­­­

NHS Digital Identity Agent v2.3.2.0

Release Notes

­­­­­

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



[Introduction 3](#_Toc129955506)

[Audience 4](#_Toc129955507)

[Release Details 4](#_Toc129955508)

[Content 4](#_Toc129955509)

[Changes 4](#_Toc129955510)

[Previous version v2.3.0.0 5](#_Toc129955511)

[Content 5](#_Toc129955512)

[Changes 5](#_Toc129955513)

[Previous version v2.2.3.9 5](#_Toc129955514)

[Content 5](#_Toc129955515)

[Changes 6](#_Toc129955516)

[Previous version v2.2.3.7 6](#_Toc129955517)

[Changes 6](#_Toc129955518)

[Previous version v2.2.2.0 6](#_Toc129955519)

[Content 6](#_Toc129955520)

[Changes 6](#_Toc129955521)

[Previous version v2.2.1.0 7](#_Toc129955522)

[Content 7](#_Toc129955523)

[Changes 7](#_Toc129955524)

[Previous version v2.1.2.16 10](#_Toc129955525)

[Content 10](#_Toc129955526)

[Changes 10](#_Toc129955527)

[Previous version v2.0 10](#_Toc129955528)

[Content 10](#_Toc129955529)

[Changes 11](#_Toc129955530)

[Warranted use 11](#_Toc129955531)

[Dependencies policy 12](#_Toc129955532)

[Tested components 12](#_Toc129955533)

[System requirements 12](#_Toc129955534)

[Lifecycle policy 12](#_Toc129955535)

[Known issues 13](#_Toc129955536)

[Installation 13](#_Toc129955537)

[Terminal services (remote desktops) 14](#_Toc129955538)

[Spine application / Portal 14](#_Toc129955539)

[Authentication / logout behaviour 15](#_Toc129955540)

[Windows 10 17](#_Toc129955541)

[CMS (Card Management Services) via CIS (Care Identity Service) 17](#_Toc129955542)

[Third Party Application Issues 17](#_Toc129955543)

[Notable exclusions 18](#_Toc129955544)

[‘Mobility mode’ 18](#_Toc129955545)

# Introduction

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 clinician 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.

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 desktop 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 enhancements to the previous versions and bug fixes.

## Audience

The intended audience for this document includes:

* Registration Authority Agents and Managers
* IT Administrators and Managers
* Suppliers of products and services to the NHS

# Release Details

## Content

This release is the NHS Digital Identity Agent v2.3.2.0 dated 24th May 2021 on the digital signature.

This release contains all features introduced in the previous releases of NHS Digital Identity Agent and adds the support and issue resolutions as described below.

## Changes

**Identity 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.

**Windows Hello Service**

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.

**MSI Package version update**

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.

# Previous version v2.3.0.0

## Content

This release is the NHS Digital Identity Agent v2.3.0.0 dated 12th June 2020 on the digital signature.

This release contains all features introduced in the previous releases of NHS Digital Identity Agent and adds the support and issue resolutions as described below.

## Changes

**Shorter Session Length Than Expected**

Resolves an issue where the calculation of session length during British Summer Time (BST) was incorrect. This issue is now resolved and the session length during GMT and BST will be as per the duration set by the backend servers.

**Security Fixes**

Minor security updates on Smartcard removal.

**Virtual Smartcard**

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.

**Locked Smartcard**

Introduced with this version of Identity Agent. The Identity Agent differentiates between physical and virtual Smartcards for the information given to a user if they attempt to use a locked Smartcard.

**NOTE:** Entrust Virtual Smartcards have not yet been warranted for use in any type of 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.

# Previous version v2.2.3.9

## Content

This release is the NHS Digital Identity Agent v2.2.3.9 dated 23rd October 2019 on the digital signature.

This release contains all features introduced in the previous releases of NHS Digital Identity Agent and adds the support and issue resolutions as described below.

## Changes

**Users Getting 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.

**Minor Memory Leak**

A minor memory leak has been resolved on all OS’s running Identity Agent.

