

Single Sign On (SSO) - England

Signing into Vision with your Smartcard



Table of Editions and Contents

Date	Version	Contents	Output
30/03/2011	001	Detached from PDS user guide.	PDF

Copyright © INPS Ltd 2011

Contents

What's New in SSO	2
DLM 320 (31.01.11)	2
DLM 202 (09.06.06)	2
How to Login into Vision Using SSO	3
Obtaining Smartcards	3
Lost, stolen or broken Smartcards	4
Care of Smartcards	4
Lost, Stolen and Broken Smartcards	4
Working Online	5
First SSO login	6
Workstation Locking	6
Removing your Smartcard from the reader.	6
Leaving your workstation inactive	6
Unlocking the workstation	7
Working Offline	7
Working Offline to Single Sign On	8
Assign Smartcard	9
Troubleshooting Single Sign-On	10
PIN/Passcode Unlocking/Changing	10
Failure to connect	10
Unlinked Status	12
Access Denied	12
Forced Vision Shutdowns	13

What's New in SSO

DLM 320 (31.01.11)

- **Workstation Locking** – From DLM 320, you are now able to lock your workstation when you are logged into Vision with your Smartcard. This is done by either:
 - Removing your Smartcard from the reader.** This will no longer result in a forced Vision shutdown. Instead, the workstation is locked and the Vision modules you are running are frozen until you unlock the workstation.
 - Leaving your workstation inactive.** The Vision screensaver now works with SSO login which means that depending on your settings in **Control Panel – Security**, the workstation will lock after a period of mouse or keyboard inactivity.See “[Workstation Locking](#)” on page 6 for further details.
- **Assign Smartcard** – Assign Smartcard is now part of File Maintenance. This was previously accessed from the front screen of Vision and automatically appeared as a prompt for those accessing Vision for the first time with their Smartcard. From DLM 320, only those with access to Control Panel – File Maintenance are able to assign Smartcards.

DLM 202 (09.06.06)

- Timeout of connection after 10 hours (see “[Forced Vision Shutdowns](#)” on page 13) - recommendation that if you are signed on with your Smartcard and you leave the room for lunch, housecalls etc, you log out of Vision and remove your Smartcard. You can then sign on again when you return.

How to Login into Vision Using SSO

Obtaining Smartcards

In order to connect to the national services, a SSO (Single Sign-On) process, provided by the SSB (Spine Security Broker), must be followed when logging into Vision.

Single Sign On access is by means of a Smartcard. Each workstation will be provided with a Smartcard reader and each member of staff with a Smartcard. There is a 12 to 14 digit Unique Identifier (UID) associated with each card, and you will be issued with a passcode or PIN to use the card. The gold chip holds all the information.



These cards are obtained for you in the first instance from the Registration Authority, normally your PCT or LSP, who will register you as a user of the Spine. The Registration Authority acts on the entries made on form RA01 by a Sponsor within the practice.

The card authenticates your access to the national services and has your unique identifier and your role profile(s). Each user is assigned a role profile. This has a baseline of functions that are suitable for that role, for example, a GP can prescribe, but a nurse cannot. The Sponsor on the RA01 form can allocate additional business functions to a role, for instance, a GP can have the additional business function of initiating Choose & Book Referrals. A separate help guide is available detailing this.

For further details, see RBAC User Guide on www.inps.co.uk – User Assistance – Regional – England (CfH).

There is no organisation name printed on issued Smartcards to allow staff to use existing cards when transferring between organisations and for improved security. It is possible for a user to have more than one role, IF they have a separate Area of Work. For general practice, the Area of Work is deemed Primary Care and those working in the practice will only have ONE role within that Area of Work. If a GP also works at a local hospital, then that is a separate Area of Work, but s/he can have a different role there.

Lost, stolen or broken Smartcards

Care of Smartcards

Smartcards should be treated with care and protected to prevent loss or damage.

