­­

NHS Digital Identity Agent v2.3.2.0

Installation Guide

|  |  |  |  |
| --- | --- | --- | --- |
| Document filename: | **NHS Digital Identity Agent v2.3.2.0 Installation Guide** | | |
| Project / Programme | **Platforms** | Project | **IAM** |
| Document Reference | **NHS Digital Identity Agent v2.3.2.0 Installation Guide** | | |
|  |  | Status | **​​Live​** |
| Owner | **Phil Gill** | Version | **​​1.0​** |
| Author | **Ashley Harris** | Version issue date | **​​17/03/2023​** |

Contents

[Introduction 2](#_Toc129950775)

[Audience 2](#_Toc129950776)

[Software & documentation 2](#_Toc129950777)

[Important Considerations 3](#_Toc129950778)

[System requirements 3](#_Toc129950779)

[Middleware 3](#_Toc129950780)

[Other components 3](#_Toc129950781)

[Usage scenarios 4](#_Toc129950782)

[Operating systems 4](#_Toc129950783)

[Environments 4](#_Toc129950784)

[Smartcards 4](#_Toc129950785)

[Installation process overview 5](#_Toc129950786)

[Previous versions of Identity Agent 6](#_Toc129950787)

[New installation 6](#_Toc129950788)

[Update installation from BT Identity Agent to NHS Digital Identity Agent v2.x 7](#_Toc129950789)

[Update installation from HSCIC Identity Agent v1 to NHS Digital Identity Agent v2.x 7](#_Toc129950790)

[Update installation from a previous version of Identity Agent v2.x 8](#_Toc129950791)

[Installing the Identity Agent 9](#_Toc129950792)

[System tray notifications 12](#_Toc129950793)

[Gem Heal 12](#_Toc129950794)

[Post installation configuration changes 12](#_Toc129950795)

[Troubleshooting 12](#_Toc129950796)

[Installation 12](#_Toc129950797)

[Authentication 14](#_Toc129950798)

# Introduction

The Identity Agent is an installable component that resides on every device that acts as a point of access to Spine systems where a smartcard is being used to authenticate the user that is, every Windows device in a hospital, GP surgery, or other organisation where a clinical role is performed.

NHS Digital Identity Agent v2.x is the latest version of this software. It has been designed to provide more secure and convenient ways of working with identity access than previous versions, through the introduction of additional features and bug fixes which build on the previous version.

Please see the IA v2.x User and Administrator Guides for more details.

## Audience

The document is aimed at IT Managers, IT Administrators, suppliers of desktop build and support services, and any other person who has responsibility for installation, configuration, support and management of the Identity Agent.

# Software & documentation

All software and administrative documentation can be downloaded from

<https://nww.digital.nhs.uk/dir/downloads/>

The latest Warranted Environment Specification (WES) can be downloaded from    
<https://digital.nhs.uk/services/spine/spine-technical-information-warranted-environment-specification-wes>

The latest path to live (PTL) certificates can be downloaded from    
<https://digital.nhs.uk/services/path-to-live-environments>

# Important Considerations

**Please note that by default, the IA will clear all the certs from the user’s personal certificate store. In order to retain certificates in this store from other publishers, e.g. for a VPN, please refer to the Registry settings section in the Identity Agent Admin Guide and set the registry key for TrustedCertificateIssuers.**

# System requirements

The Identity Agent requires a Windows operating system from the list stated in the [Usage Scenarios](bookmark://_Usage_Scenarios) section of this document (other operating systems may work but are not warranted). 

## Middleware

NHS Digital Identity Agent v2.x requires the presence of at least Gemalto Middleware.    
   
Oberthur Middleware is additionally required **only** if performing CMS RA activities on Oberthur (Series 8) Smartcards on the CIS application. User level CMS activities (self-renew and self-change PIN) can be performed on Series 8 Smartcards **without** the requirement of Oberthur Middleware.

|  |  |  |
| --- | --- | --- |
| **Component** | **Description** | **Minimum Version** |
| **Gemalto Classic Client** | Middleware component providing the interface between CryptoAPI and Gem / Gem app cards. | 6.1 Patch 3 for NHS  32-bit ***or*** 64-bit |
| **Oberthur AWP** | Middleware component providing the interface between CryptoAPI and Oberthur cards. | Oberthur AWP 5.2.0 SR8 32-bit ***or*** 64-bit \* |

\* Oberthur Middleware SR8 provides the ability to perform all RA functions and so should be used for any new installations. Oberthur Middleware SR1 and SR5 are now blocked from performing any CMS activities.

