

Remote VA Access

- The Very Short Story
 - Apply for Remote Access through the SFVA Home Page
 - Get a USB PIV card reader for Remote Access (free from HR where you pick up your PIV card)
 - If you don't get a PIV card reader for remote access, set up the "MobilePASS" app on your smartphone
 - Call the National Service Desk [855-673-HELP (4357)] to be sure you are not "PIV enforced" (otherwise you cannot use MobilePASS with a UCSF, SFGH, or other PC/device that does not have a PIV card reader). Tell them your exemptions are (use these to get permanent access):
 - **Philips Intellispace PACS [our Radiology system]**
 - **CAG - Non-VA Hospital [equipment furnished by other entities (E.g. University-owned) for remote clinical documentation]**
- The most important websites for help setting up a home PC/Mac for PIV card remote use are:
 - <https://raportal.vpn.va.gov> (has all the VA help info, software and certificate downloads for PCs and Macs)
 - <http://militarycac.com> (has practical tips for setting up a PIV card reader, reviews of readers, etc.)
- The best remote access site for VA is <https://citrixaccess.va.gov>

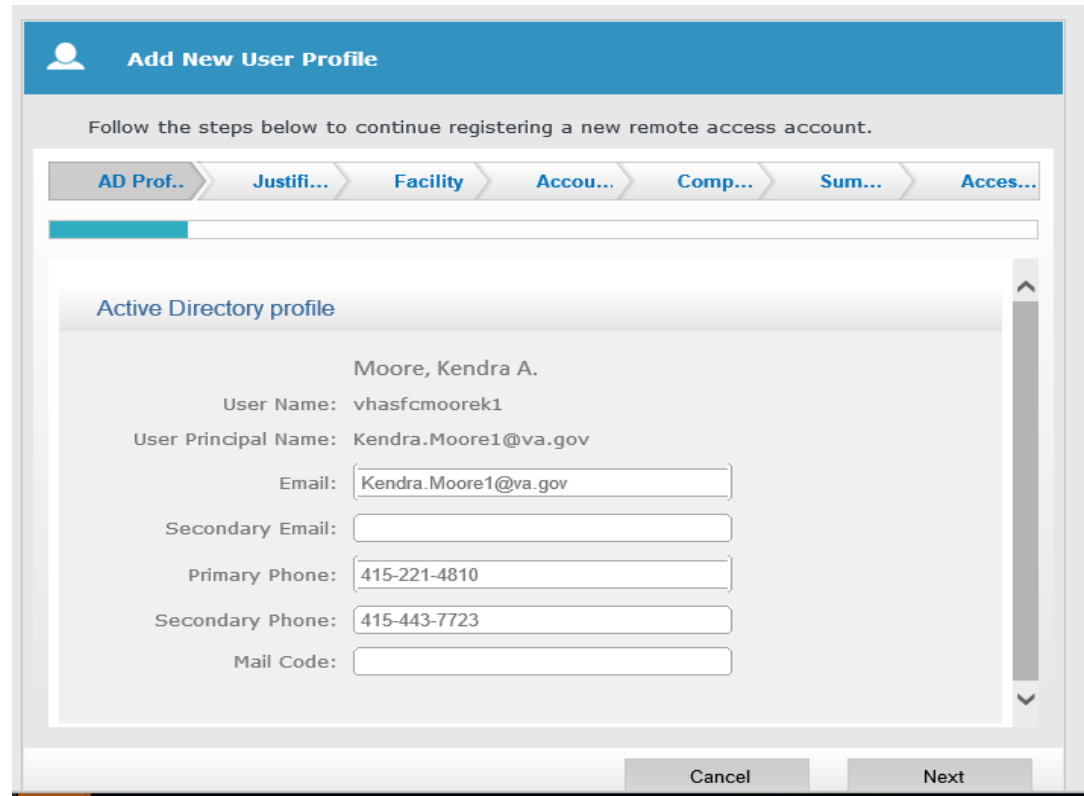
*CAG = Citrix Access Gateway

Request Remote Access Details

Go to the VA home page (open Internet Explorer on a VA computer- this should be the home screen)

Look at the links under the “Top Facility Resources” column on the webpage and click on “Remote Access Request”

From there, click on “Self Service Portal” at the top of the page to “Request Access” for Remote Access.



