NHS England Identity Agent v2.4.6.0

Administrators Guide

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

**Contents**

[Introduction 4](#_Toc159596956)

[Audience 4](#_Toc159596957)

[NHS England Identity Agent v2.4.6.0 4](#_Toc159596958)

[Software & documentation 4](#_Toc159596959)

[Important Considerations 5](#_Toc159596960)

[System Requirements 5](#_Toc159596961)

[Middleware 5](#_Toc159596962)

[Other components 6](#_Toc159596963)

[Usage Scenarios 6](#_Toc159596964)

[Operating Systems 6](#_Toc159596965)

[Environments 6](#_Toc159596966)

[Smartcards 7](#_Toc159596967)

[Installation Process 7](#_Toc159596968)

[Configuration 8](#_Toc159596969)

[Registry Settings 9](#_Toc159596970)

[Primary Care System Suppliers 12](#_Toc159596971)

[Environments 13](#_Toc159596972)

[Certificates 13](#_Toc159596973)

[Registry Editor Utility 14](#_Toc159596974)

[Troubleshooting 15](#_Toc159596975)

[Incorrect Smartcard Reader Drivers 20](#_Toc159596976)

[Problem Areas 21](#_Toc159596977)

[No PIV mini driver 21](#_Toc159596978)

[Locked Smartcard (Series 9 Only) 21](#_Toc159596979)

[Logging out 21](#_Toc159596980)

[Follow-me-sessions (RDP) 22](#_Toc159596981)

[Follow-me-sessions (VDI) 23](#_Toc159596982)

[Follow-me-sessions (RDP) 23](#_Toc159596983)

[Fast-User-Switching 23](#_Toc159596984)

[Connectivity 24](#_Toc159596985)

[Support 27](#_Toc159596986)

# Introduction

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

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

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

## Audience

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

# NHS England Identity Agent v2.4.6.0

This release has the following enhancements -

* Additional enhancement to assist with hardware checks on VDI platforms \*\*NEW
* Upgrade to .NET4.8 framework, .NET4.8 is a prerequisite to installing the Identity Agent MSI
* TLS 1.2 is enabled by default.
* Removed Certs and Installation Cert form while installation.
* Passcode length is now set to a maximum of 8 alphanumeric only.
* Self-Service unlock URL updated to https://digital.nhs.uk/unlock
* UI improvements
* A new registry key value named "TrustedCertificateIssuers" of type REG\_SZ for Primary Care System Suppliers.

# Software & documentation

All software and documentation can be downloaded from <https://nww.digital.nhs.uk/dir/downloads/>

The latest Warranted Environment Specification (WES) is located here   
<https://digital.nhs.uk/services/spine/spine-technical-information-warranted-environment-specification-wes>

# Important Considerations

**By default,** the IA will clear all the certs from the user’s personal certificate store. To retain certificates in this store from other publishers, e.g. for a VPN, please 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 England Identity Agent v2.x requires the presence of Gemalto Middleware.   
  
and PIV Middleware.

Oberthur Middleware is also required **by users performing the RA functions.**

|  |  |  |
| --- | --- | --- |
| Component | Description | Minimum Version |
| Gemalto Classic Client | Middleware component providing the interface between CryptoAPI and S4, S5 & S6 smartcards. | 6.1 Patch 3 for NHS  32-bit ***or*** 64-bit |
| AWP Identity Manager  / OT Middleware | Middleware component providing the interface between CryptoAPI and S8Smartcards. | Oberthur Middleware SR8 32-bit ***or*** 64-bit |
| PIV Middleware | Middleware component providing the interface between CryptoAPI and S9 Smartcards. | Xxxxx\* |

|  |  |  |
| --- | --- | --- |
| **Component** | **Normal User** | **RA User** |
| Gemalto Classic Client | Yes | Yes |
| AWP Identity Manager  / OT Middleware | No | Yes |
| PIV Middleware | Yes | Yes |

\* If the PIV/CIVMiniDrver middleware is installed through Windows update, components providing interface will not be installed on the machine. The interface is installed when installation is done via the .msi file.

## Other components

|  |  |  |
| --- | --- | --- |
| Component | Description | Minimum Version |
|  | | |
| .NET Framework  The programming infrastructure created by Microsoft for building, deploying, and running applications and services that use .NET technologies.  Microsoft .NET 4.8. needs to be installed even if the user has installed a higher version of .NET \*\*\* | | |
| Smartcard Reader Drivers \*\* | Any driver required to support the Smartcard reader used within your organisation.  Link to supported drivers for various Smartcard readers is provided on the [DIR website](https://nww.digital.nhs.uk/dir/downloads/). | N/A |
|  |  |  |

**Note** - 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/)

# Usage Scenarios

## Operating Systems

The operating systems warrantied for use are listed here:

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

## Environments

The Identity Agent is warrantied 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 smartcard operations under these configurations are **NOT** supported including self-renewal. The registry value **UseCardReaderPolling** needs to be set to True to allow the Smartcard details to pass to the Citrix environment.

