NHS Digital Identity Agent v2.3.2.0

Administrators Guide

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

**Contents**

[Introduction 4](#_Toc694166911)

[Audience 5](#_Toc1993285062)

[NHS Digital Identity Agent v2.3.2.0 5](#_Toc952047513)

[NHS Digital Identity Agent v2.3.0.0 6](#_Toc19672656)

[Virtual Smartcard Users 6](#_Toc494441913)

[NHS Digital Identity Agent v2.2.3.9 6](#_Toc984952174)

[NHS Digital Identity Agent v2.2.3.7 7](#_Toc640693597)

[NHS Digital Identity Agent v2.2.2.0 7](#_Toc1096352585)

[Multiple Smartcard Error 7](#_Toc2064314463)

[The User is Logged Out of Windows When Their Smartcard is Removed 7](#_Toc1772076001)

[NHS Digital Identity Agent v2.2.1.0 8](#_Toc438637572)

[Oberthur Cache Clear 8](#_Toc1564711866)

[Self Service Unlock Link 9](#_Toc1467524688)

[Citrix Support 9](#_Toc133008895)

[EnableNHSEnrollment Flag 10](#_Toc976593085)

[Normal mode 10](#_Toc619551426)

[NHS Certificates 10](#_Toc1389100596)

[Software & documentation 11](#_Toc1785732418)

[Important Considerations 11](#_Toc943193653)

[System Requirements 11](#_Toc986155145)

[Middleware 11](#_Toc1046844563)

[Other components 12](#_Toc1792008183)

[Usage Scenarios 12](#_Toc1615315129)

[Operating Systems 13](#_Toc1635758628)

[Environments 13](#_Toc1435907618)

[Smartcards 13](#_Toc2085619808)

[Middleware Requirement Matrix 14](#_Toc1648369969)

[Deployment 15](#_Toc1148718102)

[Configuration 18](#_Toc36439711)

[Registry Settings 20](#_Toc660919218)

[\*\*Config Themes 23](#_Toc591200201)

[Spine Environments 23](#_Toc1632135108)

[Series 4 Smartcards 24](#_Toc856431529)

[Windows 7 “Device driver software was not successfully installed” 25](#_Toc829152031)

[Windows 2008r2 “Device driver software was not successfully installed” 26](#_Toc1367778411)

[Troubleshooting 27](#_Toc109374580)

[Installation 27](#_Toc1655109746)

[Authentication 27](#_Toc327248265)

[Following Java upgrade (‘Java Runtime Error’) 27](#_Toc1820943933)

[‘You have been logged out…’ 28](#_Toc334378253)

[Following Smartcard issue / update 29](#_Toc1131143663)

[Following abnormal termination of an Oberthur CMS operation (‘Invalid Signature’) 29](#_Toc1931956094)

[Slow authentication 30](#_Toc769992448)

[‘There was a problem reading your Smartcard….’ 30](#_Toc979943379)

[Renew performed on a different machine to the one the user is using for authentication 30](#_Toc367661394)

[Smartcard content has been incorrectly generated during issuance (Series 8) 31](#_Toc1602955575)

[\*The above is left in for historic reference as all RA renewals of Oberthur cards are now done by SR8 following the deprecation of SR1 / SR5.Invalid / missing middleware 31](#_Toc893710237)

[‘Gem Heal’ required 31](#_Toc918033420)

[Slower machines 31](#_Toc958752938)

[Reboot your machine 32](#_Toc1062517440)

[The Smartcard is blank 32](#_Toc138751146)

[Incorrect Smartcard Reader Drivers 32](#_Toc91021595)

[Incorrect Registry TrustedCertificateIssuers 32](#_Toc2120289381)

[‘3606: [AuthValidate] Failed to validate user’ 33](#_Toc524262901)

[Wrong environment 33](#_Toc2106689297)

[Deleted / Closed User 33](#_Toc1989898945)

[‘The remote name could not be resolved’ 33](#_Toc1090269305)

[‘Certificate Error’ 34](#_Toc474028091)

[Following installation of VMWare – Horizon 3.5 and above 34](#_Toc1282075866)

[‘Could not establish trust relationship for the SSL/TLS secure channel’ 34](#_Toc276367784)

[‘This app can’t be activated when UAC is disabled’ 35](#_Toc1434043049)

[Multiple Smartcard Errors – “Phantom Smartcards” 36](#_Toc1850991289)

[Unable to authenticate following self-renew with Oberthur Smartcards 37](#_Toc940418885)

[Series 8 Smartcard renewal is not currently supported on this machine 38](#_Toc1049057046)

[Yubikey presents Identity Agent popup dialog box 39](#_Toc459219118)

[Passcodes 40](#_Toc503231606)

[Smartcard locked after two incorrect passcode entries 40](#_Toc6416018)

[Logging out 40](#_Toc1172706932)

[All browser windows shutting down 40](#_Toc1775317016)

[Unexpected logout 40](#_Toc1180205770)

[Unexpected logout of Windows 41](#_Toc1252728752)

[Follow-me-sessions (RDP) 41](#_Toc222595380)

[Re-joining a Spine application over RDP (‘Access Denied’) 41](#_Toc95040361)

[Re-authenticating after re-joining a Spine session (‘There was a problem reading your Smartcard…’) 41](#_Toc1734190691)

[CPU at 100% on remote session 42](#_Toc919920812)

[Follow-Me-Sessions and Normal or Mobility modes 42](#_Toc1732919606)

[The Smartcard is not the correct one for this session …… 42](#_Toc1178214969)

[Follow-me-sessions (VDI) 43](#_Toc859506715)

[Follow-me-sessions (RDP) 43](#_Toc1373943066)

[Fast-User-Switching 43](#_Toc1458708841)

[Issues with CMS (via CIS) 43](#_Toc1294394510)

[‘Reverification’ screen appearing during CMS operations 44](#_Toc1844496626)

[‘Failed to delete key container’ or ‘Failed to create keys’ during CMS operations 44](#_Toc94916171)

[Java crashes whilst performing CMS operations 45](#_Toc92081948)

[Connectivity 47](#_Toc447753337)

[Firewall settings 47](#_Toc1895117924)

[DNS Checks 47](#_Toc568491051)

[Proxy and Routing Checks 48](#_Toc1322188014)

[Issues with EMIS Web 49](#_Toc56071886)

[No Popup Bubble After Logging In 50](#_Toc777166859)

# 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 device in a hospital, GP surgery, or other organisation where a clinical role is performed.

The latest NHS Digital Identity Agent v2.x has been designed to provide more secure and convenient ways of working with identity access than previous versions, through the introduction of authentication using Citrix / VDI / Terminal Services, including bug fixes for Windows 10 and correctly enforcing the precedence order for Mobility/Session Lock/Enhanced Normal Mode/Normal Mode.

## Audience

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

# NHS Digital Identity Agent v2.3.2.0

This release of NHS Digital Identity Agent Version is a bug fix 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.
* 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

# NHS Digital Identity Agent v2.3.0.0

This release of NHS Digital Identity Agent Version is a bug fix 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.
* Revision to the security updates on Smartcard removal.

## Virtual Smartcard Users

* 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.

# NHS Digital Identity Agent v2.2.3.9

This release of NHS Digital Identity Agent Version is a bug fix release which resolves the following issue. There are no new features added with this release.

* Users being logged out.
  + All users of Identity Agent from v2.2.1.0 onwards using Normal mode only 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.

# NHS Digital Identity Agent v2.2.3.7

This release of NHS Digital Identity Agent Version is a bug fix release which resolves the following issues. There are no new features added with this release.

* 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. This issue is now resolved.

# NHS Digital Identity Agent v2.2.2.0

This release of NHS Digital Identity Agent is a minor update to the previous release (NHS Digital Identity Agent v2.2.1.0) and NHS Digital Identity Agent v2.2.2.0 introduces the following resolutions to issues:

## Multiple Smartcard Error

There have been multiple reports from users with machines running Windows 10 build 1803 or later with mobile SIM readers in the machine that Identity Agent gives an error of multiple Smartcards being inserted when the user attempts to authenticate, or the PIN form is launched when the user first logs into Windows and no Smartcards are inserted. We believe this is down to the drivers for the SIM card reader now being part of Windows rather than provided by the hardware manufacturer and Windows presents the mobile SIM card as an additional Smartcard.

This build of Identity Agent now ignores the mobile SIM card as a Smartcard to alleviate this issue.

## The User is Logged Out of Windows When Their Smartcard is Removed

Under the following circumstances, the user can be logged out of Windows rather than the machine being locked if their Smartcard is removed.

1. Session lock is enabled
2. Windows is displaying a screensaver
3. Windows is at version 8.1 or higher

In the above circumstances, the user will get logged out of Windows rather than the Lock/Logout form being displayed when the Smartcard is removed.

This build of Identity Agent now correctly displays the Lock/Logout form when the user removes their Smartcard in the above circumstances.

# NHS Digital Identity Agent v2.2.1.0

Since Identity Agent v.2.2.1.0 (v2.2) was only launched towards the end of 2018, all the features and enhancements introduced by this version are also listed below for completeness.

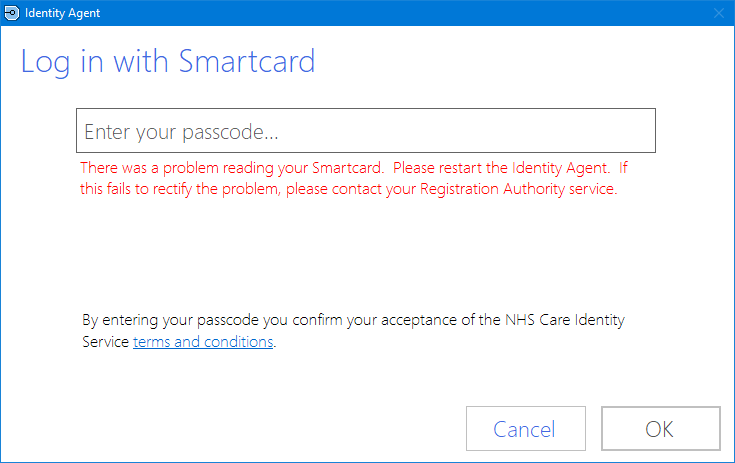
## Oberthur Cache Clear

If there is a problem reading a Series 8 (Oberthur) Smartcard during authentication, with previous versions of either HSCIC Identity Agent v1 or NHS Digital Identity Agent v2.x, the user would have received the message “There is a problem reading you Smartcard. Please remove and reinsert it”. Now, the Identity Agent will run the cache clearance process when a Smartcard is inserted and attempt to read the Smartcard again before giving the user an error message.

This functionality is applicable only for users with both Oberthur Middleware installed and Series 8 Smartcards.

NOTE: Due to how the logic works internally, if a user is in the situation where they have locked their Smartcard and it also requires a cache clear on their machine, the user will get the “Problem reading Smartcard” error rather than the expected locked Smartcard error. The user needs to have their Smartcard unlocked by their RA and then the Identity Agent will be able to perform cache clearance successfully.

In the event the cache cleaning fails for any reason (or the Smartcard is blank), the user will be given the message below to retry. Should this fail, the user will now need to visit their RA.

