

# UCLH VPN User Guide

January 2009

VPN User Guide v1.3 20090106

## 1. What is the VPN?

The VPN (Virtual Private Network) provides users with secure access, using a web browser, to a standard terminal screen at the UCLH site. The terminal service has a selected set of UCLH systems, and presents an icon on screen which takes the user to their personal profile mapped drives. The service lets UCLH staff and approved third parties use some of the UCLH applications from locations outside of UCLH including home. It is the only way of accessing UCLH systems using broadband.

The gateway to the UCLH systems is provided by a Juniper SSL VPN. The authentication of users onto the UCLH terminal server is handled by RSA ACE servers. These provide two factor authentication, something the user knows <user name> and <PIN> and something the user has <a token generating one-time numeric passwords>. A registered user is issued with an RSA token and is taken through the login stages as part of the issue process so they can see the VPN service working and then log in for the first time from their remote site with confidence.

## 2. What are the limitations of the VPN?

The VPN connects the user to a standard terminal service desktop, this is NOT the user's desktop and it does not have any of the personal shortcuts or other user's personal desktop icons available. The user's current drive mappings are added to the user profile at setup. The user cannot add drive mappings to the user profile themselves. A Logica IT Service desk call can be made to add new drive mappings.

The users e-mail service is available using Outlook on the terminal server; it is part of the user's individual profile, but as it is on a different computer so it does not have access to personal folders held on the users own PC. This may take a little getting used to.

The VPN service requires the remote user to connect to a specific URL over the internet from a Windows Internet Explorer browser. No other web browser is useable. The initial setup requires some patience and so the token issue process will take a user through the setup of their account on a trust PC. This is particularly important for a Trust laptop as there is software to install for the Juniper VPN service. Trust laptops need to be configured/reconfigured to work with wireless LAN access to a home broadband router. This is necessary to work with the Trust's PC security settings for use at the UCLH sites. A UCLH laptop will not work with a home internet DSL Modem which plugs into the USB socket, or the cabled Network Interface card (NIC)

It is not possible to print to a home printer from the virtual terminal (which is at UCLH) and for security reasons it is preferable not to take local copies of Trust data. All users are reminded of their obligations under the Trust Information Governance policy to maintain security and confidentiality in all access to Trust data.

The remote desktop cannot be used to store any personal files, as this is a shared workspace. All files should be filed back into the user's file areas, accessed through their user profile. Any files left on the desktop will be deleted. Care must be taken when logging out of the VPN service to ensure that the files in use have been properly closed and the session has been carefully shut down. Failure to do this will leave a remote session active and any files open in the virtual session will be inaccessible from the user's normal desktop at work.

The initial live VPN service provides a standard desktop with access to the following computerised services at UCLH. PACS is available from the Juniper screen – not the terminal services desktop, see section 6.2 below.

1. Your home and mapped drives as set up in your user profile. This should get you to all your stored data around the UCLH network.
2. Microsoft Internet Explorer, Outlook, Word and Excel
3. CDR Workstation ( + CDR Test)

4. Chemocare 4.5
5. Hippo
6. PIMS
7. Radcentre 6 - *Requires the Imaging system manager to set up a special user terminal file and send that to Logica before the VPN can be made to work, request on the VPN application form*
8. Sunquest – via terminal emulator
9. Theatre manager – PICIS
10. Teamworks – web URL link shortcut

Please note that Carecast is not routinely available on the VPN. A very limited number of users can be allowed rights to access so that they can provide remote system support. At present that only includes ICT Enterprise system management staff. A maximum of about 50 users could be supported, so any requests for Carecast access rights via VPN will need to be approved by the ICT Senior Management Team.

The above list is the total extent of the software systems available under the current version of VPN. Users who would like other systems to be considered should e-mail suggestions to the ICT Enterprise systems manager who will keep a running tally so potential candidates for a future expansion project can be identified and considered.

### 3. How to get a VPN access service?

There is an application form available to users on the Trust Intranet and can be found at <http://insight/departments/Corporateboard/ICT/ICTRecords/ICTEnterpriseSystemsManagement/VPN/Pages/default.aspx> or by searching for VPN.