## Smartcards

Support for versions of Smartcards is determined by several factors, including the operating system, the Card Service Provider (CSP) Middleware and the support of APIs used to access the Smartcards.

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

|  |  |
| --- | --- |
|  | Supported Operating Systems |
| Series 9 (PIV) | ü |
| Series 8 (Oberthur) | ü |
| Series 6 (Gemalto) | ü |
| Series 5 (Gemalto) | ü |
| Series 4  (Gemalto) | X |

# Installation Process

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

# Configuration

The agent is supplied with built-in defaults for all settings. The built-in defaults can be overridden through the application of specific registry values either directly or via Group Policy settings using an Administrative Template.   
  
**Note:** Registry entries will not be created in the registry locations described in this document. It will need to be created manually. 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 “authenticate against Live”. This will create the required sub-trees in the registry. Administrative rights are required to run the tool.

The Identity Agent reads 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.

* **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. 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 runs as a 32-bit process regardless of whether the OS is 32-bit or 64-bit.

* **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

**Notes**

* After making registry changes, restart NHS England Identity Agent v2.x to allow the changes to take effect as not all registry changes are dynamic.
* By default, NHS England Identity Agent v2.x will operate under ‘Normal Mode’ and will authenticate against the live environment and close all Web browsers on logging out.

## Registry Settings

|  |  |  |  |
| --- | --- | --- | --- |
| Setting | Default | Possible Values | Purpose |
| ActivatePOSTURL  (REG\_SZ) | <https://gas.national.ncrs.nhs.uk/login/authactivate>  Built into the IA |  | The URL where activate / challenge requests are sent. |
| LaunchAppsType (REG\_SZ) | *None* | files | 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* | https://portal.national.ncrs.nhs.uk/portal/ | 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 Portal. |
| EnableTrainingOption (REG\_SZ) | false | true  false | If enabled the training mode option is displayed on the passcode form. |
| IdleWaitPeriodInSeconds  (REG\_DWORD) | 1800 | Between 0 & 36000 | The time (in seconds) that the user session is allowed to be idle before it ‘Windows locks’ the screen   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, mobility idle timer takes over and ‘IdleWaitPeriodInSeconds’ is stopped. |
| TimeAllowedLockedUntilLogoffInSeconds (REG\_SZ) | 15000 | Between 15000 & 28500 | The time (in seconds) that the user is allowed to maintain a locked (Windows) screen before the user is logged out. |
| MobilityPersistence\_Available (REG\_SZ) | false | true  false | If enabled, this setting makes the mobility persistence toggle available on the passcode form. |
| ConfigTheme\*\* (REG\_SZ) | Off | Off’, ‘Minimal’, ‘Medium’, ‘Maximum | Defines the theme for timers used in ‘Mobility mode’.  The settings associated with each theme are defined in the [‘Config Themes](#_**Config_Themes)’ section below. |
| SessionLockPersistence\_Enabled (REG\_SZ) | false | True  false | Switch on session lock persistence.  Setting this value to ‘false’, or removing the key, enables the Identity Agent to operate under ‘Normal mode’. |
| ProcessesToKill  (REG\_SZ) | java;iexplore;chrome;firefox;msedge |  | The names of executables to kill when a Smartcard is removed, or another logoff event occurs. This can /include the names of on browser applications.  Note: Do not add the .exe to the end of the process. |
| NoRolesLogoff  (REG\_SZ) | true | True  false | 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 | True  false | **For RA/RAMs** this registry value should be changed to‘false’. |
| TrustedCertificateIssuers  (REG\_SZ) | ***None*** | **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;CN=NHS INT Level 1C, OU=CA, O=nhs;CN=NHS INT Level 1D, OU=CA, O=nhs | The String is semicolon delimited allowing for multiple entries to be defined.  If the user requires the presence of certificates other than those related to NHS Smart Cards place the following value in the registry entry |
| CardHealingEnabled  (REG\_SZ) | true | True  false | 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.  When working in Citrix environments it is recommended to set CardHealingEnabled to “false” on the Citrix client machine |
| EnhancedNormalMode  (REG\_SZ) | false | True  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 in during the lock/unlock operation.  Setting to true will force the user to enter their passcode on unlocking Windows. |
| UseCardReaderPolling  (REG\_SZ) | false | False  true | 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. |

#### \*\*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 **  **Timer ** | **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 |

## Primary Care System Suppliers

A new registry key value named "TrustedCertificateIssuers" of type REG\_SZ is  
supported for prescription signing actions using signing API libraries. It is searched for in the registry in the following locations and, in the following order:

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

By setting the registry string to contain the Issuer details for NHS Certificate Authorities you can ensure that the API will only remove stale X.509 Certificates issued by those defined Certificate Authorities.