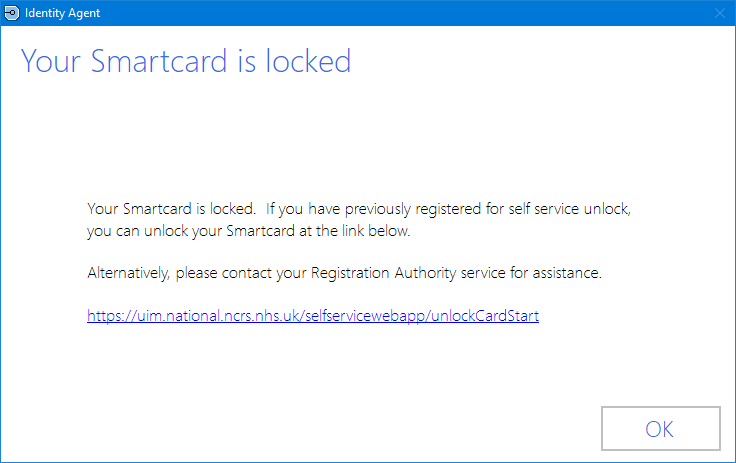


## Self Service Unlock Link

If the user tries to use a locked Smartcard or locks the Smartcard due to too many incorrect PIN entries when trying to authenticate, the Identity Agent now displays a form with a link to the automated Smartcard unlock service.

The URL link supplied by the Identity Agent is for the live unlock service and will not change to redirecting the user to the Path-to-Live environments regardless of registry settings.

NOTE: At the time of writing, the link below is **ONLY** applicable to physical Smartcards. Users with a locked Entrust Virtual Smartcard will need visit their RA Manager and have their existing virtual Smartcard de-registered and then re-register for a new virtual Smartcard.



## Citrix Support

The Identity Agent now supports authentication over Citrix.

**Only authentication is supported**. Any other CMS activities, e.g. User or RA functions, including self-renew are not supported via this method.

Additional registry changes are also required to support Citrix. See Registry Settings for further information.

It is required to enable Card Reader Polling. It is also suggested that Card Healing is disabled when using Citrix.

The configuration of the Citrix environment to support USB pass through and all other configuration is outside of the scope of this document. The Citrix client needs to have the correct Smartcard reader drivers installed from the manufacturer as the generic ones can cause issues.

## EnableNHSEnrollment Flag

If a CMS operation on an Oberthur Smartcard is prematurely terminated (such as by removing any Smartcard, or a system crash), then subsequently attempting authentication with **any** Oberthur Smartcard can give the error ‘Invalid Signature’.

If the registry key HKCU\Software\Oberthur Technologies\Minidriver\PIVMinidriver\EnableNHSEnrollment exists with any value other than 0, Identity Agent v2.2.1.0 and above now set this value to 0 every time a Smartcard is inserted to avoid users getting the above error.

The user will not see any difference during authentication as this is dynamic change in registry.

If this registry key does not exist, the Identity Agent continues without generating an error.

## Normal mode

By default (without any registry configuration), NHS Digital Identity Agent v2.2.and above will operate in ‘Normal mode’. This is a legacy-style mode of operation, whereby removing a Smartcard automatically and immediately terminates the Spine session.

Identity Agent v2.2 and above now also operates in the legacy-style mode if the user locks and then subsequently unlocks their machine with the Smartcard still inserted in, then the user is taken directly back to their desktop without the need to re-enter the PIN for the Smartcard. This change has been made following feedback from the previous version of Identity Agent.

It is still possible to force the user to enter their PIN when locking and unlocking their machine if required by use of a registry key. See Registry Settings for more information on EnhancedNormalMode. Multiple incorrect passcode attempts at this point will lock the user’s Smartcard.

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

## NHS Certificates

New SubCA certificates for the live platform. Extra certificates are now installed during the installation of Identity Agent to enable the user to continue authenticating when the live certificates are updated in the future.

# 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>

Ensure the certificates are placed into the correct store, do not follow the defaults  
RootCA. Place into Trusted Root Certification Authorities  
SubCA. Place into Intermediate Certification Authorities

# 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 and set the registry key for TrustedCertificateIssuers.**

# System Requirements

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

## Middleware

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

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

\* Oberthur Middleware SR8 provides the ability to perform all RA functions and so should be used for any new installations. Oberthur Middleware versions SR1 and SR5 are now deprecated and are blocked from performing any certificate-based operations. Any users with either of these Middleware versions are strongly recommended to upgrade to SR8 or they will not be able to update their Smartcard when the certificates expire.

\* Users without any version of Oberthur Middleware can self-renew their Smartcard via PKCS11# (the self-renew process on machines with only Gemalto Middleware). Users with BT Identity Agent will have only one applet renewed but any users using any version of HSCIC or NHS Digital Identity Agents both applets will be renewed.

## Other components

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

\*\* Optional components

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

# Usage Scenarios

## Operating Systems

The following operating systems are warranted for use:

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

## Environments

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

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

The use of the Identity Agent under other environments such as Citrix / VDI / Terminal Services is supported, but for authentication only. Any CMS activities under these configurations are **NOT** supported; this also includes self-renewal. The details on how to configure these environments is outside of the scope of this document. The value **UseCardReaderPolling** needs to be set to True to allow the Smartcard details to pass to the Citrix environment.

It is also recommended to turn off card healing when working on remote environments. See Registry Settings section for further information on the value **CardHealingEnabled**.

# Smartcards

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

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

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

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

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

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

**3** Compatible with contact readers only. This precludes authentication on tablet devices using NFC technology.

**4** Physical Windows 8.1 and Windows 10 machines only. Entrust Virtual Smartcards are not currently warranted for use in any virtualised environment. The Entrust Virtual Smartcard also does not yet support digital signing and therefore cannot be used to sign prescriptions.

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

# Middleware Requirement Matrix

Despite Series 8 Smartcards and Oberthur Middleware being in circulation for over four years at the time of writing, there is still confusion and mixed messages over what the requirements are to perform day to day functions. Refer to the matrix below for what is actually required.

|  |  |  |
| --- | --- | --- |
| **Activity** | **Smartcard Version** | |
|  | Gemalto Series 4/5/6 | Oberthur Series 8 |
| **RA Activities** | NHSD Identity Agent | |
| **Issue & Print Smartcard** | Gemalto | Min Oberthur SR8**1** |
| **Renew Smartcard** | Gemalto | Min Oberthur SR8**1** |
| **Repair Smartcard** | Gemalto | Min Oberthur SR8 **1** |
| **Change PIN** | Gemalto | Gemalto |
| **Unlock Smartcard** | Gemalto | Gemalto |
| **Cancel Smartcard** | Gemalto | Min Oberthur SR8 **1** |
| **Print Only** | Gemalto | Gemalto |
| **Self-renew Smartcard** | Gemalto | Gemalto **2, 3** |
| **Self-change PIN** | Gemalto | Gemalto |
| **Self Service Unlock** | Gemalto | Gemalto |
| **Authentication** | Gemalto | Gemalto |

**1** SR1 and SR5 are now blocked from performing certificate-based operations. All users performing RA activities on Series 8 Smartcards need to install Oberthur Middleware SR8.

**2** If the user has performed a self-renew when they have only Gemalto Middleware and BT IA installed, this renewal will update the certificates on the compatibility applet only. The user will not be able to authenticate on a system with Oberthur Middleware after the original certificate expiry and within the expiry window they will be prompted to renew, which they will be unable to do. Now users with HSCIC IAv1, NHSD IA v2.0 or later will have both applets renewed with only Gemalto middleware system.

**3** If the user has either SR1 or SR5 Middleware installed, this will stop them being able to perform a self-renew. Either remove SR1 / SR5 or update to SR8. Refer to the Oberthur Installation Guide on the DIR site on how to do this.

NOTE: SR1 and SR5 Middleware are now blocked from performing any CMS operations. It is recommended that users with SR1 or SR5 Middleware update as soon as possible to SR8 Middleware, or for non-RA users remove Oberthur Middleware or no certificate-based operations will function. This **will not** affect the user’s ability to authenticate; only CMS operations are affected.

As can be seen from the above matrix, only users performing RA functions on Series 8 (OT) Smartcards need to install Oberthur Middleware. All user-based activities on any Smartcard type can be completed with just Gemalto Middleware.

All versions of BT Identity Agent are incompatible with Oberthur Middleware and any user performing RA functions will need to install the latest NHS Digital Identity Agent v2.x in addition to SR8 Oberthur Middleware.

# Deployment

*For detailed assistance please refer to the latest NHS Digital Identity Agent v2.x Installation Guide.*

NHS Digital Identity Agent v2.x is packaged as a discrete .msi and includes the components:

* Identity Agent
* Root CA certificates for production (including updated Sub CA certs 1C & 1D) and optionally NIS1 (inc. all path-to-live)
* GATicket.jar (Java applet component used by portal applications)

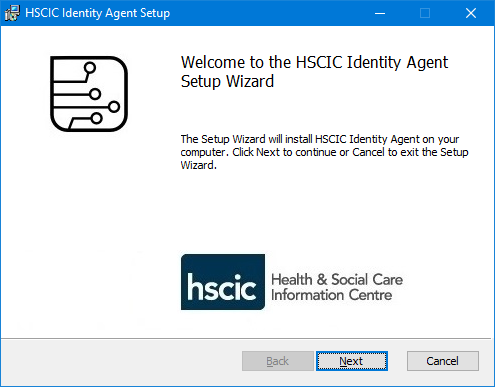
Other dependencies as listed in the [System Requirements](#_System_Requirements) section must be installed separately and before the installation of the Identity Agent package.

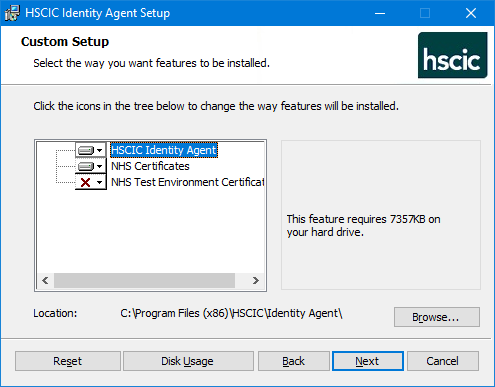
**Note: Uninstallation of any previous version of Identity Agent prior to installation of the latest NHS Digital Identity Agent v2.x (\*) is *strongly recommended*. Failure to do so may cause issues authenticating with Spine when using the new version of Identity Agent. Identity Agent does not currently remove any previous versions of Identity Agent during the installation process.**

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

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

Installation is a straightforward process using the Windows Installer framework (msiexec), however installation of the program does require administrative rights.





The ‘Custom Setup’ screen defaults to the likely options that would be used in a production environment. As such, the core Identity Agent is installed along with the certificates needed for the production environment. By default, the ‘NHS Test Environment Certificates’ feature is not selected for installation as these would typically only be required for development or test purposes.  
  
For a scenario where switching between production and pre-production environments is required then installation of both the ‘NHS Certificates’ and ‘NHS NIS1 Certificates’ at the same time is valid.

The agent supports a silent installation using standard deployment toolsets that recognise .msi packages, or if installing via a script the following command line can be used:

%SystemRoot%\System32\msiexec.exe /i "NHS-Digital-Identity-Agent-2.x.msi" /qn

Although the default configuration will satisfy the requirements for most installation scenarios, each feature can be included as part of a silent install by specifying the additional parameter as:

%SystemRoot%\System32\msiexec.exe /i "NHS-Digital-Identity-Agent-2.x.msi" ADDLOCAL=*featurenames* /qn

Where *featurenames* is a comma separated list using the ‘Component ID’ values from the below table. E.g. ADDLOCAL=IA,CertsTest.

|  |  |  |
| --- | --- | --- |
| Feature Name | Component ID | Description |
| HSCIC Identity Agent | IA | Main product feature \* |
| NHS Certificates for Production | CertsProd | Required for production environments |
| NHS Certificates for NIS1 | CertsTest | Only required for test / development (PTL) |

Once installed, launch the program through the ‘Identity Agent’ icon in the Programs | Identity Agent area of the Start Menu, or on Windows 8.1 / Windows 10 through the ‘Identity Agent’ icon on the Applications screen. Identity Agent will automatically start when the user logs into Windows subsequently.

