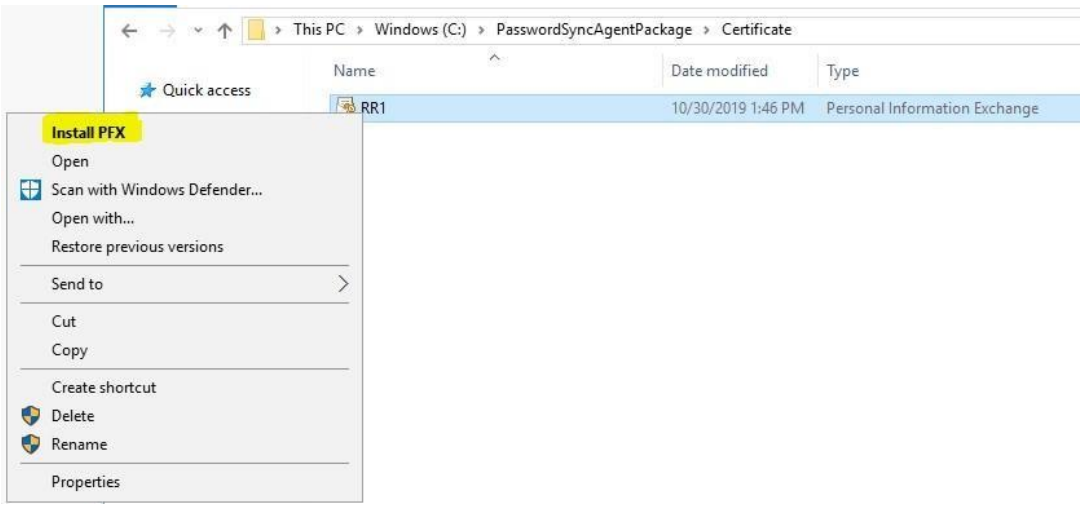
The certificate must be installed on the Domain Controllers’ Local Machine certificate store. The root certificate authority certificate must be added to the Trusted Root Certificate Authority subfolder in the certificate store.

Below are instructions on how to install the certificate:

1. Navigate to C:\PasswordSyncAgentPackage\Certificate

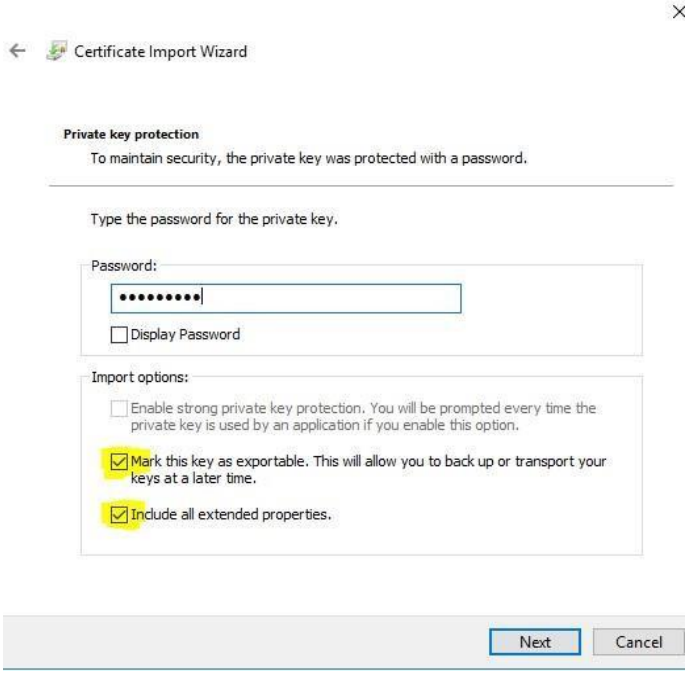


2. Double click the **PFX certificate file** to open the import wizard. Alternatively, click the right mouse button whilst selecting the certificate. When the menu appears, select the option “**Install PFX**”)

