­­­

NHS England Identity Agent v2.4.6.0

User Guide

­­­­­

|  |  |  |  |
| --- | --- | --- | --- |
| Document filename: | **NHS England Identity Agent v2.4.6.0 User Guide** | | |
| Project / Programme | **Platforms** | Project | **IAM** |
| Document Reference | **NHS England Identity Agent v2.4.6.0 User Guide** | | |
|  |  | Status | **​​Live​** |
| Owner | **Phil Gill** | Version | **​​1.0​** |
| Author | **Ashley Harris** | Version issue date | **​​06/08/2024** |

Contents

[Overview 3](#_Toc173851690)

[What is the Identity Agent? 3](#_Toc173851691)

[What’s different in version 2.4.6.0 of the Identity Agent? 3](#_Toc173851692)

[How do I know which mode I am running in? 4](#_Toc173851693)

[How do I get it to work in Session Persistence or Mobility mode? 5](#_Toc173851694)

[What if I need it to work as it previously did? 5](#_Toc173851695)

[My VPN certificates are being deleted do I need to do anything differently? 5](#_Toc173851696)

[System requirements 5](#_Toc173851697)

[Operating Modes 5](#_Toc173851698)

[Scenario 1 card removal – ‘Lock’ chosen 6](#_Toc173851699)

[Scenario 2 Card Removal – ‘Log out’ chosen 8](#_Toc173851700)

[Scenario – care worker with NFC enabled Windows tablet 10](#_Toc173851701)

[Initial logon 10](#_Toc173851702)

[Checking timeouts 11](#_Toc173851703)

[Re-verification 11](#_Toc173851704)

[Logging Out 13](#_Toc173851705)

[Operating Mode Precedence Order 13](#_Toc173851706)

[Role Selection improvements 14](#_Toc173851707)

[Citrix Support 17](#_Toc173851708)

[Fast-User-Switching 17](#_Toc173851709)

[Follow-Me-Sessions (RDP) 17](#_Toc173851710)

[Follow-me-sessions (VDI) 17](#_Toc173851711)

[Support 18](#_Toc173851712)

# Overview

The NHS consists of over 27,000 individual organisations providing care across the country through primary and secondary care sites, community care settings, adult and social care, pharmacies, opticians, dentists and education & training establishments all of which contribute to the improved care options available for individual patients.

NHS Care Identity Services are an identity, authentication & authorisation management system, responsible for ensuring that every clinician within the NHS has the appropriate level of access to national clinical and non-clinical systems. The services provided by NHS Care Identity Services are used and supported 24 hours a day, 365 days a year and is highly resilient.

At the front line of the identity solution is the Smartcard and Identity Agent. The Identity Agent is an installable component that is installed on every device that is used as a point of access to clinical systems and a Smartcard is used to authenticate the user.

## What is the Identity Agent?

The Identity Agent is an installable component that resides on every device that acts as a point of access to national clinical 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.

The purpose of the Identity Agent is to:

* Communicate to Smartcard readers to verify that the current user has a valid Smartcard and knows the passcode.
* Obtain an Access Token that can be used by applications on the users’ behalf to access national services.
* Present a Role Selection Menu so that the user can choose which of their associated roles should be used in their current activities.

## What’s different in version 2.4.6.0 of the Identity Agent?

NHS England Identity Agent Version 2.4.6.0 is an updated release which has below changes updated.

* **Additional enhancement to assist with hardware checks on VDI platforms \*\*NEW**
* **Upgrade to .NET4.8 framework**

Installation of new Identity Agent requires .NET framework 4.8

* **Removed Certs and Installation Cert form while installing**

Certs selection section has been completely removed during the installation of the latest version of Identity Agent

* **Pin length is now set to a maximum of 8 characters**

User can enter maximum 8 characters in the Passcode section of the latest version of the Identity Agent. As all smartcard types (GEM/OT & PIV) can allow up to 8 digits of passcode as per new change in CIS (Care Identity Service)

* **Self-Service unlock is updated to new URL**

New Self-Service URL has been added in this version of Identity Agent. Users can unlock the smartcard through a simplified process and only need a valid email address against their identity profile.

