

Remote Access to the Private Physician Network

**Last Updated:
May 30, 2011**

Version: 2.3





Disclaimer

The Province of British Columbia cannot guarantee the accuracy of this document's contents. By proceeding with the information in this document, each reader waives and releases the Province of British Columbia, its employees, representatives and contractors, to the full extent permitted by law from any and all claims related to the usage of material or information made available. In no event shall the Province of British Columbia, its employees, representatives or contractors, be liable for any incidental or consequential damages resulting from the use of this material.

Copyright © Province of British Columbia

All rights reserved



Table of Contents

1.0	Overview	4
1.1	Virtual Private Network (VPN) Concept	4
1.2	Two Factor Authentication	4
1.3	When to Use the VPN	5
2.0	Receiving Your VPN Token	6
3.0	VPN Orientation	7
4.0	Requirements to access VPN	8
5.0	Signing into the VPN	9
5.1	Starting Your VPN Session	9
6.0	Using the VPN Web Portal	14
6.1	Windows users	14
6.2	Non-Windows Users	19
	6.2.1 Automatic Launch	20
	6.2.2 Manual Launch	20
6.3	Browsing the Internet	28
6.4	Other Features of the VPN Web Portal	29
6.5	Ending Your VPN Session	29
7.0	Troubleshooting	30
7.1	Unsuccessful Sign In	31
7.2	Next Tokencode Prompt	31
7.3	Multiple Sessions	31
7.4	Automatic Sign out of VPN session	32
7.5	VPN Server Busy	35
8.0	Security Recommendation	36
9.0	Token Management Practices	37
9.1	Request for Additional Tokens	37
9.2	Token Deactivation, Reactivation, Reassignment	37
9.3	Lost or Stolen Tokens	38
9.4	Faulty Token	38
9.5	Tokens for Locums	39
	9.5.1 Requesting A Token	39
	9.5.2 Departure of Locum	39
9.6	Tokens for Residents	39
	9.6.1 Requesting A Token	39
	9.6.2 Departure of Resident	39
9.7	Departure of Physician From Practice	40
	9.7.1 Physician Move to a Practice Using a PITO-Eligible EMR Vendor	40
	9.7.2 Physician Move NOT to a Practice Using a PITO-Eligible EMR Vendor	40
9.8	Departure of Staff From Practice	41
9.9	Returning Tokens No Longer Needed	41
10.0	Quick Reference Summary	43
11.0	Supported Platforms	44
11.1	Minimum Requirements	45
11.2	Recommended Requirements	47

1.0 Overview

This document contains detailed instructions for connecting to the Private Physician Network (PPN) using a virtual private network (VPN) from outside your practice.

The PPN provides VPN technology and two factor authentication to keep electronic medical record (EMR) data safe as it travels from remote access locations to the PPN network. The VPN service is an integrated component of the PPN.

The PPN can be accessed outside of the practice from a standard computer with an Internet connection and Internet browser software such as Internet Explorer or Mozilla Firefox. The Ministry of Health Services has contracted with TELUS to maintain two VPN portal sites.. Two factor authentication is required to log in to both “VPN Web Portal” sites.



Please use URL: <https://vpn1ppn.bc.ca> as the Primary site.
The Secondary site URL: <https://vpn2ppn.bc.ca> should be used if you are experiencing difficulties using the Primary site.

1.1 Virtual Private Network (VPN) Concept

VPNs maintain data privacy by encrypting data before transmitting it over a network. The data is encrypted by special software at the sending end and then decrypted at the receiving end. This technology provides a secure "tunnel" for transmitting information that is not accessible to unauthorized users.

Once you have signed into the VPN Web Portal, you can launch your EMR application (see instructions below) and all traffic over the Internet is contained within the secure VPN “tunnel” and is encrypted for added security.

Your EMR vendor will provide you with the network address to launch your EMR application from the VPN Web Portal.

1.2 Two Factor Authentication

Two factor authentication is a security process in which a user provides two means of identification to logon to a computer application. Using two factors is a more secure method of authentication compared to providing a single password alone. The two factors involved are sometimes spoken of as ‘*something you have*’ and ‘*something you know*’. The “something you have” is typically a physical token, such as a smart card or a one time password generator (E.g.. key fob), and the other is something memorized such as a security code or password.



The VPN uses a generated password from the TELUS-supplied RSA SecurID token (as shown on the left) that displays a ‘*tokencode*’ that changes every sixty seconds. This is the ‘*something you have*’ factor. A personal identification number (PIN) that you are required to choose when you sign up for the service is the ‘*something you know*’ factor (see below for instructions).

1.3 When to Use the VPN

You **must always** use the VPN Web Portal to access your EMR application from remote locations outside your practice. All network traffic to your EMR application will be encrypted and will flow through the VPN to the security services provided by the PPN.



The URLs or IP addresses provided for your EMR application will not be accessible through the Internet without first establishing a VPN session. This is an additional security feature to ensure that clinical data from your EMR cannot travel over the Internet.

If you have registered for a PPN email account, you must use the VPN Web Portal to access your PPN email from remote locations outside your practice.



Note: Although the PPN Email bookmark is in the VPN portal, the PPN Email service is not yet available. You will be notified when this service is available.

The VPN Web Portal is **not** recommended for accessing:

- All other Internet sites (e.g. Google or Up to Date): Only the EMR applications for qualified EMRs are tested for security and reliability on the SSL VPN. Continue to use your current approach for accessing these other Internet sites from remote locations using an Internet connection outside of the VPN service.
- Your external email accounts (e.g. Hotmail, Gmail): Again, your current approach for accessing your email from remote locations through an application such as MS Outlook or browser should be followed. All of this network traffic will travel on a standard path to the Internet.

IMPORTANT: The use of Internet sites and Email services through the VPN Web Portal, other than qualified EMR applications and PPN email, is not supported through an EMR vendor's 'Tier 1 support' helpdesk.





2.0 Receiving Your VPN Token

A VPN Token package will be couriered, by TELUS, to the PPN contact at your practice. The package will contain RSA SecurID Tokens for those staff designated to receive them. TELUS will also email or fax, to the PPN contact, the information associated with each RSA SecurID Token (E.g. Username) along with this user guide. Users will select their own PIN when they initially log in.

It is critical that each user keeps the RSA SecurID Token, Username and PIN safe. If an unauthorized person learns your PIN and obtains your token, this person could access the PPN using your identity. Always take the following precautions:

- Select a PIN that uses the full 8 (maximum) characters rather than just the minimum 4 characters;
- Select a PIN that has a combination of alpha and numeric characters (e.g. witt9751);
- Never reveal your PIN to anyone;
- Keep your token safe – one suggestion is to clip it to either of your personal home/car/office key rings; and
- If you think someone has learned your PIN notify the EMR vendor '**Tier 1 support' helpdesk** immediately, so a request can be put forward to TELUS to reset your PIN; and
- If your token is missing (lost or stolen) report this to TELUS.

Once you have a RSA SecurID Token, a Username and a PIN, you can sign into the VPN.



3.0 VPN Orientation

It is recommended that each practice contact their EMR vendor or technical support vendor to determine if a VPN orientation can be provided as part of their implementation process.

The orientation should be a walkthrough of the VPN service including sign in, accessing the EMR application, and other features mentioned in this guide.



4.0 Requirements to access VPN

Before you proceed to access the EMR application via the VPN, please step through the following checklist. This will minimize the possibility of you having any issues when accessing the EMR application through the VPN.

Step Required	Step Completed <input checked="" type="checkbox"/>	More Information
Verify Juniper's "qualified" operating systems and browsers are installed on your machine.	<input type="checkbox"/>	Section 10: Supported Platforms
Allow VPN websites through local network and user machine firewalls.	<input type="checkbox"/>	Your local IT Support
Install "Juniper Supported" Java	<input type="checkbox"/>	Section 10: Supported Platforms
Install required EMR software (Citrix, RDP or other clients)	<input type="checkbox"/>	EMR Vendor Support
Allow install of ActiveX from both VPN sites.	<input type="checkbox"/>	Your local IT Support
Allow running ActiveX from both VPN sites.	<input type="checkbox"/>	Your local IT Support
Allow pop ups from both VPN sites.	<input type="checkbox"/>	Your local IT Support
<p>* Ensure the following can occur on user machines:</p> <p>When EMR applications are launched on user machine, Juniper launches executables and tries to connect to additional ports on the loopback addresses on (range 127.0.0.0 to 127.255.255.255)</p> <p>Note: this step is usually automated unless your computer is strictly locked down</p>	<input type="checkbox"/>	Your local IT Support
Ensure you have the unique and correct VPN token assigned to your name	<input type="checkbox"/>	Your clinic's PPN Contact

* contact your IT support if you are not sure what this means

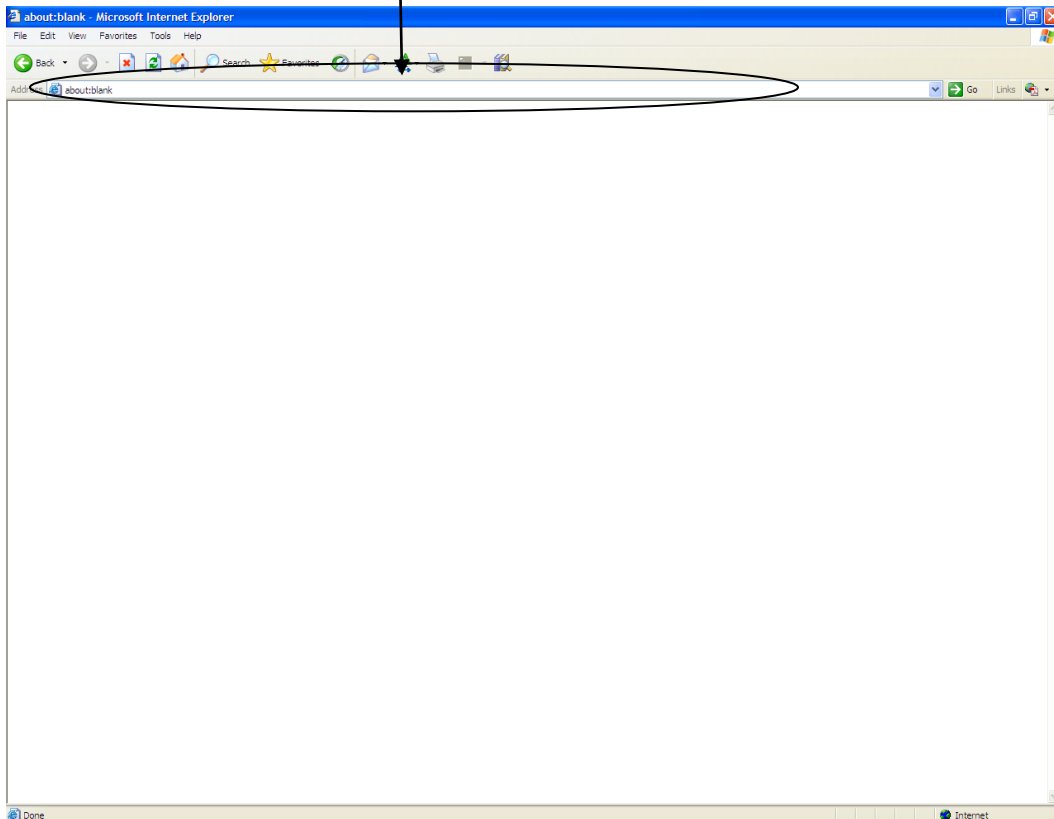
5.0 Signing into the VPN

Once you have followed the checklist above , you may sign into the VPN.

5.1 Starting Your VPN Session

Follow these instructions to access and sign into the VPN Web Portal:

1. Open up your Internet browser.
2. In the URL field, type the following URL's and hit enter
<https://vpn1ppn.bc.ca> (Primary) or <https://vpn2ppn.bc.ca> (Secondary).



3. Once the URL loads, you will get the Sign In page (see next page):

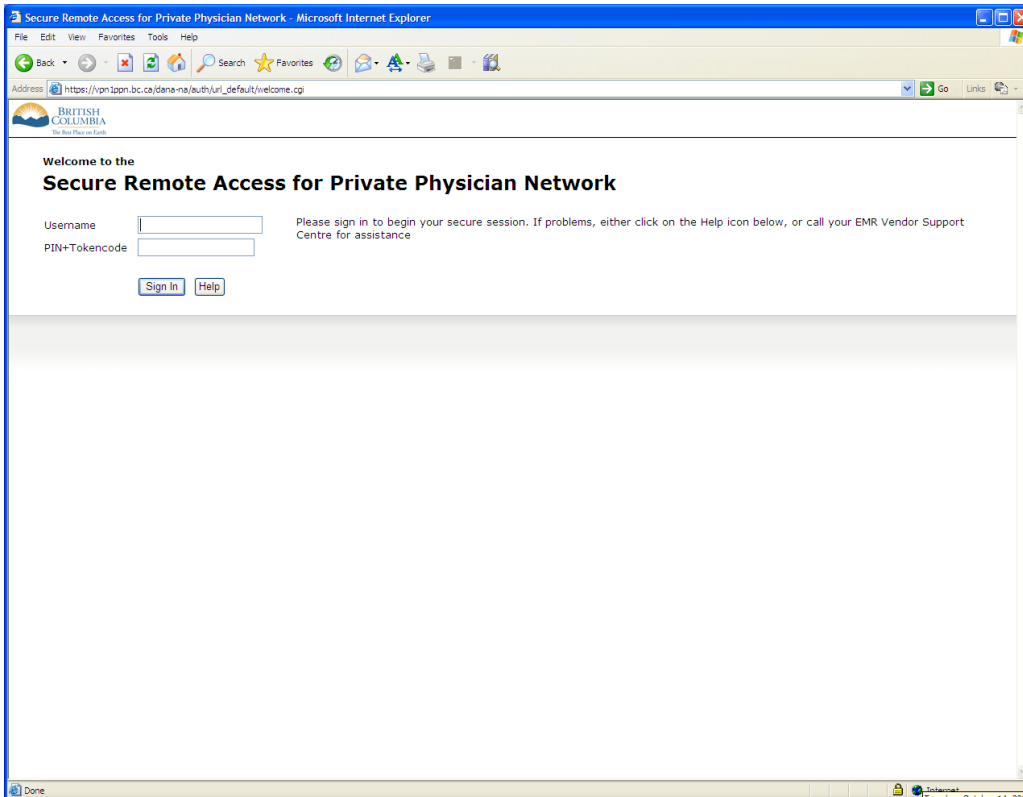


Figure 1: Sign In Page

4. In the **Username** field, type the user name provided in the information sent by TELUS. (Your main practice contact “PPN Contact” will have this information).