\* If the user is performing a command line installation using the ADDLOCAL option, ensure that “IA” is included along with the required certificates. If ADDLOCAL is not used, by default Identity Agent and Production certificates will be installed.

# Configuration

The agent is supplied with built-in defaults for all settings, meaning that by default there will be no settings present in the registry (including the directory path). The built-in defaults can be largely overridden through the application of specific registry values either directly or via Group Policy settings using an Administrative Template.   
  
**Note:** The location for registry settings matches that of HSCIC Identity Agent v1 / NHS Digital Identity Agent v2.x and this differs from BT Identity Agent registry locations. Any admin or ‘environment switcher’ type tools will need to be updated to reflect these locations.

**Note:** On a new Identity Agent installation, there will be no registry entries created in the registry locations described further down in this document. The user will need to manually create the sub trees in the registry for first use. If the user is not sure of the entries to make, it is suggested that the Registry Editor Tool is downloaded from the [**DIR website**](https://nww.digital.nhs.uk/dir/downloads/)and the user selects to authenticate against Live. This will create the required sub trees in the registry. Admin rights are required to run the tool.

The Identity Agent will attempt to read settings from three separate areas of the registry. The locations have different purposes, and this is reflected in the order in which they are prioritised. The priority order is controlled by Windows and not the Identity Agent.

* **Set by Group Policy** – these settings will be applied by group policy. System administrators can create their own temple(s) from the registry setting information provided in this document for policy rollout if required. You should not attempt to create or modify settings manually or via a script in this part of the registry. These settings will always take precedence.
* **All Users (Local Machine)** – these settings are machine-wide and will apply to any user who logs in to the system. The settings will remain machine specific, meaning that a user will always adopt these in preference to user settings.
* **Current User** – these settings apply only to the current logged in user and will persist with the user profile. If the user has a roaming profile, then the settings will travel with the user between machines.

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

Please review the settings below to ensure that they are appropriate for your configuration, and that the secure operation of any other application that exposes patient identifiable or sensitive data under a Spine authentication context is considered.

**Notes**

* Subsequent to making registry changes, stop / restart NHS Digital Identity Agent v2.x to allow them to take effect as not all registry changes are dynamic.
* Without any explicit registry settings, NHS Digital Identity Agent v2.x will operate under ‘Normal Mode’ and will authenticate against the live Spine environment and close all Web browsers on logging out of Spine.
* To enable Mobility mode, set ‘**MobilityPersistence\_Available**’ to ‘true’. The mode is then toggled ‘on’ and ‘off’ from the passcode form (‘Work with Smartcard removed’) on a per login basis, the previous setting is not retained, and the default is always set to off. \*
* To enable Session Lock mode, set ‘**SessionLockPersistence\_Enabled**’ to ‘true’.
* To enable Enhanced Normal mode, set ‘**EnhancedNormalMode**’ to ‘true’. This will make Identity Agent v2.x behave in the same manner as Identity Agent v2.1.2.16 did running in Normal Mode.
* If any of the above settings are changed in the registry, they operate in the order of precedence in the order they are described above.
* On logging out of Spine, NHS Digital Identity Agent v2.x is configured by default to close **all** the following browsers running under the current user context: IE.x, Chrome, Firefox. To alter this behaviour, consider using the ‘ProcessesToKill’ registry key detailed below.
* The ‘**RoleSelectionGETPOSTURL**’ and ‘**LogoffPOSTURL**’ entries are no longer required as NHS Digital Identity Agent v2.x now derives these programmatically.

\* 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.

## Registry Settings

|  |  |  |
| --- | --- | --- |
| Setting | Default | Purpose |
| ActivatePOSTURL  (REG\_SZ) | <https://gas.national.ncrs.nhs.uk/login/authactivate>  Built into the IA | The Spine URL where activate / challenge requests are sent. |
| LaunchAppsType (REG\_SZ) | *None* | Used to launch applications upon successful authentication. Options are ‘none’, ‘directory’ or ‘files’. If ‘none’ is selected, no applications are launched.   If ‘files’ is selected, the files or URLs specified in LaunchAppsPath are launched. (e.g: set this to “Files” and LaunchAppsPath to the portal URL).  If ‘directory’ is selected a shell execute will be attempted on all non-hidden files in the specified directory. |
| LaunchAppsPath  (REG\_SZ) | *None* | If ‘files’ is specified for LaunchAppsType, this will be either a semi-colon delimited set of paths to launch applications or URI’s. If ‘directory’ is specified, this will be a single path for the directory in question. A typical entry would be the URL for the Spine Portal. |
| EnableTrainingOption (REG\_SZ) | false | If enabled the training mode option is displayed on the passcode form. |
| IdleWaitPeriodInSeconds  (REG\_DWORD) | 1800 | The time (in seconds) that the user session is allowed to be idle before it ‘Windows locks’ the screen (1800s = 30m).  **IT Administrators** might want to review this timing in relation to individual needs within the service.  No maximum value.  This timer is active in ‘Session Lock’ and ‘Normal’ modes, and ‘Mobility mode’ whilst the Smartcard is present. In ‘Mobility mode’ whilst the Smartcard is removed, the Identity Agent v2.x mobility idle timer takes over and ‘IdleWaitPeriodInSeconds’ is stopped. |
| TimeAllowedLockedUntilLogoffInSeconds (REG\_SZ) | 15000 | The time (in seconds) that the user is allowed to maintain a locked (Windows) screen before the user is logged out of Spine (15000s = 4h 10m).  Maximum value is 28500. Values higher than this will be ignored, and force set to 28500.  **IT Administrators** might want to review this timing in relation to individual needs within the service. |
| MobilityPersistence\_Available (REG\_SZ) | false | If enabled, this setting makes the mobility persistence toggle available on the passcode form. Possible values are ‘false’ and ‘true’. |
| ConfigTheme\*\* (REG\_SZ) | Default | Defines the theme for timers used in ‘Mobility mode’. Possible values are ‘Off’, ‘Minimal’, ‘Medium’, ‘Maximum’.   The settings associated with each theme are defined in the ‘[Config Themes](#_*Config_Themes)’ section below. |
| SessionLockPersistence\_Enabled (REG\_SZ) | false | Switch on session lock persistence. Possible values are ‘false” and ‘true’.   Setting this value to ‘false’, or removing the key, enables the Identity Agent to operate under ‘Normal mode’. |
| ProcessesToKill  (REG\_SZ) | java;iexplore;firefox;chrome | The names of executables to kill when a Smartcard is removed, or another logoff event occurs. This can / should include the names of native Spine applications (non-browser) to ensure IG standards are adhered to.  Note: Do not add the .exe to the end of the process you want to kill. |
| SmartcardReaderDeniedList  (REG\_SZ) | MICROSOFT UICC ISO READER;WINDOWS HELLO FOR BUSINESS; | There is a currently undocumented feature in the Identity Agent that allows certain devices to be ignored as potential card readers.  To add a reader to the list, provide the name separated by a semi-colon for example:- adding a YubiKey should look like  MICROSOFT UICC ISO READER;WINDOWS HELLO FOR BUSINESS;Yubico YubiKey |
| NoRolesLogoff  (REG\_SZ) | true | Action to take if a user attempts to login with no roles assigned. If set to ‘true’ a log out will occur, otherwise the user will remain logged in. |
|  |  |  |
| CardRemovalCheck  (REG\_SZ) | true | This registry entry should be placed with a value of ‘false’ by RA / RAMs performing CMS on CIS, in order to resolve Known Issue KE20 in the Identity Agent v2.x Release Notes. |
| TrustedCertificateIssuers  (REG\_SZ) | ***None*** | By default, the user’s personal certificate store is cleared on successful Spine authentication.  If the user requires the presence of certificates other than those required for Spine authentication, place the following value for this registry entry:  **LIVE**  CN=NHS Level 1C, OU=CA, O=nhs;CN=NHS Level 1D, OU=CA, O=nhs;CN=NHS Authentication G2, OU=CA, O=nhs, C=GB;CN=NHS Signing G2, OU=CA, O=nhs, C=GB  For the test environments, place the following value in the registry:  **INT**  CN=NHS INT Authentication G2,OU=CA,O=nhs,C=GB;CN=NHS INT Signing G2,OU=CA,O=nhs,C=GB |
| CardHealingEnabled  (REG\_SZ) | true | By default, GemHeal is enabled and will check and attempt to heal a Gemalto Series 4/5/6 Smartcard on each login by the user.  This is unlikely to need modifying, however it may resolve issues with the GemHeal module, if advised so. \* |
| EnhancedNormalMode  (REG\_SZ) | false | By default, Normal mode is enabled, and the user does not have to enter their PIN on unlocking Windows when their Smartcard is left inserted and logged into Spine during the lock/unlock operation.  Setting to true will enforce the user requiring their passcode on unlocking Windows in the same manner as the previous version of Identity Agent. |
| UseCardReaderPolling  (REG\_SZ) | false | By default, card reader polling is disabled. Set this value to true to allow the Identity Agent to poll card readers when using Citrix environments. \* |

\* When working in Citrix environments it is recommended to set CardHealingEnabled to false on the Citrix client machine. Restart Identity Agent when the setting has been changed.

### \*\*Config Themes

A key feature of ‘Mobility mode’ is that the user is periodically asked to re-authenticate, either by one-factor (presenting the Smartcard), or by two-factor (presenting the Smartcard and passcode)

The timings of these events can be specified by the use of ‘Config Themes’ - pre-set collections of mobility timer settings. The possible registry values for this setting are ‘off’ (default), ‘Minimal’, ‘Medium’, and ‘Maximum’. The individual values for these timers are described below:

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

## Spine Environments

The Identity Agent can be configured to operate against alternate environments through the use of registry settings.

This table lists the Path-to-Live environments and their respective settings:

|  |  |
| --- | --- |
| Registry setting | Value |
| Environment: NIS1 (INT) |  |
| ActivatePOSTURL | <https://gas.nis1.national.ncrs.nhs.uk/login/authactivate> |
| Environment: VNIS1 (DEP) |  |
| ActivatePOSTURL | https://gas.vn1.national.ncrs.nhs.uk/login/authactivate |
| Environment: TSP (TRAINING) |  |
| ActivatePOSTURL | https://gas.tsp.national.ncrs.nhs.uk/login/authactivate |
| Environment: Live |  |
| ActivatePOSTURL | https://gas.national.ncrs.nhs.uk/login/authactivate |

**Note**

* The value for Live is listed for reference only, it is not necessary to present an ActivatePOSTURL value in the registry to authenticate against the live environment.

In the event that the certificates for Path-to-Live are updated, the latest certificates for the environments can be downloaded from the URL below. Follow the link for ‘Root and SubCA Certificates’.

<https://digital.nhs.uk/services/path-to-live-environments>

These certificates need to go into the correct certificate stores for all users on the machines and require administrative rights to install them. Please contact your local ICT department to arrange this.