* **UI (User Interface) changes**

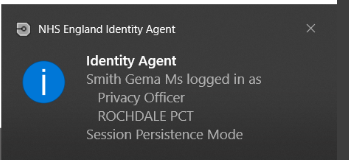
Have replaced the HSCIC logo with NHS logo from all the places in the latest version of Identity Agent

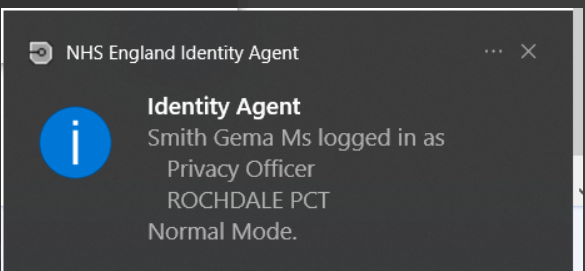
* **New registry key**

A new registry key which ensures prescription signing using the new signing APIs continue to work. When stale X.509 Certificates issued by those defined Certificate Authorities are removed

### How do I know which mode I am running in?

When you log in for the first time the pop-up will inform you which mode the Identity Agent is running in:





With Windows 10 & Windows 11, this notification is not always visible. This is due to the font size used by Windows and the text box size available. This is outside of the control of Identity Agent. Trusts with shorter names may see the logged in mode displayed correctly.

.

### How do I get it to work in Session Persistence or Mobility mode?

Please contact your local IT administrator and they will be able to confirm the applications you are using are compatible with these new modes of operation, and then configure the Identity Agent for you.

The settings are covered in the Identity Agent v2.4.6.0 Administrators Guide.

### What if I need it to work as it previously did?

By default, Identity Agent v2.4.6.0 will operate in ‘Normal mode’.   
   
However, if the Identity Agent has been configured to use one of the new modes you will need to contact your local IT administrator request that it is set back to ‘Normal mode’.

### My VPN certificates are being deleted do I need to do anything differently?

By default, the IA will clear all the certs from the user’s personal certificate store. To retain certificates in this store from other publishers, e.g. for a VPN, please ask your IT team to publish the ‘TrustedCertificateIssuers’ registry entry. The settings are covered in the Identity Agent v2.4.6.0 Administrators Guide

# System requirements

The operating systems warrantied for use are listed here:

<https://digital.nhs.uk/services/spine/spine-technical-information-warrantied-environment-specification-wes>

# Operating Modes

The Identity Agent supports the following modes of operation:

* **Normal Mode**

Identity Agent operates in a Normal Mode whereby when Windows is locked and unlocked with the user remain authenticated, they are taken back to their main desktop and do no need to enter their passcode.

* **Enhanced Normal Mode**

In Enhanced Normal Mode The user will need to confirm their passcode on unlocking Windows if they are still authenticated and have a valid session

Graphical user interface, text, application, email

Description automatically generated

Session Lock Mode

When Session Lock Persistence mode is active if the user removes their Smartcard during an active Spine session, the user gets the option to -

1. log out fully
2. the user is able to lock their session.

If the user locks the session, on re-inserting their Smartcard, the user is then able to re-enter the passcode and continue their session, with no loss of state.

## Scenario 1 card removal – ‘Lock’ chosen

A care worker needs to help a colleague in another room for a few minutes and plan to return to their workstation afterwards. When they remove their Smartcard from the reader the following screen will appear:

Graphical user interface, text, application, email

Description automatically generated

As the professional knows they will be returning shortly they can now choose the Lock option button on the screen (if they do not make a choice then the screen will still lock after the specified time period which is counting down on the presented form).

The user will then be taken to a windows lock screen.

Graphical user interface, application, website

Description automatically generated

This Figure Shows the Windows 7 Lock Screen

The care worker can then leave the workstation knowing their Spine session is protected.