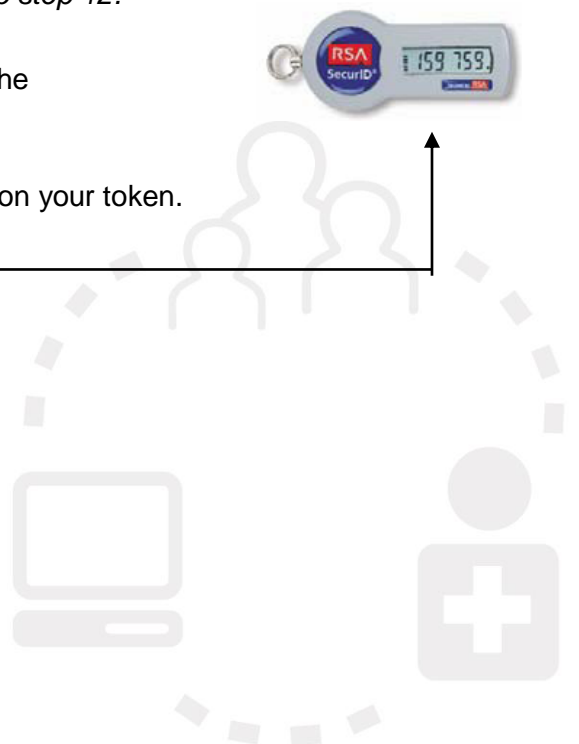
*Important: If this is the **first** time you are logging in then follow steps 5 to 11 below. For any subsequent logins please skip to step 12.*

5. Hit your <Tab> key to move your cursor to the **PIN+tokencode** field.

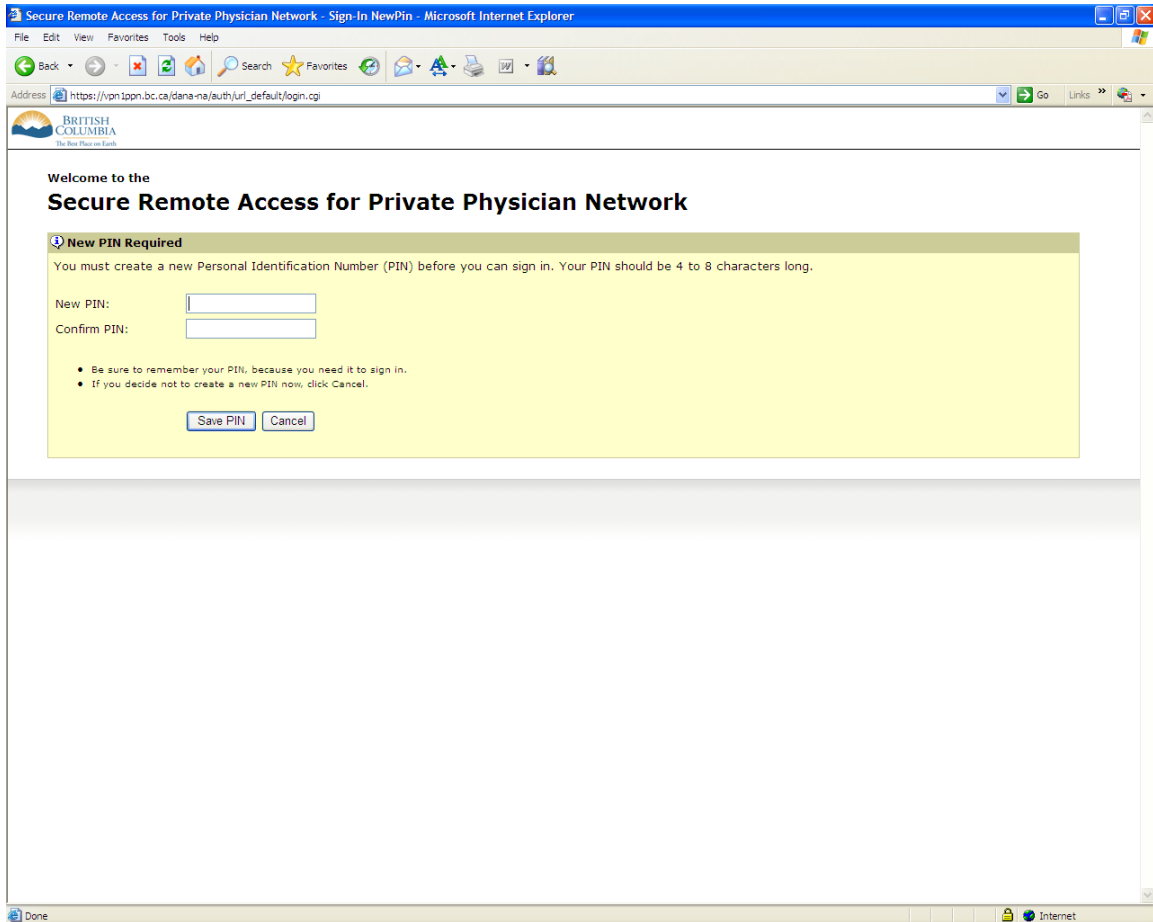
6. Type in your tokencode currently displayed on your token.



7. Click the **Sign In** button.



You will get the following page:

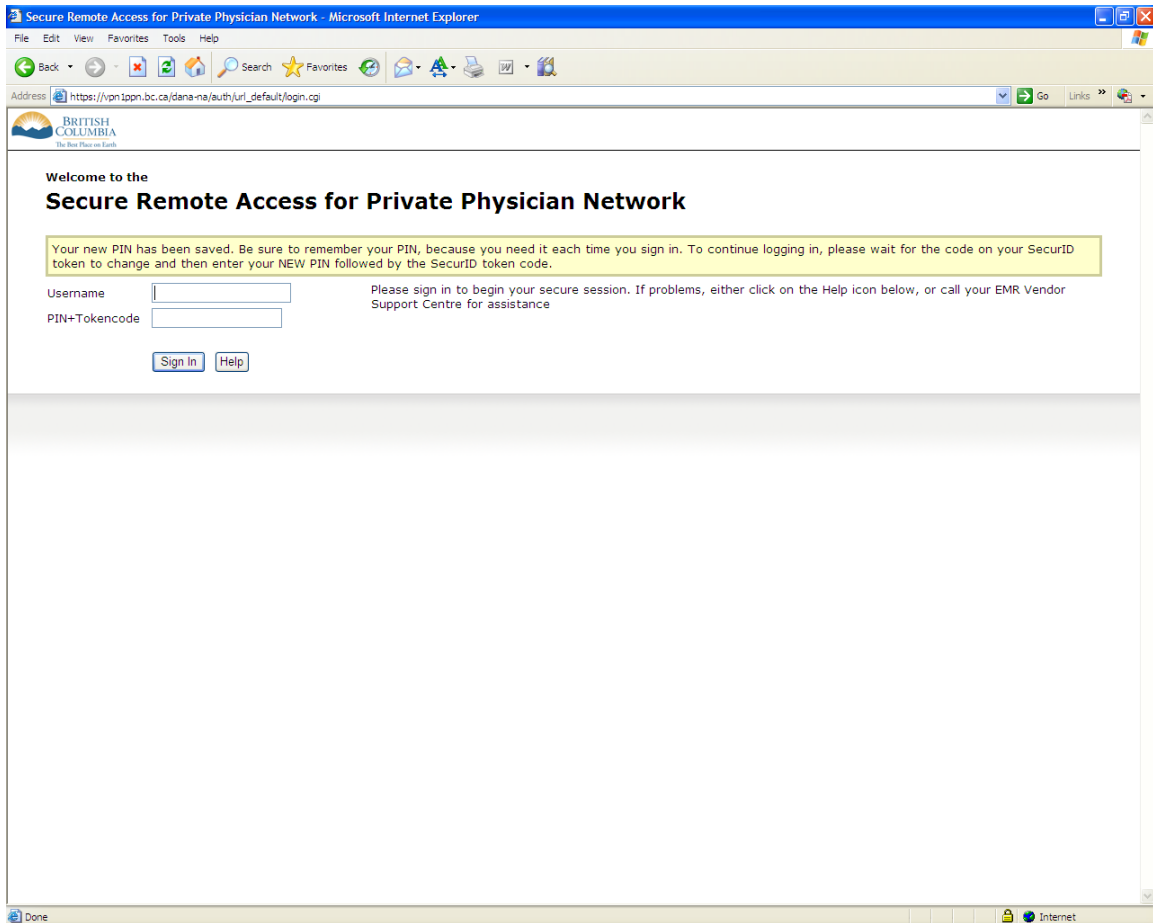


8. In the **New PIN** field type in a PIN that only you will know and remember. As stated on the screen displayed above your PIN can be 4 to 8 characters long.

Note: For security reasons it is highly recommended that you use all 8 characters rather than the minimum 4 and that you use a combination of alph and numeric characters (e.g. witt9751)

9. Hit your <Tab> key to move your cursor to the **Confirm PIN** field.
10. Re-type the PIN to make sure there are no typing errors.
11. Once finished click on **Save PIN** button.

You will get to the following page:



12. In the **Username** field, type the user name provided by TELUS and sent to your practice's PPN Contact..
13. Hit your <Tab> key to move your cursor to the **PIN+tokencode** field.
14. Type the PIN you chose followed by the tokencode currently displayed on your token. For example, if your PIN is **1234**, and the current tokencode is **800261**, enter **1234800261** without any spaces.
15. Click the **Sign In** button.

*Note: The sign in process can often take a few seconds. Please be patient and avoid pressing the **Sign In** button multiple times. After five unsuccessful attempts, the VPN network will assume that there is an unauthorized access attempt, and you will be required to call the EMR vendor “Tier 1 Support” help desk to have it reset.*

If your sign in is successful, you will be re-directed to the VPN Web Portal homepage (see below)

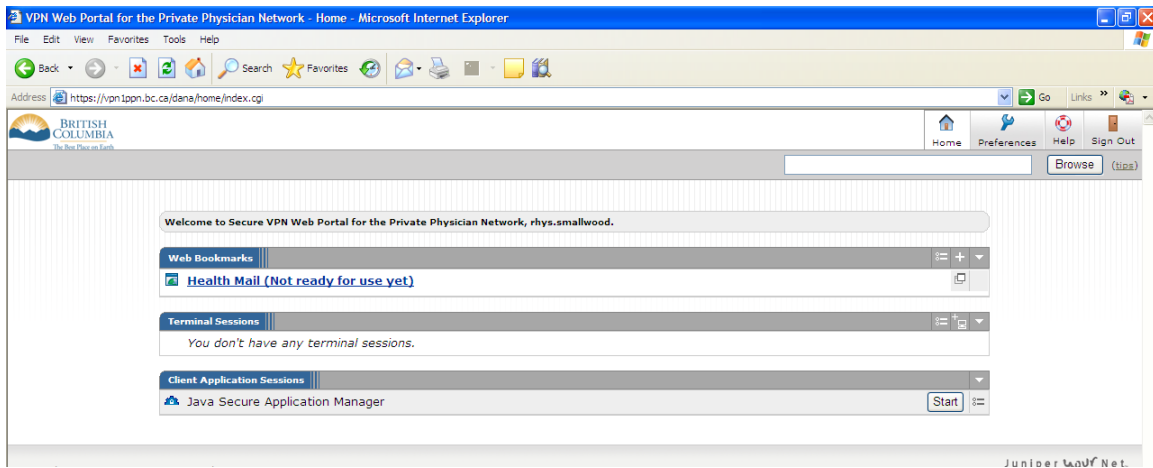


Figure 2: VPN Web Portal homepage

You are now inside the PPN virtual private network. The following sections provide instructions to add or modify an EMR vendor bookmark to the Web Bookmarks section of the VPN Web Portal. The network traffic for any bookmarks launched from this section will be sent over a secure and encrypted VPN tunnel to the PPN.





6.0 Using the VPN Web Portal

Your VPN Web Portal allows you to access your practice's EMR application remotely. To launch your EMR application, you need to log in to the VPN Web portal.

To launch your EMR application, you need to log in to the VPN Web portal for either a Windows or non-Windows computer (E.g.: Macs). Each requires a different set of steps.

Important: Windows users should only use the method described in the section 6.1 below and NOT the Java Secure Application Manager method (section 6.2) which has been only set up to support non-Windows computers. Similarly non-Windows users should only use the method described in section 6.2.

6.1 Windows users

The first time you log in to the VPN Web Portal you will not see a bookmark for your EMR vendor. Application. You will need to add this bookmark in order to access your EMR application. This only needs to be done once. Once it has been added, the EMR vendor bookmark will be visible every time you log in to your VPN account.

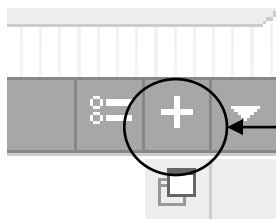
Note: If you add a bookmark to the Primary 'https://vpn1ppn.bc.ca' portal page first time you visit it, it will not be visible on the Secondary 'https://vpn2ppn.bc.ca' site and will need to be added when you log to that site for the first time.

Log in to your VPN Web Portal homepage in the browser (see figure 2: VPN Web Portal Home Page). You will see a 'Web Bookmarks' bookmarks section:



Follow these steps to add a Web bookmark:

1. Click the '+' symbol (see image below)



You will see the "Add Web Bookmark" page displayed as follows:

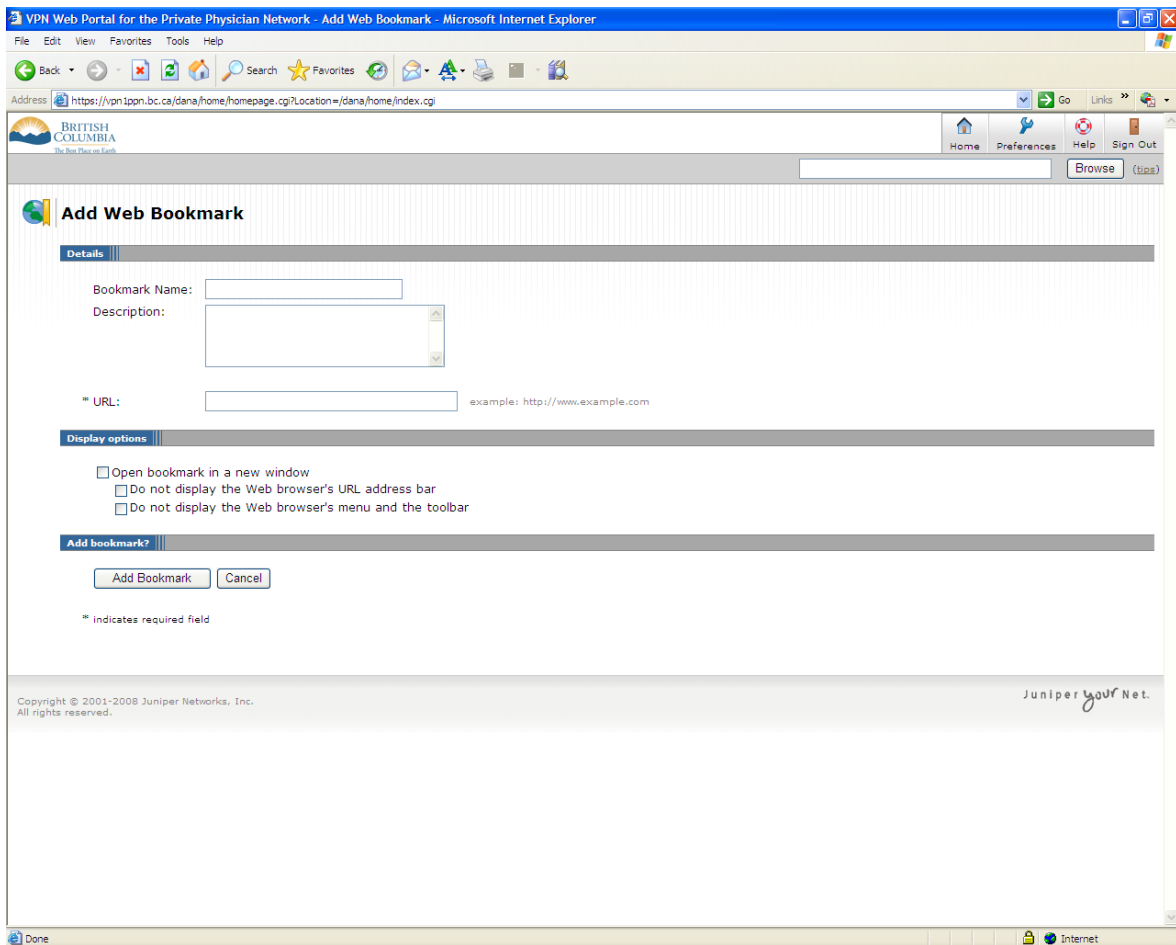


Figure 3: Add Web Bookmark page

2. Fill out the fields as follows:

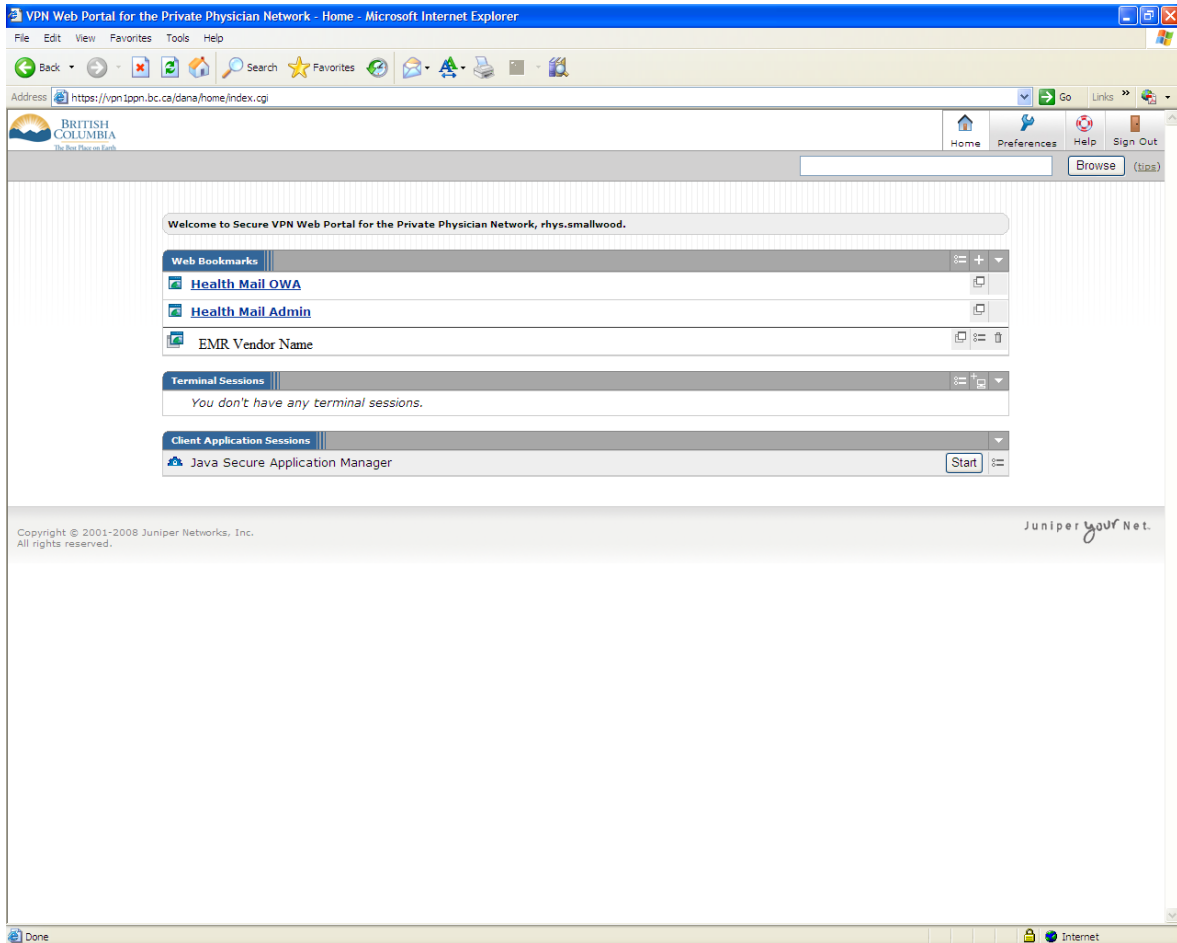
Bookmark Name: “EMR vendor name” (at your discretion to choose a different name)

Description: If you want to add a description to the bookmark you can enter it here.

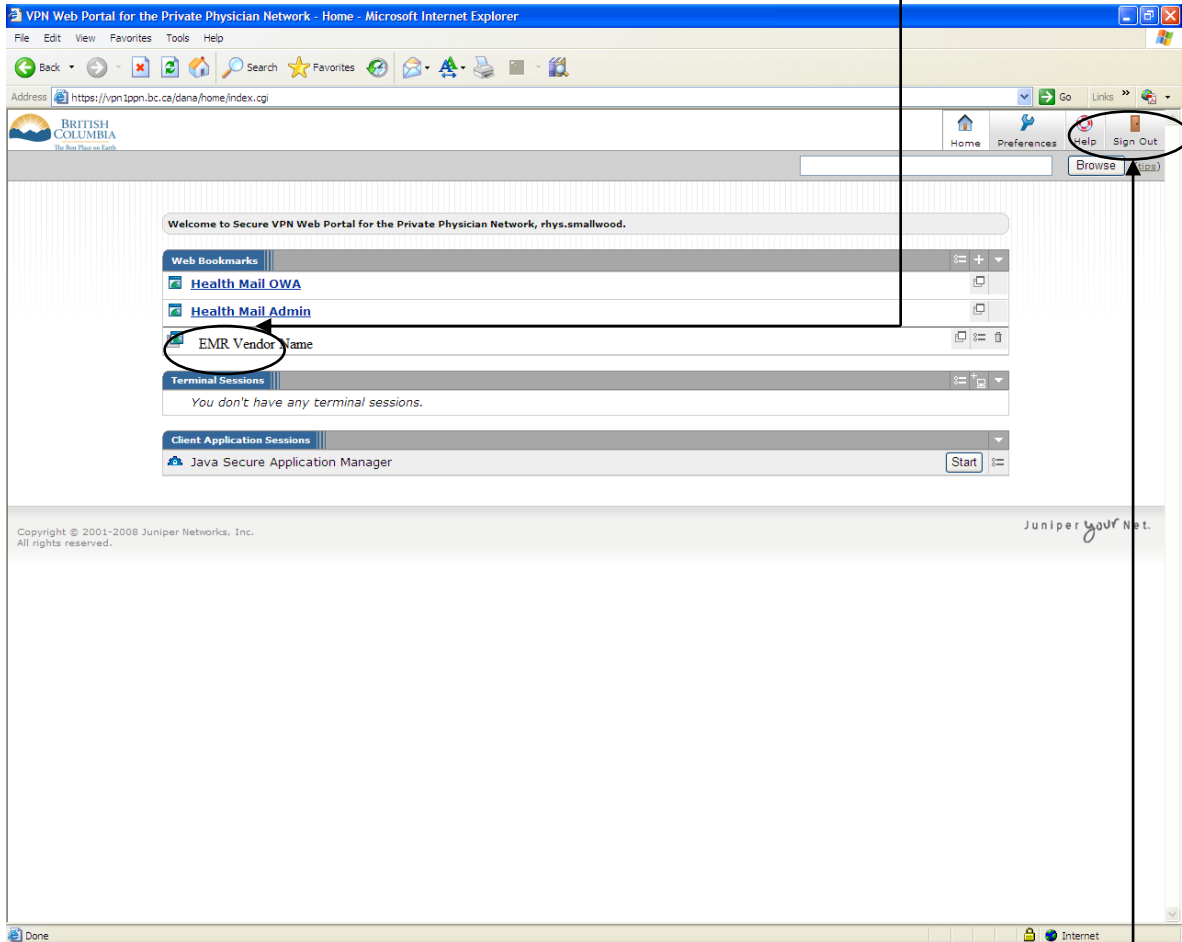
URL: Your EMR vendor is responsible for providing you with the exact URL (or IP address).

Under Display Options check the “Open bookmark in a new window” option. Uncheck the other options.

Once completed press “Add Bookmark” button at the bottom of the page. Your Web Portal home page should now look like this:



3. To launch the EMR application click on “EMR vendor” bookmark in the Web Bookmarks section of the portal. A new browser window will open up and take you to EMR application login page.



Note: In order to access the EMR application over the SSL VPN, you will still require software clients for the specific EMR vendor application (example: Citrix or RDP clients). Traffic from these clients will go over the PPN when you launch the EMR application. (Contact your EMR vendor to find out where you can download the supported clients):

4. Once the EMR application is launched, please follow the instructions from your EMR vendor on how to proceed.

To exit the EMR application and VPN, log out of the application first then use the “Sign Out” link on the VPN Web portal page.

Editing or Deleting Bookmarks

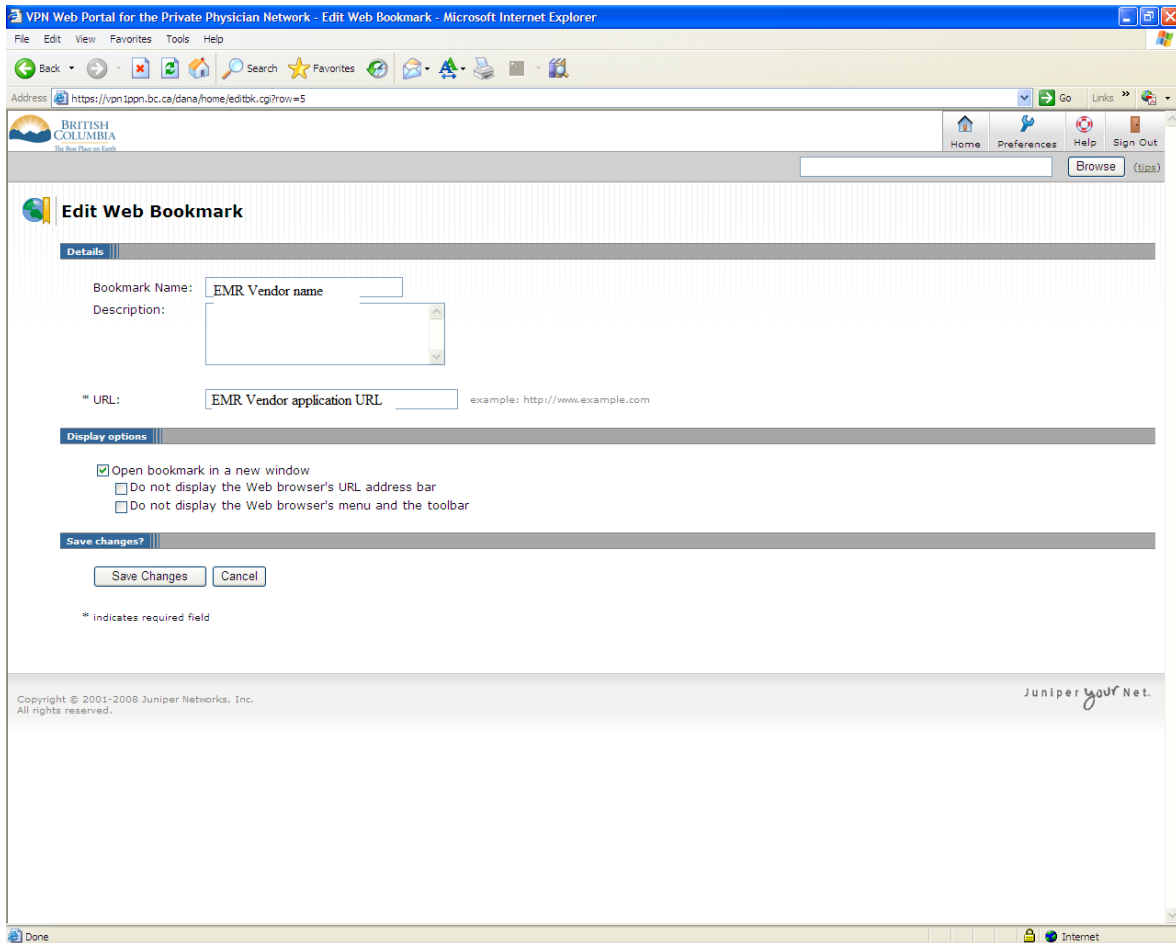
If for some reason information was entered incorrectly for a Web Bookmark or you want to change its name you can use the “Item Properties” feature to edit the setting again.

Click the “Item Properties” button to edit the Web Bookmark properties. Click the “Delete Bookmark” button if you want to delete the bookmark completely.



If you click the “Item Properties” button for editing you will be taken to the following page:





Here you can make your changes and then press “**Save Changes**” at the bottom of the page.

6.2 Non-Windows Users

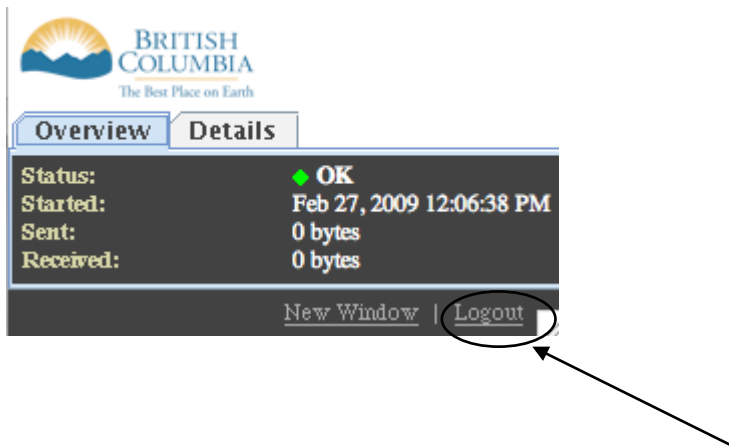
This section is for non-Windows users only. See previous section for Windows users.

The steps to access the EMR application using a non-Windows system are different from those for a PC user. Non-Windows users will utilize the JSAM (JAVA Secure Application Manager) to create a connection to the EMR application.