**Note:**  
The old logic has been superseded now and the API performs similarly to the Identity Agent with regard to this functionality.

By default, the user's personal certificate store is cleared of X.509 certificates that do not match those that have been currently read from the target Smart Card.

To disable this and to ensure that only stale X.509 certificates that have been issued by NHS for Authentication and Signing are removed the following must  
be done:

|  |  |  |  |
| --- | --- | --- | --- |
| Setting | Default | Possible Values | Purpose |
| TrustedCertificateIssuers (REG\_SZ) | ***None*** | **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;CN=NHS INT Level 1C, OU=CA, O=nhs;CN=NHS INT Level 1D, OU=CA, O=nhs | The String is semicolon delimited allowing for multiple entries to be defined. If the user requires the presence of certificates other than those related to NHS Smart Cards place the following value in the registry entry |

## 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: INT |  |
| ActivatePOSTURL | <https://gas.nis1.national.ncrs.nhs.uk/login/authactivate> |
| Environment: DEP |  |
| ActivatePOSTURL | https://gas.vn1.national.ncrs.nhs.uk/login/authactivate |
| Environment: 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.

## Certificates

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.

## Registry Editor Utility

A simple-to-use tool, the **IA Registry Editor Tool v3.3.16.1** is available to download from the [DIR website](https://nww.digital.nhs.uk/dir/downloads/). This allows you to update settings and switch between environments. This tool requires Admin rights.

# Troubleshooting

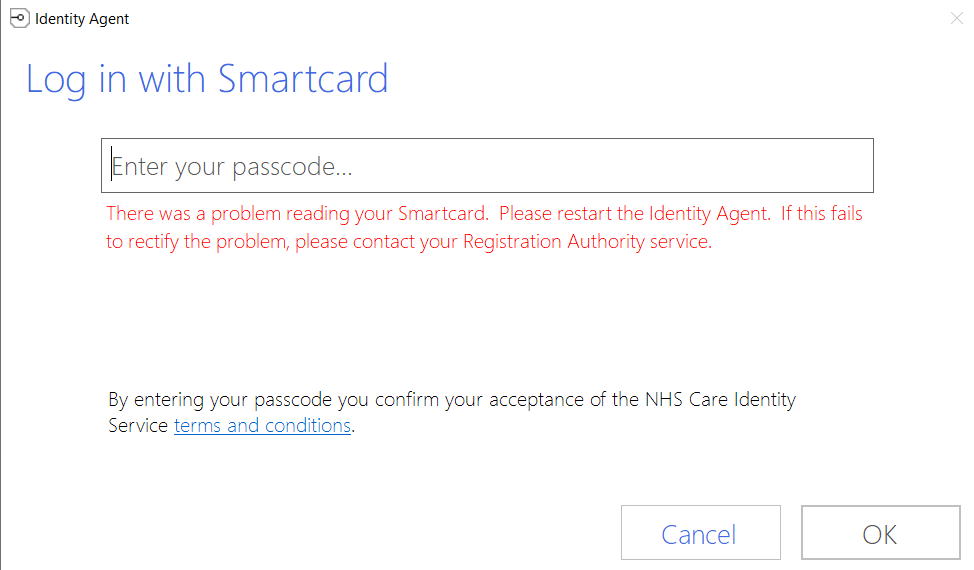
**Invalid/missing middleware**

If this error is seen immediately after installing NHS England Identity Agent v2.x then missing Middleware is the most likely cause of this error.

The Middleware will need to be re-installed before re-attempting authentication.

