­­­

NHS Digital Identity Agent v2.3.2.0

User Guide

­­­­­

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

Contents

[Overview 3](#_Toc129948540)

[Spine overview 3](#_Toc129948541)

[What is the Identity Agent? 4](#_Toc129948542)

[What’s different in version 2.3.2.0 of the Identity Agent? 4](#_Toc129948543)

[What’s new in version 2.3.2.0 4](#_Toc129948544)

[What’s different in version 2.3.0.0 of the Identity Agent? 4](#_Toc129948545)

[What’s new in version 2.3.0.0 5](#_Toc129948546)

[What was different in version 2.2.3.9 of the Identity Agent? 5](#_Toc129948547)

[What’s new in version 2.2.3.9 5](#_Toc129948548)

[What was different in version 2.2.3.7 of the Identity Agent? 5](#_Toc129948549)

[What was new in version 2.2.3.7 5](#_Toc129948550)

[What was different in version 2.2.2.0 of the Identity Agent? 6](#_Toc129948551)

[What was in version 2.2.2.0 6](#_Toc129948552)

[What was new in version 2.2 6](#_Toc129948553)

[Registry Locations 7](#_Toc129948554)

[How do I know which mode I am running in? 8](#_Toc129948555)

[How do I get it to work in Session Persistence or Mobility mode? 8](#_Toc129948556)

[What if I need it to work as it previously did? 8](#_Toc129948557)

[I’m an RA do I need to do anything differently? 9](#_Toc129948558)

[Software & documentation 9](#_Toc129948559)

[Important Considerations 9](#_Toc129948560)

[System requirements 9](#_Toc129948561)

[System Requirements 9](#_Toc129948562)

[Operating Mode Precedence Order 10](#_Toc129948563)

[Normal Mode 10](#_Toc129948564)

[Enhanced Normal Mode 10](#_Toc129948565)

[Session Lock Persistence Mode of Operation 11](#_Toc129948566)

[Scenario 1 card removal – ‘Lock’ chosen 11](#_Toc129948567)

[Scenario 2 Card Removal – ‘Log out’ chosen 14](#_Toc129948568)

[Mobility mode 14](#_Toc129948569)

[Scenario – care worker with NFC enabled Windows tablet 15](#_Toc129948570)

[Initial logon to Spine 15](#_Toc129948571)

[Checking timeouts 16](#_Toc129948572)

[Re-verification 17](#_Toc129948573)

[Logging Out 19](#_Toc129948574)

[Role Selection improvements 19](#_Toc129948575)

[Citrix Support 22](#_Toc129948576)

[Entrust Virtual Smartcard Users 22](#_Toc129948577)

[Previous Identity Agent Improvements 23](#_Toc129948578)

[Fast-User-Switching 23](#_Toc129948579)

[Follow-Me-Sessions (RDP) 23](#_Toc129948580)

[Follow-me-sessions (VDI) 24](#_Toc129948581)

# Overview

## Spine overview

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

The Spine is part of the critical national infrastructure that supports the delivery of these services and the health care provision in the UK. As such it is part of "those facilities, systems, sites and networks necessary for the functioning of the country and the delivery of the essential services upon which daily life in the UK depends".

The Spine provides the infrastructure that enables increased patient safety, improved quality of healthcare, greater clinical effectiveness and better administrative efficiency. It is used and supported 24 hours a day, 365 days a year and is highly resilient.

Supporting the operation of the Spine is an identity management system, responsible for ensuring that every care worker within the NHS has the appropriate level of access to Spine and associated systems. At the front line of the identity solution is the Smartcard and Identity Agent.

## 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 Spine systems were 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 their passcode.
* Obtain an Access Token that can be used by applications on the users’ behalf to access Spine 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 2.3.2.0 of the Identity Agent?

NHS Digital Identity Agent Version 2.3.2.0 is an updated release which resolves the following issues.

* Identity Agent Pin form default focus issue
* When the smart card is inserted, the Identity agents pin form is displayed. If this form has input focus then the user can insert the passcode. If an application takes ownership of the input focused, the passcode is not accepted in that pin form window and can end up being typed elsewhere. This fix endeavours to ensure that the input focus remains on the pin form as expected and no competing application maintains focus.
* Fix for Windows Hello for Business service detection issue with Identity Agent on Virtual RDS environments like VDI and Citrix which, was causing the I.A to fail.