## Other components

|  |  |  |
| --- | --- | --- |
| **Component** | **Description** | **Minimum Version** |
| **Java Runtime** | The Java Runtime Environment provides the minimum requirements for executing a Java application; it consists of the Java Virtual Machine (JVM), core classes, and supporting files. The IA only makes use of Java 32-bit. | Java SE versions 7.x and 8.x (32-bit), up to and including Java 1.8.251. |
| **.NET Framework** | The programming infrastructure created by Microsoft for building, deploying, and running applications and services that use .NETtechnologies. | Microsoft .NET 3.5.1 SP1. However, this version needs to be installed as well currently even if the user installs a higher version of .NET \*\*\* |
| **004 Card.inf \*\*** | Used to prevent device installation messages when an NHS logo branded (series 4) Smartcard is used. | N/A |
| **Smartcard Reader Drivers \*\*** | Any driver required to support the Smartcard reader used within your organisation.     A link for the supported drivers for various Smartcard readers is provided on the [DIR website](https://nww.digital.nhs.uk/dir/downloads/). | N/A |
| **Windows 10 Default Smartcard Reader Drivers** | Later versions of Windows 10 do not always install the OmniKey smartcard reader derivers correctly. The user needs to ensure the correct drivers are installed from  the [DIR website](https://nww.digital.nhs.uk/dir/downloads/) | N/A |

\*\* Optional components

\*\*\* If the user has 32bit Windows and needs to also install Oberthur Middleware, ensure that .Net 4.5.5.x is not installed as this version does not work with the Oberthur Middleware installer due to a bug introduced by Microsoft. Earlier and later versions of .Net work with the installer.

# Usage scenarios

## Operating systems

The following Windows operating systems are warranted for use:

* Windows 10 (x64 only) – Excluding IOT x64
* Windows Server 2012 R2

## Environments

The Identity Agent is warranted for use in a number of specific Windows based environments:

* Local installation on a desktop, laptop or tablet.
* Installation on a Remote Desktop server (via Microsoft RDS) with no IA installed locally.

The use of the Identity Agent under other environments such as Citrix / VDI / Terminal Services is supported, but for authentication only. Any CMS activities under these configurations are **NOT** supported. The details on how to configure these environments is outside of the scope of this document. 

# Smartcards

Support for versions of Smartcards is determined by a number of factors, including the operating system, the Card Service Provider (CSP) middleware and the support of API’s used to access the cards. 

Identity Agent has not been tested against series 1 to 3 Smartcards. They are not expected to be functional against any middleware type or host operating system.

The following matrix sets out the Smartcards that are supported against the warranted environments:

|  |  |  |
| --- | --- | --- |
|  | **Windows 10 (x64)** | **Windows Server 2012 R2** |
| **Entrust Virtual Smartcards** | ü(**Windows 10 only**) | û |
| **Series 8  (Oberthur)** 1 | ü | ü2 |
| **Series 6  (Gemalto)** | ü | ü2 |
| **Series 5  (Gemalto)** | ü | ü2 |
| **Series 4** 3**(Gemalto)** | ü | ü2 |
| **Series 3 and previous  (Gemalto)** | û | û |

**1** Oberthur Smartcards are warranted against all Identity Agents with regard to authentication.    
   CMS operations (within ‘Care Identity Service’) performed on these Smartcards requires the installation of    
   Oberthur middleware – SR8 should be installed to support all RA CMS functions.    
       
    See ‘OT Support Documents’ on the [**DIR website**](https://nww.digital.nhs.uk/dir/downloads/) for more information.

**2** Tested for authentication only. Requires the correct card reader drivers to be installed.

**3** Compatible with contact readers only. This precludes authentication on tablet devices using NFC technology.   
   
**4** Physical Windows 8.1 and Windows 10 machines only. Entrust Virtual Smartcards are not currently warranted for use in any virtualised environment. The Entrust Virtual Smartcard also does not yet support digital signing and therefore cannot be used to sign prescriptions.