A simple to use tool (IA Registry Editor Tool v1.2) is available from the [DIR website](https://nww.digital.nhs.uk/dir/downloads/) to quickly update registry setting to switch between environments. Please note, this tool requires Admin rights to update the registry.

## Series 4 Smartcards

Series 4 Smartcards do not have a driver in the Windows driver library, and as such will prompt for driver installation when used. This does not impact the functionality of the Smartcard as it is accessed directly through the Gemalto Middleware; it is however unsightly and may raise additional support calls from users.

To resolve this, you will need the ’004 Card.inf’ file held on the [DIR website](https://nww.digital.nhs.uk/dir/downloads/) (‘Identity Agent Supporting Components’).

The following steps need to be completed under an administrative context.

|  |  |  |
| --- | --- | --- |
| Step | Objective | Process |
| 1 | Manually associate the Series 4 card .inf file | * Insert a Series 4 Smartcard * Open **Device Manager** * Locate **Other devices | Smart Card** * Right click **Smart Card** and select **Update Driver Software…** * Select **Browse my computer for driver software** * Select **Let me pick from a list of device drivers on my computer** * Click **Next** * Click **Have Disk…** * On the **Install From Disk** window, click **Browse…** * Navigate to the folder where **004 Card.inf** is stored * Select **004 Card.inf**, and click **Open** * Click **OK** * A warning is shown indicating that **This driver is not digitally signed!** * Click **Next** * A further warning is displayed. Click **Yes** * Another warning is now displayed. Click **Install this driver software anyway** * Finally a success message should be displayed. Click **Close** * Observe in **Device Manager** that there is now a **Smart cards | Generic Smart card** object |

## Windows 7 “Device driver software was not successfully installed”

On some Windows 7 machines, the user may get an error in the system tray with the text “Device driver software was not successfully installed. Click here for details”

This is due to Windows attempting to install the Smartcard as a device on the system and failing to find the correct driver as one does not exist.

System administrators can resolve this problem by adding a registry value in the following locations:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | Registry Key | Name | Type | Value |
| 32-bit machine | HKLM\SOFTWARE\Policies\Microsoft\ Windows\ScPnP | EnableScPnP | REG\_DWORD | 0 |
| 64-bit machine | HKLM\SOFTWARE\Policies\Microsoft\ Windows\ScPnP  HKLM\SOFTWARE\Wow6432Node\Policies\ Microsoft\Windows\ScPnP | EnableScPnP  EnableScPnP | REG\_DWORD  REG\_DWORD | 0  0 |

From the command line with and admin CMD window, the following command can be run:

|  |  |
| --- | --- |
| 32-bit machine | reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\ScPnP" /t REG\_DWORD /v EnableScPnP /d 0 /f |
| 64-bit machine | reg add "HKLM\SOFTWARE\Policies\Microsoft\Windows\ScPnP" /t REG\_DWORD /v EnableScPnP /d 0 /f  reg add "HKLM\SOFTWARE\Wow6432Node\Policies\Microsoft\Windows\ScPnP" /t REG\_DWORD /v EnableScPnP /d 0 /f |

## Windows 2008r2 “Device driver software was not successfully installed”

The issue is the same as above with Windows 7, however the server operating system requires a different method to resolve. Further information can be found on the Microsoft website at the URL below.

<https://support.microsoft.com/en-us/help/976832/error-message-when-you-insert-a-smart-card-in-a-reader-on-a-windows-7>

The information below is an extract from the site on how to make this change via group policy. A restart or logging out and back in may be required for the change to take effect.

To disable Smart Card Plug and Play in local Group Policy, follow these steps:

1. Click **Start**, type gpedit.msc in the **Search programs and files** box, and then press ENTER.
2. In the console tree under **Computer Configuration**, click **Administrative Templates**.
3. In the details pane, double-click **Windows Components**, and then double-click **Smart Card**.
4. Right-click **Turn on Smart Card Plug and Play service**, and then click **Edit**.
5. Click **Disabled**, and then click **OK**.

# Troubleshooting

## Installation

When attempting to install NHS Digital Identity Agent v2.x (or HSCIC Identity Agent v1), the following error may occur:



The installation is then rolled back. This is seen to be caused when trusts have previously pushed the NHS certificates (both Root and SubCa) to the NTAuth store via Group Policy, on a previous Identity Agent installation or during the machine build process. This causes the Identity Agent v2.x installer to error when trying to overwrite them.

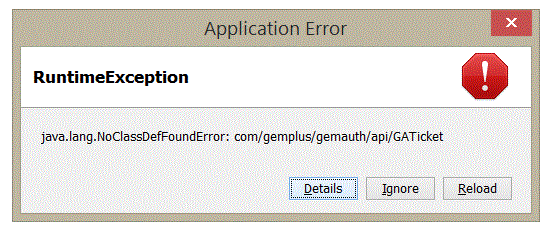
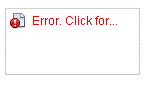
This issue can also be caused by the Admin account being used not fully uninstalling the previous version of Identity Agent.

To resolve this, on the next attempt to install the Identity Agent, ‘uncheck’ the option for ‘NHS Certificates’ on the ‘Custom Setup’ screen. The install process will then not attempt to install the certificates (they already exist), and the installation should complete successfully.

NOTE: If the trust does install the NHS certificates in this manner that Identity Agent v2.x has additional new SubCA certificates. These will need extracting and adding to the build moving forwards or the users will no longer be able to authenticate when the live certificates are updated.

## Authentication

### Following Java upgrade (‘Java Runtime Error’)

Following a Java version upgrade on a user’s local machine (for example from Java 7 to 8), the following errors may be seen after authenticating and accessing the Portal (or similar errors when accessing Spine systems):  
  
  
  
This is caused by Java creating a new directory structure, but not copying the required custom file GATicket.jar to the new location.

Simply locate the file (GATicket.jar) in the original directory location for Identity Agent, such as:   
C:\Program Files (x86)\HSCIC\Identity Agent – Remove the (x86) on 32-bit machines  
  
and copy to the new location, such as:  
C:\Program Files (x86)\java\jre1.8.0\_251\lib\ext

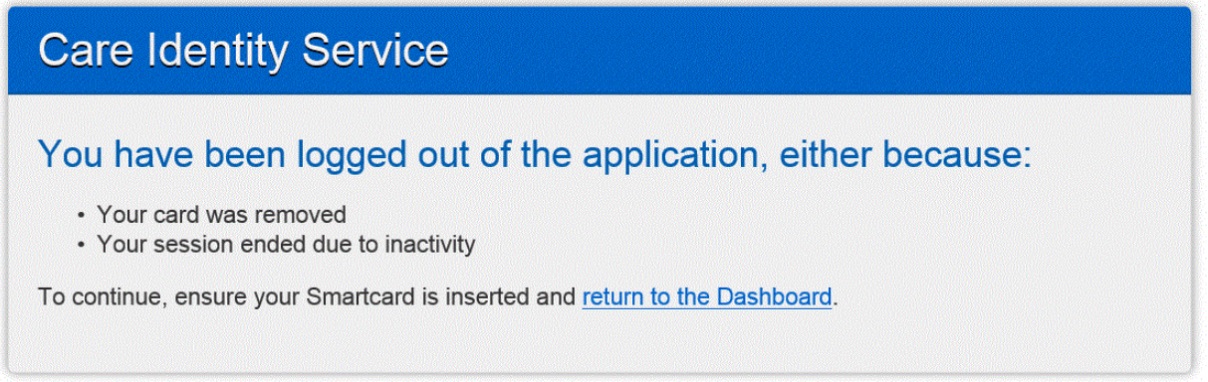
Restart Identity Agent v2.x and attempt re-authentication.

Administrative access may be required to copy this file.

It has been reported that users upgrading to Java 1.8.181 and higher have had the entire contents of the previous Java directory deleted. This will also remove GATicket.jar. If this occurs, the file can be copied from the installation directory of Identity Agent located at C:\Program Files(x86)\HSCIC\Identity Agent. The file needs copying in the directory C:\Program Files(x86)\Java\jre.x\lib\ext. On 32-bit systems, the (x86) part will be absent on the Program Files directory structure. Administrative access may be required to copy this file.

### ‘You have been logged out…’

Following uninstallation of a BT Identity Agent and subsequent installation of any version of NHS Digital Identity Agent, the following error may be seen whilst authenticating and accessing the Portal (or similar errors when accessing Spine systems):



This may be caused by an old version of the file ‘Ticketapidll.dll’ left behind by the BT Identity Agent, in the Java directory structure, e.g. in:  
  
c:\program files\java\jre6\lib\ext\

c:\program files\java\jre6\lib\ext\x86\  
  
This file should be removed, as NHS Digital Identity Agent v2.x will inadvertently attempt to use it. (It should instead **only** have access to a more recent version of the file, which should have already been placed into the following directory structures on installation:

C:\Windows\System32 (32-bit machines)

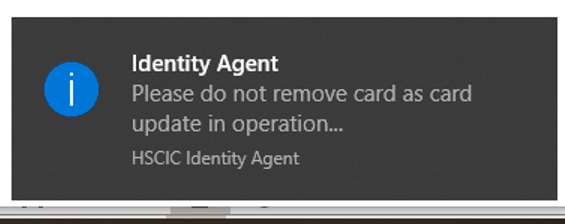
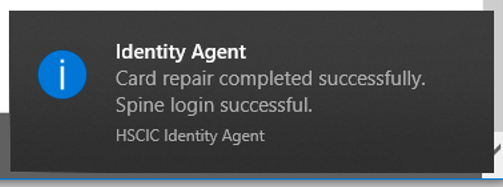
C:\Windows\SysWow64 (64-bit machines)  
  
After the errant file has been removed, restart Identity Agent v2.x, and attempt re-authentication.

Administrative access may be required to delete this file.

This issue may also be caused immediately after a Java upgrade – in which case please see section [following Java upgrade](#_Following_Java_upgrade).

### Following Smartcard issue / update

On first use of a Gemalto Smartcard, or after any renewal or repair, it is likely that the Identity Agent will perform an update on the Smartcard using the ‘Gem Heal’ process. A pop-up box is given to the user to notify the start and end of these activities.

It is **important** that the Smartcard is not removed during this operation otherwise the Smartcard could be rendered inoperable (various errors) necessitating the user to obtain a replacement Smartcard to be able to login.

### Following abnormal termination of an Oberthur CMS operation (‘Invalid Signature’)

If a CMS operation on an Oberthur Smartcard is prematurely terminated (such as by removing any Smartcard, or a system crash), then subsequently attempting authentication with **any** Oberthur Smartcard can give the error ‘Invalid Signature’.

In this case it is almost certain that a registry key has been ‘flipped’ during the CMS operation, but because the process did not fully complete, the registry key did not ‘flip back’.

Navigate to:   
*HKEY\_CURRENT\_USER\SOFTWARE\Oberthur Technologies\Minidriver\ PIVMinidriver*      
and in there you should find a key named '**EnableNHSEnrollment**". If this is set to '1', this is the culprit. Set it to '0' and you should see immediate results.

Identity Agent from v2.2.1.0 onwards now set this value to 0 each time a Smartcard is inserted if the above registry value exists to stop the issue from occurring. The troubleshooting information above is left in for reference only for any users of previous Identity Agent versions.