The VPN section of the Intranet has the current copy of the VPN User Guide. The last page of which has instructions for the completion of the application form.

Applicants requesting a token themselves should ensure they are logged in to the Trust PC they are using in their own user name, as the application system collects this information as part of the application form process. The line manager named in the process will be contacted by email to approve the request.

Line managers requesting a token for an applicant should ensure they are logged in to a Trust PC in their own user name, as the application system collects this information as part of the application form process. The applicant named in the process will be given access later and will need to log in under their own user name to accept the terms and conditions at some stage before the token can be issued. Forms correctly completed by line managers will not need the email confirmation process for line manager approval.

Most of the application form items are mandatory and are marked with a red asterisk (\*). The applicant must provide telephone contact points as that is how the Logica ITSD will make contact to arrange pickup and initial setup of the token. The applicant must provide a budget code to cover the £75 cost of the token, and select from the Trust directory the name of the authorising manager.

The applicant will be asked to confirm that you have read the VPN User Guide, and the Trust's Information Governance policy. This confirms you understand and accept your responsibilities whilst accessing trust computing resources from remote locations.

If you are a trust laptop user and wish to have VPN access from your home broadband internet connection there are special provisions to be made and checked with you. You can indicate that you have a Trust laptop on the application form.

When completed 'click' on **OK** to submit the application.

The ICT Enterprise team will automatically respond to the submission. They will process it slightly differently depending on who completes the form (line manager, applicant or other person). Once the Enterprise team are happy that the line manager has approved and the person the token is for has accepted the terms and conditions the validated request is then passed electronically to the ITSD for setup. The applicant will be contacted by phone or email to discuss pickup arrangements when the token is available. This must be done in person

VPN token applicants can track progress of their token application via an online application system available through the UCLH intranet or by following the links on automated emails sent during the approvals process.

Non UCLH staff, such as UCL employees, and certain employees of other healthcare organisations will require a UCLH login before they can apply for a VPN token. The IT Service desk (ITSD) (<http://insight/departments/Corporateboard/ICT/ICTOperations/ITservicedesk/Pages/default.aspx>) is the place to start the application process for a UCLH user account; and their UCLH line manager has to make an application to Logica to set up a UCLH account for the user, along with the UCLH software applications they need to access. In most cases the user will have to attend system user training before they will be allowed to access UCLH software applications, (with the exception of UCLH e-mail.)

It is not possible to apply for a VPN access until a normal UCLH account has been created.  
It is not possible to add more than one person to a token

Once the completed, and approved, application is available, the IT Service desk handles the creation of the token and user privileges. Once setup the VPN user will be invited to make an appointment to collect the token, and go through the setup process with a member of the Logica team.

In order to organise the appointment at the Logica offices, the user needs to provide contact information, preferably a telephone number/mobile number at which you can be reached, so the Logica desktop team can co-ordinate the process. E-mail tends to be too slow to co-ordinate a timely appointment to carry out the token setup and handover.

The supervised initial login has been chosen as it is essential that new users get to see the expected behaviour of the system, and the steps which a new installation requires. Without this stage it will be difficult for the user to install the service at their remote location. For this reason there can be no 'untrained' issue of tokens.

The computer which you will use must have access to the Internet and must be running up to date anti-virus software.

**You must have administrator access to the computer which you will use as there is software to download and install.**

**You should note that Logica only support the VPN and do not support your end user device or your internet service.** If you have problems with either of these you should use your home PC or internet support service. One relatively simple way to identify local PC problems is to connect to a different PC, preferably using a different internet connection. A repeat of the supervised initial logon process can also be arranged by contacting the IT Service Desk.

The setup of a user's own PC is not supported other than in providing advice, and a set of notes in section 8 of this document relating to the experiences of other users whilst setting up their VPN connection. Different PCs with different operating systems, security software and levels of service pack patching behave in different ways when setting up to access the UCLH VPN. It is not possible to give anything other than general guidance on the setup of the VPN service on a home computer. Windows Vista has security actions which can be hidden to the average user, and can be temperamental when trying to set up the VPN client on the user's PC.