**The Smartcard is blank**

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

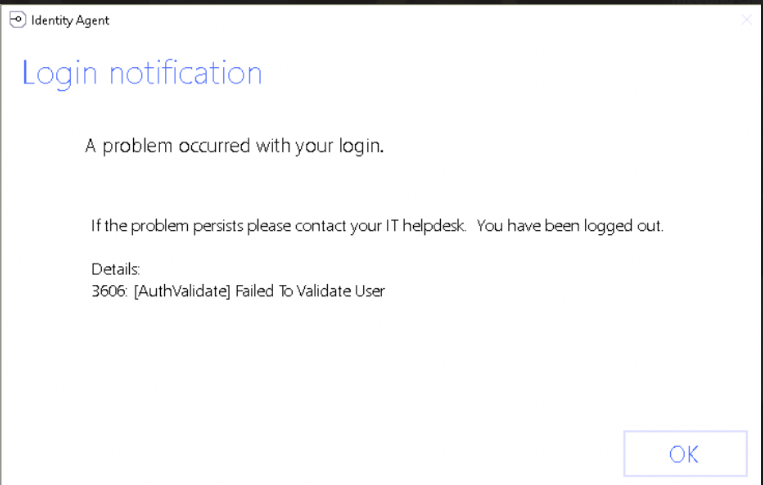


**Incorrect Smartcard Reader Drivers**

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.

#### ‘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 [Environments](bookmark://_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.  
  
**Revoked Card**

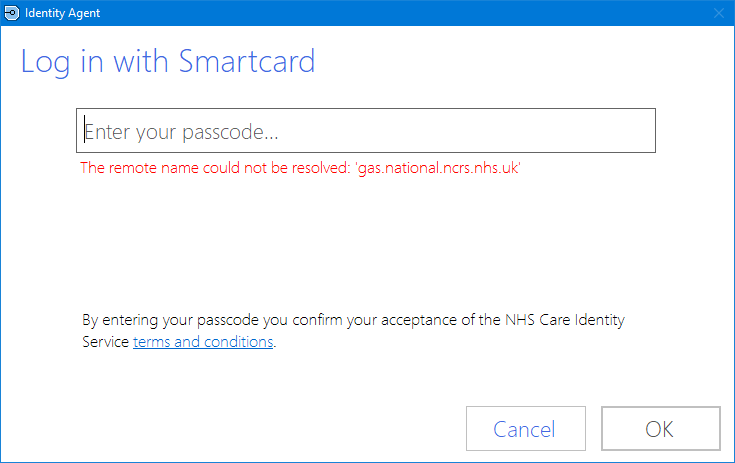
When a card has been Destroyed/Revoked/Corrupt, this error is also generated when you try to authenticate with the same card.

**NOTE:** On occasion cards can become corrupted and enter into an unrecoverable state. In this circumstance after all card repair operations have failed, a new card will need to be issued.

#### ‘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 HSCN network is not directly internet accessible.



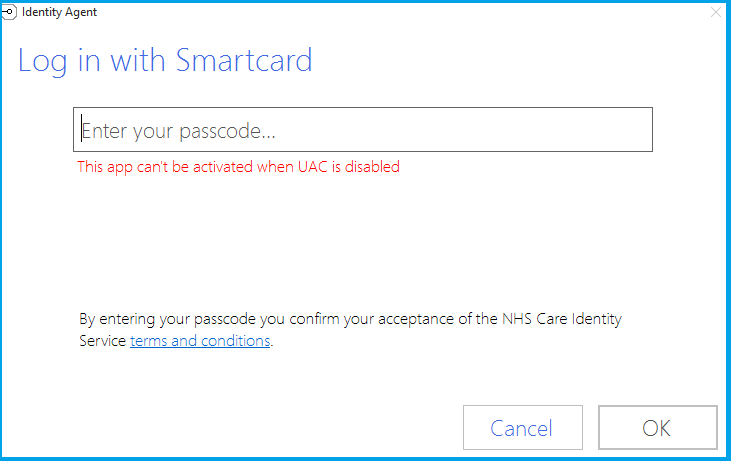
If the user has network connectivity issues, they should raise a support call with their local IT support help desk.

#### ‘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.

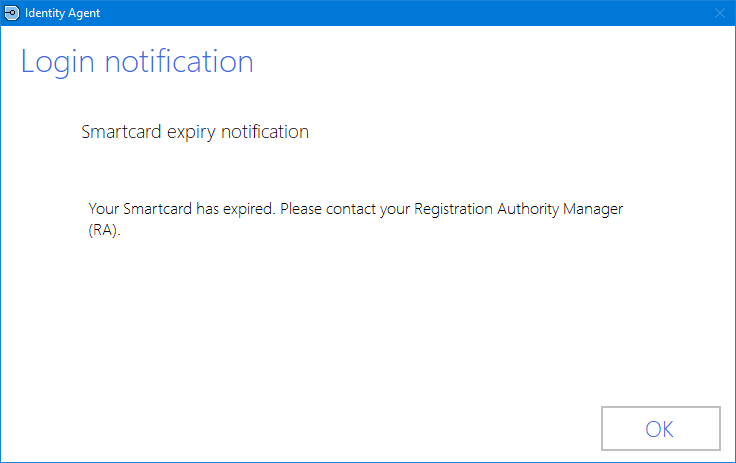
The Smartcard will need to be either repaired or cancelled and then re-issued by an RA Agent / Manager.