**Security Fixes**

Security enhancements introduced.

**Cache Clear**

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.

# Previous version v2.2.3.7

## Changes

**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 is not presented when the Smartcard is inserted. This issue is now resolved.

# Previous version v2.2.2.0

## Content

This release is the NHS Digital Identity Agent v2.2.2.0, dated 31st January 2019 on the digital signature.

This release contains all features introduced in the previous releases of NHS Digital Identity Agent and adds the support and issue resolutions as described below.

## Changes

**Multiple Smartcard Error**

On machines with later builds of Windows 10 (1803 and newer), Microsoft has made the drivers for the chips being used to provide mobile SIM services part of Windows. On some machines this now makes Identity Agent believe there is more than one Smartcard inserted when the user has a mobile SIM in the socket and a Smartcard.

In this release, NHS Digital Identity Agent v2.2.2.0 now ignores the mobile SIM reader as a Smartcard and the user can authenticate normally. It is anticipated this update will remove the necessity to make registry changes to the Identity Agent to resolve the issue. However, as new chipsets come out, further releases of Identity Agent may be required to continue ignoring these as Smartcards.

**Logged Out on Smartcard Removal**

On machines with Windows 8.1 and above, if the following is true the user may get logged out on Smartcard removal instead of the machine being correctly locked.

* SessionLockPersistence\_Enabled is True
* Windows is showing a screen saver rather than a lock screen
* The user removes their Smartcard and allows the Identity Agent timer to timeout and attempt to lock Windows

In the above scenario, instead of the user’s machine being correctly locked, they are logged out at the end of the timeout period.

The above does not affect users running Windows 7.

# Previous version v2.2.1.0

## Content

This release is the NHS Digital Identity Agent v2.2, dated 23rd October 2018 on the digital signature.

This release contains all features introduced in the previous release (IA v2.1.2.16) and also adds the support and issue resolutions as described below.

## Changes

**Precedence Order**

The Identity Agent now correctly uses the precedence order of Mobility Mode / Session Persistence / Enhanced Normal Mode / Normal Mode depending upon whether any of the options are set to true in the registry.

**Citrix**

Support for authentication via Citrix. To enable Citrix support, add the following value to the Identity Agent registry ‘UseCardReaderPolling’ and set the value to ‘true’.

Note that CMS operations are **NOT** supported on VDI / Terminal Services / Citrix, only authentication is supported.

Testing has been conducted using Windows Server 2012R2 for this functionality.

It is recommended to turn card healing off when using Citrix.

**Cache Clearance**

The cache clearance tool for Oberthur Smartcards to be used if the Series 8 (OT) Smartcard gives the message “There is a problem reading your Smartcard…” is now built into the Identity Agent and will be triggered if the user has both Oberthur Middleware and a Series 8 Smartcard and the Identity Agent cannot read the Smartcard. Following installation of Identity Agent v2.2, there should no longer any need to run the cache clearance tool to resolve the “Problem reading Smartcard” error.

**Update to the URL called for T&C’s**

A change of URL used for the Terms and Conditions link on the PIN form.

**Locked Smartcard**

If the user attempts to use a locked Smartcard or inadvertently locks their Smartcard due to too many incorrect PIN entries, the Identity Agent now provides a link to the self-service unlock URL so that users who have previously registered for this service can access it easily.

Note 1: The Identity Agent does not provide a link to register for self-service as you have to be authenticated in order to register.

Note 2: The Identity Agent only redirects to the live Smartcard unlock service regardless of the current registry settings. Users wishing to use Path-to-Live self-service unlock will still need to enter this address manually.

Note 3: If the user locks their Smartcard on the secure desktop when unlocking their machine, the self-service unlock link will only be visible on their main desktop after the machine is unlocked.

**NHS Enrollment Flag**

In some circumstances where CMS operations have failed unexpectedly, the registry has been left with the **NHSEnrollment** flag set to 1.