## 4. RSA SecureID Token features

The RSA SecureID token displays a 6 digit number and up to 6 grey bars near the left hand side of the display. Every 10 seconds one bar will disappear and after all bars have gone a new 6 digit number and 6 bars will be displayed making the old number invalid.

The token's number generation sequence is time synchronised to the central server when initially set up for the user. The six digit number is used with a user selected four digit PIN, creating a ten digit password that changes every minute.

Tokens have a fixed life and will need to be replaced when they life expire, it is expected that the cost will remain around £75 each. Lost tokens will require another request to be made and another £75 will be charged.

## 5. How to use your PIN and VPN login

During your first supervised setup of your VPN you will need to set up your four digit PIN. You must be able to remember this; it is four digits and cannot start with a zero. Your VPN trainer will help you through this process, which is documented at the end of this section.

To use the VPN from an internet connected computer type the URL of the gateway <https://gateway.uclh.nhs.uk/secid> into your Internet Explorer browser. Note the very important **HTTPS** leading segment of this URL. You will get a login screen which carries a clear reminder of the security and Trust information governance rules to which you are bound as a user of the remote access service. You will be prompted to enter your username and password. Enter your UCLH Windows login ID in the username box and enter your four digit PIN followed by the current six digit number on the RSA secure ID token to complete the password in the password box. You will then be authenticated to use the VPN.

### PIN reset

Should you forget your PIN and need to have it reset this will only be done when you present personally at the Logica office with your ID badge. This is necessary to ensure the continued security of your UCLH user account when operating remotely.

### **FIRST TIME TOKEN ACCESS**

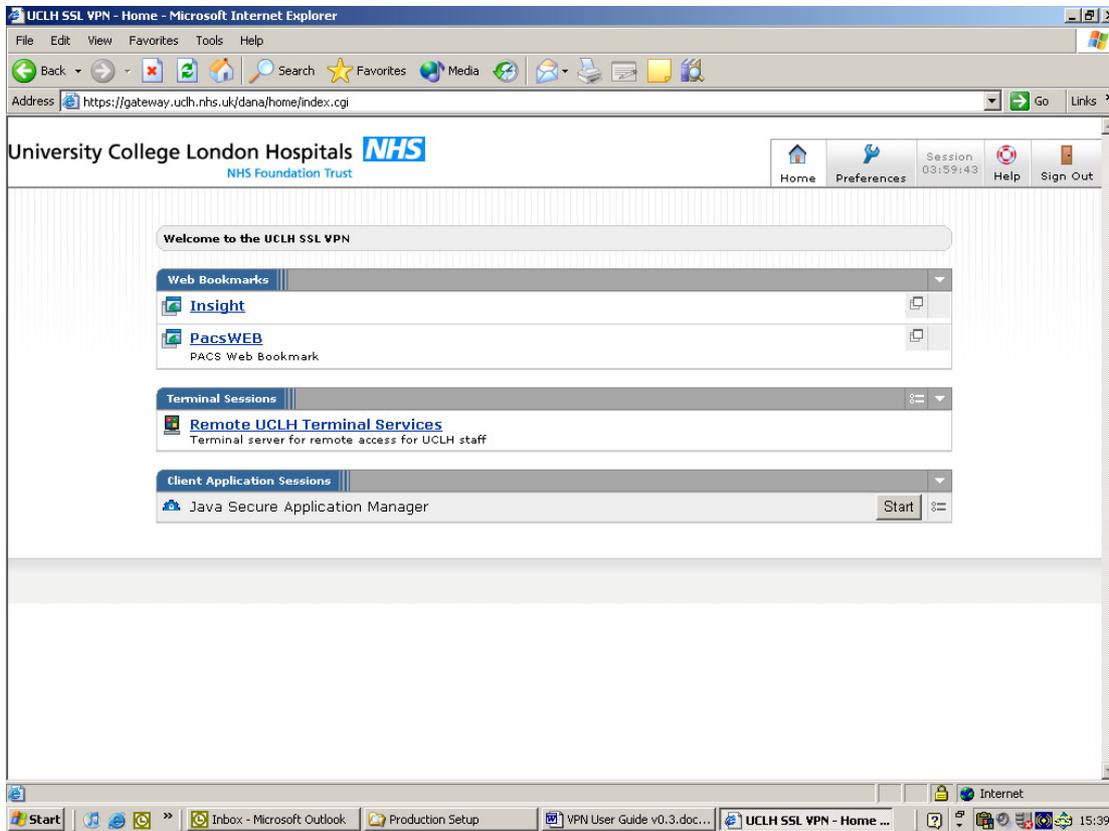
The first time that you access the site you will need to set up your PIN.