NHS Digital recommend IT Administrators and Managers liaise with local Registration Authority staff before deploying NHS Digital Identity Agent v2.x to determine any local impact on users as per the matrix above, so that plans can be put in place to identify any affected Smartcard users and then replace their cards as necessary.

# Installation process overview

The NHS Digital Identity Agent is packaged as a discrete .msi and includes the components:

* NHS Digital Identity Agent v2.x
* Root CA certificates for production (including updated Sub CA certs 1C & 1D) and optionally NIS1
* GATicket.jar (Java component used by the portal applications)

Other dependencies as listed in the [System Requirements](bookmark://_System_Requirements) section must be installed separately and before the installation of the Identity Agent package but are referenced below in the installation process for completeness.

The Identity Agent will need to be manually started on first installation but will be automatically launched after any subsequent machine reboots or when the user next logs in to Windows.

The Identity Agent is supplied with built-in defaults for all settings, meaning that by default there will be no settings present in the registry, and the Identity Agent keys will not be created. The built-in defaults can be largely overridden through the application of specific registry values either directly or via Group Policy settings using an Administrative Template. The user can login and access applications on the Live systems, permissions depending, without making any changes to the Identity Agent registry settings.

Confirm with your local IT support that any Spine applications you are using will work correctly if any registry changes are applied to the Identity Agent, prior to making changes.

**Note: All users performing CMS activities are recommended to set the following value in the Identity Agent registry.**   
**CardRemovalCheck = False**

## Previous versions of Identity Agent

Prior to the installation of the latest version of NHS Digital Identity Agent v2.x (\*) it is **strongly recommended** to uninstall any other versions of Identity Agent. The NHS Digital Identity Agent v2.x does not currently remove any previous versions of Identity Agent (any version from either BT or NHS Digital) during the installation process.

**\*Note** – Installation of latest Identity Agent v 2.3.2.0 does not need any prior uninstallation of the previous versions of NHS Identity Agent (v1.x& v2.x)

On uninstallation of BT Identity Agent, bespoke files added subsequent to installation of that Identity Agent may not be removed. It is recommended that these files are manually deleted (if present) to avoid any conflicts with NHS Digital Identity Agent v2.x. 

**Delete these directories (if present)**

* C:\Program Files\Gemalto\GAC
* C:\Program Files (x86)\Gemalto\GAC

**Delete these files (if present)**

* C:\Program Files\java\*installed version of jre*\lib\ext\TicketAPDLL.dll
* C:\Program Files (x86)\java\*installed version of jre*\lib\ext\TicketAPDLL.dll

**CAUTION:** As uninstalling BT Identity Agent also uninstalls the Gemalto Middleware, users upgrading from any version of the BT Identity Agent will also need to re-install the Gemalto Middleware manually, prior to installing NHS Digital Identity Agent v2.x (ensuring that the correct version for 32-bit or 64-bit machines is installed).

This Middleware is available from <https://nww.digital.nhs.uk/dir/downloads/>   
   
Users uninstalling either HSCIC Identity Agent v1 or any version of NHS Digital Identity Agent v2.x will not be required to perform this step as the Gemalto Middleware will still remain installed.

## New installation

The installation order for a new machine installing NHS Digital Identity Agent v2.x should be as follows:

* Install Java. Version 7 or 8 up to 8.251 are supported. The latest version supported in the WES is recommended for security. Only 32-bit is used by the Identity Agent and CIS, however 64-bit may also be installed for other uses.
* Install 32-bit or 64-bit Gemalto Middleware as appropriate (required for all installations of Identity Agent)
* Install NHS Digital Identity Agent v2.x
* Perform any registry changes, for example if enhanced normal mode, session persistence or mobility modes are required, (including settings for mobility timers) \*
* Perform any registry changes to enable automatic launch or selective closure of web browsers \*
* Start the Identity Agent.
* Windows 10: Click on the Windows Icon, search, ‘Identity Agent’.