Usually this registry key is set to 0 when Oberthur middleware is installed, this points the Middleware to the Agile applet on the Oberthur Smartcard.

CMS flips this registry key to 1 in order to write certificates to the Compatibility applet on the Smartcard, this enables the Smartcard to be used for authentication on machines with just Gemalto Middleware installed.

If **NHSEnrollment** key is left set to 1, then on that machine in some circumstances authentication will not be possible.

The Identity Agent now sets the **NHSEnrollment** key to 0 (if it isn't already) on machines with Oberthur middleware installed or the registry key exists. This is done each time the Smartcard is inserted.

**Gem Heal**

Gem Heal now only run on Series 4/5/6 Smartcards. Specifically, it is now never invoked on Series 8 Smartcards.

**Broken Spring Check (CardRemovalCheck)**

**CardRemovalCheck** can now be turned on and off dynamically, rather than requiring a restart of Identity Agent.

This means that self-renewals of Series 8 Smartcards on machines without Oberthur middleware will no longer require an Identity Agent restart.

**New Certificates**

New live Sub CA 1C and 1D Certificates are installed into the Intermediate Certificate Store to support future live certificate updates.

**Normal Mode**

The introduction of having to reverify when unlocking a machine which has been left authenticated with Spine (the Smartcard has been left in the card reader during lock period) has caused issues for some users. There have also been feature requests to be able to turn this feature on and off.

By default, Identity Agent v2.2 operates in a normal mode where the user does not have to reverify when they unlock Windows, the same as Identity Agent v1 behaviour. If the trust wishes to use the behaviour of the previous version of Identity Agent v2.x, this can be invoked by setting the registry key ‘**EnhancedNormalMode’** to ‘True’.

This change is dynamic and does not need the Identity Agent to be restarted when enabled.

**Resolved issues**

* If using the previous version of Identity Agent Windows was locked, then the network connection removed, the Smartcard removed and finally Windows was unlocked. Instead of going directly to the user’s desktop, the user could be presented with a black screen forcing them to log out of Windows and back in. The logic flaw causing this issue has been resolved
* Black screen issues. There are various black screen issues when locking and unlocking Windows. Identity Agent v2.2 attempts to resolve many of these. However, we are aware of some that still remain.

These are mainly around the locking of Windows when on the second secure desktop when the user performs either **Win+L** or **‘Ctrl+Alt+Del** and then lock to lock their machine. These issues seem only to affect machines running Windows 10 and this issue is currently under investigation by Microsoft support as this is a Windows bug and not an Identity Agent bug.

It should be noted that locking the machine by clicking the ‘Lock’ button on the reverify PIN form will stop this from occurring.

# Previous version v2.1.2.16

## Content

This release is the NHS Digital Identity Agent v2.1.2.16, dated 18th October, 2016.

This release contains all features introduced in the previous release (IA v2.0) and also adds the support and issue resolution as described below.

## Changes

**Fast-User-Switching**

Fast-user-switching (operating with multiple Windows accounts and different Spine sessions on a single workstation) is now supported as a feature for NHS Digital Identity Agent v2, subject to the capabilities of the machine to support multiple logins concurrently.

**Follow-Me-Sessions**

Remote Desktop or VDI is now supported as a feature for NHS Digital Identity Agent v2 and the previous issue of being unable to re-launch Spine applications has been resolved.

**Resolved issues**

The previous issue of Gemheal.dll being created in a Program Files (x86) directory on 32-bit systems has been resolved.

# Previous version v2.0

## Content

This release is the HSCIC Identity Agent v2.0.5828.26592, dated 18th December 2015.

This identity agent is designed as a direct replacement for existing identity agents, including HSCIC Identity Agent 1.0 and BT Identity Agent (all versions).