Type the URL of the gateway stated above into the browser. You will be prompted to enter your username and password. Enter your UCLH Windows login ID in the username box and just the number displayed on the screen of the SecureID token in the password box.

You will be asked to create a new PIN for use on subsequent logins. This is 4 digits and cannot start with a zero. The system will confirm acceptance of the PIN. The subsequent process to login is described above, with the password being both the PIN **and** the six digit RSA token number.

## 6. Accessing Applications

Once you have successfully logged in to the system you will be presented with a screen of options. What you are offered depends on how you have been set up but most people will be offered the screen shown below.



It is worth noting, and can be quite difficult to appreciate, that the applications you access from terminal services are running in UCLH, and that the computer you are using is just a window into the UCLH environment. Applications you are running on the local PC are operating in a completely different space, and you cannot move anything between them on the desktop.

A valuable consequence of this however is that any clinical data you have to access, and any person identifiable data you access remains on the UCLH computers, and is not recorded on your PC or laptop. As long as you make no attempt to copy such information onto your local PC then the data you have accessed remains secure.

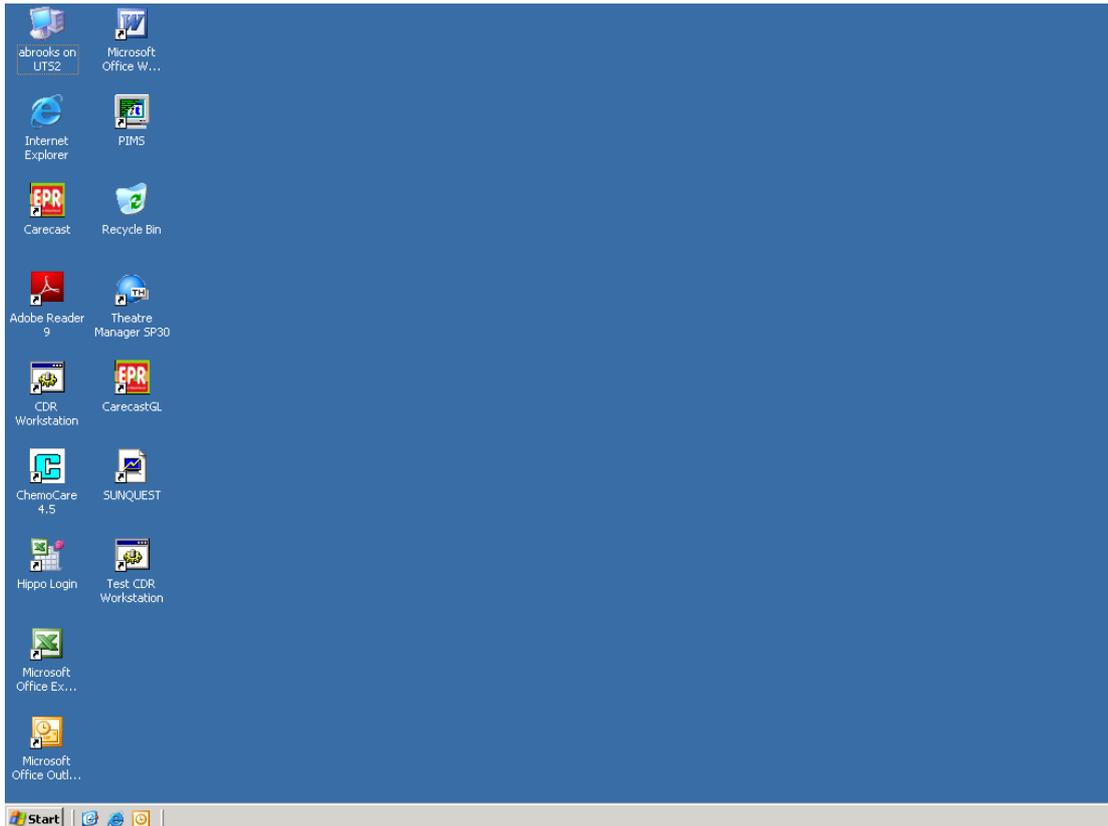
**You should take great care with Trust data accessed via your home computer or laptop. Copying unencrypted Patient identifiable, Staff identifiable or commercially sensitive data onto your home PC contravenes UCLH's Information Governance policy and should not be done under any circumstances.**