IMPORTANT: JSAM must be launched (manually or automatically) before you can sign into your EMR application.

Depending on which EMR vendor you have signed up with, JSAM will either launch automatically or manually.

To make sure the JSAM window is launched, look for the following on your screen (usually in bottom right of the screen):



To exit JSAM, log out of the application first then use the “Log Out” link on the VPN Web portal page.

6.2.1 Automatic Launch

Some EMR vendors have only a single URL or IP address for all their users. In this case JSAM is configured to launch automatically.

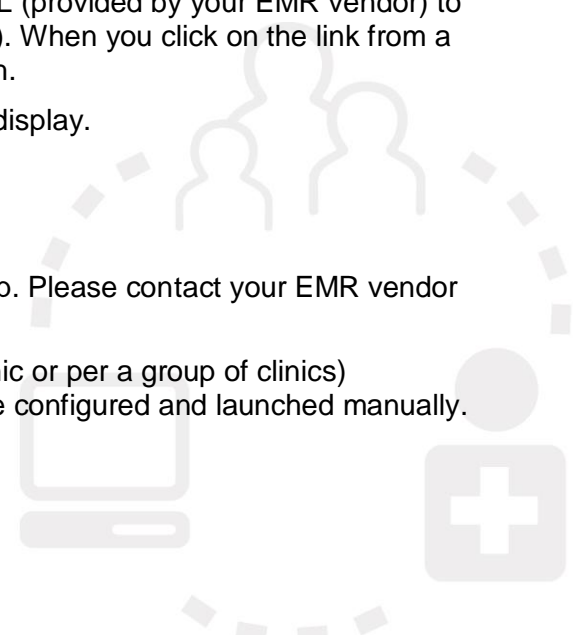
To get access to your EMR, add the IP address or URL (provided by your EMR vendor) to the Web Bookmarks section (see previous section 6.1). When you click on the link from a non-Windows machine, JSAM will automatically launch.

After JSAM is launched, your EMR login page should display.

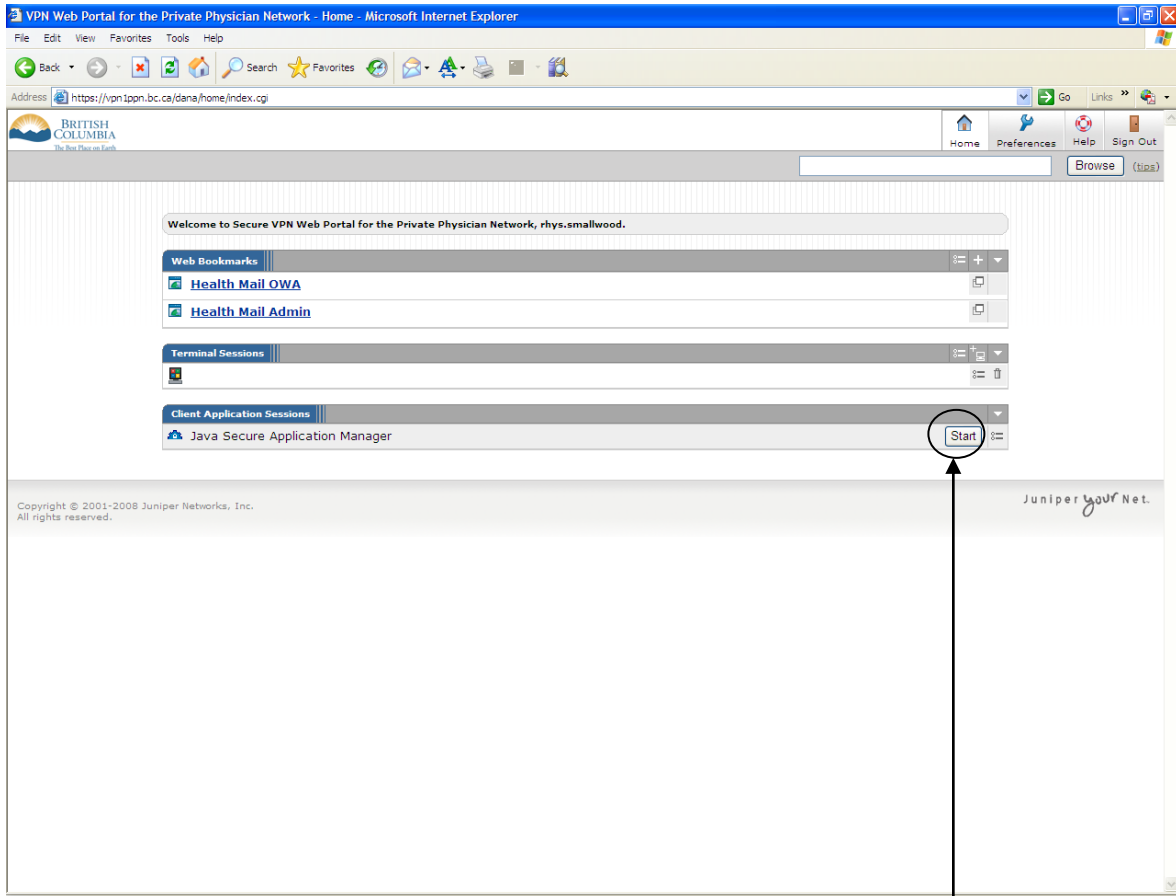
6.2.2 Manual Launch

Important: Not all EMRs require this configuration step. Please contact your EMR vendor support for questions regarding this.

Some EMR vendors have multiple URLs or IP (per clinic or per a group of clinics) addresses for their users. In this case JSAM has to be configured and launched manually.



Log in to your VPN Portal homepage in the browser. You will see a 'Client Application Sessions' section with Java Secure Application Manager" (JSAM). Follow these steps to setup your Connection:

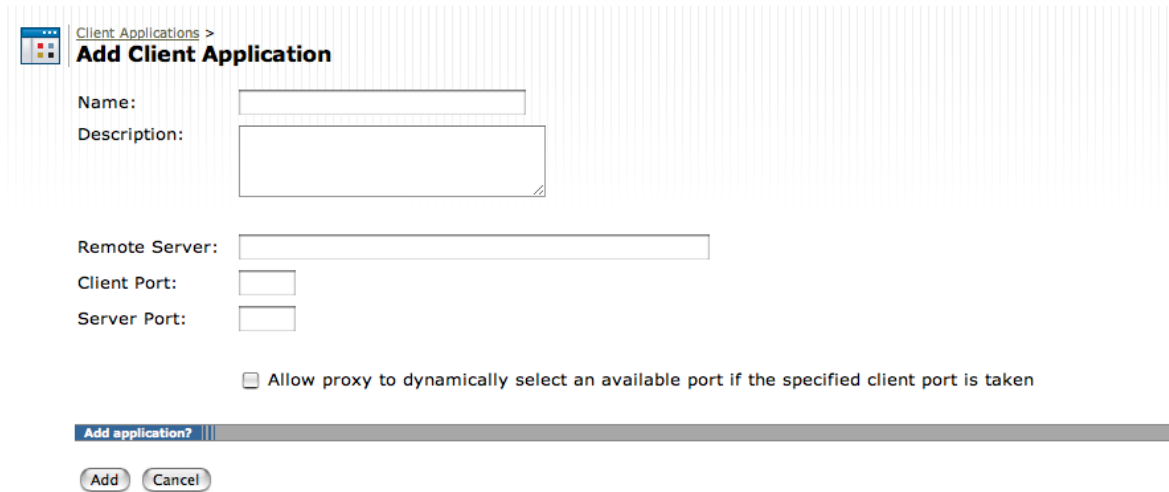


1. Click the JSAM "Item Properties" button.

You will see with the following screen:



2. Click “Add Application...”. You will see the following screen:



The screenshot shows a dialog box titled "Client Applications > Add Client Application". It contains the following fields and options:

- Name: [Text Input Field]
- Description: [Text Area]
- Remote Server: [Text Input Field]
- Client Port: [Text Input Field]
- Server Port: [Text Input Field]
- Allow proxy to dynamically select an available port if the specified client port is taken

At the bottom, there is a progress bar labeled "Add application?" and two buttons: "Add" and "Cancel".

Enter the information provider by your EMR Vendor.

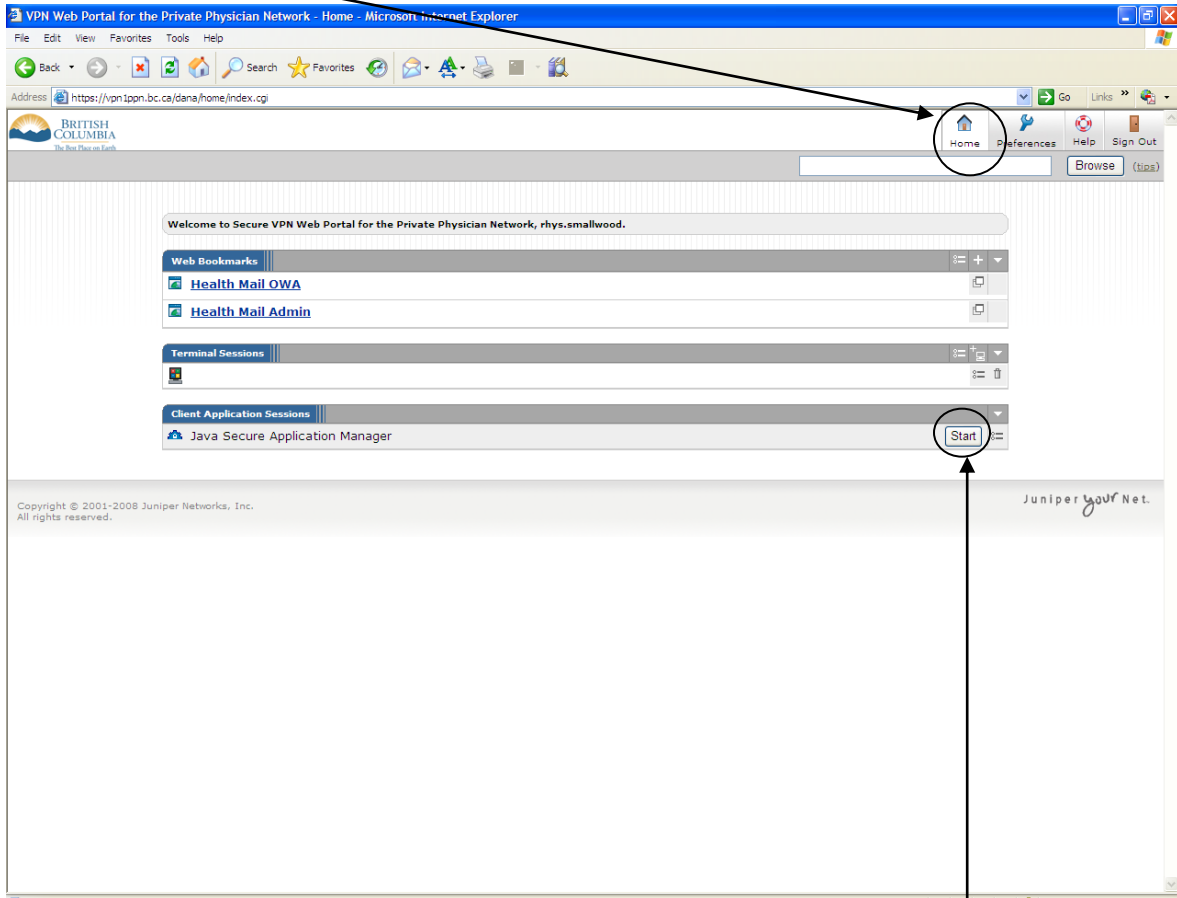
3. Click “Add”. You will see the following screen:



The screenshot shows the main "Client Applications" interface. It features a title bar with a window icon and the text "Client Applications". Below the title bar are two buttons: "Add Application..." and "Options". A table is visible below the buttons, with a header row containing "EMR Name" and a search icon on the right. The table content is currently empty.

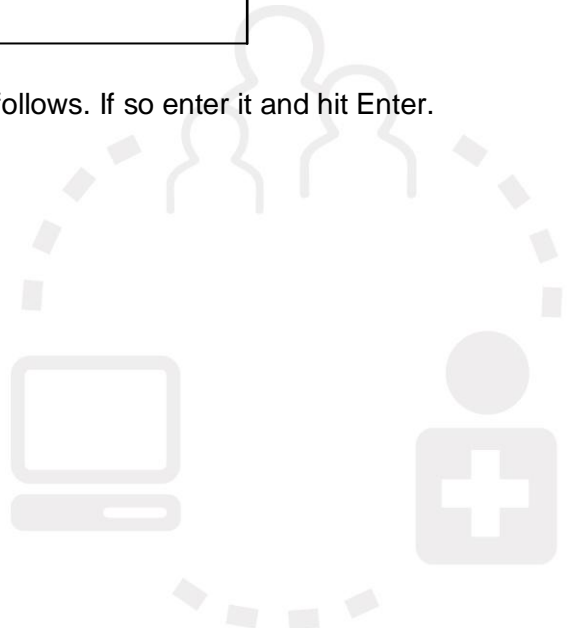


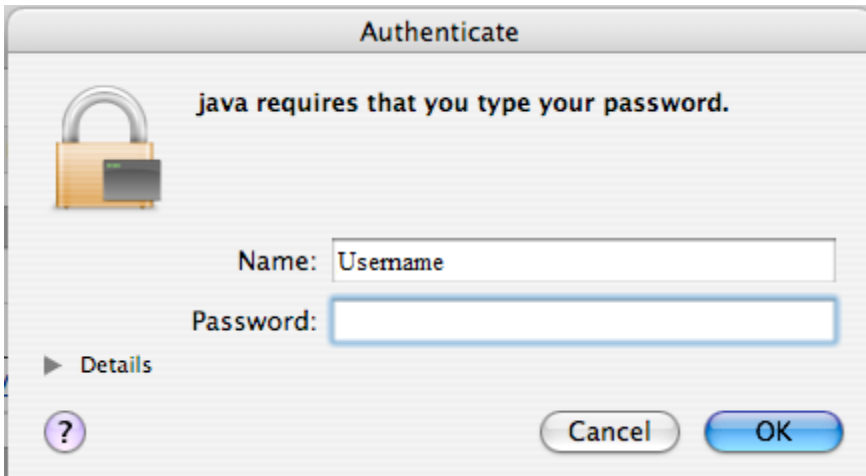
4. Click the “Home” link in the top right corner of the window. You will see:



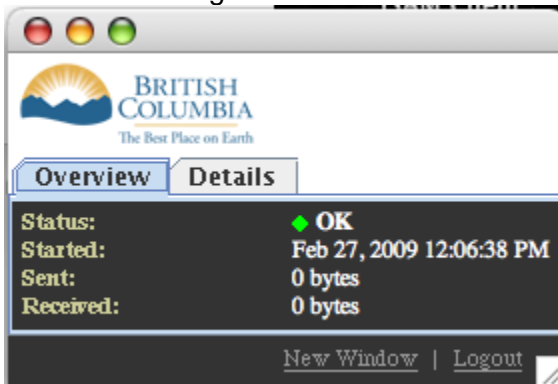
5. Click the JSAM “Start” button.