New features include:

* Session Lock Persistence. This allows users to remove their Smartcards without losing application state
* Mobility Persistence. This allows users to work with Windows tablet devices without continual presence of the Smartcard
* Display of Organisation Code in Role Selection
* General performance and usability enhancements
* Product support for:
* Windows 7, 32-bit and 64-bit
* Windows 8.1, 32-bit and 64-bit
* Windows 10, 64-bit – Excluding IOT x64
* Windows Server 2008 R2 and 2012 R2 (via terminal services)

There will be no centrally led deployment of this product to organisations. Instead it will be the responsibility of organisations to formulate their own deployment plans based on their own priorities and needs.

## Changes

Whilst in terms of authentication this identity agent is broadly functionally equivalent to existing identity agents, there are some significant application changes to allow maintenance of Spine sessions on removal of Smartcard, depending on the ‘mode’ chosen.  

**Session Lock Persistence**

If a user removes their Smartcard during an active Spine session, the user is able to lock their session. On re-inserting their Smartcard, the user is then able to re-authenticate and continue their Spine session, with no loss of state.

This mode is targeted at ‘desktop’ usage, and can be enabled by the use of a registry key which is detailed in the IA v2 Administrators Guide (section ‘Registry Settings’).

**Mobility mode**

This mode enables users of mobile devices running a Windows OS to authenticate, remove their Smartcard from the device for secure storage (lanyard etc.), and then continue working as normal.

For the purposes of maintaining identity security, a number of timers trigger in this mode, ensuring the user is periodically required to re-authenticate.

This mode is targeted at ‘tablet’ usage, and can be enabled by the use of a registry key which is detailed in the IA v2 Administrators Guide (section ‘Registry Settings’).

**Normal mode**

By default, (without any registry configuration), Identity Agent v2 will operate in ‘Normal mode’. This is a legacy mode of operation, whereby removing a Smartcard automatically and immediately terminates the Spine session. This ensures the broadest possible compatibility with 3rd party applications.

**For more details, please see the NHS Digital Identity Agent v2 User Guide.**

# Warranted use

NHS Digital Identity Agent v2.x will follow a warranted use lifecycle, meaning that it will remain warranted and supported for a limited amount of time, after which organisations will be expected to adopt a later version of the agent to remain supported and warranted. The terms of this lifecycle are set out in the ‘Prospective Lifecycle Dates’ section below. Refer to the [WES](https://digital.nhs.uk/services/spine/spine-technical-information-warranted-environment-specification-wes) for the current warranted systems and roadmap.

## Dependencies policy

NHS Digital recognise that trusts have an obligation to maintain currency on their desktop environments. Therefore, the policy on dependencies is based upon an approach whereby a minimum level of component is specified, and the support for newer component levels can be assumed within certain constraints. Where issues do occur with a component version that NHS Digital have not yet certified, then the Trust may be asked to revert to a previous version of the component(s) as part of the fault resolution process. At this point should an update to the identity agent be required to support a specific component version, this will need to be change managed into the identity agent release cycle and may not be resolvable within a normal support timescale.

Not all dependencies have been tested against all other versions of each component. Trusts are responsible for integration testing of components within their own environments, and NHS Digital cannot be held accountable for systems failure arising from a lack of testing or software conflicts.

## Tested components

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 7 SP1, x86 & x64  Windows 8.1, x86 & x64   Windows 10, x64 \*  Windows Server 2008 R2  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

## System requirements

For a full list of system requirements, please refer to the accompanying **NHS Digital Identity Agent v2.x Administration Guide** document.

## Lifecycle policy

NHS Digital Identity Agent v2.x is released with a lifecycle policy that aims to limit the life of the component in line with the Warranted Environment Specification, dependant component lifecycles and a desire to reduce complexity and associated cost within the NHS Digital support remit.

Each released version of the identity agent will have 3 lifecycle stages, defined as:

* Warranted – the identity agent is warranted against central systems and can be adopted by organisations (subject to confirmation from partners it is compatible with their systems), with support from the NHS Digital as outlined within this document.
* Sunset – a new version has been available for some time (min. 12 months). Support is available but depending upon the nature of the issue, the expectation will be to reproduce the issue with a warranted identity agent in the first instance. No code level fixes will be made.
* End-of-Life – the identity agent version is no longer warranted by NHS Digital. It will not be possible for organisations to receive support for issues with an End-of-Life version.