## What’s new in version 2.3.2.0

* Fixing Identity Agent MSI upgrade code string update (GUID value). This means that installation of latest IA v 2.3.2.0 (and future releases) can done directly without uninstalling the previous IA versions

## What’s different in version 2.3.0.0 of the Identity Agent?

The release version has been incremented to 2.3.x to reflect the inclusion of virtual Smartcard functionality.

NHS Digital Identity Agent Version 2.3.0.0 is an updated release which resolves the following issues.

* GMT/BST bug. During the British Summer Time (BST) period, the session length was one hour shorter than expected. This issue is now resolved.
* Revisions to the security updates on Smartcard removal.

## What’s new in version 2.3.0.0

* Users with an Entrust Virtual Smartcard will now have their details (Username and UUID) displayed on the initial Passcode form of the Identity Agent. This allows the user to be clear which virtual Smartcard the Identity Agent has detected to prevent a user inadvertently locking another user’s card through incorrect passcode entry. Note that the user’s username and UUID is only displayed if a virtual Smartcard is detected, if the Identity Agent has detected a physical card in the card reader and is prompting for the physical card passcode it will not display the username and UUID.
* The form displayed if a user attempts to use a locked Smartcard will display different information depending on whether the Smartcard is a physical or virtual one.

**NOTE:** Entrust Virtual Smartcards have not yet been warranted for use in any type virtual environment and are not currently to be used as a replacement for a physical Smartcard for users performing any type of card management activity. The Entrust Virtual Smartcard also does not yet support digital signing and therefore cannot be used to sign prescriptions.

## What was different in version 2.2.3.9 of the Identity Agent?

NHS Digital Identity Agent Version 2.2.3.9 is a bug fix release which resolves the following issue.

* Users being logged out
* All users of Identity Agent v2.2.1.0 onwards using only Normal mode can be logged out 4h 10m after they first lock their machine with the default registry settings. This issue is now resolved.
* Security updates on Smartcard removal
* Minor memory resolved
* Logic issue resolved when calling OT cache clear. Cache clear is no longer called if the middleware is configured for GEM and the correct error messages are put into the log file

## What’s new in version 2.2.3.9

There are no additional features with this release.

## What was different in version 2.2.3.7 of the Identity Agent?

NHS Digital Identity Agent Version 2.2.3.7 is a bug fix release which resolves the following issues.

* Memory Leak. On machines with Win8.1 or Win10, versions of Identity Agent from v2.2 onwards can exhibit a memory leak causing instability in the Identity Agent. This issue is now resolved.
* No PIN Form. A bug was inadvertently introduced in Identity Agent v2.2.2.0 whereby on certain operating systems the PIN form would not be presented when a Smartcard is inserted. This issue is now resolved.

## What was new in version 2.2.3.7

There are no additional features with this release.

## What was different in version 2.2.2.0 of the Identity Agent?

NHS Digital Identity Agent Version 2.2.2.0 has the following aims for users upgrading from BT Identity Agent (any version) or HSIC Identity Agent v1 or any previous versions of NHS Digital Identity Agent:

* To make the Identity Agent more intuitive and efficient. To align with this the Role Selection filter has been updated to facilitate quicker discovery of a care workers desired role.
* To allow users easy access back to their desktop if locking and unlocking Windows without removing their Smartcard, i.e. still authenticated into Spine. By default, the configuration of “**Normal**” mode does not force the user to re-enter their passcode on unlocking Windows. The behaviour of this mode was changed following user feedback, so it now behaves the same as BT Identity Agent or Identity Agent v1. Enhanced normal mode can be enabled with a registry key and Identity Agent v2.2 and later will then have the same behaviour as the previous versions of Identity Agent v2.x.
* To allow a user to securely leave a computer for a short amount of time without losing the application sessions and data currently displayed and also remove their Smartcard. This facility is called “**Session Lock Persistence**”.
* To enable users of mobile devices running a Windows OS to authenticate, remove their Smartcard from the device for secure storage (e.g. lanyard), and then continue working on Spine applications as normal. This facility is called “**Mobility**”mode.