Users performing CMS RA activities on Oberthur Smartcards (Series 8) will also require the Oberthur Middleware SR8 to be installed. This can be obtained from <https://nww.digital.nhs.uk/dir/downloads/>

## Update installation from BT Identity Agent to NHS Digital Identity Agent v2.x

The installation order for a machine being updated from any version of BT Identity Agent to NHS Digital Identity Agent v2.x should be as follows:

* Close down (‘exit’) the BT Identity Agent
* Uninstall BT Identity Agent (through Control Panel). Please refer to section ‘[Previous versions of Identity Agent](bookmark://_Previous_versions_of)’.
* Reboot if prompted
* Install 32-bit or 64-bit Gemalto Middleware as appropriate (required for all installations of Identity Agent)
* Install NHS Digital Identity Agent v2.x
* Perform any registry changes, for example if enhanced normal mode, session persistence or mobility modes are required, (including settings for mobility timers) \*
* Perform any registry changes to enable automatic launch or selective closure of web browsers \*
* Start the Identity Agent.
* Windows 10: Click on the Windows Icon, search, ‘Identity Agent’.

Users performing CMS RA activities on Oberthur Smartcards (Series 8) will also require Oberthur Middleware SR8 to be installed. This can be obtained from <https://nww.digital.nhs.uk/dir/downloads/>

## Update installation from HSCIC Identity Agent v1 to NHS Digital Identity Agent v2.x

The installation order for a machine being updated from HSCIC Identity Agent v1 to NHS Digital Identity Agent v2.x should be as follows:

**NOTE:** There is no requirement to install Gemalto Middleware as it will remain installed when following the process below.

* Close down (‘exit’) HSCIC Identity Agent v1
* Uninstall HSCIC Identity Agent v1 (through Control Panel)
* Install NHS Digital Identity Agent v2.x
* Perform any registry changes, for example if enhanced normal mode, session persistence or mobility modes are required, (including settings for mobility timers) **\***
* Perform any registry changes to enable automatic launch or selective closure of web browsers **\***
* Start the Identity Agent:
* Windows 10: Click on the Windows Icon, search, ‘Identity Agent’.

Users performing CMS RA activities on Oberthur Smartcards (series 8) will also require Oberthur Middleware SR8 to be installed. This can be obtained from <https://nww.digital.nhs.uk/dir/downloads/>

## Update installation from a previous version of Identity Agent v2.x

The installation order for a machine being updated from a previous version of HSCIC / NHS Digital Identity Agent v2.x should be as follows:

**NOTE:** There is no requirement to install Gemalto Middleware as it will remain installed when following the process below.

* Close down (‘exit’) HSCIC / NHS Digital Identity Agent v2.x
* Uninstall the previous version of HSCIC / NHS Digital Identity Agent v2.x (through Control Panel)
* Install the **new** version of NHS Digital Identity Agent v2.x
* By default, Identity Agent v2.x uses registry settings from Identity Agent v1 or Identity Agent v2.x if they exist. The user may need to change some of these following the installation. Refer to the Identity Agent Administrator Guide for further information.
* Perform any registry changes, for example if enhanced normal mode, session persistence or mobility modes are required, (including settings for mobility timers) \*
* Perform any registry changes to enable automatic launch or selective closure of web browsers \*
* Start the Identity Agent:
* Windows 10: Click on the Windows Icon, search, ‘Identity Agent’.

Users performing CMS RA activities on Oberthur Smartcards (Series 8) will also require Oberthur Middleware SR8 to be installed. This can be obtained from <https://nww.digital.nhs.uk/dir/downloads/>

\* Check with your local IT support if the Spine applications in use will support session persistence or mobility modes. Specific registry settings are detailed in the Identity Agent v2.x Administrators Guide, section ‘Registry Settings’.

# Installing the Identity Agent

**NOTE:** Admin rights are required to install or uninstall Identity Agent.

To install the Identity Agent, double-click on the .msi file in the folder the file was downloaded to and follow the prompts by clicking ‘Next’ on each window as required.

**Graphical user interface, text, application

Description automatically generated**

**Graphical user interface, text, application

Description automatically generated**

If certificates are required for the path-to-live (test) environments, click on the drop-down arrow next to the red X and select “Will be installed on the local hard drive”. If the user will only ever access the live Spine systems, leave this option as default (not installed).