**Only securely encrypted devices can be used for transfer of such person identifiable data. Encrypted USB memory sticks are available via ICT Operations that could be used, if you have a justifiable need to move such data to another computer. This can only be done if such movement and use of data meets the requirements of data confidentiality under the Caldicott guidelines.**

## 6.1. *Remote UCLH Terminal Services*

This is the route for accessing all available applications with the exception of PACSWEB and Insight. For unavoidable security reasons certain features that you have on your UCLH desktop will not be available on the terminal server eg. right click of the mouse.

Click on the link and it will briefly display “Connecting ...” and then will prompt for username and password. Enter the username and password that you use at UCLH and click on OK. This will give you the Terminal Server desktop and you should click on the relevant icon for any of the applications that you wish to use.



It should be noted that the full list of applications will be offered to you but you can only access those to which you have access at UCLH. If you are not set up with access at UCLH you will not have access from other locations.

## 6.2. *PACSweb*

To use PACSweb simply click on the web bookmark and after several seconds it will present you with the login screen. Please note that this may take a while.

Log in using your UCLH Windows login ID and password. You will only get access if you have access at UCLH.

## 6.3. *Insight*

There is a web link for accessing the Trust intranet, Insight. Double click on this then enter your network ID and password.

## 7. Good Practice Guidelines

There are a number of things that you can do to minimize problems with using the VPN.

### Never leave your PC unattended

Leaving your PC unattended with a session open is a security risk and could lead to unauthorised access to patient data. It may also mean that the session times out leaving documents open which will give you problems accessing them when you get back to the office.

### Save your work regularly

This is good practice generally and will ensure that you do not lose work if your internet connection is lost or you are timed out of your VPN session.

### Log out cleanly from the VPN

You should always log out cleanly from the terminal server and from the Juniper by selecting the options to log out. Do not just close the window as this will leave sessions running in the background. Leaving sessions running may mean that your documents will be inaccessible to you back in the office as they will be locked by the open session.

Don't attempt to leave documents saved to the desktop, it is a shared desktop between all users of VPN,. So file your work away in your own filing space.

## 8. Common Problems

This section contains notes arising from experience gained during the pilot operation.

There are a number of frequently occurring problems which can be dealt with as follows:

### Entering URL does not take you to the Sign on Page

- Check that your Internet access is working by trying another site such as Google
- Check that you have typed the name correctly, in particular that you have entered **https** and not just http
- Ring the ITSD on (020 7380 9367) to find out if the VPN service is running OK.