On a Mac you may be prompted for your password as follows. If so enter it and hit Enter.

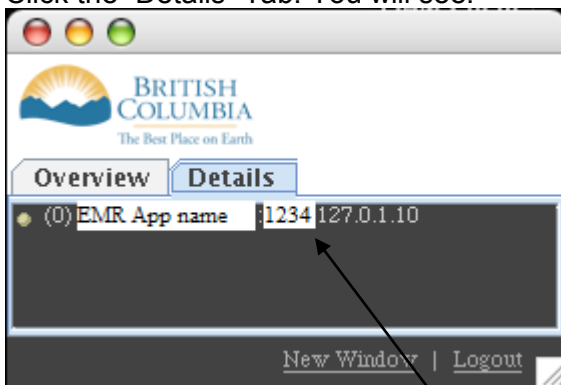




6. The following window will load outside of your browser.

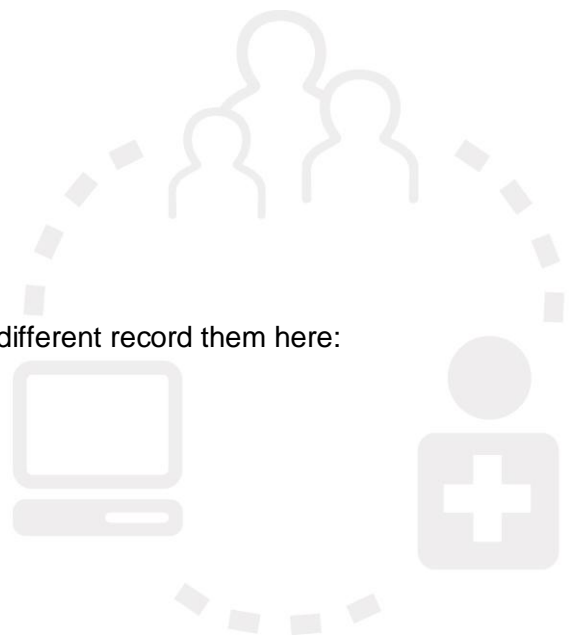


7. Click the “Details” Tab. You will see:



8. Make note of the numbers noted here. If yours are different record them here:

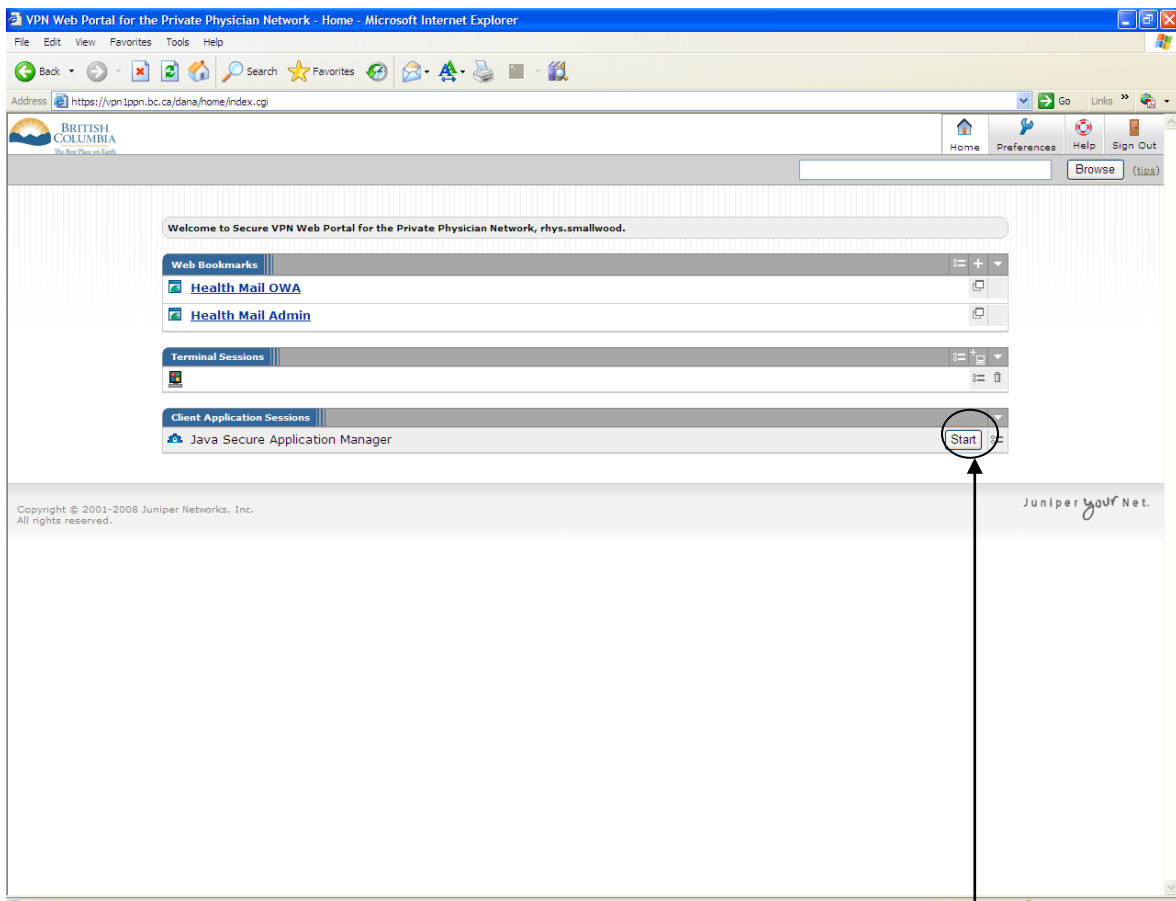
1234 _____
 127.0.1.10 _____



Open our EMR application and use the numbers above to connect to the EMR application.
(Note: You may require additional instructions from your EMR vendor)

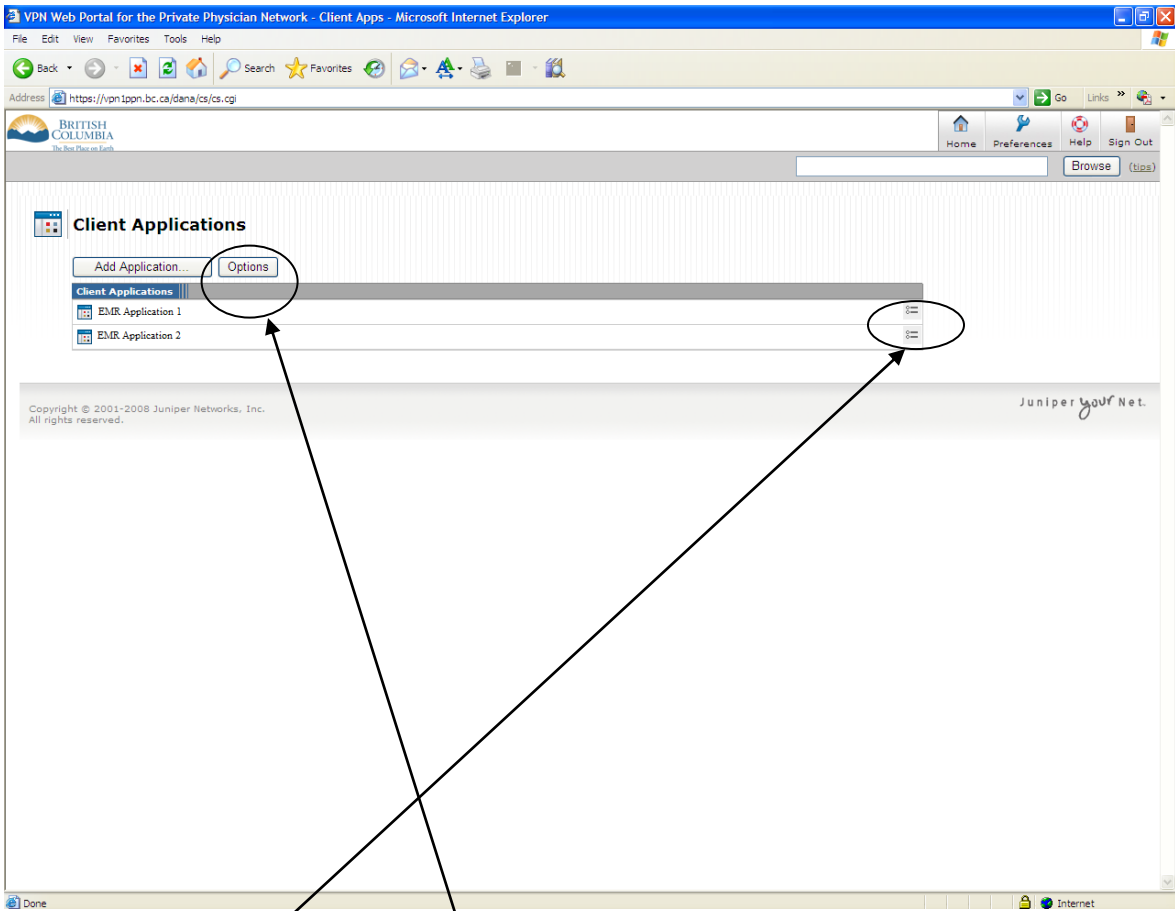
Editing or Deleting JSAM Client Applications

If for some reason information was entered incorrectly for a JSAM application or you want to change its name you can use the “Item Properties” feature to edit the setting again.



1. Click the JSAM “Item Properties” button.

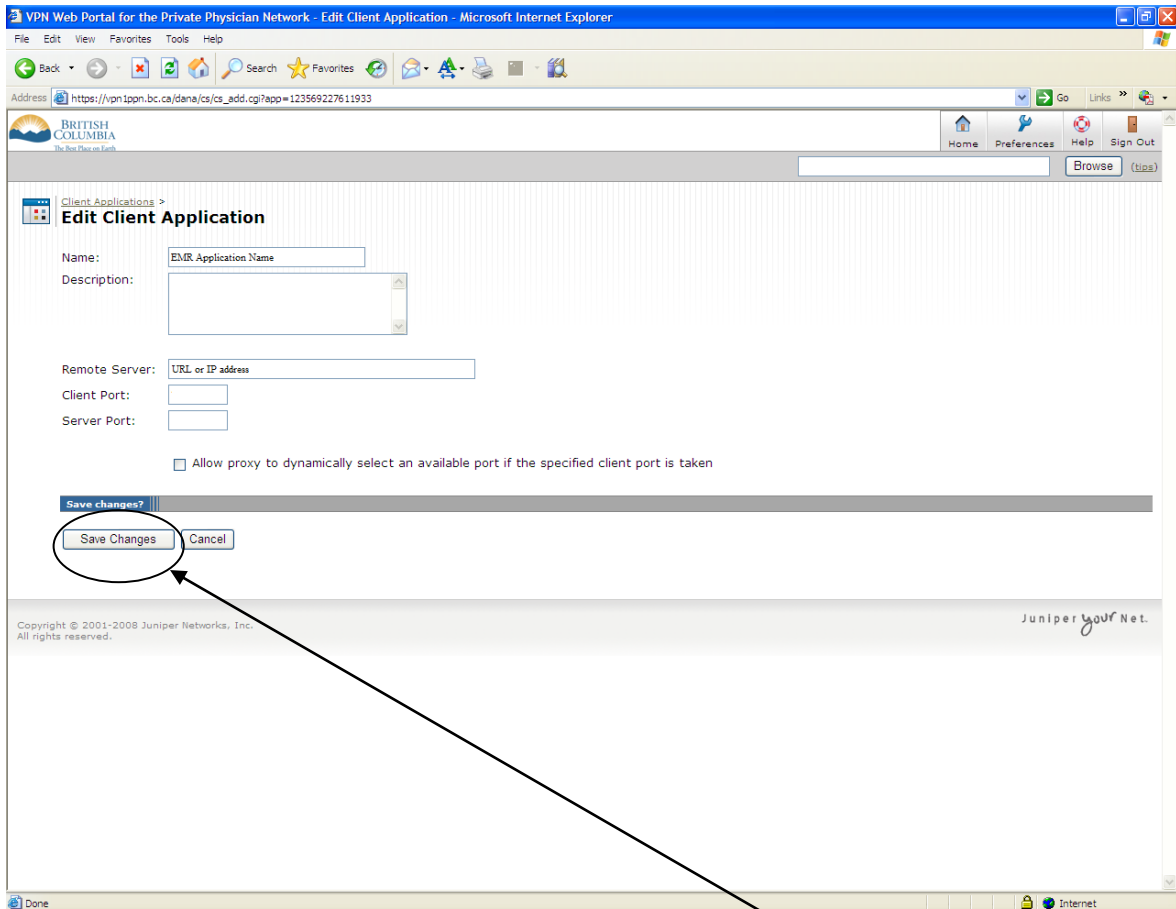




2. Click on “Item Properties” to edit the application.
3. To delete the application click “Options” and skip to instruction 4 below.



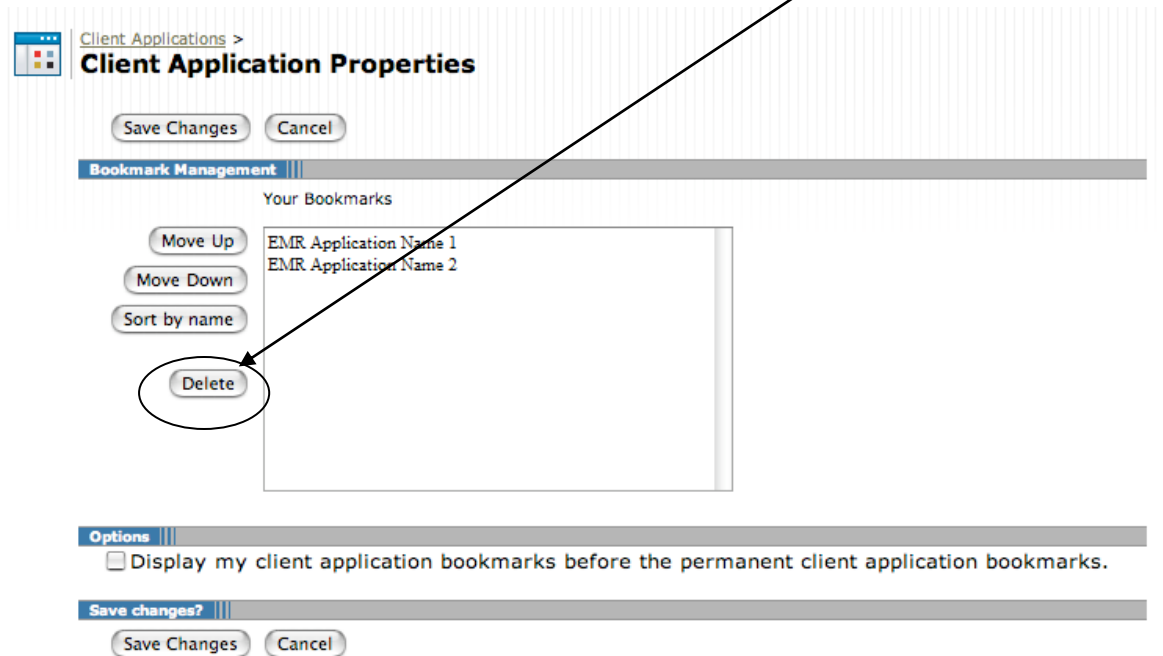
4. You will see a screen similar to:



You can make changes here and when done press “Save Changes”.