For details on how Enhanced Normal Mode, Session Lock Persistence or Mobility Modes work please see the relevant sections in this guide.

Users upgrading from NHS Digital Identity Agent v2.0 onwards will get the benefits of additional features and bugs fixes in the latest releases.

## What was in version 2.2.2.0

* The error presented to the user of multiple Smartcards being inserted when they attempt to authenticate or the IA giving the PIN form when no Smartcard is inserted when they first log into Windows and the user has a mobile SIM reader with a SIM card inserted is now resolved.
* The issue of the user being logged out of Windows when they remove their Smartcard instead of the machine being locked if the user has W8.1 or later, Session Lock is enabled, and the machine is displaying a screensaver is now resolved.

See the Identity Agent v2.2.2.0 Administrator Guide for further information.

### What was new in version 2.2

This information is left in to advise the user of previous fixes and enhancements due to how close the Identity Agent releases are.

* Now supports authentication via Citrix / VDI / Terminal Services. **Only** authentication is supported. **No** RA functions are supported over Citrix, neither is self-renew. A registry change is required for Citrix.
* Normal Mode has been updated to behave the same as Identity Agent v1 and older versions of Identity Agent by default. Identity Agent 2.x behaviour can be invoked if required.
* Cache clearance is built into Identity Agent for users with both Oberthur (Series 8) Smartcards and Oberthur Middleware if they receive the “Problem reading Smartcard” error. The Identity Agent now attempts to clear the Oberthur Smartcard cache prior to advising the user to see their RA.
* Change of the URL called when a user clicks on T&C’s from the passcode form.
* The URL is provided to the self-service unlock service if the user either locks their Smartcard due to too many incorrect passcode attempts or tries to authenticate with a previously locked Smartcard. The user needs to have previously registered to use this service.
* EnableNHSEnrollment. The value for this flag is now set to 0 on every Smartcard insertion to resolve the invalid signature error. If the key does not exist on the machine, the Identity Agent continues as normal.
* Update to Gem heal process. This process is now only invoked on Gemalto 4/5/6 Smartcards requiring healing.
* Broken spring check (CardRemovalCheck). This setting can now be changed dynamically without a need to restart Identity Agent. This will make the process of self-renewal for Series 8 cards simpler.
* New Sub CA certificates for the live platform. Extra certificates are installed during the installation of Identity Agent to enable the user to continue authenticating when the live certificates are updated in the future.
* Resolved an issue where the user was not correctly logged out of Spine if the network cable became disconnected with the machine locked and the Smartcard left inserted.
* Black screen issues have been resolved (where possible) when the machine is locked or unlocked. Please be aware, that not all black screen issues can be resolved, and NHS Digital currently have support tickets open with Microsoft to resolve issues relating to locking the machine from the second desktop using Windows keys (Win+L or Ctrl+Alt+Del & Lock).

### Registry Locations

The Identity Agent process will run as a 32-bit process regardless of whether the OS is 32-bit or 64-bit. As such it is important to note that the registry path for the Identity Agent will alter depending upon which OS variant is in use.

* **32-bit Operating System:**
* **Set by Group Policy:** HKLM\SOFTWARE\Policies\HSCIC\Identity Agent
* **All Users:** HKLM\SOFTWARE\HSCIC\Identity Agent
* **Current User:** HKCU\SOFTWARE\HSCIC\Identity Agent
* **64-bit Operating System:**
* **Set by Group Policy:** HKLM\SOFTWARE\Policies\HSCIC\Identity Agent
* **All Users:** HKLM\SOFTWARE\Wow6432Node\HSCIC\Identity Agent
* **Current User:** HKCU\SOFTWARE\HSCIC\Identity Agent

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

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

**Graphical user interface, text, application

Description automatically generated**

**Text

Description automatically generated**

As can be seen from above, with Windows 10, this notification is not always visible. This is due to the font size used by Windows 10 and the text box size available. This is outside of the control of Identity Agent to display this. Trusts with shorter names may see the logged in mode displayed correctly.