### You click on the Terminal Server but you do not get a Login screen

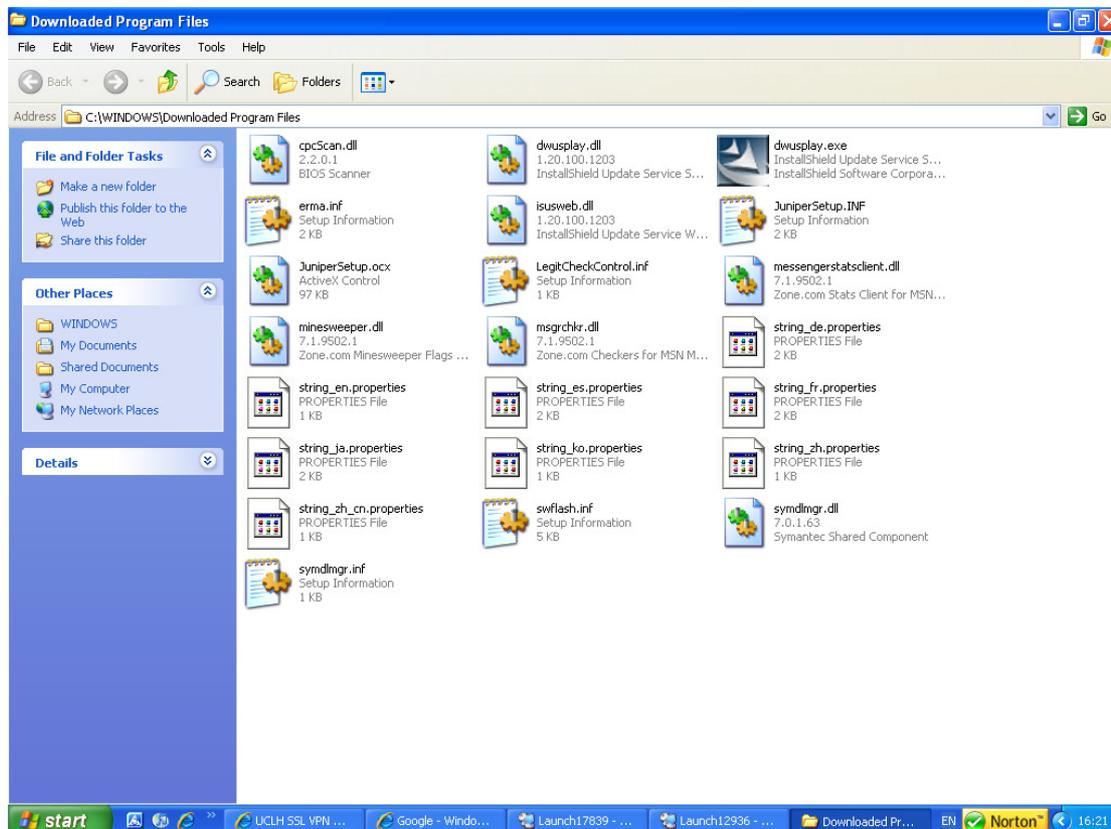
This may be a result of the need to download additional programs or amend security settings. If you get a Security warning or an install warning like the ones below please click on '**Allow**', '**Install**', or '**Unblock**'. Watch out for warning panels and dialogue boxes requiring a response that are hidden behind other windows. It can be that a login failure is due to a hidden question needing you to make a positive response.



Accept any downloads and allow any necessary access (if dialogues appear) particularly any that refer to ActiveX controls. Also, be aware of a yellow bar at the top of the window, under the address bar asking if you would like to install an ActiveX control and say “yes” if it refers to Juniper Networks. You must have administrator rights on the PC you are setting up. This is generally the case for personal PCs, but it is entirely possible that other healthcare organisations and UCL staff wishing to use UCLH VPN will need to get their IT support organisation to carry out the initial setup and load the Juniper software.

If you still have problems after this you should force re-installation of the certificates as follows. Please note that the exact sequence will depend on your home PC so you may need to use a slightly different process.

In Internet Explorer select Tools, Internet Options then Settings. Select View Objects and you will be given a list of objects similar to those below.



Right click on “JuniperSetSp1” and select Remove or Delete.

Shut the internet window then connect to the Internet again.