The screenshot shows a web form titled "Add New User Profile" with a blue header bar. Below the header, there is a navigation bar with several steps: "AD Prof..", "Justifi...", "Facility", "Accou...", "Comp...", "Sum...", and "Acces...". The "AD Prof.." step is currently selected and highlighted in blue. Below the navigation bar, there is a section titled "Active Directory profile" with a scrollable area containing the following information:

- Name: Moore, Kendra A.
- User Name: vhasfcmoorek1
- User Principal Name: Kendra.Moore1@va.gov
- Email: Kendra.Moore1@va.gov (input field)
- Secondary Email: (input field)
- Primary Phone: 415-221-4810 (input field)
- Secondary Phone: 415-443-7723 (input field)
- Mail Code: (input field)

At the bottom of the form, there are two buttons: "Cancel" and "Next".

Request Remote Access Details

For justification, can say
“resident physician,
need remote access for
patient care”

Add New User Profile

Follow the steps below to continue registering a new remote access account.

AD Profile > **Justification** > Facility > Account Type > Company > Summary > Access Type

Justification

Justification for the account:

primary care provider, needs remote access for patient care

Cancel Previous Next

Add New User Profile

Follow the steps below to continue registering a new remote access account.

AD Prof.. > Justifi... > **Facility** > Accou... > Comp... > Sum... > Acces...

Facility

State: CA

Facility: San Francisco VA Medical Center

Cancel Previous Next

Request Remote Access Details

For account type, choose VA employee

For approving official, Enter **Susan Wlodarczyk (inpatient)** or **Chris Sha (outpatient)**

Add New User Profile

Follow the steps below to continue registering a new remote access account.

AD Prof.. > Justifi... > Facility > **Accou...** > Comp... > Sum... > Acces...

Account Type

I am a: Contractor
 VA Employee

Cancel Previous Next

Add New User Profile

Follow the steps below to continue registering a new remote access account.

AD Prof.. > Justifi... > Facility > **Accou...** > **Comp...** > Sum... > Acces...

Company & Approving Official

Company: Department of Veterans Affairs

Approving Official: Sha, Christopher | x

Check here if Approving Official is not

Cancel Previous Next

Request Remote Access Details

Follow the rest of the prompts to submit your request → this will then need to be approved by Susie Wlodarczyk or Chris Sha, and then your request can move forward!

The screenshot displays a web interface for requesting remote access. At the top, a blue header bar contains the text "Request Access" with a yellow arrow icon. Below this, a grey bar contains the instruction "Follow the steps below to request remote access." A progress bar below the instruction shows four steps: "Access Type" (highlighted in blue), "Access Settings", "Summary", and "Terms and Conditions". The main content area is titled "Access Type" and contains the text "Listed types do not include already requested access types." Below this text is a dropdown menu labeled "Access Type:" with the selected option "CAG Access (supports all device types)". At the bottom right of the form, there are two buttons: "Cancel" and "Next".

USB Card Reader from HR

(go to militarycac.com for info)

There are lots of types of CAC or PIV card readers.