5. To delete the EMR application for JSAM select the application and press delete.



6.3 Browsing the Internet

Browsing the internet is not recommended through the SSL VPN service since only EMR applications and PPN Email services have been tested for security and reliability.

While the Internet browse feature is currently available on the VPN Web Portal it is not recommended for use and it may be removed at a future date.

To access the Internet without going through the VPN "tunnel", exit from the VPN Web Portal, either by ending your session (see section 5.5 below) or minimizing the Portal browser window. Once done, you will be returned to your standard computer desktop display, and you would follow your current procedure for Internet access through your preferred browser.

IMPORTANT:

- It is highly recommended that you have up to date Anti Virus software installed and running on your computer when accessing Internet sites with sensitive information.
- Do not go to or open files from unknown or untrusted Internet sites.

- Follow your practice's current procedures for protecting any patient care data accessed over the Internet from a remote location.

6.4 Other Features of the VPN Web Portal

There are other features available on the VPN Web Portal. Some of these are described below:

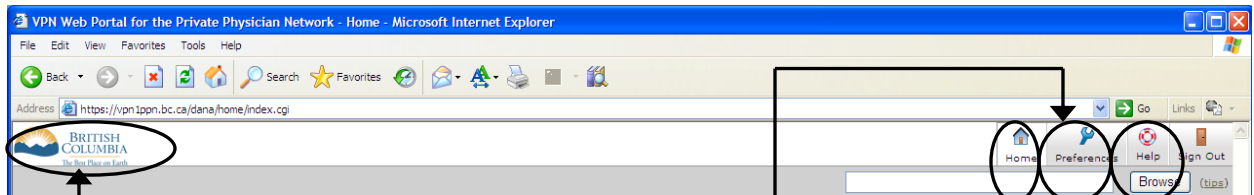
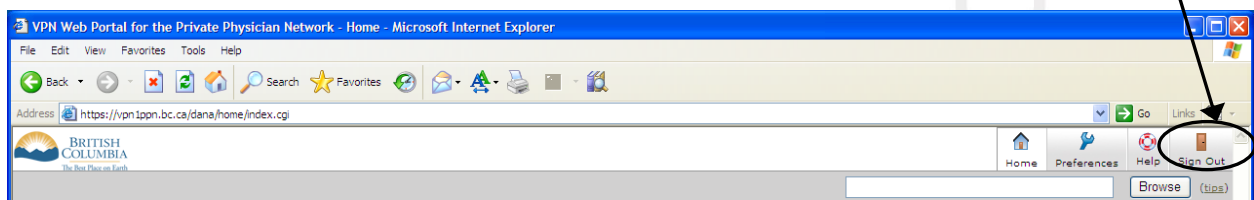


Figure 4: VPN Web Portal Features

- VPN Web Portal homepage shortcuts
 - Click on the British Columbia logo on top left of the screen or Home icon near the top right of your screen to go back to your VPN Portal homepage
- Preferences
 - Clicking on this will allow you to re-order sections (Web Bookmarks, Web Bookmarks) and change other preferences for the VPN Web Portal.
- Help
 - This link will provide you with general information on the VPN User Interface.

6.5 Ending Your VPN Session

1. To close the VPN session, simply click on "Sign Out" located at top right of the screen.



2. Once the screen below is displayed, you have successfully signed out of the VPN.

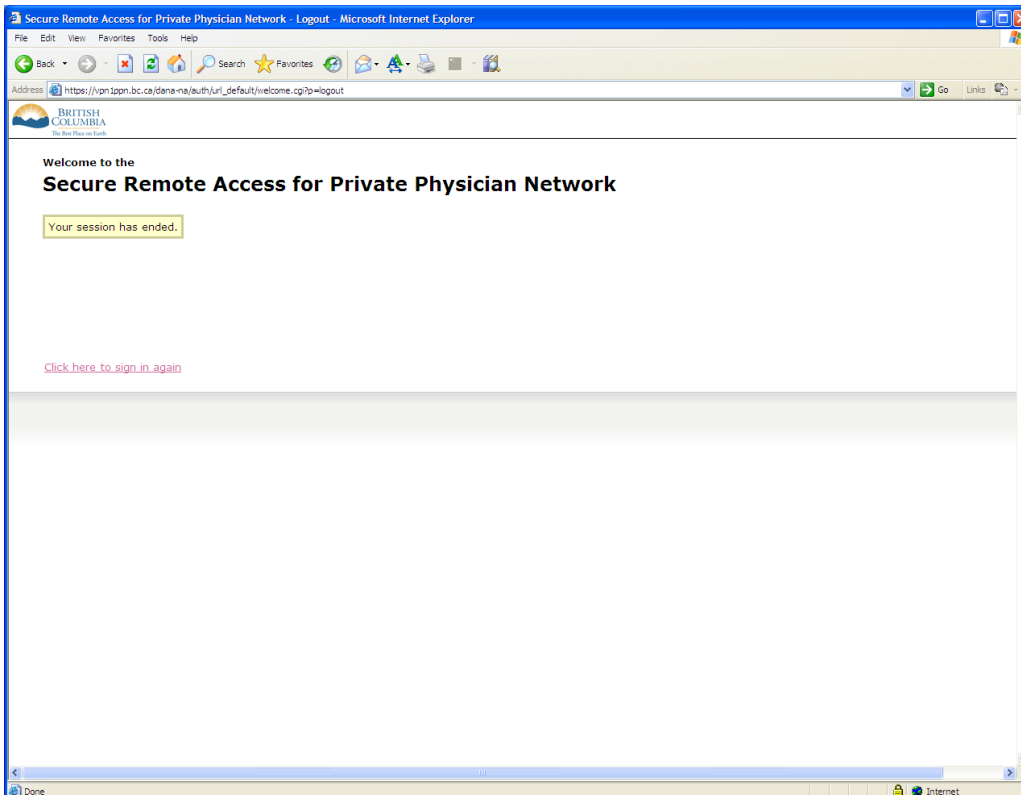


Figure 5: Confirmation of Ending the Session

7.0 Troubleshooting

Your EMR vendor 'Tier 1 Support' help desk is your first line of support when accessing your EMR vendor EMR or PPN email service through the VPN Web Portal. Other Internet access from a remote location (E.g. home) through a standard Internet connection is not supported through EMR vendor 'Tier 1 Support'.



Support information is available in:

- "EMR and PPN Support Quick Reference": A quick reference summary for physicians and staff about the technical support they can expect to receive when experiencing EMR and PPN related problems, as well as what they are responsible to resolve; and
- "EMR and PPN Support Responsibility Matrix": A detailed description of the roles and responsibilities for all parties involved in supporting EMR and PPN implementations through PITO.

Both documents are available on the PITO web site at <http://www.pito.bc.ca/>

7.1 Unsuccessful Sign In

If this message displays: **Invalid username or password. Please re-enter your user information.**, wait for the tokencode to refresh and try again.



After five unsuccessful attempts, call the EMR vendor 'Tier 1 Support' help desk.

7.2 Next Tokencode Prompt

On occasion, even after you type your PIN or tokencode correctly, the system will prompt you to enter the next tokencode in order to confirm your possession of the token. This is called a *'token resync'*. If this happens, the following screen will display.

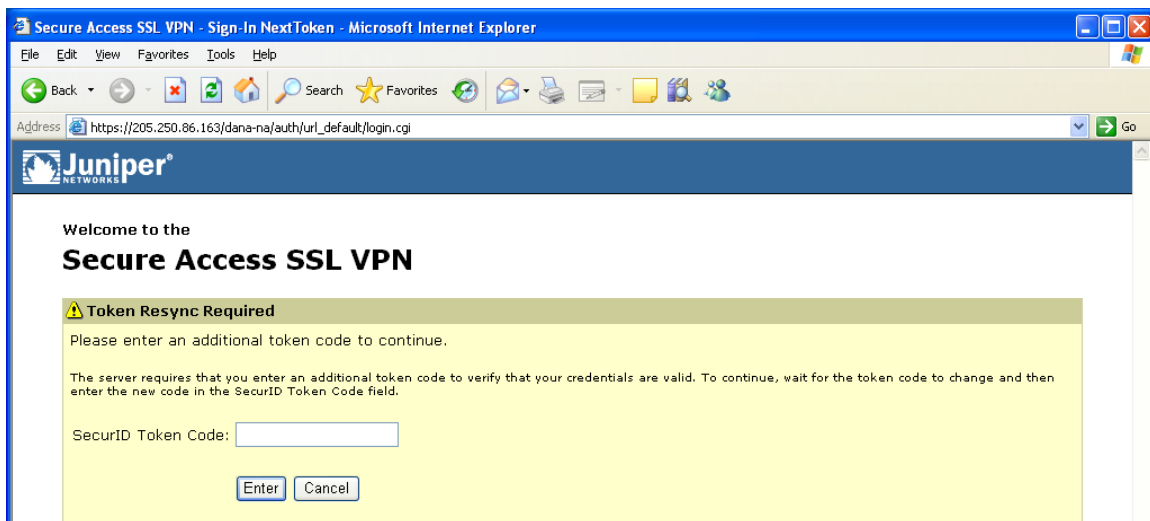


Figure 6: Token Resync Screen

1. Wait until the tokencode changes, and then type the new one. Enter only the tokencode - do not enter your PIN. *Note: The tokencode changes every 60 seconds.*
2. If you are not granted access after correctly entering the next tokencode, call the EMR vendor 'Tier 1 Support' help desk.

7.3 Multiple Sessions

If you try to open the VPN when a prior session is already established, (often due to not signing out of a previous session), the following screen will display:

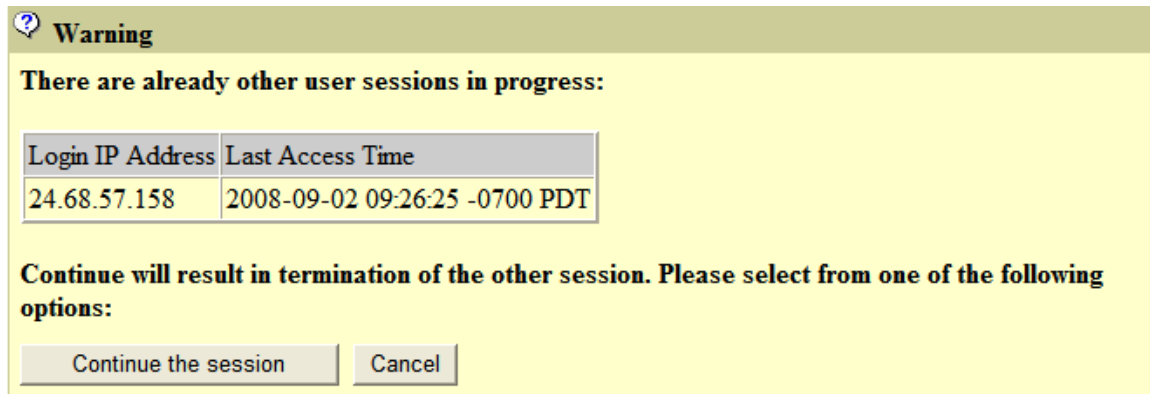


Figure 7: Multiple User Session Warning Screen

Click the button to proceed.

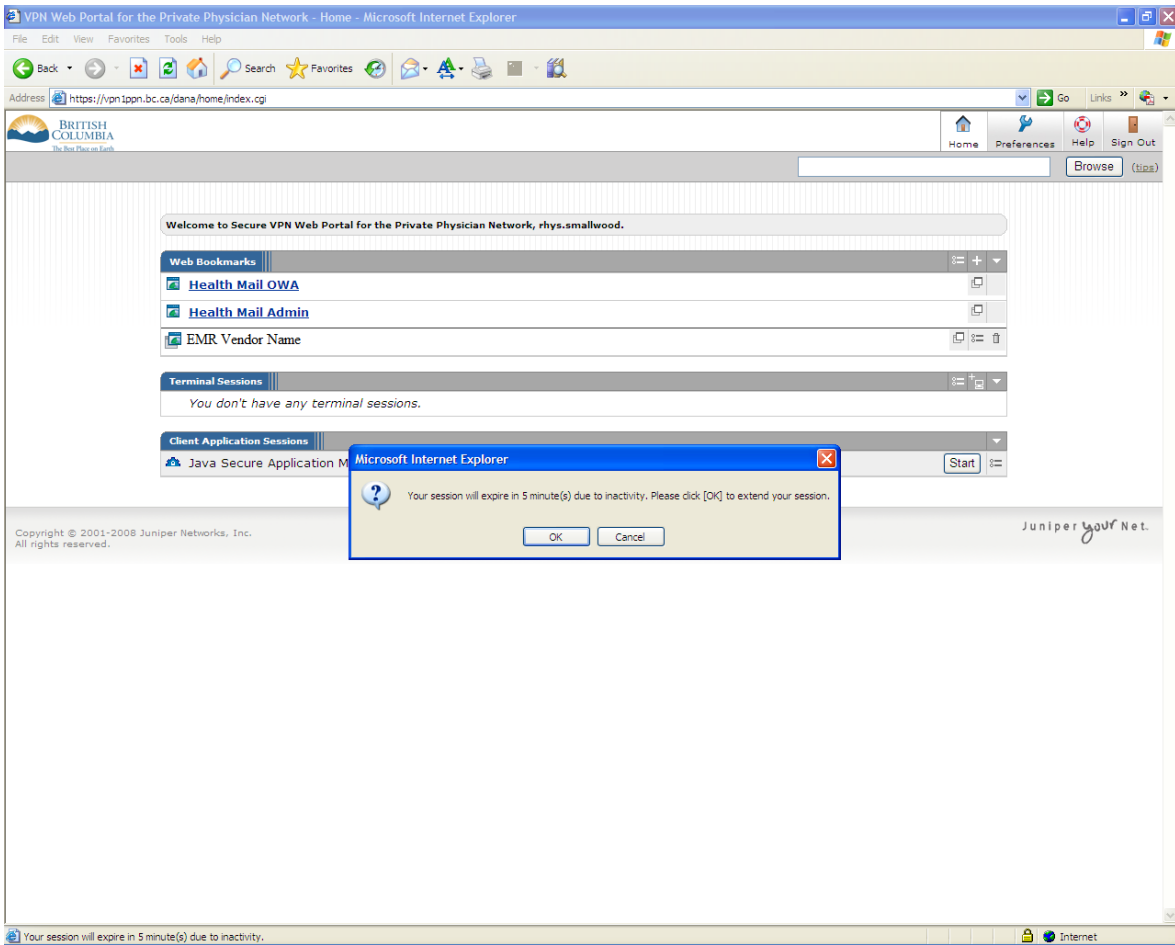
7.4 Automatic Sign out of VPN session



Current settings on the VPN only allow for 8 hours of active use. After that you will be required to log back in.