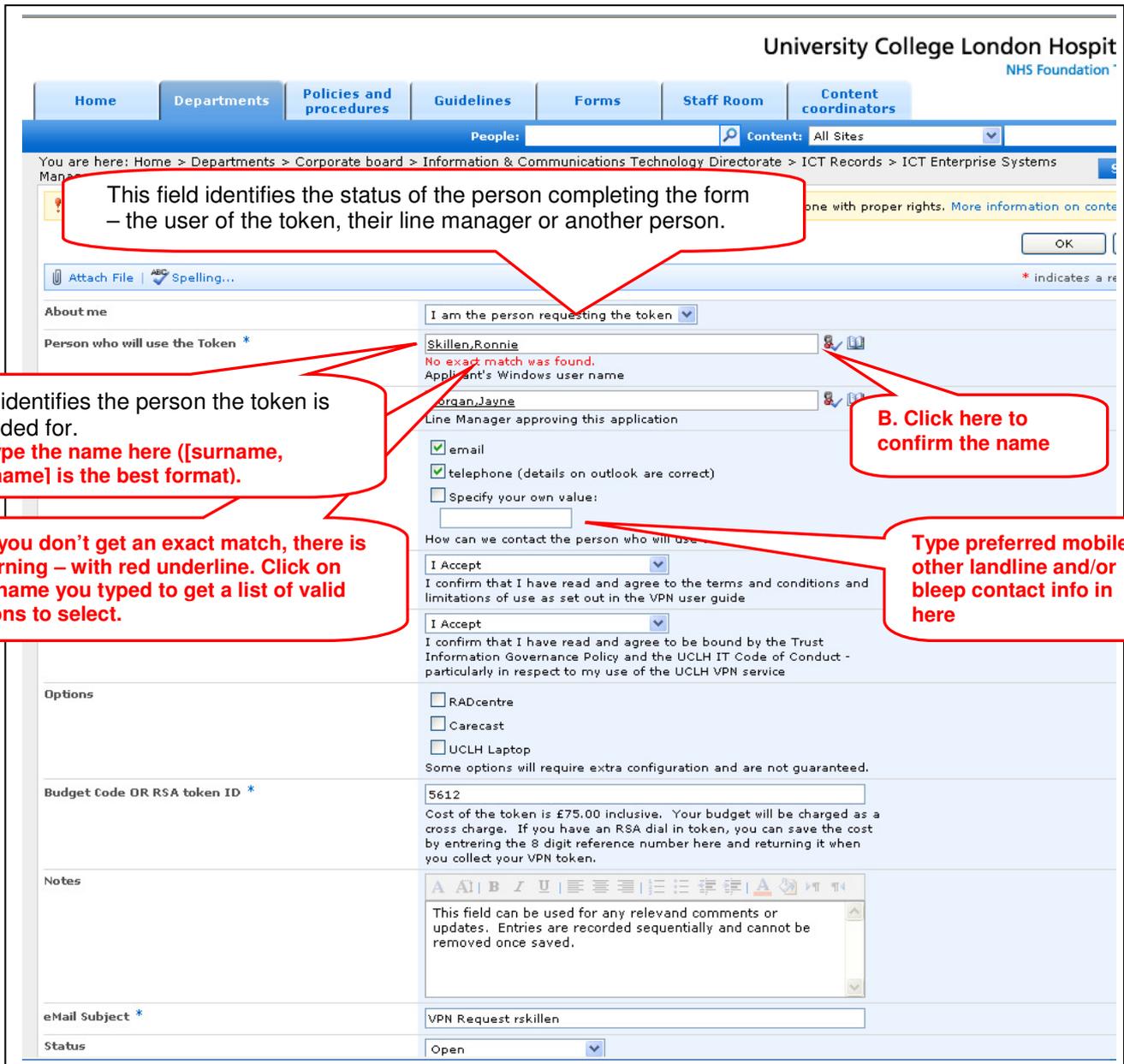
Click on the Active Control “JuniperSet1” link at the top of the screen the ‘Install Active Control link’ - Install the ‘Juniper Network Inc’