Lost, Stolen and Broken Smartcards

- Lost and damaged Smartcards should be reported to the RA Team at the PCT as soon as is practicable.
- Once notified that a Smartcard has been lost or damaged, the RA should arrange to have the lost/damaged Smartcard revoked and replaced as soon as possible. In the case of loss or theft, the RA Manager must be informed so that checks may be made to ensure that the Smartcard has not been misused.
- When an issued Smartcard becomes unusable or it is lost or stolen, the Smartcard certificate must be revoked, which renders the Smartcard useless.
- As long as the Smartcard holder's identity can be verified at a face to face meeting a new Smartcard may be issued.
- If there is any difficulty verifying the user's identity the user's Sponsor must be contacted and the users identity verified. It is vital that the Sponsor's identity can be relied upon when contacting them to verify the user's identity.
- See also "[PIN/Passcode Unlocking/Changing](#)" on page 10.

Working Online

You must use your Smartcard to single sign-on and login to Vision in order to link to the national services including the Spine, PDS, making referral bookings, ETP etc. You may work offline (for example, if you have lost your card or just want to use Vision locally) but you will not be able to access the national services, such as Choose and Book, ETP and PDS queries. If you have full Role Based Access Control (RBAC) enabled (available from DLM 340), your role profile is mapped to your Vision security settings, hence you must login with your Smartcard to use offline elements of Vision.

You should already be logged on to your computer with your desktop on screen.

1. Place your card in the cardholder at your workstation (this may be built in to the keyboard or be a USB plug-in device).
2. You will then be prompted to enter your passcode or PIN on the GEM Authenticate screen and after reading the attention message, select *Yes I accept and wish to proceed for the purpose of patient care*.

If you enter your PIN incorrectly three times, the card will be locked (see "[PIN/Passcode Unlocking/Changing](#)" on page 10).

NOTE - If the system does not recognise you and it is your first time signing on, you may be able to add yourself as a new user - see "[First SSO login](#)" on page 6.

3. Click Yes to proceed if you see a security alert.
4. Click Yes when asked "Do you want to close this window?"

NOTE - If you have trouble logging in, see "[Troubleshooting Single Sign-On](#)" on page 10.

5. You have now successfully logged on to the Spine. Successful login creates a "token" which is lodged with SSB. If unsuccessful, Vision will terminate (see "[Access Denied](#)" on page 12 and "[Failure to connect](#)" on page 10).

6. To access the Vision front menu, double click on the Vision icon



. Note that when working online through SSO, the Vision User name and password are not used.

7. If you have more than one role set up for you, you will now see the **Select Role** box for VISION. Select the appropriate **Role** from the pick list of roles, click in the **Assigned Profiles** box, then click OK.
8. On the Vision front menu, the title bar carries your name and the role in which you are signing on.

The Smartcard issued to you by the PCT incorporates the role assigned to you. This role determines which parts of Vision you can access. This means that some Vision front menu options may be hidden from you after login and role selection. If your login leads to hidden Vision modules that you used to use as part of your job, then you will need to see either your practice Sponsor, who will submit an RA02 form (to edit the role profile on your Smartcard) or your RA at the PCT.

First SSO login

Before you can login to Vision with your Smartcard, your Smartcard must be assigned to a Vision profile. The Vision system administrator is able to do this via Control Panel – File Maintenance.

Workstation Locking

You can lock your workstation when you are logged into Vision with your Smartcard. This is done by either removing your Smartcard from the reader or leaving your workstation inactive:

Removing your Smartcard from the reader.

Removing your Smartcard from the reader without logging out of Vision first will no longer result in a forced Vision shutdown. Instead, the workstation is locked and the Vision modules you are running are frozen until you unlock the workstation.

Leaving your workstation inactive

The Vision screensaver now works with SSO login which means that depending on your settings in **Control Panel – Security**, the workstation will lock after a period of mouse or keyboard inactivity. Please see Control Panel – Security on-screen help for further details.