Following the release of a new version of the identity agent, NHS Digital will endeavour to maintain the previous version within ‘warranted’ status for a period of at least one year, with a further one year in ‘sunset’ status. This will provide trusts with a period of up to two years in which to transition to the new version in order to maintain a warranted state, or up to one year for a fully warranted state. 

**Prospective lifecycle dates**

|  |  |
| --- | --- |
| **Lifecycle Stage** |  |
| **Warranted** | As per the date on the front of this document. |
| **Sunset** | **March 2022 to March 2023 inclusive**.  Note: Based upon release schedules and demands from the service, these dates may be amended forward, i.e. to give organisations an extended amount of time to transition. |
| **End-of-Life** | **April 2023 onwards** |

# Known issues

The following tables list any non-critical issues that are known to exist with the current release. The majority of workarounds are further detailed in the NHS Digital Identity Agent v2.x Administrators Guide, section ‘Troubleshooting’ – this is denoted by ‘**TS**’.

## Installation

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ref** | **Description** | **Behaviour** | **Workaround** | **Roadmap** |
| **KE1** | Installing IA v2.x on machines with previous installations of identity agent gives an error. | When trying to install IA v2.x, if the NHS root certificates already exist, the installation can error with:    "The installer has encountered an unexpected error installing this package. This may indicate a problem with this package. The error code is 26352."    This is also known to happen with HSCIC IA v1. | User manually deletes the NHS root certificates and ICA certificates prior to installation of IA v2.  **TS** | This will be considered for resolution in a future release. |

## Terminal services (remote desktops)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ref** | **Description** | **Behaviour** | **Workaround** | **Roadmap** |
| **KE2** | Unable to authenticate using OT cards, from a remote connection. | If logging in using a machine which has the Oberthur software (OT) installed and the remote machine only has Gemalto software installed, the user may get error ‘There was a problem reading your Smartcard’. | Authenticate on machines with a supported middleware mix. **TS** | Currently under investigation. |
| **KE3** | ‘Access denied’ when re-joining a Spine application from remote machine. | If having launched a Spine application (such as DSA or SCR), and access to the same session is attempted from a remote machine, the error ‘Access Denied’ may be received. | Re-launch the Spine application. Save any work prior to switching to a remote session.  **TS** | Currently under investigation. |
| **KE4** | Unable to launch IA v2.x successfully with VMWare Horizon v3.5 or above also installed. | Having installed VMWare Horizon v3.5 and above, IA v2.x may not launch successfully, unless launched as ‘Admin’.    IA v1’s authentication progress bar may hang at ‘Connecting to Spine…’ unless also run as ‘Admin’. | Revert to VMWare Horizon v3.2. **TS** | Currently under investigation. |

## Spine application / Portal

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Ref** | **Description** | **Behaviour** | **Workaround** | | **Roadmap** |
| **KE5** | Unable to access the Spine Portal | When trying to access the Spine Portal, the user receives the error “Unauthorised access is strictly prohibited”.  This can happen when previous versions of Identity Agent have been removed and TicketAPIDll.dll has not been deleted from the Java directory. | Manually delete any copy of TicketAPIDll.dll from C:\Program Files\Java\*installed version*\lib\ext  (Note: Program Files (x86) on a 64 bit system). **TS** | | Automatic deletion of legacy IA files may be considered for a future release. |
| **KE6** | EMIS Web closes down when using ‘Mobility’ mode | When removing the Smartcard in ‘Mobility’ mode, EMIS Web closes down. | Remain in ‘Normal mode’. | | Awaiting feedback from partner. |
| **KE7** | EMIS Web still running after logging out from the reverification form when using ‘Session Lock’ mode | When a user logs out of Spine from the re-verification form or System Tray icon (but with the Smartcard still present), EMIS Web may not close down. | Users can specify to kill EMIS Web on logout via the IA v2.x registry    See setting ‘ProcessesToKill’ in the section ‘Registry Settings’ in the IA v2.x Admin Guide.  Alternatively remain using ‘Normal mode’. | Awaiting feedback from partner. | |
| **KE8** | Unable to associate Smartcards with EMIS Web | When a user is associating a new Smartcard in EMIS Web, error can be received “Login failed: unknown card error”.    This error is also possible whilst using IA v1. | Use a BT IA for EMIS Web Smartcard association. | Awaiting feedback from partner. | |
| **KE9** | Closing Millennium logs user out of Spine | Closing Millennium logs user out of Spine | Use a previous version of Identity Agent known to be compatible with Millennium (according to Cerner, BT IA v7). | Awaiting feedback from partner. | |
| **KE10** | ‘Problem reading your Smartcard’ when locking / unlocking SystmOne, or changing password | If the user has Oberthur middleware installed on the same workstation as SystmOne, then they may get an error ‘There was a problem reading your Smartcard’ with Oberthur Smartcards, when attempting to lock / unlock SystmOne, or when changing the SystmOne password. | Use SystmOne (clinical) and CIS (Identity Access) on separate workstations. | This will be considered for resolution in a future release. | |