Upon returning the care worker can enter their Windows password and the following screen will then be displayed:

Graphical user interface, text, application, email

Description automatically generated

Upon inserting the Smartcard into the reader and entering the passcode the user will now be returned to their desktop with all their applications and data still available.

## Scenario 2 Card Removal – ‘Log out’ chosen

A care worker is called to help with a procedure; they have just finished performing some work on their desktop which involved referencing summary care data. When they remove their Smartcard from the reader the following screen will appear:

Graphical user interface, text, application, email

Description automatically generated

As the care worker knows they will be away some considerable time they choose to log out of Spine and select the corresponding “Log out” button. This means that their Spine session will be ended, and all web browsers will be closed (although this is configurable – see the Identity Agent v2.x Administrators Guide, section ‘Configuration’ for details). The care worker can then log out or lock their desktop.

Mobility Mode

This mode allows a Windows based tablet device with an NFC-type reader to be used with only the occasional presentation of the Smartcard. Typically, the card would be kept away from the device (held back in the Lanyard) but presented directly and held to the NFC area of the device for specific operations, such as logging in, and signing a request.

This mode is targeted at ‘tablet’ usage and requires configuration to enable it (see the Identity Agent Administrators Guide ). It is not recommended to use this mode in a ‘desktop’ setting.

NOTE: If Mobility mode is set to true, but the “Work with Smartcard removed” toggle is not set to on, the precedence order will drop back to the next mode set to true in the registry. If no other modes are set to true, this will then default to Normal mode. If the user needs to preserve the session in addition to the ability of working with the Smartcard remove, ensure that both Session Lock and Mobility modes are enabled in the registry.

For the purposes of maintaining security, a number of timer’s trigger in this mode.

They require the user to periodically re-authenticate, either by presenting their Smartcard (“one-factor”) or presenting their Smartcard *and* passcode (“two-factor”). The timers for these modes begin when the Smartcard is removed for the first time and cannot be overridden once started.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Mobility Mode **  **Timer ** | **Default** | **Minimal** | **Medium** | **Maximum** |
| Time allowed idle before one-factor re-verification is forced | 300s | 60s | 180s | 300s |
| Regardless of activity, time allowed before one-factor re-verification is forced | 1800s  (30m) | 900s (15m) | 1800s   (30m) | 3600   (1h) |
| Regardless of activity, time allowed before two-factor re-verification is forced | 7200s    (2hours) | 3600s   (1hour) | 7200s   (2hour) | 14400s   (4hours) |
| Advance System Tray notification before idle timer prompt | 60s | 20s | 60 | 120s |
| Advance System Tray notification before one-factor re-verification prompt | 180s | 120s | 180s | 180s |
| Advance System Tray notification before two-factor re-verification prompt | 420s | 300s | 600s | 600s |
| Time before two-factor re-verification timer expires, where if the one-factor re-verification about to be shown (either due to a forced re-verification or due to the user presenting their card voluntarily) – that a two-factor re-verification is forced instead.  (Prevents a two-factor re-verification being required shortly after a one factor re-verification has been completed.) | 900s  (15m) | 600s (10m) | 900s  (15m) | 1200s   (20m) |
| Countdown timer on the one-factor re-verification form. | 240s | 120s | 240s | 240s |
| Countdown timer on the two-factor re-verification form. | 240s | 240s | 240s | 240s |

## Scenario – care worker with NFC enabled Windows tablet

### Initial logon

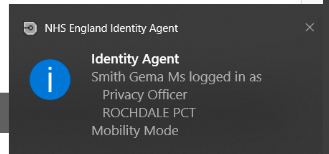
The care worker has a Windows tablet with NFC reader equipped and has ‘Mobility mode’ enabled. When signing infor the first time the logon screen will appear with the option to “Work with Smartcard removed”. The care worker can now toggle this on and sign in (as shown below).

**NOTE**: This toggle has to be set on each login. The setting is not remembered between sessions. This is by design so that the user has to actively select to use Mobility Mode.