Note – If you have disabled your Vision screensaver or timeout setting in Control Panel – Security, your workstation will lock after 30 minutes of inactivity. This is a setting on the Spine Security Broker (SSB) and cannot be changed in Vision.

Unlocking the workstation

When your workstation is locked and you move your mouse or type on your keyboard, the Unlock Session screen displays:



Vision - Unlock Session

To unlock the session you must re-enter your Smartcard passcode and you will be returned to Vision as it was when it was locked.

Alternatively, you can select End Session to close Vision. You are warned that any unsaved work will be lost.

Working Offline

Vision can be used offline without Single Sign On if you do not have full Role Based Access (RBAC) enabled.

However, offline working is discouraged as it is advantageous for all staff to be using the same methods at all times. Offline working could cause inconsistencies in registration procedures in particular, and opportunities to update the Personal Demographic Service will be missed by those offline, forcing this task on to those who will be working online.

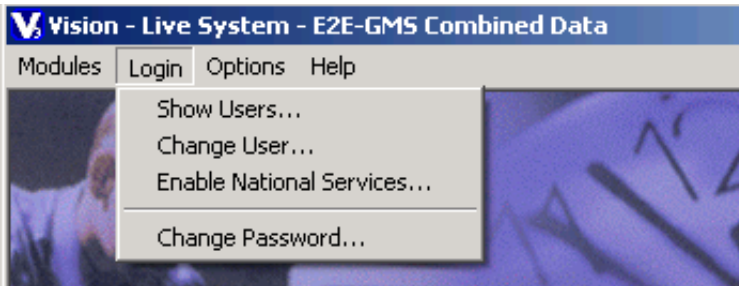
Offline Working will allow clinical data to be viewed or recorded but will not give any access to national applications. In particular, users will not be able to make electronic bookings through Choose and Book and changes made to the PDS (Patient Demographic details) will not be passed to or retrieved from the Spine. You are strongly encouraged to work online at all times as this will aid familiarity and increase consistency of use.

1. To use Vision offline, double click on the Vision icon. This produces a prompt to enter a Smartcard. You should press Cancel to this prompt.
2. Next you will be presented with a Network Error dialog box giving choices for the next action one of which is Work Offline.
3. At this point you are presented with a Vision Login screen for you to enter your user name and password.
4. When working offline patients records will be displayed with the annotation '(OFFLINE)' after the patient's name on the title bar.

Working Offline to Single Sign On

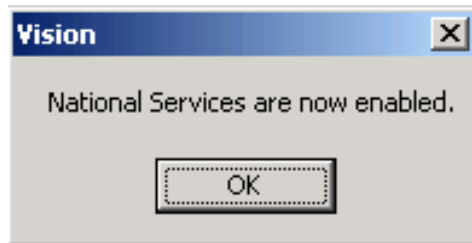
You can login with your Smartcard from within a Vision Offline session:

1. Put your Smartcard in the reader and enter your Passcode
2. From the Vision front screen go to **Login – Enable National Services** (if you have not entered your Smartcard you will be prompted to do so).



Vision Front Screen – Login – Enable National Services

3. On successful sign in, you are prompted that "national services are now enabled". Click OK to continue.



National Services Enabled Message

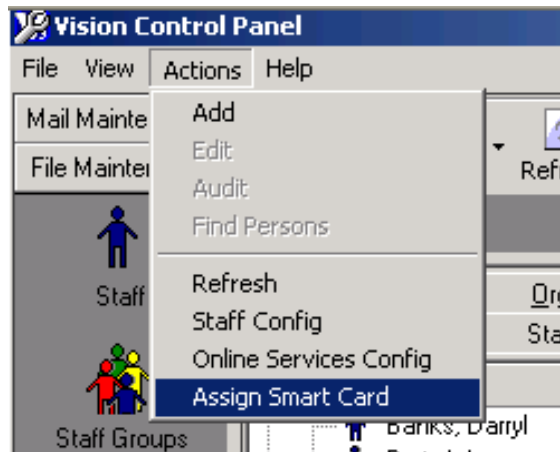
Assign Smartcard

Assign Smartcard is now part of File Maintenance. This was previously accessed from the front screen of Vision and appeared as a prompt for those accessing Vision for the first time with their Smartcard. From DLM 320, only those with access to **Control Panel – File Maintenance** are able to assign Smartcards. You will need the new users Smartcard to do this.