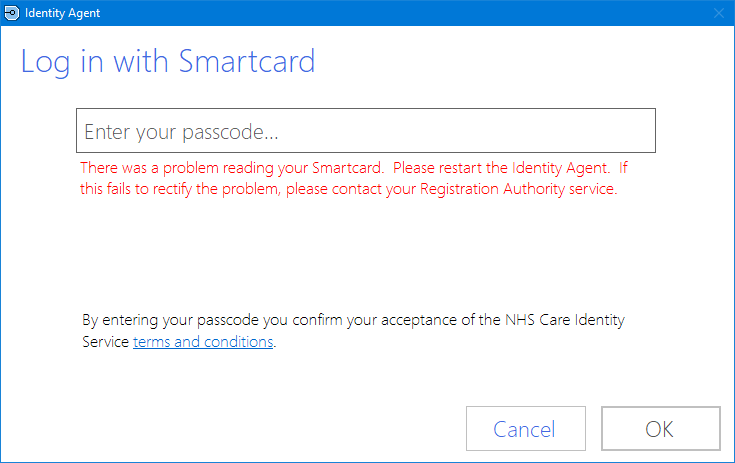
### Slow authentication

NHS Digital Identity Agent v2.x is quicker to authenticate than HSCIC Identity Agent v1. However, users may consider it is slower to authenticate than with BT Identity Agents.

This is particularly noticeable with Gemalto Series 5 and 6 Smartcards. This is owing to the type of cryptography inherited from Identity Agent v1.

Users may consider migrating to Series 8 (Oberthur) Smartcards, as they allow the quickest possible method of authentication, regardless of the type of Identity Agent in use. Also, contactless Smartcard readers are faster to authenticate than contact Smartcard readers.

### ‘There was a problem reading your Smartcard….’



This error may be generated due to a variety of reasons, as explained in the sections below:

### Renew performed on a different machine to the one the user is using for authentication

There is a known issue whereby when the Smartcard is renewed on a different machine to the one the user is trying to authenticate with, e.g. by an RA renew/repair, the machine holds a cache of the original certificates for the Smartcard. When the updated Smartcard is attempted to be read, the cache and current certificates do not match, and the above error can be given. Identity Agent v2.x intercepts this message and runs a built-in version of the cache clearance tool available from the DIR site. It then attempts to re-read the Smartcard. The user is only given the message if Identity Agent still cannot read the Smartcard following cache clearance. It may be necessary to run this tool more than once and restart Identity Agent to correctly clear the cache and resolve the issue.

### Smartcard content has been incorrectly generated during issuance (Series 8)

There are known issues with Oberthur Middleware (both ‘SR1’ and ‘SR5’), whereby Series 8 Smartcards are not generated properly, despite apparent success during the RA issuance process. This is more likely to be noticeable on workstations with just Gemalto Middleware installed (so any testing performed by the RA on their own machine, *with* Oberthur Middleware installed, may not manifest the issue). SR8 Middleware went live in June 2018 and RA users performing CMS operations are strongly advised to upgrade to this version as this resolves the issues previously seen with SR1 and SR5 issuing Series 8 Smartcards.

#### \*The above is left in for historic reference as all RA renewals of Oberthur cards are now done by SR8 following the deprecation of SR1 / SR5. Invalid / missing middleware

If authenticating after immediately installing NHS Digital Identity Agent v2.x, missing Middleware is the most likely cause of this error.

If a user is migrating from BT Identity Agent to NHS Digital Identity Agent, be aware that uninstalling BT Identity Agent will also uninstall the machine’s Gemalto Middleware at the same time. The Middleware will need to be re-installed prior to attempting to authenticate and is available from the [DIR website](https://nww.digital.nhs.uk/dir/downloads/) (in the vast majority of cases, only Gemalto Middleware is required).

If the user has and Oberthur (Series 8) Smartcard, these can be used for authentication and self-service operations with just Gemalto Middleware installed.

**Only users performing CMS operations (within the CIS application) against Oberthur Smartcards as the ‘subject card’ will require both types of Middleware (Gemalto and Oberthur)**. Again, these components can be retrieved from the [DIR website](https://nww.digital.nhs.uk/dir/downloads/).

#### ‘Gem Heal’ required

When a Smartcard is first issued, it may be in a state where a “Gem Heal” is required. A potential fix for this is to ‘heal’ the Smartcard using the Classic Client Toolbox (available on most machines that have Gemalto Middleware installed). Go to ‘Card Properties’, select the reader for the Smartcard, log in with the Smartcard PIN code, select ‘Advance’, select ‘Diagnosis’ – which heals the Smartcard if required. Identity Agent v2.x now only attempts to perform a Gem Heal on Gemalto Series 4/5/6 cards.

One last option for performing a Gem Heal is to authenticate using the Smartcard in a machine which has BT Identity Agent v13 installed. This version of Identity Agent reads the card in a different manner to Identity Agent v2.x, so may be able to authenticate with problematic Smartcards – it also performs ‘Gem Heal’ on problematic Smartcards after authentication so this may resolve the issue.

#### Slower machines

It has been observed that rapid user entry of the passcode can cause this error on slower set-ups, particularly when using virtual machines / remote connections.

In this case, simply delay entry of the passcode by a few seconds by waiting for the Smartcard reader to finish reading the information on the Smartcard prior to entering the PIN. This issue is being investigated.

#### Reboot your machine

We have seen caching issues causing Smartcards to be unreadable until the machine has had a clean restart. This should, hopefully, no longer be required as Identity Agent v2.x has a built-in version of the standalone cache clearance tool.

#### The Smartcard is blank

The above error will also be given if for any reason, the user attempts to authenticate with a blank Smartcard.

#### Incorrect Smartcard Reader Drivers

With the later builds of Windows 10, by default, the wrong drivers are being installed for the Omnikey 3121 Smartcard reader (installed as a 3021) which can cause a variety of issues from the card being unable to be read to CMS activities failing.

If you experience any of these issues after getting a new machine, check the correct drivers have been installed. Run the CIS diagnostic tool and look at the .txt file on your desktop. The tool is available from <https://nww.digital.nhs.uk/dir/downloads/>. Check if the OmniKey 3121 Smartcard reader driver is shown as a 3021 CCID reader. If it is, download and install the correct drivers, from the link above and re-run the report. The Omnikey 3121 Smartcard reader driver should now have the correct drivers installed.

#### Incorrect Registry TrustedCertificateIssuers

There is a small chance that users authenticating with a smartcard that has been issued, renewed, or repaired after the CIS release on Wednesday 25 January 2023 receive the following error.

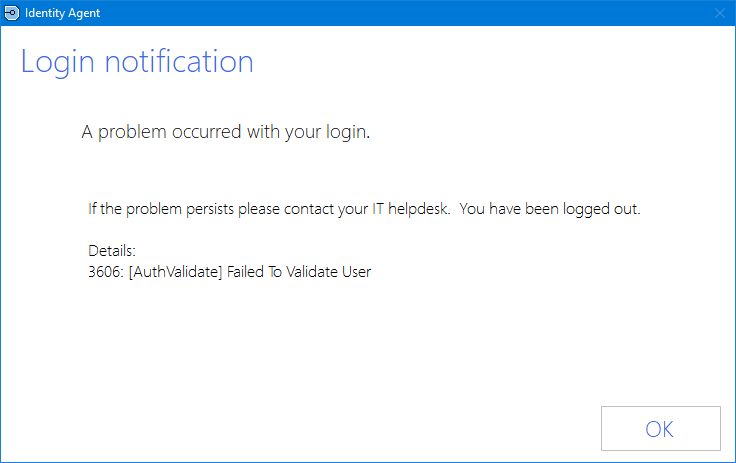
Modify the registry entry to include the following value:

|  |  |
| --- | --- |
| Name | Value |
| TrustedCertificateIssuers | CN=NHS Level 1C, OU=CA, O=nhs;CN=NHS Level 1D, OU=CA, O=nhs;CN=NHS Authentication G2, OU=CA, O=nhs, C=GB;CN=NHS Signing G2, OU=CA, O=nhs, C=GB |

This registry entry is found in the following locations:

* **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

#### ‘3606: [AuthValidate] Failed to validate user’



This error shown above may be generated for one of two reasons:

#### Wrong environment

The user may have attempted to log into the wrong environment, for example using a Smartcard for Live when their machine is configured to connect to a test environment, or vice versa.

To resolve this, modify the registry keys given in the [Spine Environments](#_Spine_Environments) section of this document, or download the IA Registry Editor tool V1.0 from the [DIR website](https://nww.digital.nhs.uk/dir/downloads/). For accessing Live, it is recommended to delete any environment-specific registry keys and allow Identity Agent to use the default live setting.

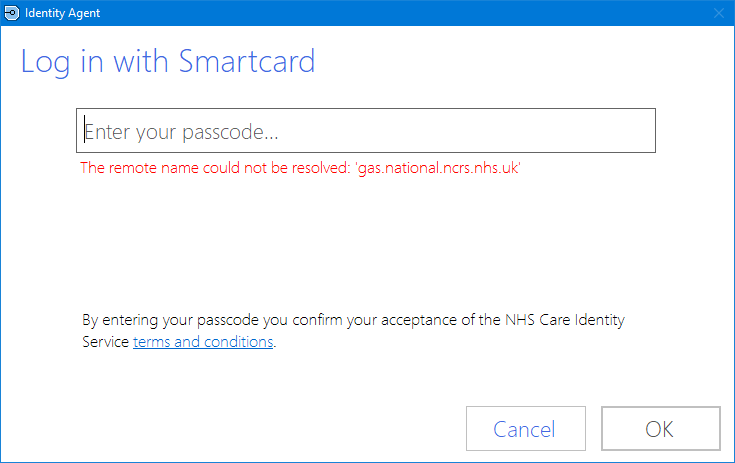
#### Deleted / Closed User

The user may have been deleted or closed in Spine. The user will need to be re-opened or a new user created. In either case, any positions assigned to the user will need to be added again and a new Smartcard issued for the user.

#### ‘The remote name could not be resolved’

The error shown below will be generated if there is a network connectivity issue, DNS issue, or the environment the user is attempting to connect to is offline. The URL will differ depending on the environment.

The issue could also occur is the user is working remotely and has not established a VPN connection into their trust as the Spine network is not directly internet accessible.



If the user has network connectivity issues, they should raise a support call with their local IT support help desk.

#### ‘Certificate Error’

This error can follow the self-renewal of a Smartcard through the CIS application, and indicates there have been problems writing the new certificate(s), even though a success message has been given to the user.

The Smartcard will need to be either repaired or cancelled and then re-issued by an RA Agent / Manager.

#### Following installation of VMWare – Horizon 3.5 and above

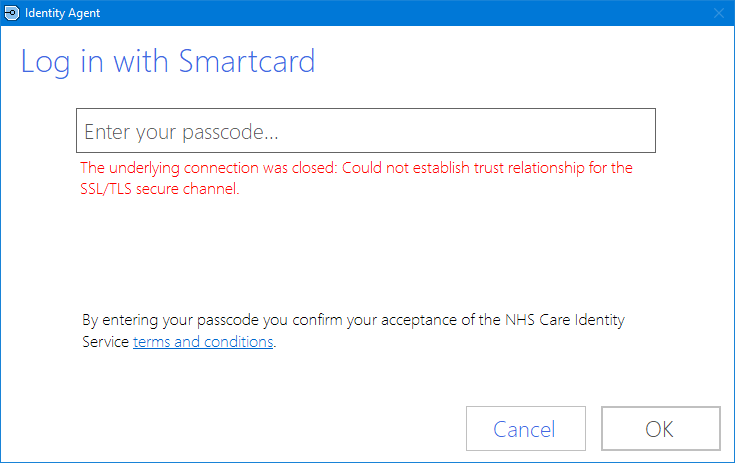
Installing Horizon VMWare v3.5 or above on a machine can prevent reliable authentication with all version of the NHS Digital Identity Agent unless the Identity Agent is launched as Administrator. (BT Identity Agents unproven).