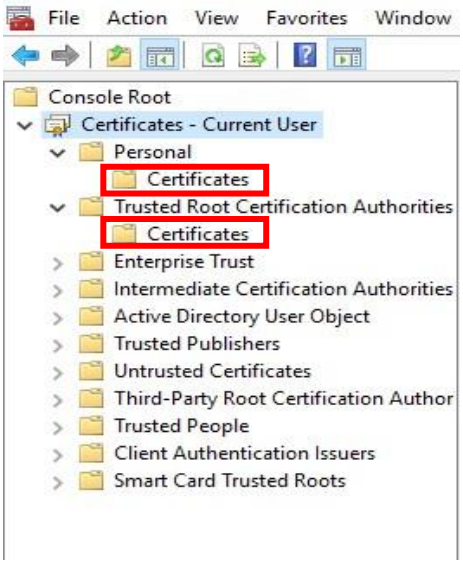


3. Follow the certificate import wizard by selecting Local Machine:

4. Enter the password in the Password input box and enable the import options

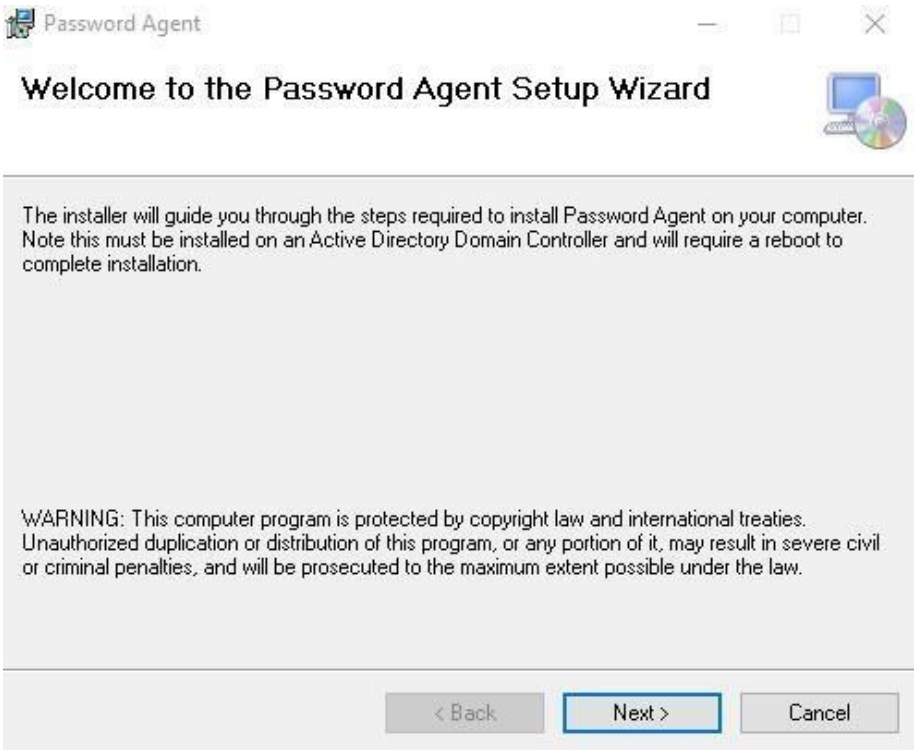


5. Once successfully imported, organisations should see a Success prompt message. Make sure that **root and issuing certificates** in the chain are in **Trusted Root Certificate Authority**. You should also see the 'ODS.cer' / Child certificate (this will be done automatically however it is worth manually checking to confirm) in the Personal Certificates folder as shown below.