Graphical user interface, text, application, email

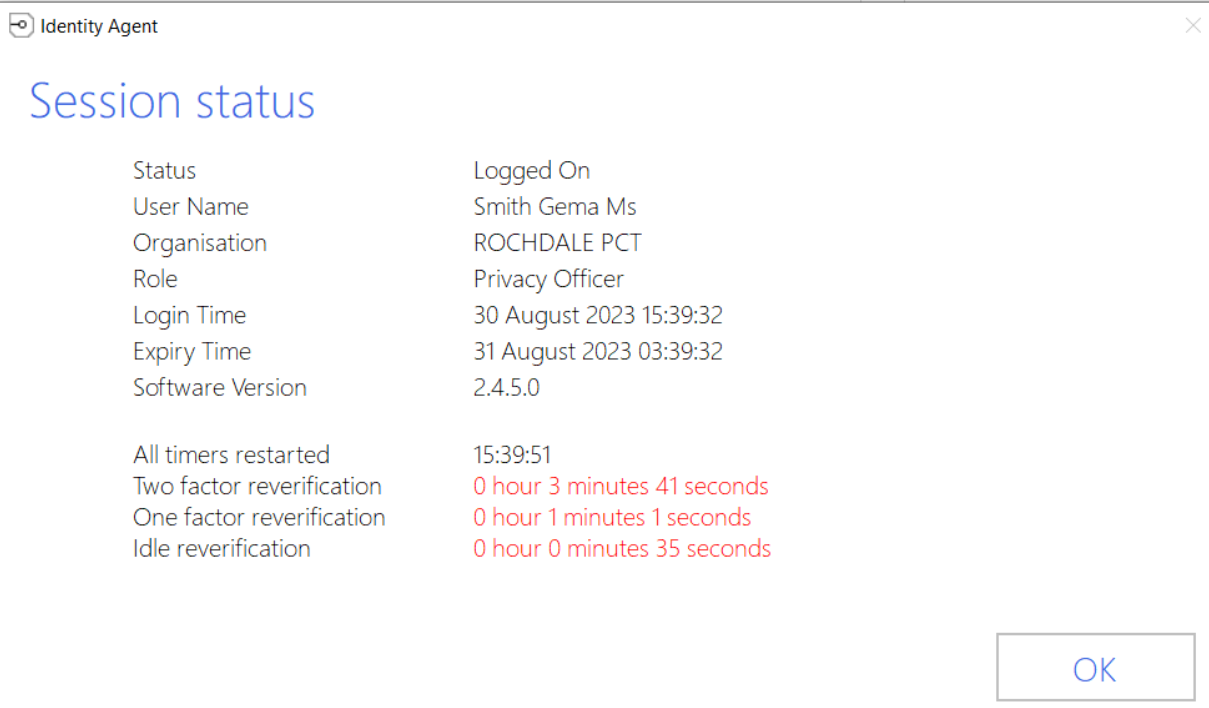
Description automatically generated

Once the passcode has been entered and the user has fully logged in(including any required role selection), a pop-up will appear (see below). The care worker can now remove and re-holster the Smartcard in their Lanyard and work for extended periods without being prompted for authentication using the Smartcard.



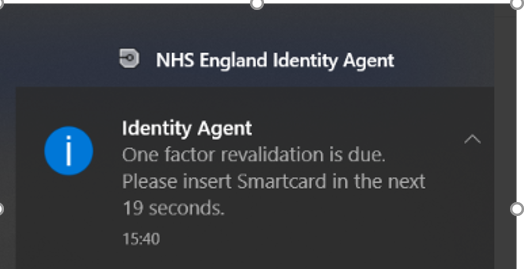
### Checking timeouts

At any time, the care worker can check the status of the time allowed before authentication is required by clicking on the Identity Agent logo in the taskbar, right clicking then choosing ‘Status’. The following screen will then be displayed:



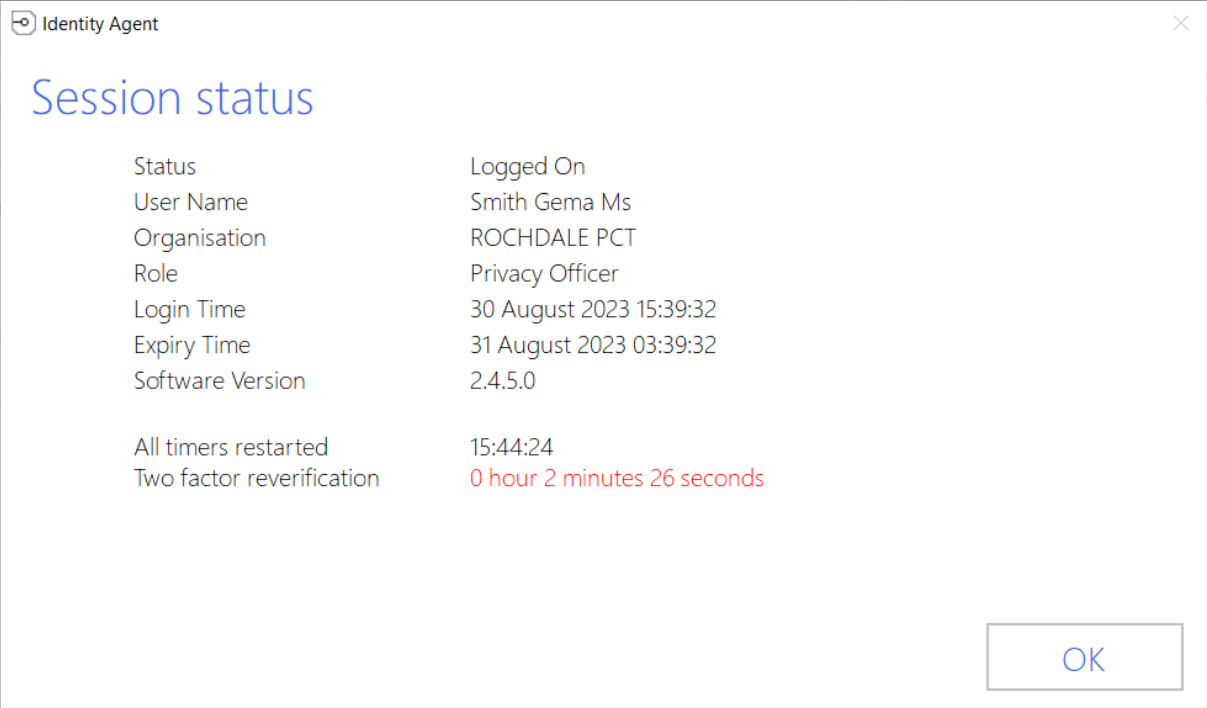
### Re-verification

When One-Factor re-verification is required, the following pop-up will appear:



The care worker will need to present their Smartcard to the NFC reader only. If this is not done within the time, then a screen lock will be instigated after 30 seconds.

When Two-Factor re-verification is required, the following pop-up will appear:



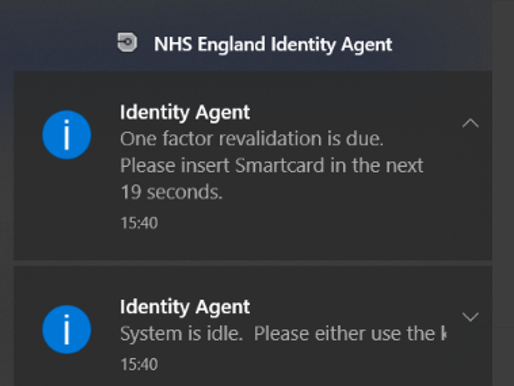
The care worker will then need to present their Smartcard to the NFC reader and then enter the passcode (as shown below). If this is not done within the time, then a screen lock will be instigated after 30 seconds.

Graphical user interface, text, application, email

Description automatically generated

Entering the correct passcode will then result in the desktop being unlocked and with the applications present remaining in their existing state.