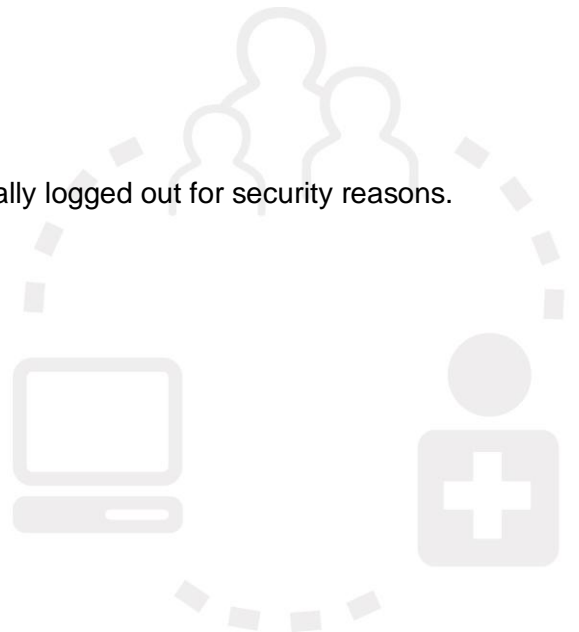
If you are inactive on the VPN for 10 minutes you will get a warning message:

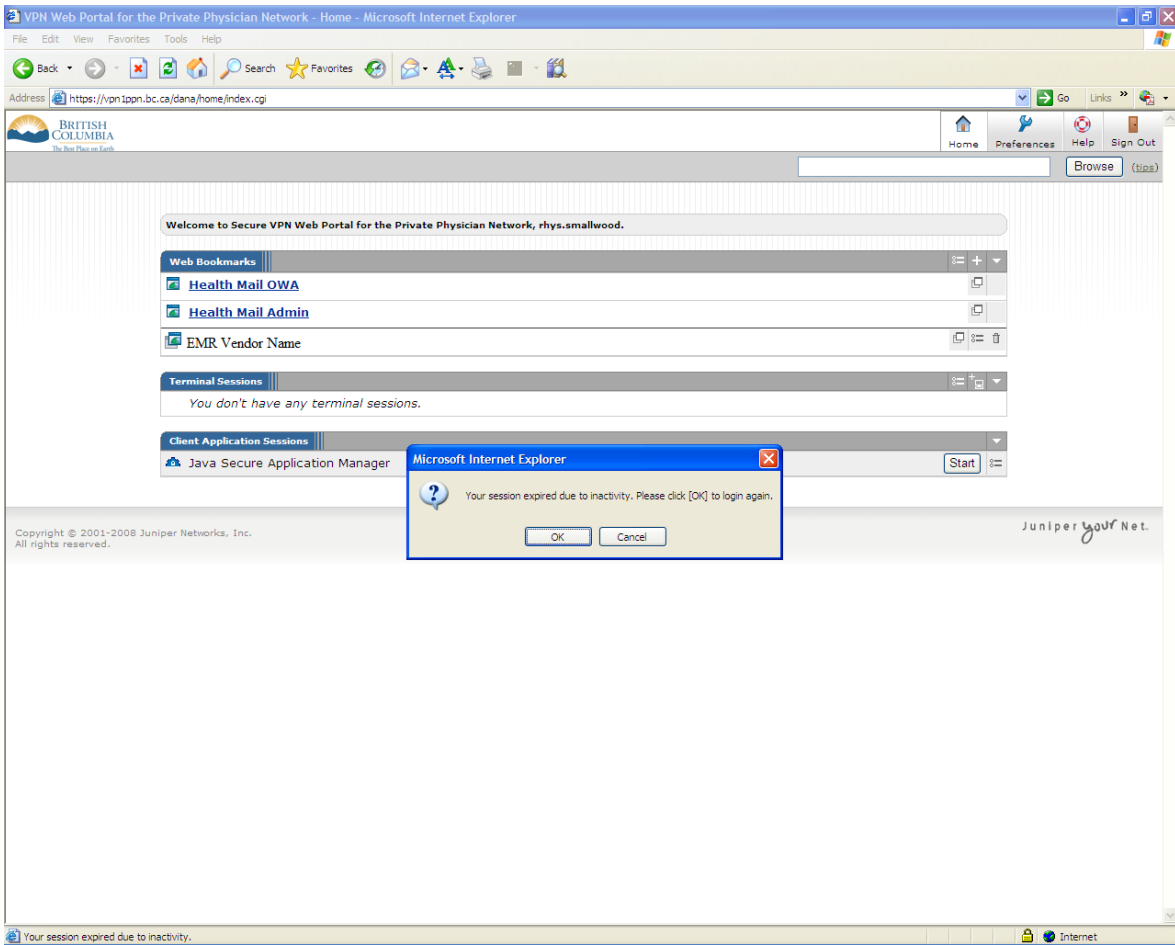




Click “OK” button to continue the VPN session.

If you are inactive for 15 minutes you will be automatically logged out for security reasons. You will get the following message:





If you click “OK” button then you will get following message:

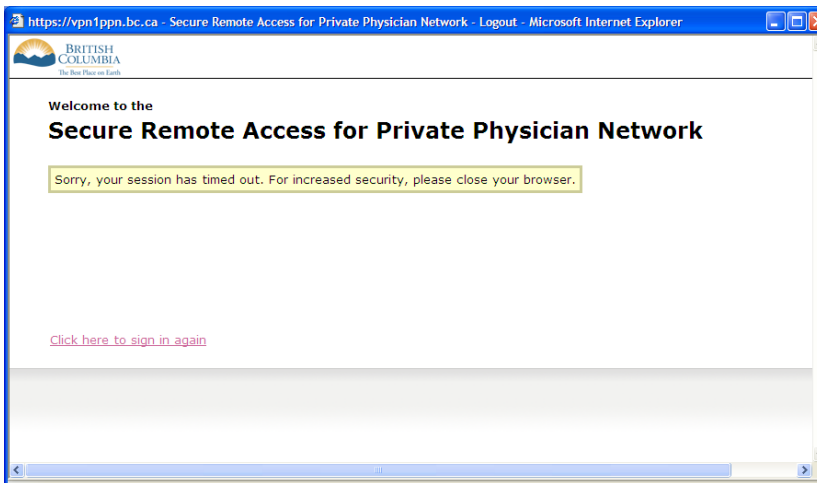


Figure 8: Session Expired Dialog Box

To sign back in to the VPN Web Portal, use your username and pin+tokencode as described earlier in this document.

7.5 VPN Server Busy

TELUS maintains two VPN Web Portal sites. The Primary site (<https://vpn1ppn.bc.ca>) and the Secondary site (<https://vpn2ppn.bc.ca>)



Please use URL: <https://vpn1ppn.bc.ca> as the Primary site.
The Secondary site URL: <https://vpn2ppn.bc.ca> should be used if you are experiencing difficulties using the Primary site.





8.0 Security Recommendation

PITO provides a general requirement that the location and remote computer used for accessing the VPN Web portal must be secure



See the Section 8 (Privacy and Security Policies) of the PITO Policies document under the 'Documents Library' link at <http://www.pito.bc.ca/Documents/default.htm>.

More specifically, the Ministry of Health Services recommends that you have AntiVirus software installed with the most up to date virus definitions and automatic updating enabled. This will assist with preventing viruses and other malicious code from getting to the PPN through your remote computer.

In the future, the Ministry may **require** some type of AntiVirus software prior to physicians and their staff connecting to the VPN service.

Please contact your practice's computer support person for recommended AntiVirus software programs.

9.0 Token Management Practices

This section describes the rules and procedures to be followed by the practice regarding the management of tokens. This includes how to order new tokens, what to do when a token is lost or stolen and what to do with a token when a staff member leaves the practice.

9.1 Request for Additional Tokens

As part of the PPN services, each practice is entitled to a VPN Token for the following staff (Baseline Allowance):

- Every PITO-qualified physician in the practice; and
- One token for the lead MOA/Administrative staff member

A PITO-qualified physician is a physician that has signed a PITO Registration Agreement and has qualified for PITO funding.

Tokens are normally ordered, by the practice, in conjunction with the PPN circuit order through the PITO Relationship Manager. This is done prior to the practice going live with their EMR.

Additional tokens can be ordered by providing a valid business reason describing the purpose and frequency of the token use. To request additional tokens the practice must fill out the *Additional Tokens Request* form which can be found on the PITO Web Site at : <http://www.pito.bc.ca/cms/document-library/>. For help in filling out this form please contact your PITO Relationship Manager.

9.2 Token Deactivation, Reactivation, Reassignment

Deactivation

Tokens not being used should be deactivated. This will ensure the token is not used by an unauthorized user.

The deactivation of a token is requested by completing the *Token Deactivation Request* form and sending it to the email included on the form. This form can be found on the PITO Web Site at: <http://www.pito.bc.ca/cms/document-library/>

Reactivation

Tokens which have been deactivated can be reactivated for use by the originally assigned user. As an example, a practice may wish to deactivate a token if a physician goes on sabbatical and then reactivate it on the physician's return.

The reactivation of a token is requested by completing the *Token Reassignment or Reactivation Request* form and sending it to the email included on the form. This form can be found on the PITO Web Site at: <http://www.pito.bc.ca/cms/document-library/>

Reassignment

Tokens can be reassigned to another user if the original user no longer needs the token and a new user requires it for their work. Tokens that were deactivated can also be reassigned. Some examples of when a token can be reassigned are described below. Tokens should only be reassigned to another authorized practice member.

The reassignment of a token is requested by completing the *Token Reassignment or Reactivation Request* form and sending it to the email included on the form. This form can be found on the PITO Web Site at: <http://www.pito.bc.ca/cms/document-library/>

9.3 Lost or Stolen Tokens

If a user loses a token or a token is stolen, a replacement token can be provided. However the missing token must first be deactivated so that it is not used by an unauthorized individual.

The deactivation of a missing token and the request for a replacement token is requested by completing the *Token Deactivation Request* form and sending it to the email included on the form. This form can be found on the PITO Web Site at: <http://www.pito.bc.ca/cms/document-library/>

9.4 Faulty Token

If a user believes a token to be faulty a call should be placed to the EMR Vendor's Helpdesk. The EMR Vendor will triage the call to TELUS and confirm that the token is faulty (based on a set of questions asked of the EMR Vendor). If the token is deemed to be faulty it needs to be sent back to TELUS for confirmation and for a credit to the Ministry.

MSS - Managed Secure Authentication Operations Team

Managed Authentication SecurID - RMA Department

9 - 3777 Kingsway

Burnaby B.C.

V5H-3Z7 Canada

In the meantime the faulty token should be deactivated and a replacement token requested by completing the *Token Deactivation Request* form and sending it to the email included on the form. This form can be found on the PITO Web Site at: <http://www.pito.bc.ca/cms/document-library/>



9.5 Tokens for Locums

9.5.1 Requesting A Token

A practice may request a token for a locum who is providing coverage for a PITO-qualified physician at the practice. This request is made by completing the *Additional Tokens Request* form which can be found on the PITO Web Site at:

<http://www.pito.bc.ca/cms/document-library/>

9.5.2 Departure of Locum

When the locum's term of coverage at the practice has ended the VPN Token must be left at the practice. The individual in charge of managing the tokens at the practice (usually the PPN Contact) must then:

- Request that the token be deactivated; OR
- Request a reassignment of the token to another user.

The deactivation of a token is requested by completing the *Token Deactivation Request* form and sending it to the email included on the form. This form can be found on the PITO Web Site at: <http://www.pito.bc.ca/cms/document-library/>

The reassignment of a token is requested by completing the *Token Reassignment or Reactivation Request* form and sending it to the email included on the form. This form can be found on the PITO Web Site at: <http://www.pito.bc.ca/cms/document-library/>

NOTE: To ensure data security and patient privacy it is very important to collect and deactivate or reassign a token left by the locum at the end of their term.

9.6 Tokens for Residents

9.6.1 Requesting A Token

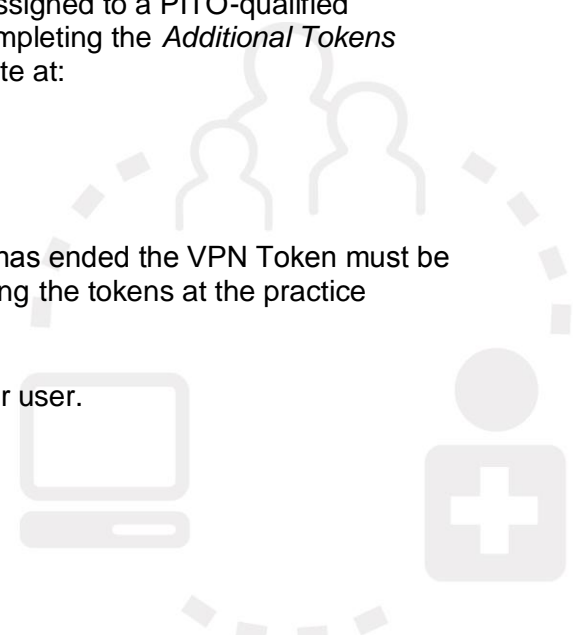
A practice may request a token for a resident who is assigned to a PITO-qualified physician at the practice. This request is made by completing the *Additional Tokens Request* form which can be found on the PITO Web Site at:

<http://www.pito.bc.ca/cms/document-library/>

9.6.2 Departure of Resident

When the Resident's term of coverage at the practice has ended the VPN Token must be left at the practice. The individual in charge of managing the tokens at the practice (usually the PPN Contact) must then:

- Request that the token be deactivated; OR
- Request a reassignment of the token to another user.



The deactivation of a token is requested by completing the *Token Deactivation Request* form and sending it to the email included on the form. This form can be found on the PITO Web Site at: <http://www.pito.bc.ca/cms/document-library/>

The reassignment of a token is requested by completing the *Token Reassignment or Reactivation Request* form and sending it to the email included on the form. This form can be found on the PITO Web Site at: <http://www.pito.bc.ca/cms/document-library/>

NOTE: To ensure data security and patient privacy it is very important to collect and deactivate or reassign a token left by the resident at the end of their term.