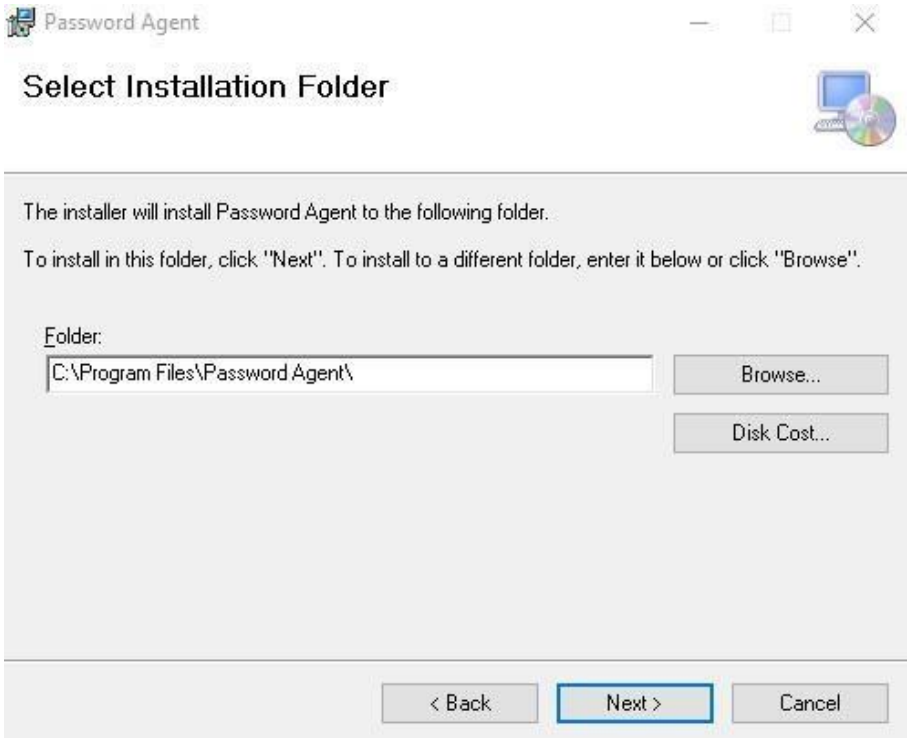


9.2 Installation of the Agent

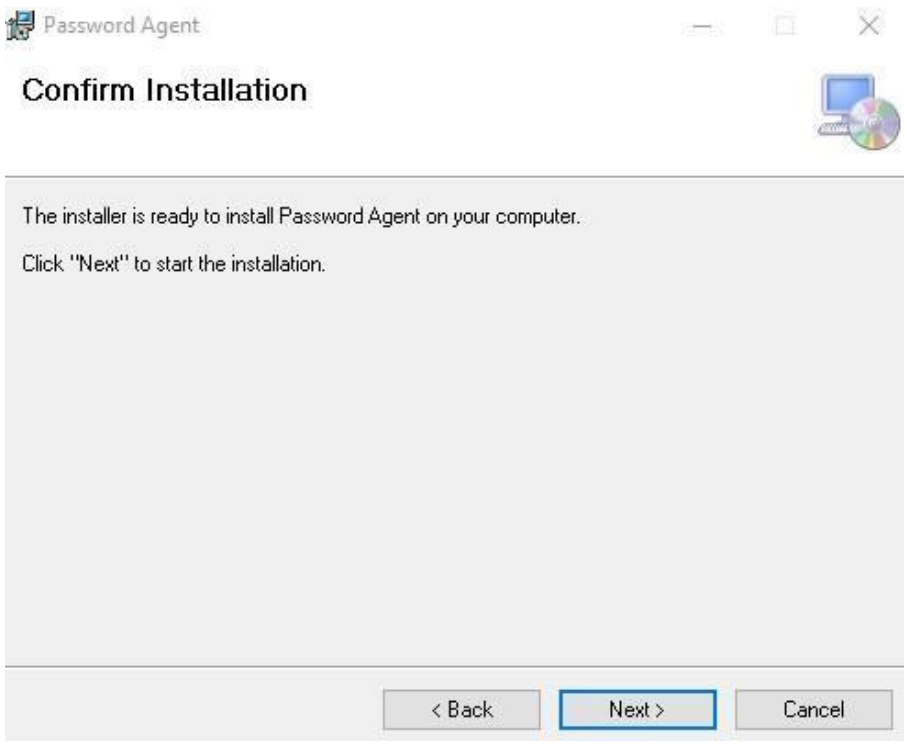
1. Navigate to downloaded and unzipped PasswordSyncAgentPackage and run Setup.exe file in AgentBinary folder
2. Click **Next** to progress