If your trust installs the NHS certificates via Group Policy and you do not need these installing as part of the Identity Agent, click on the drop-down arrow next to the red X and select “Entire feature will be unavailable”. Ensure your trust has correctly extract all the certificates normally installed by the Identity Agent as these have been updated in Identity Agent v2.x for supporting future live certificates.

Click ‘Next’ to continue.

**Graphical user interface, text, application, email

Description automatically generated**

Click ‘Install’ to continue. Select ‘Yes’ should any prompts be given from User Account Control regarding changes to the computer.

**Graphical user interface, application, Word

Description automatically generated**

Click ‘Finish’ once the installation has completed to close the installation dialogue box.

Once the Identity Agent has been installed, an icon will be placed in the Programs / Identity Agent area of the Start Menu on a Windows 7 machine, or on a Windows 8.1 / 10 machine under the Identity Agent heading on the Applications screen.

Launch the Identity Agent in the appropriate manner.

## System tray notifications

The Identity Agent uses the System Tray notification area to pop-up information regarding status changes and other notifications for the application. If no notifications are provided, this may be resolved by opening Control Panel and selecting ‘Notification Area Icons’ and changing the drop-down for HSCIC Identity Agent v2.x to “Show icons and notifications”.

On Windows 10, open Settings (the cog icon), System, Notifications and Actions and turn the toggle to On for HSCIC Identity Agent.

## Gem Heal

NHS Digital Identity Agent v2.x incorporates the Gem Heal module and this will now check only Gemalto Smartcards (series 4 / 5 / 6 Smartcards) on each login to determine whether they require healing or not. If the Identity Agent performs the healing operation, a system tray notification will be given. Should this notification be given, it is vital that the user **does not** remove their Smartcard during the update process, or the Smartcard could be rendered inoperable leaving the user unable to login and requiring a replacement Smartcard.

## Post installation configuration changes

For any configuration changes post-installation which may need to be made in the registry, refer to the section ‘Registry Settings’ in the Identity Agent v2.x Administrators Guide, downloaded from <https://nww.digital.nhs.uk/dir/downloads/>

Confirm with local IT support that any Spine applications in use are compatible with the changes requested to be made, prior to making them.

Many changes made in the registry are not dynamic and will require the Identity Agent to be closed and restarted for them to take effect. It is good practice to close and restart Identity Agent after any registry changes have been made to ensure there are no unexpected results.

# Troubleshooting

## Installation

If during the installation process error code ‘26352’ is given, it is most likely that the NHS Root Certificate is still installed on the machine after removing a previous version of Identity Agent (any). Manual intervention is required to remove this certificate for installation of the Identity Agent to succeed.

Follow the steps below for removing the certificate and then run the Identity Agent setup process again. The friendly name may not be displayed on the local machine.

**NOTE:** Admin rights are required make changes in Certificate Manager.

1. Start \ Run certmgr.msc
2. Expand Trusted Root Certification Authorities
3. Click on Certificates
4. Scroll down and check if a certificate exists for NHS Root Authority

1. Attempt to delete this certificate

If the user is unable to delete this certificate, they will need to raise a request with their local IT support to have this certificate deleted, prior to running the Identity Agent setup process.

**Table

Description automatically generated with low confidence**

The Intermediate Certification Authorities certificates may also still be present on the machine, and these also require removal prior to attempting to install a new version of Identity Agent.

1. Start \ Run certmgr.msc
2. Expand Intermediate Certification Authorities
3. Click on Certificates
4. Scroll down and check if certificates exists for NHS Root Authority and SubCA02 (test system certificate)
5. Attempt to delete the certificate(s)

**Graphical user interface, application

Description automatically generated with medium confidence**

**NOTE:** If the NHS certificates are installed via Group Policy by your trust, the installation of Identity Agent can be tried again, but this time opt not to install NHS certificates on installation. Be aware that if the NHS certificates are installed in this manner, the new Sub CA 1C and 1D certificates will need extracting from the Identity Agent installation and adding to those installed by the Group Policy installation.

## Authentication

Common authentication problems and their workarounds are described in the Identity Agent v2.x Administrators Guide (section ‘Troubleshooting’).

**For further information, feedback, and questions please visit:**

<https://www.networks.nhs.uk/nhs-networks/identity-agent>

**or sign up to our Slack channel:**

<https://identityagent.slack.com>