All other screen shots of available modes will be captured using Windows 7 or Windows 8.1 for completeness.

### 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 registry settings are covered in the Registry Settings section of the Identity Agent v2.x Administrators Guide.

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

By default, Identity Agent v2.x will operate in ‘Normal mode’, in which the behaviour most closely matches that of previous Identity Agents, BT IA and HSCIC IA v1.   
   
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’. This can be easily accomplished by deleting any registry which has been added for either Session Persistence or Mobility Modes.

### I’m an RA do I need to do anything differently?

All users performing CMS activities are advised to set the registry value   
**CardRemovalCheck = False**

The registry locations are shown in the Registry Locations section

This will stop the user being intermittently logged out when issuing Smartcard

# 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 System Requirements section below. (Other operating systems may work but are not warranted and have not been tested).

## System Requirements

The table below describes the ‘variable’ components successfully tested in conjunction with NHS Digital Identity Agent v2.x. As such it also serves as a statement of warranted versions.

|  |  |  |
| --- | --- | --- |
| **Component** | **Tested Versions** | **Upgrade Policy** |
| **Operating System** | Windows 10, x64 \*  Windows Server 2012 R2 | All patches and hotfixes. Service Pack updates should follow specific identity agent guidance published by NHS Digital. |
| **Browser** | Internet Explorer 11  \*\* Google Chrome | All upgrades. |
| **Java Runtime** | Java SE versions 7.x and 8.x, 32-bit only, up to and including Java 1.8.251 | Patches and hotfixes. Major version upgrades (e.g. Java SE v8) should follow specific Identity Agent guidance published by NHS Digital. |
| **Middleware** | Gemalto Classic Client 6.1, Patch 3  Oberthur AWP 5.2.0 SR8 | NHS Digital warranted versions only. |

\* Excluding Windows 10(x64)-IOT

\*\* Chrome with Chrome Extension

# Operating Mode Precedence Order

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

Mobility Mode   
Session Lock Mode   
Enhanced Normal Mode   
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 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.

See the Identity Agent admin guide for further details on the registry values.

# Normal Mode

By default, Identity Agent v2.x operates in a Normal Mode whereby when Windows is locked and unlocked with the user still being authenticated against Spine, they are taken back to their main desktop and do no need to enter their passcode. This differs in operation from the previous versions of Identity Agent (v2.1.2.16 and earlier) and the change has been made following user feedback.

# Enhanced Normal Mode

The use of ‘EnhancedNormalMode = True’ will change the behaviour of Identity Agent v2.x back to that of previous versions of Identity Agent (v2.1.2.16 and earlier) where the user will need to confirm their passcode on unlocking Windows if they are still authenticated against Spine.

If the Trust wants to change the behaviour of Identity Agent back to the same as the previous version, it is possible to enable Enhanced Normal Mode in the registry and the user will again be prompted to reverify when they unlock Windows whilst they are still authenticated against Spine.

**Graphical user interface, text, application, email

Description automatically generated**

# Session Lock Persistence Mode of Operation

When Session Lock Persistence mode is active. If the user removes their Smartcard during an active Spine session, as well as the option to log out of Spine fully (as is automatically the case with previous Identity Agent versions or Identity Agent v2.x in default operation), the user is able to lock their session. On re-inserting their Smartcard, the user is then able to re-enter their passcode and continue their Spine session, with no loss of state.

This mode is targeted at ‘desktop’ usage (including laptops) and requires a registry configuration to enable it (see the Identity Agent v2.x Administrators Guide, section ‘Configuration’).

## 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 registry configuration to enable it (see the Identity Agent v2.x Administrators Guide section ‘Configuration’). 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 identity 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 è**  **Timer ê** | **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 |

The appropriate Mobility mode timing scheme will be set by your IT Administrator (information on how to do this in the section ‘Config Themes’ in the Identity Agent v2.x Administrators Guide)

Two Factor Authentication (2FA) - requires “something you have” (the Smartcard in this instance) **AND** “something you know” (the Smartcard passcode).

One Factor Authentication - only requires “something you have” (presenting the smartcard to the reader in this instance) **OR** “something you know” (the Smartcard passcode).