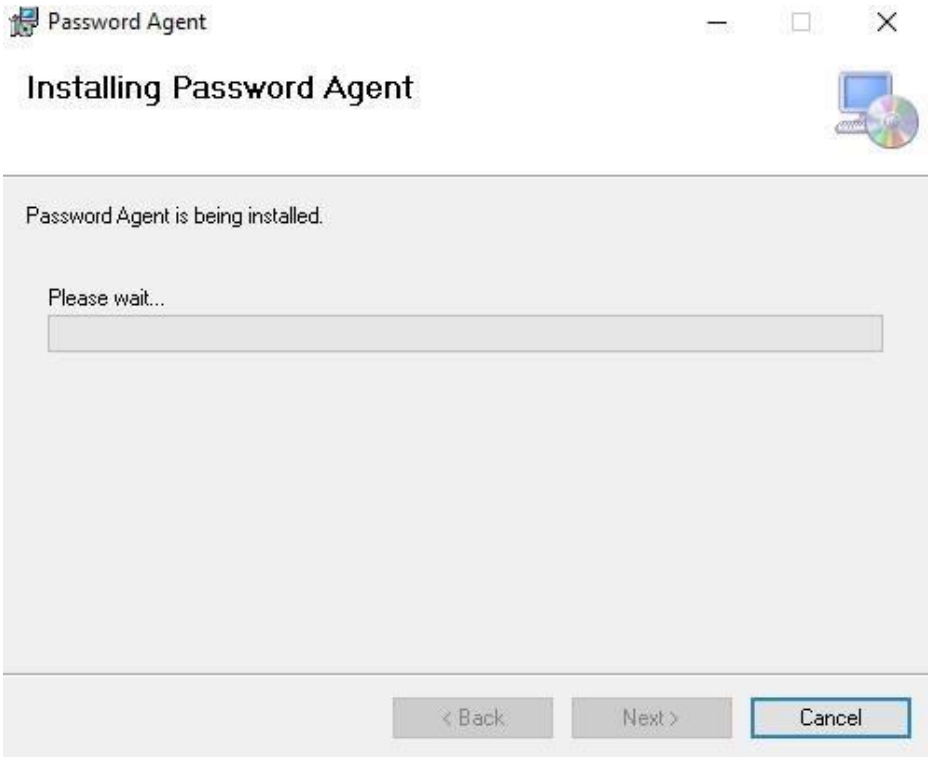
3. Click **Next**



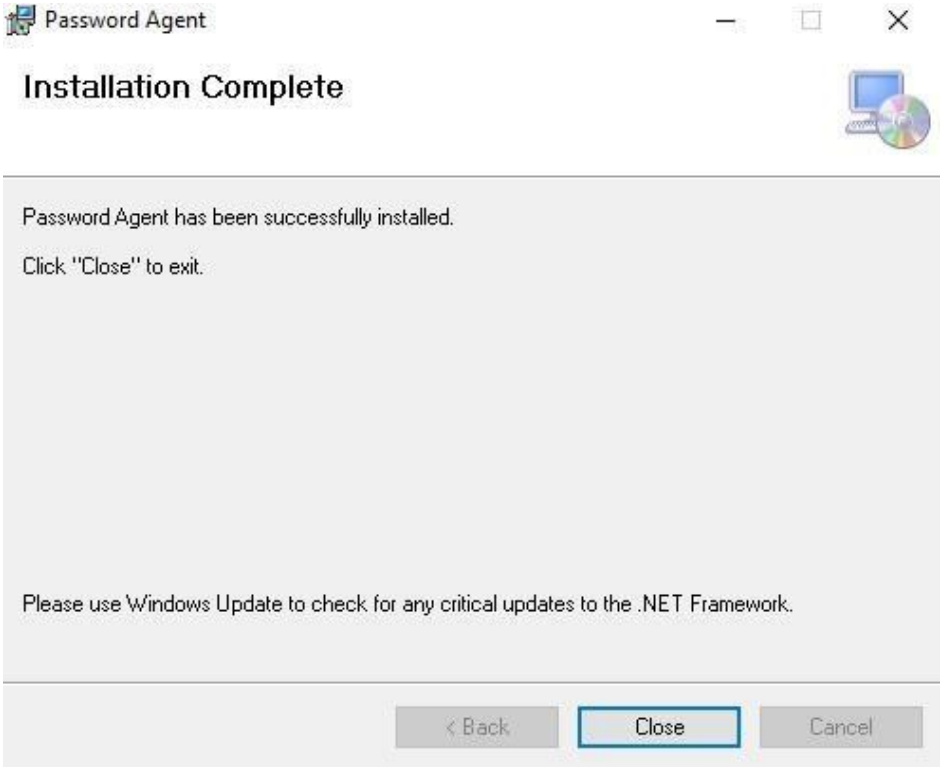
4. Click **Next** to start the installation