HSCIC Identity Agent v1: 'Progress' bar on authentication hangs (unless the Identity Agent launched as ‘Admin’)  
NHS Digital Identity Agent v2.x: Fails to launch successfully (unless the Identity Agent is launched as ‘Admin’)

Resolution: Attempt to revert back to Horizon VMWare 3.2. If this fails to work, we have seen cases where the machine needs to have a complete refresh of Windows to resolve the issue.

This issue is under investigation.

#### ‘Could not establish trust relationship for the SSL/TLS secure channel’



This error is likely caused by not checking the ‘NHS Test Environment Certificates’ option on installation and attempting to connect to a Path-To-Live environment (test / development).

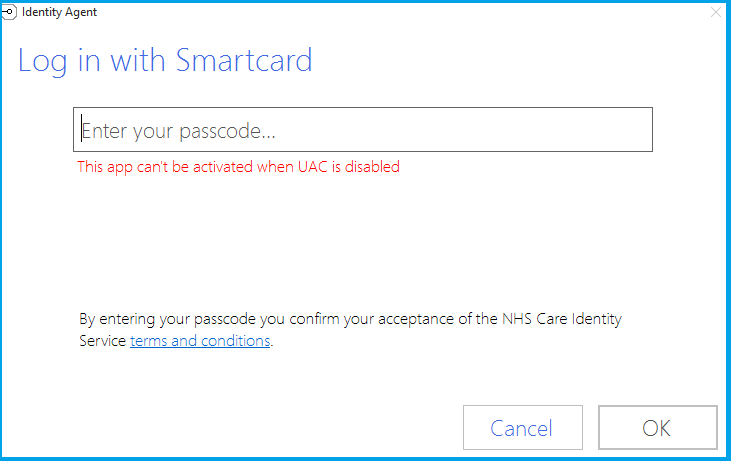
Simply uninstall, and re-install, or repair checking this option.

The Path-to-Live certificates have expired. See section [Spine Environments](#_Spine_Environments) to download and install the latest certificates for the environment you want to connect to.

Alternatively, the wrong URL is being used in the registry, again for Path-To-Live environments. See section [Spine Environments](#_Spine_Environments).

If during the installation of Identity Agent, the default options were changes, the live certificates may not have been installed. The same issue could also occur with a command line installation if the user did not specify the live certificates.

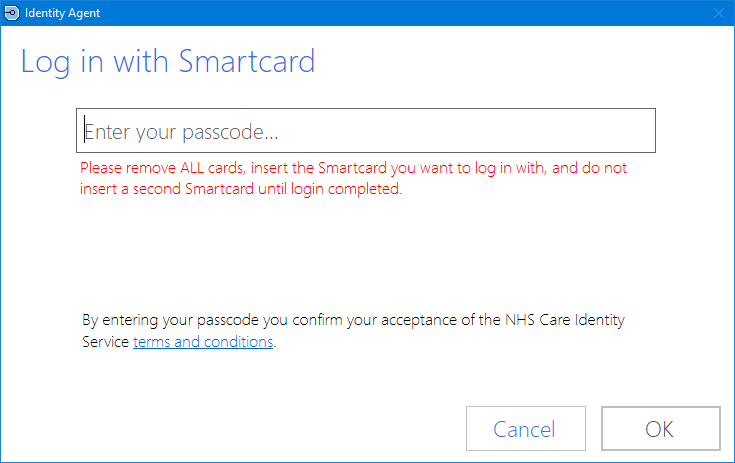
#### ‘This app can’t be activated when UAC is disabled’



This error can occur on Windows 10, where ‘Edge’ is set as the default browser and UAC is turned off. Edge requires UAC to be turned on, so this is not an Identity Agent v2.x error, but the error is communicated by Identity Agent v2.x during authentication.

#### Multiple Smartcard Errors – “Phantom Smartcards”

In a small number of cases, the user may get an error when attempting to authenticate advising them to remove all Smartcards and just insert the one they wish to login with (see below). This may occur when the user only has one Smartcard reader or Smartcard inserted.



There can be a multitude of reasons for this error:

1. The user has a HP keyboard Smartcard reader, but they are using the generic Microsoft Windows CCID drivers. This can be resolved by installing the correct manufacturer drivers for the keyboard reader
2. A SIM card reader is installed. The issue can be resolved by disabling this as a Smartcard reader \*
3. An SD card reader is installed. The issue can be resolved by disabling this reader.

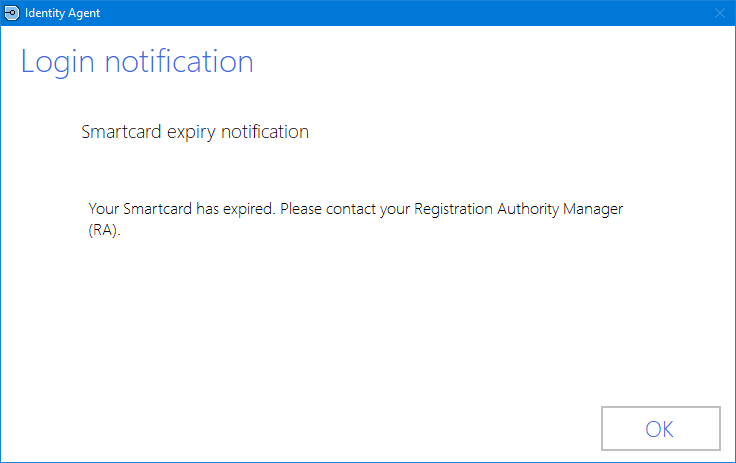
There have also been reports that when a user attempts to change their passcode, CMS reports more Smartcards than there actually are, despite the user logging in successfully. The resolutions are the same as above, in addition, if a user is using an external OmniKey reader, ensure the correct drivers have been installed for this reader.

\* The SIM card reader can be disabled in the registry at the following locations  
HKLM\Software\Microsoft\Cryptography\Calais\Readers  
HKLM\Software\Wow6432Node\Microsoft\Cryptography\Calais\Readers  
Identify the SIM card from the list of objects and change the value of “Groups” to DONOTUSE.

This issue should now be resolved with Identity Agent v2.x and the information above is mainly left in for historic purposes. However, there is always the chance that new hardware will start to exhibit the same behaviour when first launched. If this is the case, follow the advice above until such time as a new version of Identity Agent is launched rectifying the problem.

Disabling the SIM card reader as a Smartcard reader will stop the mobile SIM card being treated as a Smartcard reader by the Identity Agent and allow the user to authenticate but could also affect other applications which make use of the mobile SIM card in this way. Check with your local ICT department before making any changes.

#### **Unable to authenticate following self-renew with Oberthur Smartcards**

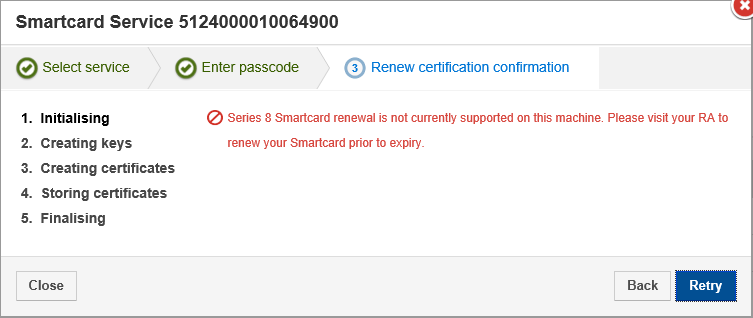


When a user performs a self-renew operation, this can be done in one of two ways:  
  
1. CSP using Oberthur Middleware

2. PKCS#11 on machines without Oberthur Middleware  
  
If the user has performed the self-renew on a machine with Oberthur Middleware SR8 installed, they will renew all the certificates on the Smartcard in both of the ‘agile’ and ‘compatibility’ containers and there should be no problems.

If the user has performed a self-renew on a machine without Oberthur Middleware using BT Identity Agent, they will renew their Smartcard using PKCS#11 and this only renews the certificates on the ‘compatibility applet’ of the Smartcard. This means that the original ‘agile applet’ certificates (the ones read when a machine has Oberthur Middleware) will remain in the same ‘about to’, or now ‘expired’ state.   
  
This is not an issue if the user authenticates on a machine *without* Oberthur Middleware as the compatibility applet is used here, and these certificates are valid. However, if the user attempts to subsequently authenticate on a machine with Oberthur Middleware (causing the ‘agile applet’ certificates to be read), they may either get the pop-up box stating the certificates are about to expire, or if they attempt to authenticate post expiry of these certificates, they will not be able to authenticate. If the user does get the certificate expiry warning, they will not be able to renew their Smartcards if they have previously just completed this activity on a machine without Oberthur Middleware.

#### Series 8 Smartcard renewal is not currently supported on this machine



The user will get the error ‘Series 8 Smartcard renewal is not currently supported on this machine……’ if they have set the value of ‘CardRemovalCheck’ to ‘true’ in one of the following Identity Agent registry locations  
Deployed to Policies : HKLM\SOFTWARE\Policies\HSCIC\Identity Agent  
Deployed to Local Machine (64 bit OS) : HKLM\SOFTWARE\Wow6432Node\HSCIC\Identity Agent   
Deployed to Local Machine (32 bit OS) : HKLM\SOFTWARE\HSCIC\Identity Agent

This is because the renewal process needs to set the ‘CardRemovalCheck’ value to ‘false’, but only has access to the HKCU area of the registry and the above areas take priority when set.

To resolve the issue, either remove the ‘CardRemovalCheck’ registry key or set the value to false. Restart Identity Agent after the change has been made. Refer to [Registry Settings](#_Registry_Settings) for more information.

#### Yubikey presents Identity Agent popup dialog box

Graphical user interface, text, application, email

Description automatically generated

This has been observed for Yubikey 5 NFC devices. It occurs because the IA 'recognizes' the device as a smartcard reader with a smartcard inserted - this is due to the fact that the devices have the capability to act as a PIV card.

To resolve this issue, please see under Registry Settings the entry - SmartcardReaderDeniedList

## Passcodes

### Smartcard locked after two incorrect passcode entries

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.

To stop this from happening, set ‘CardHealingEnabled’ to ‘false’ in the registry (see ‘[Registry Settings](#_Registry_Settings)’). Remember to restart Identity Agent v2.x after any registry changes.

This issue is under investigation but is related to Gem heal and should not affect Series 8 (Oberthur) Smartcards with Identity Agent v2.2.1.0 and higher.

## Logging out

### All browser windows shutting down

By default, (without any registry configuration) NHS Digital Identity Agent v2.x will close all browsers on logging out.

However, NHS Digital Identity Agent v2.x can be configured to only close a specific browser type (IE, Firefox, Chrome) by listing them in the registry setting ‘**ProcessesToKill**’ (see section [Registry Settings](#_Registry_Settings)).

Note: Only the process name is required, do not add the .exe on the end of the process name as this will stop Identity Agent closing the process.  
  
It is understood that BT Identity Agents could be configured in such a way that only the browser windows launched as part of authentication are closed down on logging out. However, this allowed potential IG issues, in that any browser windows not closed could in theory be used to continue to access or view Spine data, despite having logged out.