If the one-factor and two-factor timers are close to each other, e.g. a one-factor authentication is required in 60 seconds and a two-factor authentication is required in 100 seconds, then the Identity Agent will enforce a two-factor authentication instead of two separate authentications close to each other. This is done to reduce the number of times a user has to present their Smartcard for verification and is not a fault.

## Scenario – care worker with NFC enabled Windows tablet

### Initial logon to Spine

The care worker has a Windows tablet with NFC reader equipped and has ‘Mobility mode’ enabled. When signing into Spine for 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 to Spine. 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 into Spine (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.

**Shape, rectangle

Description automatically generatedGraphical user interface, text, application

Description automatically generated**

### 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:

**Graphical user interface, text

Description automatically generated**

### Re-verification

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

**Text

Description automatically generated**

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:

**A screenshot of a computer

Description automatically generated**

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:

**Text

Description automatically generated**

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.

# Role Selection improvements

This version of the Identity Agent has a much more sophisticated filtering mechanism on the Role Selection form compared to BT Identity Agent and HSCIC Identity Agent v1. As can be seen the new 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**

As can be seen above 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

Identity Agent v2.x has been tested using Citrix on Windows Server 2012R2 for authentication only. To enable Citrix support, card reader polling needs to be enabled in the registry. See the Registry Settings section in the Identity Agent Administrators Guide.

All Smartcard types have been tested for authentication, but **no** CMS activities are supported, including self-renewal. The user will need to use a physical machine which connects directly to Spine for these activities.

The configuration required to enable the USB pass through to work are outside of the scope of this documentation and the configuration is the responsibility of the IT department at the trust wishing to use Citrix.

Ensure the correct card reader drivers have been installed when using Citrix.

It is recommended to set card healing to false when using Identity Agent with Citrix.

For further information on the registry changes, refer to the Identity Agent Administrators Guide.

# Entrust Virtual Smartcard Users

The user details will be displayed on the initial Passcode form. This is especially useful in an environment with multiple machines and users so that the user knows they have connected to the machine they expected to connect for authentication, this will prevent a user inadvertently locking another user’s card through incorrect passcode entry.

**Graphical user interface, text, application, email

Description automatically generated**

A different message will be displayed to a physical Smartcard if the user tries to authenticate with a locked virtual Smartcard. At the time of writing, there is no self-service unlock available for virtual Smartcard users. The only current option is to get their RA manager to de-register and re-register the user for a virtual Smartcard.

**Graphical user interface, text, application, email

Description automatically generated**

# Previous Identity Agent Improvements

The information below is retained from previous user guides for completeness. The latest version of Identity Agent v2.x has all the features of previous versions of Identity Agent v2.x plus and enhancements or bug fixes.

## Fast-User-Switching

Introduced in v2.1.2.16, 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 Spine session, without the need to log back into Spine each time a Windows user-switch is performed.

Check with your local IT department that your applications are compatible with Session Persistence mode prior to making any changes.

The definition used for fast user switching is the switching of different Active Directory accounts on a single machine. For example, both Fred and John are logged into Windows, but only one account is active at a time. This definition differs to some other vendors who define fast user switching within the application from a single generic Active Domain account.

## Follow-Me-Sessions (RDP)

Introduced in v2.1.2.16, 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. This issue appears to occur more frequently if the user has different card reader on the host and remote machine. For example, using an internal reader on the host machine, but using an OmniKey 3121 on the remote machine.

NOTE: If the Identity Agent is installed on both the local machine and the remote desktop machine, it is the remote machine which needs to have Session Lock Persistence mode enabled.

NOTE: It has been observed during testing that occasionally the user may get an “issue reading Smartcard” error. Should this occur, remove the Smartcard and re-insert it. Allow the machine to read the Smartcard and then try to Smartcard PIN code again.

Check with your local IT department that your applications are compatible with Session Lock Persistence mode prior to making any changes.

## Follow-me-sessions (VDI)

Follow me sessions where the user is using VMWare VDI implementations are not formally 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 Spine session.

Follow me sessions may work with VDI, but no faults will be accepted on this mode should there be issues for the reasons stated above.

**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>