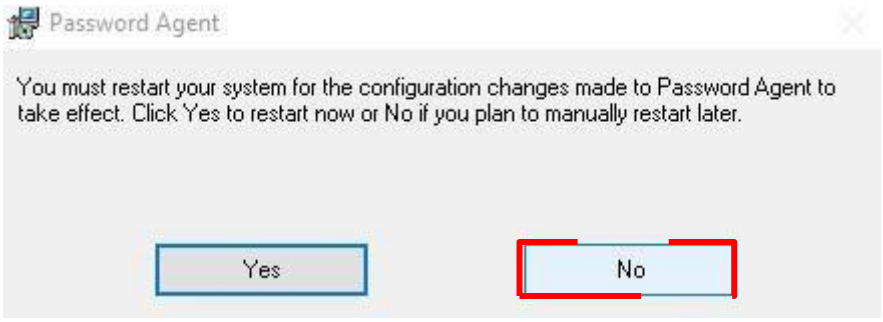
5. Wait for installation to finish



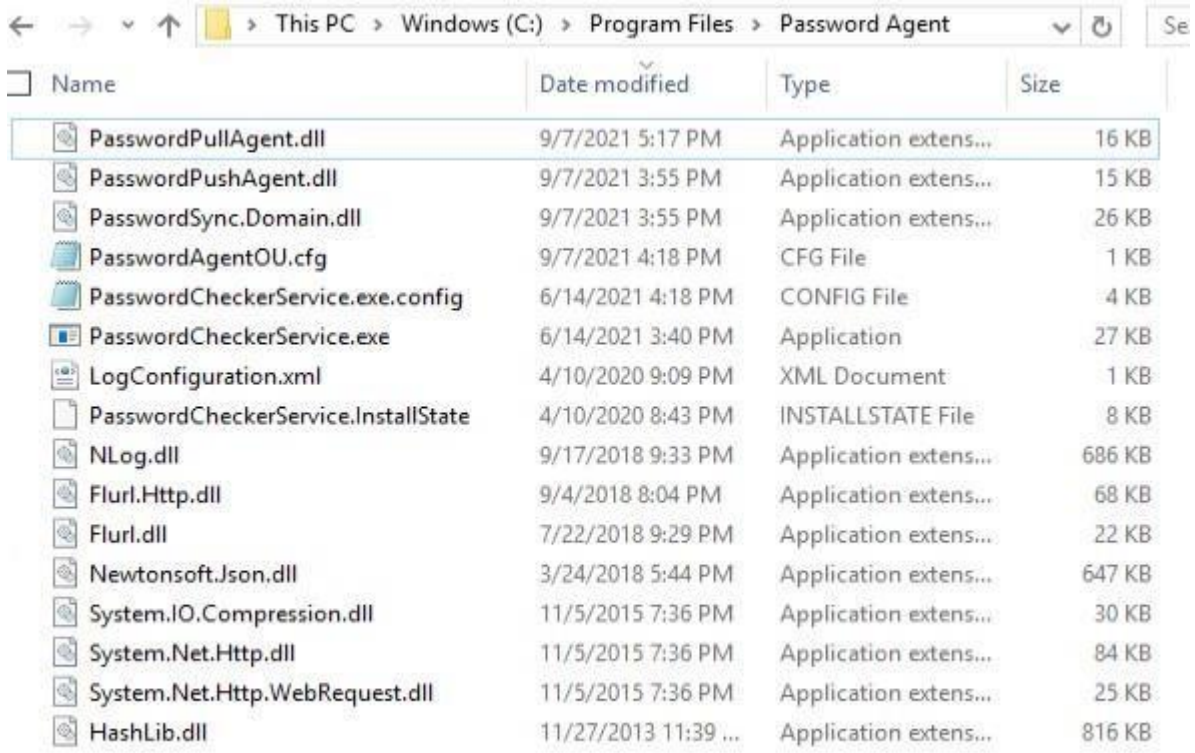
6. Click **close** to complete



7. Select **No** to defer the system reboot



8. Ensure the password synchronisation components are installed correctly in the target directory. The default location is C:\Program Files\Password Agent.



9. Update the configuration file **PasswordCheckerService.exe.config**

    a. Update network proxy settings to the proxy server of the organisation if this is required by removing the comments tags “<!—" and “-->” and specify the proxy server values for HttpProxy settings

```
<!-- Update proxy if required -->
<!--
<add key="HttpProxy" value="http://proxy:3128"/>
-->
```

    b. Uncomment the below section to enable Password Push and Password Pull agent features

```
<!-- Password Sync Section -->
<!-- Uncomment the components to load -->
<!--
<add key="LoadPushAgent"/>
<add key="LoadPullAgent"/>
-->
```

c. Update the certificate thumbprints values with the thumbprint of the installed certificate in Section 9.1. Please note, the thumbprints should be the same across the below 3 keys.

```
<add key="DecryptionCertThumbprint" value="Update to the right cert Thumprint" />
<add key="APIClientCertificateThumbprint" value="Update to the right cert Thumprint" />
<add key="SigningCertThumbprint" value="Update to the right cert Thumprint"/>
```

We would recommend that you copy and paste over the thumbprints from PowerShell rather than from the 'Details' section of the Certificates themselves. This can be done via entering the below command into your Local Machine's PowerShell ISE window. The output should show you the Thumbprints as well as Subjects of each certificate. Once you have found the relevant thumbprint, copy and paste directly from PowerShell, to avoid the possibility of any hidden characters.

```
Get-ChildItem Cert:\LocalMachine\my
```

d. Update the ODS code that the organisation has chosen to use

```
<add key="ODSCode" value="<Organisation ODSCode Case sensitive>" />
```

e. Update the Domain root distinguished name by giving the organisation's correct value

```
<add key="DomainRootDN" value="example DC=org,DC=com" />
```