## VPN user experience

1. Each user's home PC will have different operating system, antivirus software, spy ware detection and registry protection, so it is not possible to describe for any individual how their computer may respond to loading a VPN service. One author of this document found that the terminal service login would only install and run after some 85Mb of Microsoft patches had been installed on the PC. It is common to have to move windows around to see dialogue boxes requiring an answer before installation can continue. Take care to check and respond to these installation questions.
2. The use of Apple MAC computers is not specifically a supported environment, and the user's responsibility for their own computer equipment is particularly applicable in this case. MAC users have successfully connected to the UCLH VPN service. The MAC has to be running the Windows emulation software satisfactorily, and have a copy of Internet Explorer running as its browser. Only when these pre-requisites are operating correctly should an attempt be made to install the VPN client.
3. Some users have found that their over-zealous firewalls have prevented Juniper installation software from being downloaded to the PC. Whilst it is inadvisable to operate a PC without a firewall operational, it may be necessary to temporarily disable the firewall function to allow your PC to accept the Juniper installation software. If you take this step you do so at your own risk, and you must make sure you reinstate the firewall service immediately after making the necessary installations.
4. During the setup of the VPN when you get your VPN token, take care to note the expected behaviour of the installation and setup process so you can spot changes when installing on another very different PC. If all else fails you may have to engage the services of a local PC and internet expert to help you to get your PC working with the UCLH VPN service.
5. Users with UCLH laptop PCs must have a careful discussion about installation approach with the Logica team. The UCLH supplied laptops do not allow the user administration rights, so certain steps must be taken to allow local installation on a home internet connection. This involves settings for the laptop's wireless internet card.

## 9. Appendix A - On-line application form user guide

The VPN User application form found on the Trust intranet is shown below.



The screenshot shows the 'VPN User application form' on the University College London Hospital intranet. The form includes a navigation menu at the top with options like 'Home', 'Departments', 'Policies and procedures', 'Guidelines', 'Forms', 'Staff Room', and 'Content coordinators'. Below the navigation is a search bar and a breadcrumb trail: 'You are here: Home > Departments > Corporate board > Information & Communications Technology Directorate > ICT Records > ICT Enterprise Systems'. The main form area contains several sections: 'About me' (with a dropdown menu set to 'I am the person requesting the token'), 'Person who will use the Token' (with a text input field containing 'Skillen,Ronnie' and a red warning message 'No exact match was found. Applicant's Windows user name'), 'Line Manager approving this application' (with a text input field containing 'organ,Jayne'), 'Options' (with checkboxes for 'email', 'telephone (details on outlook are correct)', 'Specify your own value:', 'RADcentre', 'Carecast', and 'UCLH Laptop'), 'Budget Code OR RSA token ID' (with a text input field containing '5612'), 'Notes' (with a rich text editor area), 'eMail Subject' (with a text input field containing 'VPN Request rskillen'), and 'Status' (with a dropdown menu set to 'Open'). Red callout boxes provide instructions: 'This field identifies the status of the person completing the form - the user of the token, their line manager or another person.' (pointing to the 'About me' dropdown), 'This identifies the person the token is intended for. A. Type the name here ([surname, forename] is the best format). C. If you don't get an exact match, there is a warning - with red underline. Click on that name you typed to get a list of valid options to select.' (pointing to the 'Person who will use the Token' field), 'B. Click here to confirm the name' (pointing to a small icon next to the name input), and 'Type preferred mobile, other landline and/or bleep contact info in here' (pointing to the 'Specify your own value:' field).

### VPN Application steps :-

1. Confirm your Windows User login name
2. Confirm preferred contact details – remove those that don't work ( e.g. UCLH e-mail not used by all)
3. Confirm you accept the VPN User Guide conditions and the Trust Information Governance policy.
4. Select the name of the manager you have consulted for authorisation. (If you have real difficulty searching for them by name ask for their windows login name and use that.)

5. Enter the Budget code you have been given for the £75 cross charge.
6. If you are a UCLH laptop user and wish to use it with VPN enter the Asset number *(only wireless network equipped laptops can use VPN on a home broadband service, and then only if that is equipped with a wireless router. Upgrades to UCLH laptops to allow this will require a separate call to the ITSD, and will be chargeable.)*
7. Notify if you wish to be considered for Carecast and/or Radcentre access via VPN.
8. Click **OK** to submit the application form.