1. In Control Panel, go to File Maintenance.

Note – To assign a Smartcard you must login to Vision Offline. If you cannot remember your offline password please see Control Panel on-screen help for instructions on how to reset your offline password.

2. Next, click on **Actions – Assign Smartcard**.



File Maintenance – Actions – Assign Smartcard

3. Insert the new users Smartcard when prompted and click OK.
4. Enter the passcode for the Smartcard.
5. You are then presented with a list of Vision users. Click on the matching user and press Select. Please ensure that you select the correct user.
6. If the user is not on the list, you can click on Add User... to create a new Vision profile.
7. You are prompted with the following message:
"Warning: If you have used Vision at this practice before, and your name is not in the list, then you are advised to contact the system supervisor if this is the case and NOT create a new user. Continue to create a new user?"
8. A new staff record will be created in File Maintenance – Staff using the available SDS details (mandatory fields are surname, forename, title, sex, role, mnemonic and a unique id). For prescribing, the following is required: GMP Code, Prescriber number, formulary, Supplementary Prescriber flag and Responsible GP.

Note – For Locums, an SDS search is performed to obtain their external prescribing number. Where this is not retrieved, you can enter this manually in **File Maintenance – Staff**.

Troubleshooting Single Sign-On

PIN/Passcode Unlocking/Changing

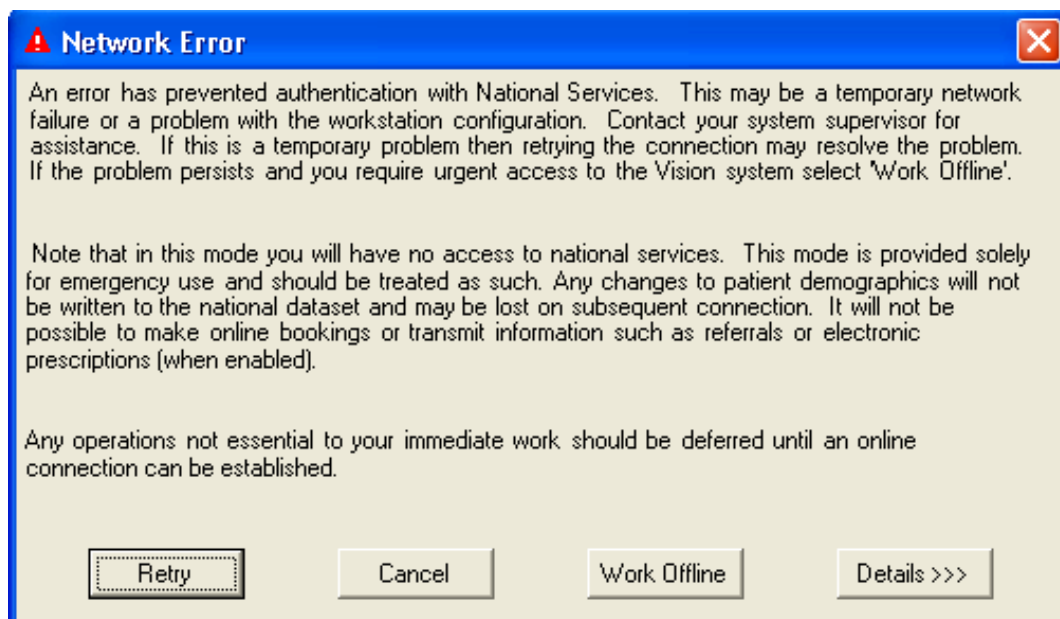
If you try to enter an incorrect passcode three times, your passcode will be locked out.