9.7 Departure of Physician From Practice

When a PITO-qualified physician leaves the practice (e.g. retirement or change of practice) the following procedures apply:

9.7.1 Physician Move to a Practice Using a PITO-Eligible EMR Vendor

If the physician is moving to another practice that is using a PITO-Eligible EMR Vendor the physician should take his/her assigned VPN Token to the new practice as long as the EMR Vendor at the new practice supports the TELUS VPN Tokens. Not all PITO-Eligible EMR Vendors support the TELUS tokens. As of **December 2010** the EMR Vendors that support TELUS VPN tokens are:

- Wolf
- Intrahealth
- Osler

9.7.2 Physician Move NOT to a Practice Using a PITO-Eligible EMR Vendor

A departing physician must leave his/her VPN Token at the practice in the following circumstances:

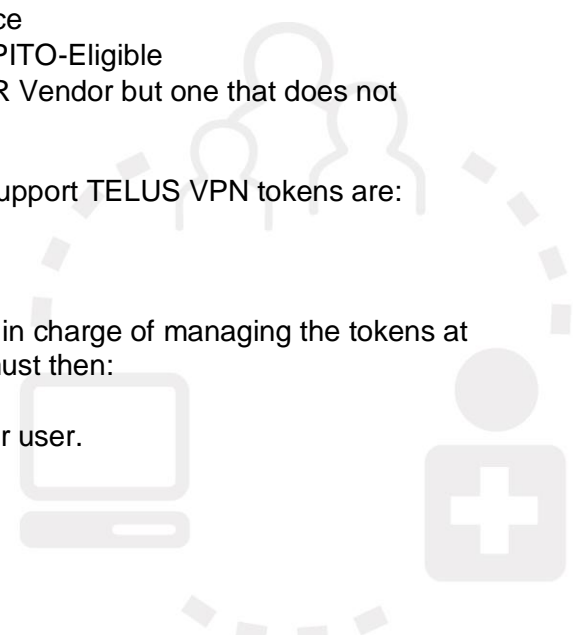
- Physician retiring
- Moving to a practice with a paper-based practice
- Moving to a practice using an EMR that is not PITO-Eligible
- Moving to a practice using a PITO-Eligible EMR Vendor but one that does not support TELUS VPN Tokens.

As of **December 2010** the EMR Vendors that do not support TELUS VPN tokens are:

- MedAccess
- EMIS

The physician must leave the token with the individual in charge of managing the tokens at the practice (usually the PPN Contact). This person must then:

- Request that the token be deactivated; OR
- Request a reassignment of the token to another user.



The deactivation of a token is requested by completing the *Token Deactivation Request* form and sending it to the email included on the form. This form can be found on the PITO Web Site at: <http://www.pito.bc.ca/cms/document-library/>

The reassignment of a token is requested by completing the *Token Reassignment or Reactivation Request* form and sending it to the email included on the form. This form can be found on the PITO Web Site at: <http://www.pito.bc.ca/cms/document-library/>

NOTE: To ensure data security and patient privacy it is very important to collect and deactivate or reassign a token left by a physician.

9.8 Departure of Staff From Practice

When a non-physician staff member leaves a practice the VPN Token should be left behind at the practice, even if they are going to a practice that supports the use of a VPN Token. A new VPN Token can be requested at the new practice if applicable.

The staff member must leave the token with the individual in charge of managing the tokens at the practice (usually the PPN Contact). This person must then:

- Request that the token be deactivated OR
- Request a reassignment of the token to another user.

The deactivation of a token is requested by completing the *Token Deactivation Request* form and sending it to the email included on the form. This form can be found on the PITO Web Site at: <http://www.pito.bc.ca/cms/document-library/>

The reassignment of a token is requested by completing the *Token Reassignment or Reactivation Request* form and sending it to the email included on the form. This form can be found on the PITO Web Site at: <http://www.pito.bc.ca/cms/document-library/>

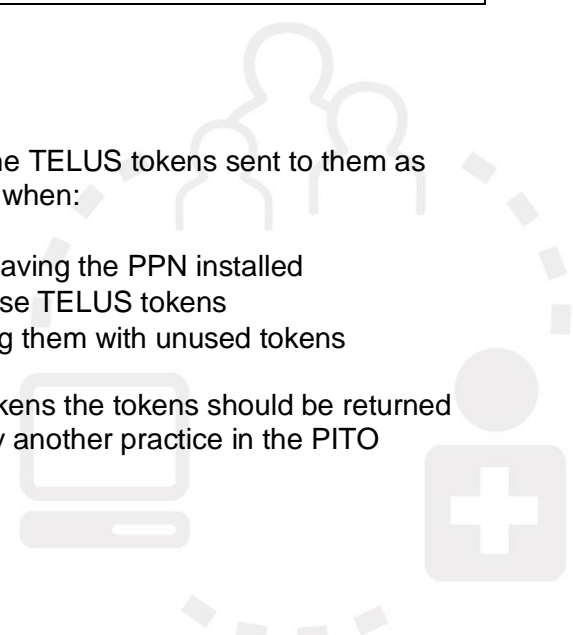
NOTE: To ensure data security and patient privacy it is very important to collect and deactivate or reassign a token left by staff member.

9.9 Returning Tokens No Longer Needed

There will be times when a practice no longer needs the TELUS tokens sent to them as part of the PITO PPN implementation. This can occur when:

- A practice shuts down
- A practice opts out of the PITO program after having the PPN installed
- A practice switches to a vendor that does not use TELUS tokens
- A practice experiences a staff decrease, leaving them with unused tokens

When a practice no longer needs one or more of its tokens the tokens should be returned to TELUS so that they can be deactivated and used by another practice in the PITO program.



To return the tokens, the *Token Return* form should be completed and the tokens should be sent, with this form to the person and address indicated on the form.

The *Token Return* form can be found on the PITO Web Site at:

<http://www.pito.bc.ca/cms/document-library/>

NOTE: To ensure data security and patient privacy it is very important to collect and return tokens no longer needed where they will be deactivated and safely stored.



10.0 Quick Reference Summary

The following are the key steps to access the EMR application from a remote Windows OS computer (for details and other OS please refer to previous sections in this guide):

1. In your browser go to one of the VPN sites. The URLs are:

Primary: <https://vpn1ppn.bc.ca>

Secondary (if primary not available): <https://vpn2ppn.bc.ca>

2. Using the tokencode from your RSA SecurID token combined with a PIN and your user name, log in to the VPN site from step 1. Note: Initial login requires you to only enter the tokencode and choose a PIN (see previous sections for details).
3. Add a Web bookmark in the Web Bookmarks section of VPN website. Use the URL (or IP Address) provided by EMR vendor.
4. You will also require an EMR application software client. If you do not have one, download and install it using instructions from the EMR vendor.
5. Once you have added a Web Bookmark for the EMR application, click on the bookmark. You will be taken to the EMR application's login screen
6. Make sure you sign out of the EMR application as well as the VPN website once you are finished.
7. Make sure your computer is secure by having a AntiVirus software installed with the most up to date virus definitions and automatic updating enabled.



11.0 Supported Platforms¹

Juniper has provided a list of “qualified” and “compatible” platforms. In the section below, you will find both. At a minimum your environment should match a scenario on the “compatible” platforms list. However it is recommended that, in order to minimize problems, your environment match a scenario in the “qualified” platforms list

i.e. “compatible” = minimum requirements
“qualified” = recommended requirements

Your environment must include a supported web browser in order to be able to log onto one of the two VPN websites provided by TELUS for VPN access.

In addition, your environment must include the certain other supported components, depending on your local platform and which EMR vendor you are using. There are three different types of technology used by the range of qualified EMR vendors.

1. **Web**—for *EMRs that use HTML/Javascript technology or EMRs that use a web interface to launch their applications*
2. **Terminal Services** —for *EMRs that use Terminal Services technology (enables a terminal emulation session on a Windows server or a Citrix Presentation Server) such as Citrix or RDP for their applications. Juniper refers to these as*
 - Citrix Terminal Services (CTS)
 - Windows Terminal Services (WTS)
3. **Java-Secure Application Manager (J-SAM)** – for EMRs that require client/server applications such as Citrix, Microsoft Terminal Services but are unable to use other access types.

At minimum, you will need to have software listed below for Web browsing in order to log onto VPN. As well you may need software listed for Terminal services or J-SAM if your selected EMR vendor requires either of these for EMR access

Note: contact your EMR support if you are unsure about the EMR application access requirements.

¹ Source: <http://www.juniper.net/support/products/sa/6.5/>
(note: current Juniper IVE version is **6.5R3.1** but may change in future. Contact your EMR support for current version)

11.1 Minimum Requirements

Web Browsing

Compatible platforms: Platform	Operating System	Browsers and Java Environment
Windows	<ul style="list-style-type: none"> • Vista Enterprise/Ultimate/Business/Home Basic/Home Premium with Service Pack 1 or 2 on 32 bit or 64 bit platforms • Windows 7 Enterprise/Ultimate/Professional/Home Basic/Home Premium on 32bit or 64 bit platforms (6.5R2 and above) • XP Professional with SP2 or SP3 on 32 bit or 64 bit • 2000 Professional SP4 • XP Home Edition SP3 • XP Media Center 2005 • Windows 2003 server SP2, 32bit and 64 bit 	<ul style="list-style-type: none"> • Internet Explorer 8.0 * • Internet Explorer 7.0 * • Internet Explorer 6.0 * • Firefox 3.5 • Firefox 3.0 • Firefox 2.0 • Sun JRE 5/1.5.07 and above • Microsoft JVM – for Windows 2000 <p>(* Wherever-applicable)</p>
Mac	<ul style="list-style-type: none"> • Mac OS X 10.6, 32 bit and 64 bit • Mac OS X 10.5.x, 32 bit and 64 bit • Mac OS X 10.4.x, 32 bit only • Mac OS X 10.3.x, 32 bit only 	<ul style="list-style-type: none"> • Safari 1.2 and above • Sun JRE 5/1.5.07 and above
Linux	<ul style="list-style-type: none"> • OpenSuse 10.x, 32 bit only • Ubuntu 7.10, 32 bit only • Red Hat Enterprise Linux 5, 32 bit only 	<ul style="list-style-type: none"> • Firefox 2.0 and above



Terminal Services

Compatible platform: Platform	Operating System	Browsers and Java Environment
Windows	<ul style="list-style-type: none"> • Vista Enterprise/Ultimate/Business/Home Basic/Home Premium with Service Pack 1 or 2 on 32 bit or 64 bit platforms • Windows 7 Enterprise/Ultimate/Professional/Home Basic/Home Premium on 32bit or 64 bit platforms (6.5R2) 	<ul style="list-style-type: none"> • Internet Explorer 8.0 (Wherever applicable) • Internet Explorer 7.0 (Wherever applicable)

Java-Secure Application Manager (J-SAM)

Compatible platforms: Platform	Operating System	Browsers and Java Environment
Windows	<ul style="list-style-type: none"> • Vista Enterprise/Ultimate/Business/Home Basic/Home Premium with Service Pack 1 or 2 on 32 bit or 64 bit platforms • Windows 7 Enterprise/Ultimate/Professional/Home Basic/Home Premium on 32bit or 64 bit platforms (6.5R2 and above) • XP Professional with SP2 or SP3 on 32 bit or 64 bit • 2000 Professional SP4 • XP Home Edition SP3 • XP Media Center 2005 • Windows 2003 server SP2, 32bit and 64 bit 	<ul style="list-style-type: none"> • Internet Explorer 8.0 * • Internet Explorer 7.0 * • Internet Explorer 6.0 * • Firefox 3.5 • Firefox 3.0 • Firefox 2.0 • Sun JRE 5/1.5.07 and above • Microsoft JVM – for Windows 2000 <p>(* Wherever-applicable)</p>
Mac	<ul style="list-style-type: none"> • Mac OS X 10.6, 32 bit and 64 bit • Mac OS X 10.5.x, 32 bit and 64 bit • Mac OS X 10.4.x, 32 bit only 	<ul style="list-style-type: none"> • Safari 1.0 and above • Sun JRE 5/1.5.07 and above



11.2 Recommended Requirements

Web Browsing

Qualified platforms: Platform	Operating System : list of browsers and Java Environment
Windows	<ul style="list-style-type: none">• XP Professional SP3 32 bit: Internet Explorer 7.0 and Firefox 3.5.Sun JRE 6• Vista Enterprise SP1 32 bit and 64 bit: Internet Explorer 7.0 and Firefox 3.5.Sun JRE 6• Windows 7 Enterprise 32 bit and 64 bit: Internet Explorer 8.0 and Firefox 3.5 Sun JRE 6 (6.5R2 and above)
Mac	<ul style="list-style-type: none">• Mac OS X 10.5.0, 32 bit and 64 bit: Safari 3.2 Sun JRE 6• Mac OS X 10.4.3, 32 bit only: Safari 2.0. Sun JRE 5
Linux	<ul style="list-style-type: none">• OpenSuse 11, 32 bit only: Firefox 3.0.Sun JRE 6• Ubuntu 8.10, 32 bit only: Firefox 3.0.Sun JRE 6

Terminal Services

Qualified platforms: Platform	Operating System : list of browsers and Java Environment
Windows	<ul style="list-style-type: none">• XP Professional SP3 32 bit: Internet Explorer 7.0, Internet Explorer 8.0 and Firefox 3.0.Sun JRE 6• Vista Enterprise SP1 32 bit: Internet Explorer 7.0, Internet Explorer 8.0 and Firefox 3.0.Sun JRE 6• Windows 7 Enterprise 32 bit: Internet Explorer 8.0 and Firefox 3.5 Sun JRE 6 (6.5R2 and above)



Java-Secure Application Manager (J-SAM)

Qualified platforms: Platform	Operating System : list of browsers and Java Environment
Windows	<ul style="list-style-type: none">• XP Professional SP3 32 bit: Internet Explorer 7.0, 8.0 and Firefox 3.0.Sun JRE 6• Vista Enterprise SP1 32 bit: Internet Explorer 7.0, 8.0 and Firefox 3.0.Sun JRE 6• Windows 7 Enterprise 32 bit: Internet Explorer 8.0 and Firefox 3.5 Sun JRE 6 (6.5R2 and above)
Mac	<ul style="list-style-type: none">• Mac OS X 10.5.0, 32 bit and 64 bit: Safari 3.2 Sun JRE 6• Mac OS X 10.4.3, 32 bit only: Safari 2.0. Sun JRE 5
Linux	<ul style="list-style-type: none">• OpenSuse 11, 32 bit only: Firefox 3.0.Sun JRE 6• Ubuntu 8.10, 32 bit only: Firefox 3.0.Sun JRE 6



CHANGE CONTROL TABLE

Version	Publish Date	Delivery Mechanism	Audience	Modified By	Change Reference
V2.1	Aug 17/10	PITO Web Site & Emailed to EMR Vendors	Clinics, EMR Vendors	M.Chauhan	New generic version (non-vendor specific)
V2.1a	Sep 30/10	PITO Web Site	Clinics, EMR Vendors	D.Von Ratenberg	Removed reference to section 9.7
2.2	Dec 7/10	PITO Web Site	Clinics, EMR Vendors	D.Von Ratenberg	Added New section on Token Management Practices
2.2a	Mar 25/11	PITO Web Site	Clinics, EMR Vendors	D. Von Ratenberg	Added security criteria re: PIN
2.2b	Apr 21/11	PITO Web Site	Clinics, EMR Vendors	D.Von Ratenberg	Correction to PITO URLs
2.3	May 30/11	PITO Web Site	Clinics, EMR Vendors	D.Von Ratenberg	Addition of section 9.9 – Returning Tokens