#### ‘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.

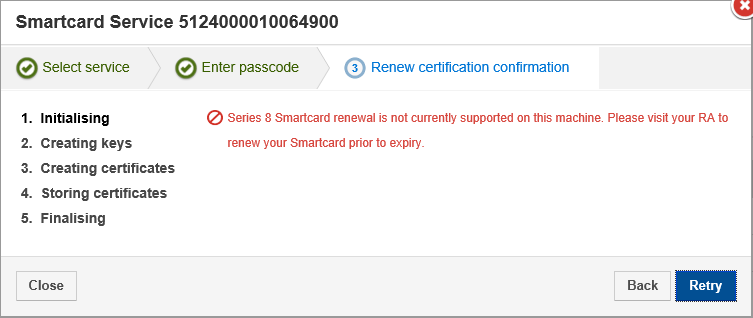
#### **Unable to authenticate following self-renew with Oberthur Smartcards**



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 ‘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 NHS England 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’   
To resolve the issue, set the value of ‘CardRemovalCheck’ to ‘false’. Restart Identity Agent after the change has been made.

## Incorrect Smartcard Reader Drivers

Smartcard not authenticating and the Identity Agent is giving an error message or Smartcard operations are failing.

A screenshot of a computer screen

Description automatically generated with low confidence

#### Guidance

With the later builds of Windows 10, by default, the incorrect 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.

## Problem Areas

## No PIV mini driver

Smartcard not authenticating and the Identity Agent is displaying an error:

A screenshot of a computer screen

Description automatically generated with low confidence

#### Guidance

Download the latest Idemia PIV mini driver, install it with administrative rights, and restart the system. Make sure the PIV Mini Driver is present in the following system path:

C:\Program Files (x86)\CivMinidriver

Path for Idemia PIV Mini Driver:

<https://na.idemia.com/wp-content/uploads/2021/09/CivMinidriver-1.2.8.zip>

## Locked Smartcard (Series 9 Only)

If you fail to enter the correct passcode via the contactless method, you will reach your maximum retries after 7 failed attempts. Should this happen, you can try an additional 3 attempts via contact to recover the smartcard. If this fails, then you will need to seek help from your local RA to unlock your smartcard.

By default, the values set for contacted attempts is 10 and 7 via contactless.

## Logging out

#### All browser windows shutdown

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

#### Unexpected logout

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

* Windows unlocked 3 times consecutively, without also re-authenticating 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)).
* A single authentication session can last for a maximum of twelve hours, this is common to all Identity Agents and cannot be changed and will occur whether the session is being actively used or the machine is locked.

## Follow-me-sessions (RDP)

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

If having authenticated into Care Identity, 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.

Please see the matrix table below for the permitted configuration:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | Middleware | | |
|  | Smartcard reader driver required\* | GEM (Gemalto) | OT (Oberthur) | PIV (MiniDriver) |
| Local Device |  |  |  |  |
| Remote Device/VDI |  |  |  |  |

#### 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 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 Care Identity 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 and log 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 to unlock the session necessitating the user to perform a full “Disconnect and Log Off” which terminates their 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 a 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 Care Identity session upon removal of the Smartcard.

#### ‘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.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.

## 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 transparency) 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

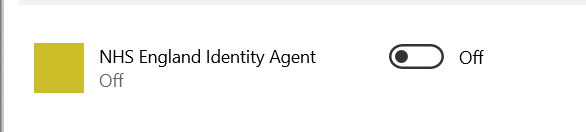
|  |  |  |
| --- | --- | --- |
| Step | Objective | Process |
| 1 | Check gas connectivity via the browser | * Navigate to:   https://gas.national.ncrs.nhs.uk/login/authactivate   * Ensure that you see a response similar to:   <?xml version="1.0" encoding="UTF-8"?>  <!DOCTYPE USER SYSTEM "https://gas.national.ncrs.nhs.uk/login/dtd">  [<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. |

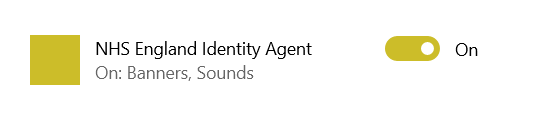
### No Popup Bubble After Logging In

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 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 Identity Agent





# Support

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

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

Telephone contact 0300 303 5035

**Alternatively write to:**

Iamplatforms@nhs.net