## Authentication / logout behaviour

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ref** | **Description** | **Behaviour** | **Workaround** | **Roadmap** |
| **KE11** | Passcode form focus on authentication | Passcode form not always correctly receiving focus on launching (esp. Windows 7 and Windows 10) | User clicks on passcode form to correctly achieve focus. | Identified as an application issue on Windows 7 & 10.    This will be mitigated if possible in a future IA release.  Update: NHS **latest IA v2.3.2.0** has fixed this issue. |
| **KE12** | Slow authentication | Authentication taking a longer time than with BT Identity Agents, especially with Smartcard series 5 and 6 Smartcards. | Migrate to Oberthur Smartcards, which are quicker to authenticate.    Contactless readers also provide faster authentication than contact devices. **TS** | This is a known issue with NHS Digital Identity Agent cryptography and Gemalto Smartcards.   It will be considered for resolution in a future release. |
| **KE13** | ‘Problem reading your Smartcard’ error on initial authentication | On slower set-ups, it has been witnessed that inserting Smartcard, entering passcode and hitting <return> in quick succession can give the error 'There was a problem reading your Smartcard'. | Wait a few seconds before clicking Ok or pressing Enter after entering your passcode. **TS** | This will be considered for full resolution in a future release. |
| **KE14** | Black screen displayed when reverification form shown | In ‘Session Lock’ mode a black screen can appear when the Smartcard is removed, or in ‘Mobility mode’, when a reverification screen appears.  This is caused by Lotus Notes (possibly other applications) switching the user back to the main desktop, which is hidden at that time by a black screen. | Do not use Lotus notes (or other applications which switch the user back to the main desktop).  Alternatively, use ‘Normal mode’.  Confirm application compatibility with local IT support. | Other black screen issues have been resolved, where possible, in the Identity Agent v2.2 and later releases |
| **KE15** | Smartcard locked after two incorrect attempts | Entering two passcodes incorrectly can lock the user's Smartcard (instead of the expected three incorrect passcodes). This is especially the case if removing / re-inserting Smartcards during the incorrect passcode attempts. | See setting ‘CardHealingEnabled’ in the section ‘Registry Settings’ in the IA v2 Admin Guide.  Migrate to using Oberthur (series 8) Smartcards. **TS** | Identity Agent v2.2 onwards now only performs a Gem heal operation on Gemalto cards. This issue no longer affects Series 8 Smartcards |
| **KE16** | Locked passcode form is visible on the main desktop after unlocking from reverify form. | If the machine has a locked Smartcard attempting to be used on the reverify form, the Identity Agent will be see this a locked Smartcard and the link to self-service unlock will be loaded on the primary desktop. This will be visible when the user successfully unlocks their machine.  The same form will also be presented if the user accidentally locks their Smartcard whilst attempting to unlock their machine on the reverify form. | None. Correct functionality | N/A |
| **KE17** | Logged out of Windows when using Session Lock mode | If the user removes their Smartcard when using Session Lock mode and they are using Win81 or Win10, they will be logged out of Windows when the countdown timer reaches zero and the Identity agent attempts to lock Windows | Only remove the Smartcard when the main desktop is showing. Exit the screen saver before removing the Smartcard | Resolved with IA v2.2.2.0  Under investigation as Windows updates may have caused the issue to occur again. Will be investigated further in a future release |
| **KE23** | Logged out when using Normal mode unexpectedly | The timer for the registry setting TimeAllowedLockedUntilLogoffInSeconds is not correctly disabled when running in Normal mode for all versions or Identity Agent from v2.2.1.0 onwards. This causes the user to be logged out of Spine 4h 10m after they first lock their machine. | The issue only affects Normal mode. Use either Enhanced Normal mode, or Session Lock mode. Tablet users can also user Mobility Mode  Set the timer for TimeAllowedLockedUntilLogoffInSeconds to be 28500 in the registry | Resolved with Identity Agent v2.2.3.9 |