### Unexpected logout

Aside from the manual forms of Spine session logout (which vary between mode, see the Identity Agent v2.x User Guide), NHS Digital Identity Agent v2.x will also perform a Spine logout in the following conditions:

* Windows unlocked 3 times consecutively, without also re-authenticating into Spine with the Smartcard Passcode when using mobility mode, session lock or enhanced normal modes.
* Being sat on the Windows lock screen for over four hours. This time period is configurable (see ‘TimeAllowedLockedUntilLogoffInSecond’ in section [Registry Settings](#_Registry_Settings)).
* The Spine session lasting in excess of twelve hours, this is common to all Identity Agents and cannot be changed as this timer is controlled on the server backend and will occur whether the session is being actively used or the machine is locked.

### Unexpected logout of Windows

It is possible to get logged out of Windows under the following circumstances.  
The machine is running W81 (x86 or x64) or W10-x64, Session Lock mode is enabled, Windows screen saver is being displayed and the user removes their Smartcard.  
When the above occurs, the IA should switch the user to the Lock/Logout screen and the countdown timer is in operation to auto lock the machine. However, from the screen saver screen, W81 & W10 do not switch to the secure desktop to allow this occur correctly. This results in an error in the IA when the countdown timer reaches zero and the user is logged out of Windows rather than a machine lock occurring.

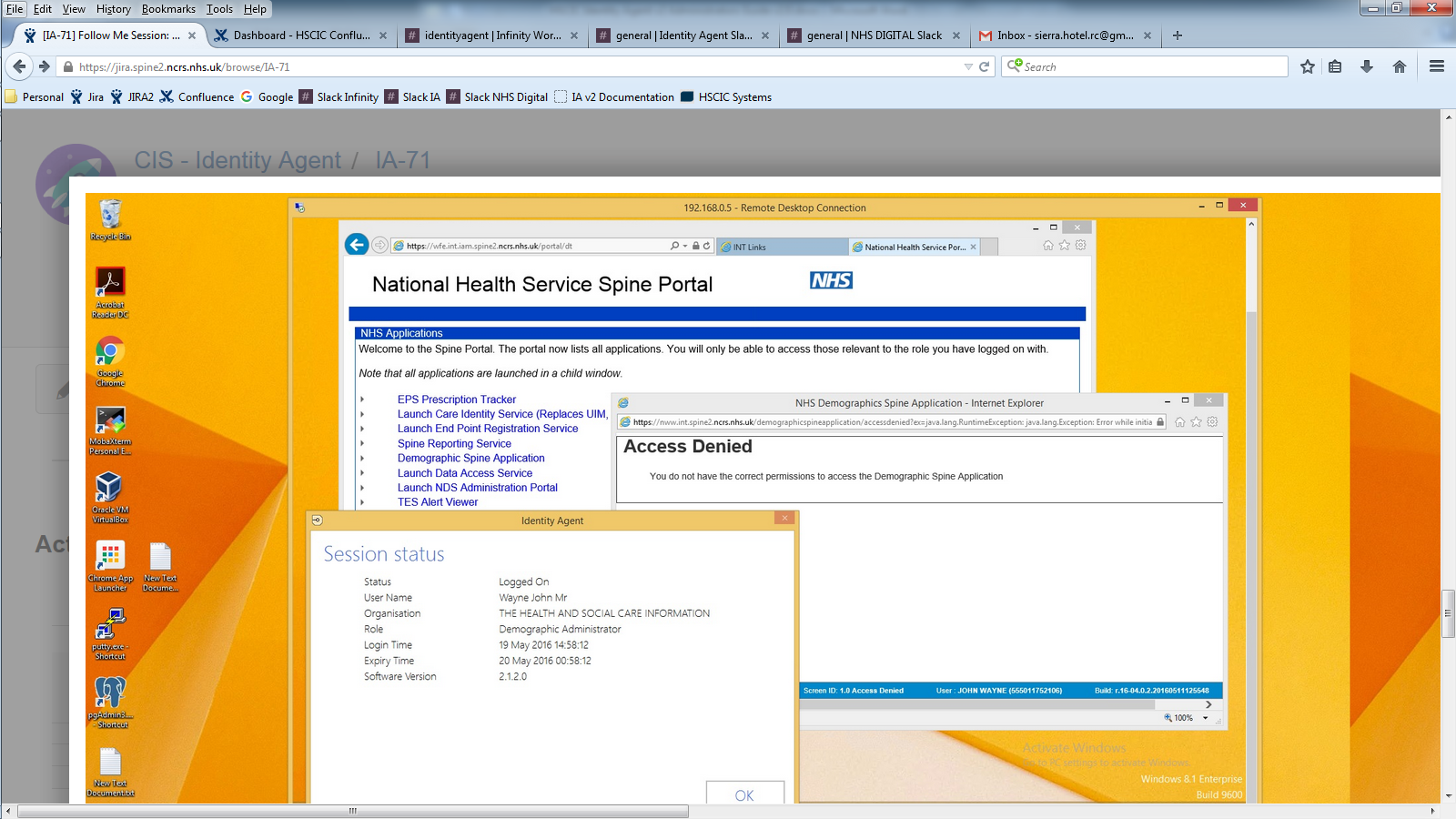
To prevent this issue occurring, ensure the Smartcard is removed only on the main desktop to allow the Lock/Logout screen to be correctly displayed.

This issue is now resolved with Identity Agent v2.2.2.0 and the above is left in for historic purposes only.

## Follow-me-sessions (RDP)

### Re-joining a Spine application over RDP (‘Access Denied’)

If having launched a Spine application (such as DSA or SCR), and access to the same session is attempted over an RDP connection, an error similar to the following may be received:



This is caused by the ‘named pipe server’ on the Identity Agent creating a new session name at the same time the Spine application is performing a ‘heartbeat’ check on the validity of your session. Re-launching the Spine application should be successful.

It is therefore recommended to save your work between switching workstations, to guard against any loss of work.

This is a known issue and will be considered for resolution in a future version.

### Re-authenticating after re-joining a Spine session (‘There was a problem reading your Smartcard…’)

If having authenticated into Spine, and access to the same session is attempted over a remote connection, the error may be received ‘There was a problem reading your Smartcard….’.

Ordinarily re-trying the passcode, or re-seating your Smartcard and entering the passcode again, will resolve this.

However, this issue can consistently happen when a user’s local machine has been configured with the Oberthur Middleware and associated registry changes, and the VDI systems do **not** have the Oberthur software installed. This issue is currently under investigation, and the table below shows the mix-and-match of installed software for RDP / VDI functionality:

|  |  |  |
| --- | --- | --- |
| Local machine | Remote machine / VDI | Permitted |
| GEM only | GEM only | YES |
| GEM only | GEM and OT | **NO** |
| GEM and OT | Gem only | **NO** |
| GEM and OT | GEM and OT | YES |

It is recommended that if local machines are updated with Oberthur Middleware, that all VDI machines also received the software updates at the same time to avoid any potential issues with the users being able to login using RDP / VDI.

Please be aware that whilst Oberthur Middleware can be installed on the remote machine, CMS activities are not supported via this connection type.

### CPU at 100% on remote session

It has been reported that the most common form of Gemalto Middleware (Classic Client 6.1 Patch 3), if used remotely (over Terminal Services or VMWare VDI for example), can lead to ‘services.exe’ using 100% of CPU, on that remote session.

This is apparently resolved by Gemalto Classic Client 6.2 Patch 1. However, this is not available on an NHS-wide license, so if Trusts require this Middleware upgrade, they should investigate licensing this product independently.

### Follow-Me-Sessions and Normal or Mobility modes

It is recommended that ‘Session Lock’ mode is used when working with ‘Follow-Me-Sessions’ (Remote Desktop). The use of ‘Mobility mode’ is not recommended as this functionality is aimed at the use of tablet machines only (rather than transferring to / from desktop machines). The use of ‘Normal mode’ or ‘Enhanced Normal Mode’ would log the user out of their Spine session upon removal of the Smartcard.

### The Smartcard is not the correct one for this session ……

If the user has either Session Persistence or Mobility modes enabled, and they have performed a self-renew during their current Spine session it is possible to get the above error when attempting to re-verify when unlocking their machine. This is due to the Identity Agent caching the Smartcard certificates at the initial logon and the certificates have changed following a self-renewal. Simply logout of Spine and back in to resolve the issue. The problem will not occur the next time the user logs in.

## 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.

## Follow-me-sessions (RDP)

Introduced in v2.1.2.16, follow-me-sessions (remote desktop RDP) is 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.

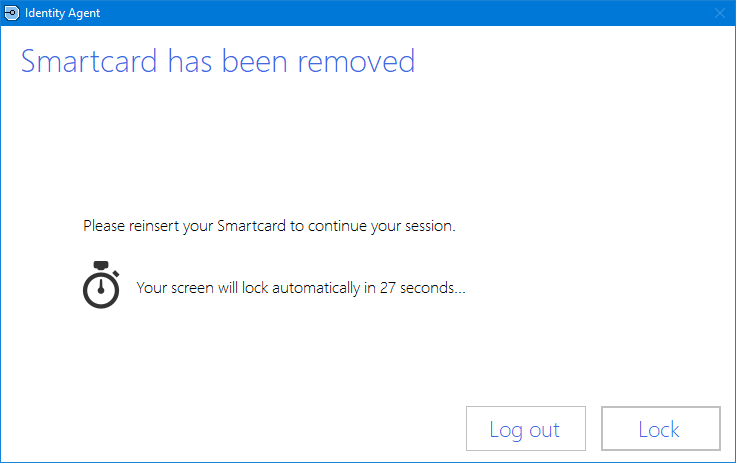
Check with your local IT department that your applications are compatible with Session Lock Persistence mode prior to making any changes

## Fast-User-Switching

It is recommended that ‘Session Lock’ mode is used when wanting to use Windows fast-user-switching to allow the sharing of a single PC resource. The use of ‘Mobility mode’ is not recommended as this functionality is aimed at a single user of tablet machines only (rather than running multiple Windows accounts on a single tablet). The use of ‘Normal mode’ or ‘Enhanced Normal Mode’ would log the user out of their Spine session upon removal of the Smartcard.

## Issues with CMS (via CIS)

### ‘Reverification’ screen appearing during CMS operations



During a CMS operation in CIS (such as issuance, repair, renewal), the ‘reverification’ screen may appear, effectively blocking the desktop. If an attempt is made to re-authenticate, they will receive an error indicating that two Smartcards are present. The Smartcard operation is still actually being performed in the background, so ask the user to:

1. Wait until the card reader for the target Smartcard stops flashing
2. Remove the target Smartcard
3. Remove the authenticated RA / RAM Smartcard

The user should be able to re-authenticate at this point, and the operation on the target Smartcard should have completed successfully.

More importantly, to prevent this happening in future the user should place the entry ‘**CardRemovalCheck = False**’ in the registry and set the value to ‘false’ (see section ‘[Registry Settings](#_Registry_Settings)’), remembering to restart the Identity Agent after doing so.

If the CMS operation is not left to fully complete before Smartcards are removed, the registry may be left in an invalid state. This should be resolved by Identity Agent v2.x on the next Smartcard insertion when it resets the EnableNHSEnrollment value back to 0.

### ‘Failed to delete key container’ or ‘Failed to create keys’ during CMS operations

These errors may be received when performing Smartcard operations using CMS and may be seen on both Gemalto and Oberthur Smartcards.