When Idle re-verification is required due to lack or mouse or keyboard activity, the following pop-up will appear:



The care worker will need to either move their mouse or use the keyboard. If this is not done within the time, then a screen lock will be instigated after 30 seconds.

### Logging Out

Since the user can work with their Smartcard removed, the normal method of Smartcard removal to logout will not work.

To logout when in Mobility Mode, the user can right click on the Identity Agent icon in the taskbar and select logout, Alternatively the user can remove and re-insert their Smartcard and select Logout from the from presented.

# Operating Mode Precedence Order

Identity Agent v2.x has an order of precedence for the modes described in the sections below. The modes are listed in the order of precedence used by Identity Agent:

1. Mobility Mode
2. Session Lock Mode
3. Enhanced Normal Mode
4. Normal Mode (default mode if no other settings applied)

If the settings for any of the options above are set to true, they will act in the order listed above. If no setting has its value set to true or they have no value set in the registry, the Identity Agent will default to operating in Normal Mode.

If Mobility mode is set to true, but the “Work with Smartcard removed” toggle is not set to on, the precedence order will drop back to the next mode set to true in the registry. If the user needs to preserve the session in addition to the ability of working with the Smartcard removed, check that both Session Lock and Mobility modes are enabled.

# Role Selection improvements

The Identity Agent has a much improved filtering mechanism on the Role Selection form. The role selection box by default has discrete information columns which can be sorted or filtered upon:

**Graphical user interface, text, application, email

Description automatically generated**

For instance, typing the word “agent” will then filter the list down to roles with “agent” in the title e.g., Registration Authority Agent:

**Graphical user interface, text, application, email

Description automatically generated**

Different Role Information Schemes can be selected by clicking on the cog icon:

Graphical user interface, text, application

Description automatically generated

The available schemes are simple (default), Full, and Legacy. Selecting the “Full” option will result in the following being displayed:

**Graphical user interface, text, application, email

Description automatically generated**

Selecting “Legacy” will result in the following column scheme:

   
**Graphical user interface, text, application, email

Description automatically generated**

# Citrix Support

The Identity Agent has been tested using Citrix on Windows Server 2016 for authentication only. All Smartcard types have been tested for authentication.

# Fast-User-Switching

Fast-user-switching is now supported. When the Identity Agent is configured to work in Session Lock Persistence mode, it is possible for multiple care workers to share the same workstation and switch between the logged-on users whilst at the same time maintaining each care worker’s CIS session, without the need to log back into CIS each time a Windows user-switch is performed.

# Follow-Me-Sessions (RDP)

Follow-me-sessions (remote desktop RDP) is now supported. When the Identity Agent is configured to work in Session Lock Persistence mode, it is possible for a care worker to log into their remote desktop session and preserve this session when moving to a different machine.

When using RDP, it is possible that the card readers appear to go to sleep and when the user attempts to unlock their machine the “Checking Smartcard” banner runs for a period of time and the user is presented with an “Unable to read Smartcard” error. If the User removes their Smartcard and attempts to unlock the machine again, this attempt should be successful.

# Follow-me-sessions (VDI)

Follow me sessions where the user is using VMWare VDI implementations are not supported as the Smartcard reader is not always correctly reconnected to the session if the user only performs a “Disconnect” rather than a “Disconnect and Log Off”. The failure to correctly reconnect the Smartcard reader leaves the user unable to reverify their session with a Smartcard when prompted on unlocking the session necessitating the user to perform a full “Disconnect and Log Off” which terminates their session.

**Common Issues**

More information about commonly occurring issues can be found here:

<https://digital.nhs.uk/services/care-identity-service/setting-up-and-troubleshooting/troubleshooting-nhs-identity-agent>

# Support

**For further support or more information, please use one of the following:**

Raise a ticket via the [NHS Digital Customer Portal](mailto:NHS%20Digital%20Customer%20Portal,) or email [ssd.nationalservicedesk@nhs.net](mailto:ssd.nationalservicedesk@nhs.net)

Telephone contact 0300 303 5035

**Alternatively write to:**

Iamplatforms@nhs.net