## Windows 10

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ref** | **Description** | **Behaviour** | **Workaround** | **Roadmap** |
| **KE18** | Windows 10 lock screen appears as a ‘blank’ screen | Choosing ‘lock’ from any of the IA v2 reverification screens presents the user with a blank screen, rather than the normal Windows 10 lock screen. | Ctrl-Alt-Del brings up the Windows login screen | Identified as a Windows 10 bug when locked with Windows control keys. Microsoft have advised this will be resolved in the 1903 release of W10.  The issue is resolved when using the Lock button on the reverification form. |
| **KE19** | Mode not displayed on the pop up bubble when logging in | When the user logs in, the mode of Identity Agent should be displayed.  Due to the size of the bubble and font used in windows 10, if the trust has a long name there is insufficient space to display the mode | None, the bubble size is fixed | None |

## CMS (Card Management Services) via CIS (Care Identity Service)

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ref** | **Description** | **Behaviour** | **Workaround** | **Roadmap** |
| **KE20** | Two-factor reverification screen appearing during CMS operations | The two-factor re-verification screen can appear during a CMS operation (prompt for insert Smartcard / passcode). During the CMS operation the user is unable to authenticate. The CMS operation completes successfully in the background. | See setting ‘CardRemovalCheck’ in the section ‘Registry Settings’ in the IA v2 Admin Guide. **TS** | This is being actively investigated. |
| **KE21** | Re-authenticating during a session after a self-renewal | User cannot re-authenticate from a locked machine and the reverify from mid-session after a self-renewal as the Smartcard certificates have changed. | After a self-renewal, user should fully log out / back in if locking and unlocking their machine. | None. |
| **KE22** | Please removed all Smartcards error with only one Smartcard | When the user inserts their Smartcard, they are given the error showing there is more than one Smartcard inserted. | This can be due to having a SIM card reader and generic drivers.  Install the correct drivers or disable the SIM card reader. | This issue is now resolved with release v2.2.2.0 onwards. |

## Third Party Application Issues

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Ref** | **Description** | **Behaviour** | **Workaround** | **Roadmap** |
| **KE24** | Unable to perform first time Smartcard association with OT cards on Identity Agent v2.2.3.7 and later | If a new user attempts to perform a first time Smartcard association with EMIS Web on Identity Agent v2.2.3.7 or later, they get a KD-2892009181 error and the association will fail. | Perform the first time Smartcard association with a version of Identity Agent lower than v2.2.3.7 | This issue is being investigated by EMIS as PRB0044107 |

# Notable exclusions

## ‘Mobility mode’

Mobility mode is not designed to support the following functions:

* CMS on Care Identity Service
* Follow-me-sessions
* Fast-user-switching
* Citrix
* VDI (VMWare)

In these cases, it is advised to use Session Lock Persistence for follow me sessions and fast user switching. Either version of normal mode or session persistence can be used in a desktop environment.

**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>

**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>