This issue has been seen when performing a second renewal on a Series 8 Smartcard which has been previously renewed, and the RA has Oberthur Middleware SR5 installed. This issue mostly affects installations on Windows 8.1 & Windows 10. It is advisable to upgrade to Oberthur Middleware SR8 as soon as practical to avoid this issue.

Investigations are also ongoing at the time of writing as to other causes. To try and resolve the issue, the user or RA can attempt a ‘retry’ of the operation on the Smartcard. If this fails, the best course of action is for an RA to cancel and re-issue the Smartcard on the same day to avoid auto certificate revocation.

The above information is left in for historic purposes as the vast majority of Series 8 Smartcards in use will have had at least one renewal and most of these will have been done using SR5. Renewing with SR8 or PKCS11# rectifies the index issue seen when renewing with SR5 and should resolve these issues.

### Java crashes whilst performing CMS operations

The above error occurs in some trusts when they uninstall BT Identity Agent v11 and install any other Identity Agent. When BT Identity Agent v11 gets uninstalled it can switch off the service ‘ScardSvr’. CIS / CMS uses this service to perform CMS operations, hence the Java crashes.

To resolve, create a new file with name “**Scardsvr.reg**” and copy the below content and save. Run the registry key by double clicking on the “**Scardsvr.reg**” file and reboot the machine. After rebooting the user should be able to perform CMS operations.

Windows Registry Editor Version 5.00

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\SCardSvr]

"DisplayName"="@%SystemRoot%\\System32\\SCardSvr.dll,-1"

"Group"="SmartCardGroup"

"ImagePath"=hex(2):25,00,53,00,79,00,73,00,74,00,65,00,6d,00,52,00,6f,00,6f,00,\

74,00,25,00,5c,00,73,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,73,\

00,76,00,63,00,68,00,6f,00,73,00,74,00,2e,00,65,00,78,00,65,00,20,00,2d,00,\

6b,00,20,00,4c,00,6f,00,63,00,61,00,6c,00,53,00,65,00,72,00,76,00,69,00,63,\

00,65,00,41,00,6e,00,64,00,4e,00,6f,00,49,00,6d,00,70,00,65,00,72,00,73,00,\

6f,00,6e,00,61,00,74,00,69,00,6f,00,6e,00,00,00

"Description"="@%SystemRoot%\\System32\\SCardSvr.dll,-5"

"ObjectName"="NT AUTHORITY\\LocalService"

"ErrorControl"=dword:00000001

"Start"=dword:00000002

"Type"=dword:00000020

"DependOnService"=hex(7):50,00,6c,00,75,00,67,00,50,00,6c,00,61,00,79,00,00,00,\

00,00

"ServiceSidType"=dword:00000001

"RequiredPrivileges"=hex(7):53,00,65,00,43,00,72,00,65,00,61,00,74,00,65,00,47,\

00,6c,00,6f,00,62,00,61,00,6c,00,50,00,72,00,69,00,76,00,69,00,6c,00,65,00,\

67,00,65,00,00,00,53,00,65,00,43,00,68,00,61,00,6e,00,67,00,65,00,4e,00,6f,\

00,74,00,69,00,66,00,79,00,50,00,72,00,69,00,76,00,69,00,6c,00,65,00,67,00,\

65,00,00,00,00,00

"FailureActions"=hex:84,03,00,00,00,00,00,00,00,00,00,00,03,00,00,00,14,00,00,\

00,01,00,00,00,c0,d4,01,00,01,00,00,00,e0,93,04,00,00,00,00,00,00,00,00,00

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\SCardSvr\Parameters]

"ServiceDll"=hex(2):25,00,53,00,79,00,73,00,74,00,65,00,6d,00,52,00,6f,00,6f,\

00,74,00,25,00,5c,00,53,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,\

53,00,43,00,61,00,72,00,64,00,53,00,76,00,72,00,2e,00,64,00,6c,00,6c,00,00,\

00

"ServiceMain"="CalaisMain"

"ServiceDllUnloadOnStop"=dword:00000001

[HKEY\_LOCAL\_MACHINE\SYSTEM\CurrentControlSet\services\SCardSvr\Security]

"Security"=hex:01,00,14,80,90,00,00,00,a0,00,00,00,14,00,00,00,34,00,00,00,02,\

00,20,00,01,00,00,00,02,c0,18,00,00,00,0c,00,01,02,00,00,00,00,00,05,20,00,\

00,00,20,02,00,00,02,00,5c,00,04,00,00,00,00,02,14,00,ff,01,0f,00,01,01,00,\

00,00,00,00,05,12,00,00,00,00,00,18,00,ff,01,02,00,01,02,00,00,00,00,00,05,\

20,00,00,00,20,02,00,00,00,00,14,00,8d,01,02,00,01,01,00,00,00,00,00,05,04,\

00,00,00,00,00,14,00,8d,01,02,00,01,01,00,00,00,00,00,05,06,00,00,00,01,02,\

00,00,00,00,00,05,20,00,00,00,20,02,00,00,01,02,00,00,00,00,00,05,20,00,00,\

00,20,02,00,00

## Connectivity

### Firewall settings

It may be necessary to configure a local or infrastructure firewall to allow access to the Spine authentication services. The address ranges should be allowed direct, un-proxied access (including transparent) to Spine services.

The settings required for the firewall configuration are listed in the table below.

|  |  |  |  |
| --- | --- | --- | --- |
| Destination | Port | Protocol | Direction |
| 155.231.9.0/24 | 443 | TCP | Inbound and Outbound |
| 155.231.9.0/24 | 636 | TCP | Outbound |

The following line can be added to a proxy auto configuration script to provide a proxy exclusion for these address ranges:

if (isInNet(resolved\_ip, "155.231.9.0", "255.255.255.0"))

                return "DIRECT";    ‘

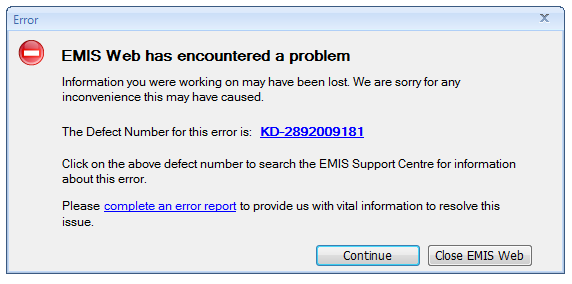
### DNS Checks

|  |  |  |
| --- | --- | --- |
| Step | Objective | Process |
| 1 | Open a Command Prompt | * Press **[Windows Key]+R** * Type cmd and press **Return** |
| 2 | Manually check resolution of spine DNS names | * Type nslookup and press **Return** * Type portal.national.ncrs.nhs.uk and press **Return** * Ensure that you see a response similar to this, indicating success (we would expect to see three addresses returned – this is due to the redundancy built into the system):   Server: cns0.nhs.uk  Address: 155.231.231.1  Non-authoritative answer:  Name: portal.national.ncrs.nhs.uk  Address: 155.231.9.135  Name: portal.national.ncrs.nhs.uk  Address: 155.231.9.69  Name: portal.national.ncrs.nhs.uk  Address: 155.231.9.50   * An invalid response would be similar to:   Server: cns0.nhs.uk  Address: 155.231.231.1  \*\*\* cns0.nhs.uk can't find portal.national.ncrs.nhs.uk: Non-existent domain   * Repeat this step for the following DNS records:   gas.national.ncrs.nhs.uk  sbapi.national.ncrs.nhs.uk |
| 3 | What next | * If the above check fails then there may be a firewall issue, in which case the next section may be of use. |

### Proxy and Routing Checks

|  |  |  |
| --- | --- | --- |
| Step | Objective | Process |
| 1 | Check gas connectivity via the browser | * Navigate to:   https://gas.national.ncrs.nhs.uk/login/authactivate   * Ensure that you see a response similar to:   <?xml version="1.0" encoding="UTF-8"?>  <!DOCTYPE USER SYSTEM "https://gas.national.ncrs.nhs.uk/login/dtd">  [<gpOBJECT>](https://gas.national.ncrs.nhs.uk/login/authactivate)  <gpPARAM name="**gas\_version**">5.2.7</gpPARAM>  <gpPARAM name="**error\_code**">7601</gpPARAM>  <gpPARAM name="**server\_ip**">172.16.132.67</gpPARAM>  <gpPARAM name="**error\_message**">[XML Parser] Invalid input request.</gpPARAM>  <gpPARAM name="**error\_reporter**">com.gemplus.gemauth.  services.servlets.AuthActivate</gpPARAM>  <gpPARAM name="**error\_url**">[https://pnbu076-uksr-ap.hosts.liveb.national.ncrs.nhs.uk:443/login/error</gpPARAM](https://pnbu076-uksr-ap.hosts.liveb.national.ncrs.nhs.uk:443/login/error%3c/gpPARAM)>  <gpPARAM name="**log\_session\_id**">QFCVjQ0vyH</gpPARAM>  </gpOBJECT>   * An error relating to certificates may be displayed but is not indicative of a connectivity error so should be ignored at this point. * A connectivity problem at this point is indicative of a problem with proxy settings, or if a proxy server is not being used with the IP routing. |
| 2 | Install the Telnet Client (if not already present) | * Open the **Programs and Features** control panel applet * In the left sidebar click **Turn Windows features on or off** * Ensure the **Telnet Client** item is checked * Click **OK** * Close any confirmation windows, and the **Programs and Features** applet |
| 3 | Check gas and ssb connectivity via telnet | * Press **[Windows Key]+R** * Type cmd and press **Return** * Type telnet gas.national.ncrs.nhs.uk 443 * The console should clear and there will be no response visible on screen. * Press **return** a few times to exit the session * An error is indicated by a response similar to:   Connecting To gas.national.ncrs.nhs.uk...Could not open connection to the host, on port 443: Connect failed   * Repeat the process for sbapi.national.ncrs.nhs.uk * An error at this stage suggests that there is a routing problem between the client and the gas service. This might be expected if there is a proxy service in place between the client and the N3 network, unless a socks client such as ISA Firewall Client is installed and configured. |

### Issues with EMIS Web



The changes required for IA v2.2.3.7 to resolve the memory leak have caused an issue with how EMIS access the Smartcard which appears to stop the first time Smartcard association from working with Series 8 (OT) Smartcards. EMIS are aware of the issue and are trying to resolve it.

The only current workaround is to perform the first-time association on a version of Identity Agent lower than v2.2.3.7. Once the Smartcard has been associated, EMIS works as expected.

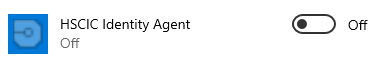
**NOTE:** EMIS have attempted to advise a fix for this issue to us which comprises the following actions.  
Install GEM, install IA, install SR8, and then revert the registry back to the GEM settings.  
This fix **must not** be used as will render any user who implements this unable to perform a self-renew on Series 8 Smartcards and a high risk of damaging the card beyond repair if attempted.

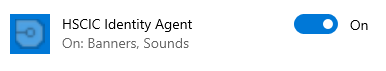
### No Popup Bubble After Logging In

It has been noted that on some Windows 10 1903 and later builds, the notification for Identity Agent is turned off by default for some reason, regardless of the option setting on earlier versions of the Windows 10 installation.

If the popup notification is required, it can be simply re-enabled by following the steps below.

Click on the Windows icon  
Click on Settings  
Click on System  
Click on Notification and Actions  
Scroll down and toggle the button to On for HSCIC Identity Agent





**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>