Unlocking of a Smartcard must be carried out by a Registration Agent (at the PCT) or the Sponsor (at the practice). The Smartcard holder must be present. Users who have forgotten their Passcode or suspect that it may be known by another, or who have been locked out of NHS CfH Applications because of three failed login attempts, should report the problem to a member of the RA Team as soon as is practicable.

In normal circumstances the local Sponsor will make changes to or reset the PIN/Pass-code. Exceptionally Passcode changes may be made by other members of the RA Team.

Failure to connect

If you fail to connect to the SSB client and server for the purposes of authentication, the following prompt will be given:



An error has prevented authentication with national services. This may be a temporary network failure or a problem with the workstation configuration. Contact your system supervisor for assistance. If this is a temporary problem, then retrying the connection may resolve the problem. If the problem persists and you require urgent access to the Vision system select 'Work Offline'.

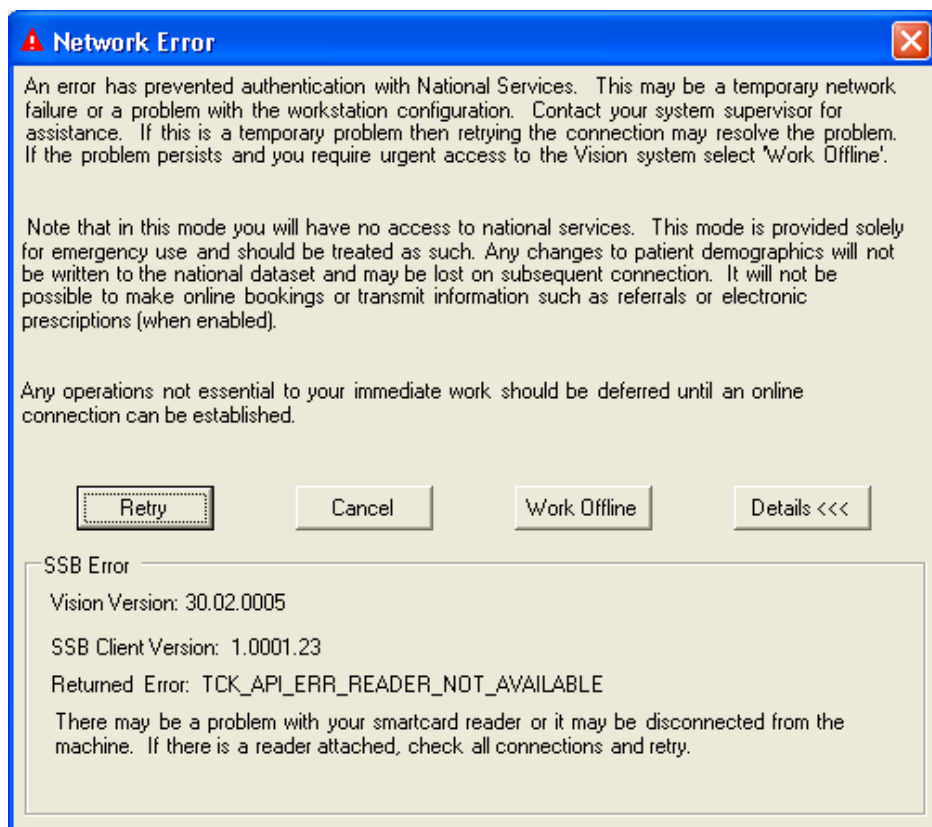
Note that in this mode you will have no access to national services. This mode is provided solely for emergency use and should be treated as such. Any changes to patient demographics will not be written to the national dataset and may e lost on subsequent connection. It will not be possible to

make online bookings or transmit information such as referrals or electronic prescriptions (when enabled).