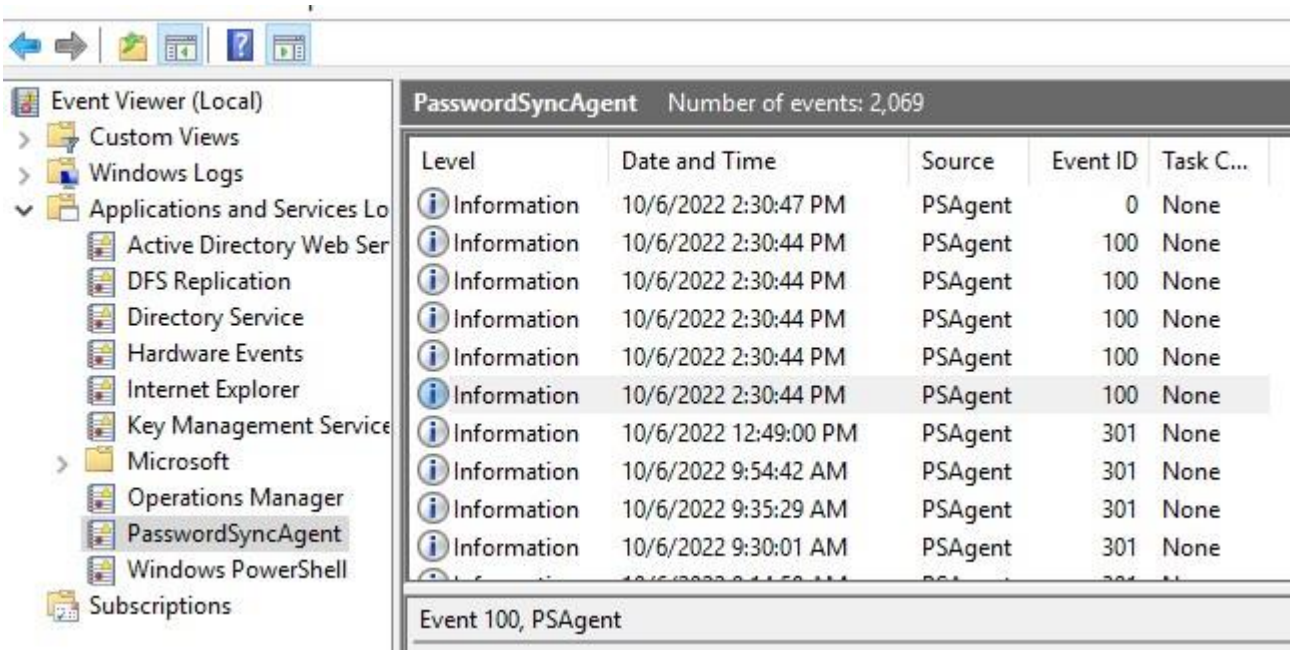
10. Update the configuration file PasswordAgentOU.cfg to include targeted users OUs

```
# filter - can enter multiple OUs Distinguished Names
FilterOU: OU=OrganisationUsers,DC=partner-org,DC=local
#FilterOU:
#FilterOU:
```

9.3 Validation

Once the organisation has completed the steps detailed in Section 9.2, it is necessary to check that Password Agent Service is running, and logs are written to windows event logs. 1. Password Agent Service is running

2. Event log indicates that the Password Sync Agent has been successfully initiated. Your Event logs should show similar to the below screenshot, ensuring that you receive 5 100 Event IDs



10 Go Live

Prior to Go-live, organisations should issue a communication to all users, informing them of the Same Sign On solution and how this will enhance user-experience. After this, organisations should take a last step to enable the synchronisation of passwords between NHSmail and their Local AD.

10.1 Password change communications

After installing the Same Sign On solution, organisations are advised to share communications material informing users that when they change their password within NHSmail or their Local AD, the password will be synchronised between the two systems. Users should be directed to raise issues and any unexpected failures with their Local Administrator.

10.2 Same Sign On Solution Go Live

After the successful installation of the Same Sign On solution components, and after users have been notified about Go Live, organisations should ensure:

- Password Sync Agent's configuration is set to send messages (PasswordCheckerService.exe.config file must contain line *<add key="SendMessage" value="True" />*) to start sending passwords to NHSmail and conclude the onboarding process

10.3 Post Implementation Tests

Once the solution is live, the organisation can optionally test the functionality following the below steps:

Local AD to NHSmail Password Synchronisation

1) Change the AD password locally on the machine
2) Check if the password changed for NHSmail by logging into NHSmail using the new password

NHSmail to Local AD Password Synchronisation

1) Change the NHSmail password from the profile tab.
2) Re-login into your workstation using the new password