*Any operations not essential to your immediate work should be deferred until an online connection can be established. **RETRY CANCEL WORK OFFLINE DETAILS***

The recommended options are:

- Contact your System Supervisor.
- **Retry** the connection.
- Select **Work offline**, if you do not need to connect to the national services for online bookings or referrals. Note that any changes to patient details will NOT be written to the national dataset and may be lost on subsequent connection.
- Select **Details** for further information. This may, for example, warn there is a problem with your Smartcard reader, and that it may be disconnected from the workstation.
- Check all connections between Smartcard reader and the machine.



Unlinked Status

If at any time, the link is dropped or does not connect, then the status is unlinked. You will see this at the top of the screen in Consultation Manager as [UNLINKED] after the patient's name and details.

The patient record will also be displayed with the annotation [UNLINKED] if after Patient Select, the local record cannot be matched against a PDS spine record by NHS Number.

As when working offline, although you will be able to make referrals, you cannot use Choose & Book, ETP or other national services while unlinked, nor access records from the Spine.

Access Denied

Access to the national services will be denied:

- if your current National Role Profile does not allow access to Vision at this practice (see Role Based Access). You should contact your Registration Authority in order to rectify this problem. (Computer Misuse Act 1990 - Unauthorised access to a system is an offence).
- if you are not currently registered as a Vision user. You should contact your System Administrator quoting the Unique Identifier code in order to rectify this problem.
- If the user's current role has no rights to any Vision function, Vision will close with the message: *It is not appropriate to grant you access rights in your current role .If you have more than one role, you should select a different role before running Vision. If you have no appropriate roles, you should contact your Registration Authority or Practice Manager.*
- if the first time you sign on using your Smartcard and log into Vision, the system identifies you as a member of staff already associated with another card.

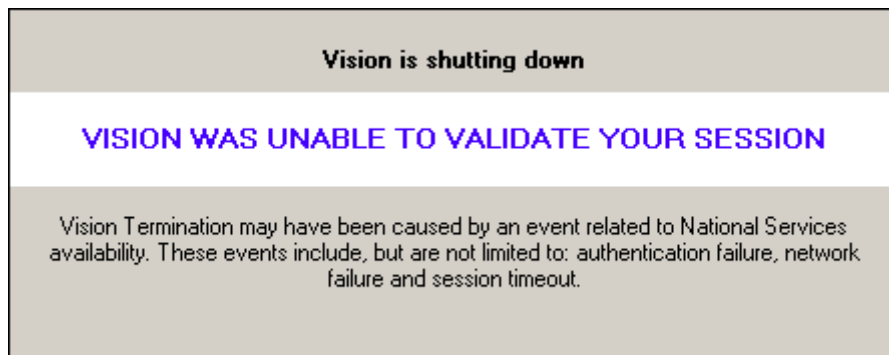
Forced Vision Shutdowns

When you sign on with your Smartcard, connection to the national services is timed to last a maximum of 10 hours. Just before this period expires, you will be warned, and after this period, you will be logged out. **This is an Spine Security Broker (SSB) setting which cannot be changed by INPS.**

Successful SSO login with the Smartcard and PIN creates a "token", lodged with SSB. It may be initiated by a Vision access but is not associated with a particular Vision session. The SSB client controls the validity and persistence of the SSO token.

There are circumstances under which the SSB client will automatically invalidate and destroy the SSO token. At the same time the SSB will instruct Vision to terminate with immediate effect. Examples of where such a forced shutdown will be effected are:

Token invalidated - The message reads: *Vision is shutting down. VISION WAS UNABLE TO VALIDATE YOUR SESSION.*



Revocation of user rights

Session timeouts (when exceeding maximum duration, currently 10 hours though this may change) (see above)

The spine ceases to function

On receipt of a shutdown instruction from the SSB, Vision will initiate an irrevocable shutdown sequence.