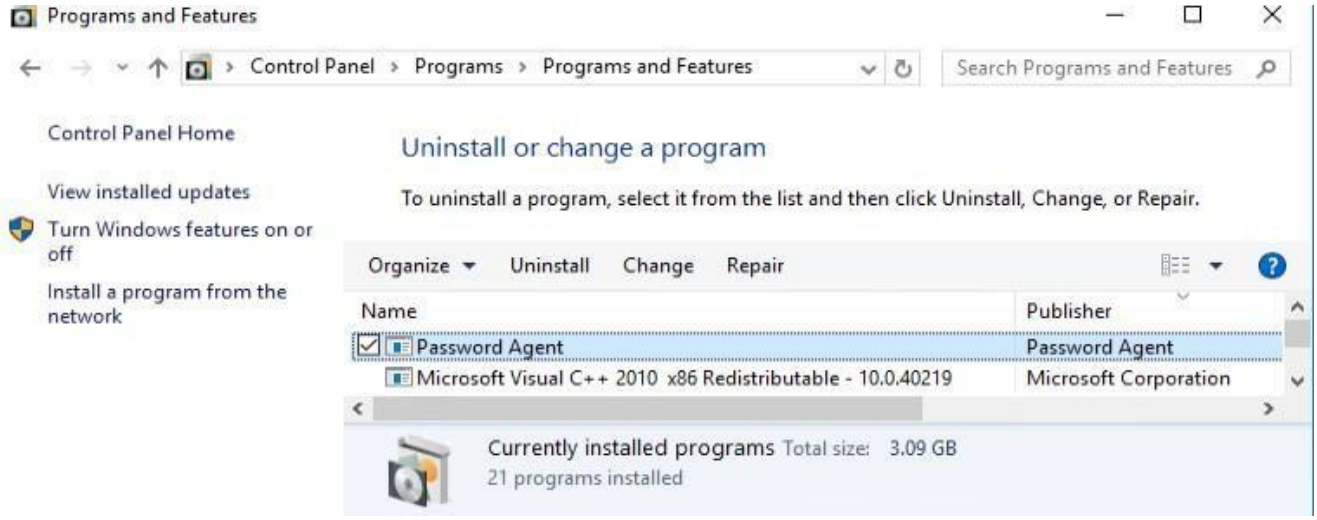
10.4 New User Created on NHSmail

If a new user is created on NHSmail for an organisation that has adopted Same Sign On, the user would need to reset their password after their account is synced to ensure both the password on the local Active Directory and NHSmail are the same. The user should wait up to 24 hours before resetting the password to allow for the account to be synced.

11 Uninstalling the Password Sync Agent

If the Same Sign On solution is no longer required, organisations should uninstall the agents following the steps detailed below.

1. Open **Program and Features** and uninstall the Password Agent



2. Remove the installed certificates as part of the Password Sync Agent installation from local machine certificate repository

12 Onboarding Support

Organisations will be required to complete Same Sign On pre-requisites independently. Once the pre-requisites have been completed organisations can complete the SNOW form on the Support Site to start onboarding. The AM team in Accenture will provide the following:

- **Password Synchronisation solution package:** The AM team will provide organisations with the solution binaries. Configuration steps for the Password Sync Agent are detailed in Section 8.
- **Provision of certificates:** Organisations will be provided with a certificate in the installation package, and this will be used for authenticating to the Password Sync Broker, signing of the message with its public key, and decryption of the received messages with its private key. The process to install the certificate is detailed in Section 9.1.
- **Access to Broker:** Organisations seeking to use the Same Sign On service will be required to contact the onboarding Team to subscribe to the service and access the Password Sync Broker. Access to the Password Sync Broker is controlled by the subscription and a certificate for authentication to the service.

13 Appendix: Password Policy and Password complexity scenarios

This section describes different scenarios regarding several possible configurations of password policies in the Local AD to track if the password synchronisation would be expected to be successful or unsuccessful. Organisations are advised to refer to these scenarios to understand what is expected to happen when the password policies of NHSmail and their Local AD are not aligned.

13.1 Scenarios of password changes from Local AD to NHSmail

The following tables explains the possible scenarios for password synchronisation from a Local AD to NHSmail depending on the configurations of Password Policy implementation in Local AD. **Password Policy is not configured correctly in Local AD**

Local AD Policy	Local Action	Local AD Result	Password Sync	NHSmail Result
Password length requirement is shorter than NHSmail	**User** sets a password that is shorter than required by the NHSmail Password Policy	Success	Deliver the password to NHSmail	Password set will fail as it does not meet the minimum length requirement
Password length requirement is shorter than NHSmail	**Admin** sets a password that is shorter than required by the NHSmail Password Policy	Success	Deliver the password to NHSmail	Password set will fail as this does not meet the minimum length requirement
Password complexity is less than NHSmail	**User** sets a password that does not meet NHSmail complexity requirements	Success	Deliver the password to NHSmail	Password set will fail as this does not meet the complexity requirement
Password complexity is less than NHSmail	**Admin** sets a password that does not meet NHSmail complexity requirements	Success	Deliver the password to NHSmail	Password set will fail as this does not meet the complexity requirement
Password history is less than NHSmail	**User** reset password with an old password than NHSmail on their machine	Success	Deliver the password to NHSmail	Success*
Password history is less than NHSmail	**Admin** reset user password with user old password on AD	Success	Deliver the password to NHSmail	Success*
Password age is less than NHSmail	**User** reset password with less age than NHSmail on their machine	Success	Deliver the password to NHSmail	Success*

Password Age is less than NHSmail	**Admin** reset user password with less age than NHSmail on AD	Success	Deliver the password to NHSmail	Success*

*Please note that organisations are best placed to benefit from the Same Sign On solution by implementing NHSmail Password Policy in their Local AD. The Password Policy is intended to enhance cyber security, and thus if an organisation does not apply NHSmail Password Policy change this could increase cyber security risks as the Same Sign On solution is not able to capture these scenarios. Success in these cases mean that the flow will happen; even though NHSmail Password Policy has not been implemented. Failure means that the password is out of sync.

Fine Grain Password Filter is not configured in Local AD

Local AD Policy	Local Action	Local AD Result	Password Sync	NHSmail Result
Password complexity, age and password length is configured the same as NHSmail, but the Fine Grain Password Filter is not configured	User resets password with required complexity, age, and length, but with compromised password on their machine	Success	Deliver the password to NHSmail	Password set will fail as the Fine Grain Password Filter will identify this issue
Password complexity, age and password length is configured the same as NHSmail, but the Fine Grain Password Filter is not configured	Admin resets password with required complexity, age and length, but with compromised password on AD	Success	Deliver the password to NHSmail	Password set will fail as the Fine Grain Password Filter will identify this issue
Password complexity, age and password length is configured the same as NHSmail, but the Fine Grain Password Filter is not configured	User resets password on their machine with either of the following: 1) Less complexity 2) Less age 3) Less length 4) Less history	Fail	Password is not delivered	User authentication to NHSmail with the new password will fail.
Password complexity, age and password length is configured the same as NHSmail, but the Fine Grain Password Filter is not configured	Admin resets user's password on AD with either of the following 1) Less complexity 2) Less length	Fail	Password is not delivered	User's authentication to NHSmail with the new password will fail.

Password complexity, age and password length is configured the same as NHSmail, but the Fine Grain Password Filter is not configured	Admin reset user's password on AD with either of the following 1) Less age 2) Less history	Success	Deliver the password to NHSmail	Success*

Password Policy and Filter is configured in Local AD

Local AD Policy	Local Action	Local AD Result	Password Sync	NHSmail Result
Password complexity, age and password length is configured the same as NHSmail, including Fine Grain Password Filter.	User resets password on their machine with either of the following 1) Less complexity 2) Less age 3) Less length 4) Less history 5) Compromised password	Fail	Password is not delivered	N/A
Password complexity, age and password length is configured the same as NHSmail, including Fine Grain Password Filter.	Admin resets user's password on AD with either of the following 1) Less complexity 2) Less length 3) Compromised password	Fail	Password is not delivered	User's authentication to NHSmail with the new password will fail.
Password complexity, age and password length is configured the same as NHSmail, including Fine Grain Password Filter.	Admin resets user's password on AD with either of the following 1) Less age 2) Less history	Success	Deliver the password to NHSmail	Success* Admin needs to be compliant while setting the passwords.

13.2 Scenarios of Password Change from NHSmail to Local AD

The following table explains the possible scenarios for password synchronisation from NHSmail to Local AD depending on the configurations of Password Policy implementation in Local AD.

The policy is setup with either of following **1) Longer password requirement than NHSmail** **2) More complex password than NHSmail**	Password within NHSmail Policy but less complex or shorter than Local Org Policy is set in Portal by User or LA on NHSmail	Success	Deliver password to Local AD	Fail as the password does not meet the requirement in Local AD

Local AD Policy	NHSmail Action	NHSmail Result	Password Sync	Local Result

The policy is setup with either of following **1) Age is more than NHSmail** **2) History is longer than NHSmail**	Password within NHSmail Policy but less age or history than Local Org Policy is set in the portal by user or LA on NHSmail	Success	Deliver password to Local AD	Success
Weaker Password Policy is configured on Local AD	Password within NHSmail Policy is set in the portal by User or LA on NHSmail	Success	Deliver password to Local AD	Success*
The same Password policy and Fine Grain Password Filter as NHSmail is configured on Local AD	Password within NHSmail Policy is set in the portal by User or LA on NHSmail	Success	Deliver password to Local AD	Success

13.3 Same Sign On Troubleshooting

The default configurations will allow the sync agent to write logs in the event logs of the servers. Organisations are advised to monitor the logs for identification of issues related to password sync i.e., connectivity to the password sync broker or incorrect processing of passwords.

14 Appendix: Bi-Annual Renewal of Certifications

Bi-annually, certificates for the Same Sign On tool will need to be renewed. To renew certificates, organisations will need to complete a ServiceNow (SNOW) form.

15 Appendix: Pre-Onboarding Checklist

Task	Tick if Completed
1. Check the number of ODS codes per AD domain and ensure only one is chosen for the Same Sign On	
2. Check how many users will belong to the ODS code chosen	
3. Install and configure an identity matching solution such as TANSync 2.0	
4. Ensure your Local AD password policy aligns with the NHSmail password policy	
5. Notify your Local IT Services of the Timelines for Same Sign On to be deployed	
6. Send out communications to the future users of the service to let them know timelines and the steps they will have to take to set up their password	
7. Plan for Password Agent installation	
8. Plan for the reboot of the Domain Controllers	

Glossary

Term	Description
AD	Active Directory
API	Application Programming Interface
DC	Domain Controller
FIM	Forefront Identity Manager
ILM	Identity Lifecycle Manager
IT	Information Technology
MIM	Microsoft Identity Manager
NHS	National Health Service
TANSync 2.0	A bi-directional interface that synchronises data between NHSmail and local Active Directories