This one has the most use in VA and is known to work on both PCs and Macs

It's more problematic to set up on a Mac than a PC, but detailed instructions are at <https://raportal.vpn.va.gov>

Hard to use "at Grandma's house" since you need your PIV card, a reader, and the driver installed at her house – use MobilePASS if possible

PIV card readers for Android or iOS devices are very expensive but they exist

SCR3310v2.0

The Premier USB Smart Card Reader Solution



Using the MobilePass “OTP”

- Requires a free download of the SafeNet MobilePASS App onto your smartphone*
- Requires that you link this App with your PIV card **once while your PIV card is on the VA network**
- You can use “at Grandma’s house” instead of a PIV card to log into CAG if you have your smartphone and the device that can log into CAG has Citrix Receiver installed (Mac, PC, tablet, or even the same phone that you installed MobilePASS onto)
- You absolutely do *not* need to have MobilePASS installed on the device that you use to access CAG
- MobilePASS generates a new 6-digit number every 30 seconds. You have to enter the “current” number along with your vha21\vhasfcxxxxxx info to get access on the PC, Mac, or tablet
- Note: *You must also have a “POA group exclusion”* to use MobilePASS (see next slide)

*Due to licensing issues, you can only install on one device, so you should install it on something that you will have with you when you are logging into CAG. If you never, ever use remote access except from your home PC, you can install it there and not your phone.

Exemption from PIV-only group

- To use MobilePASS, you cannot be in the “POA” or “PIV-only-access” group. (If in that group you must use a PIV card both on-site and remotely)
- This is a small group so you must call the National Service Desk [855-673-HELP (4357)] to ask for **LONG TERM** exemption.
- They may initially only grant you only a 15-day exemption.
- Request a **LONG TERM** exemption by stating that you need an exemption based on
 - “**CAG - Non-VA Hospital [equipment furnished by other entities (E.g. University-owned) for remote clinical documentation],”**
 - Be persistent and ask to speak with their supervisor if needed.
- This is reviewed by the VA Facility ISO and CHIO
- If the name of a supervisor is required use Rebecca.Shunk@va.gov

Linking MobilePASS with your PIV Card

- You must be on a PC on the VA network with your *active* PIV card to log into the setup site at <https://otp.strongauth.va.gov/rdweb> (use internet explorer)
- For some reason you must use the numbers that are above the “QWERTYUIOP” part of the keyboard and NOT the number pad to enter your PIN
- This PC could be a VA PC that is logged onto the VA network remotely using the Cisco AnyConnect client [which is separate from CAG]
- You must download and install the SafeNet MobilePASS app (orange logo) from your phone OS’ App store
- The link procedure requires information from your VA PC to be put into the MobilePASS App on your phone and vice versa, so your phone needs a decent cell connection
- The process takes about 10 minutes, but it can be slow due to server load
- You only have to do this ONCE!

Nitty-gritty of MobilePASS setup - 1

Log into the Enrollment Portal at <https://otp.strongauth.va.gov/rdweb>, and when prompted to login, choose to log in *with your PIV card*. **This does NOT have to be the same person who is logged into the VA PC already.**

Step 4.1:

Using your VA desktop, navigate to the VA Enrollment Portal:

<https://otp.strongauth.va.gov/rdweb>

Click the Remote Access MobilePASS Self Service link.

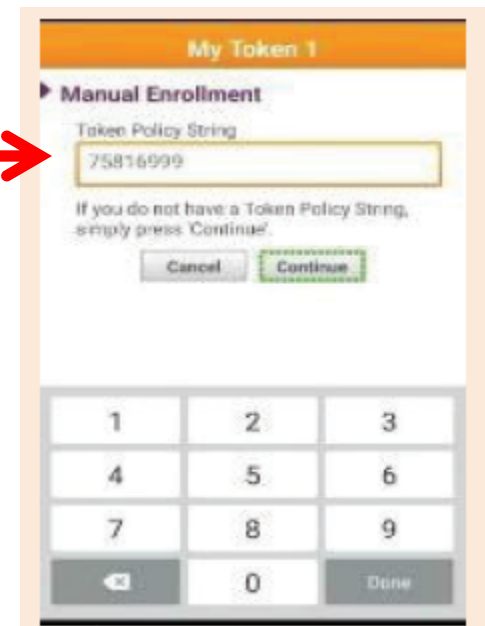
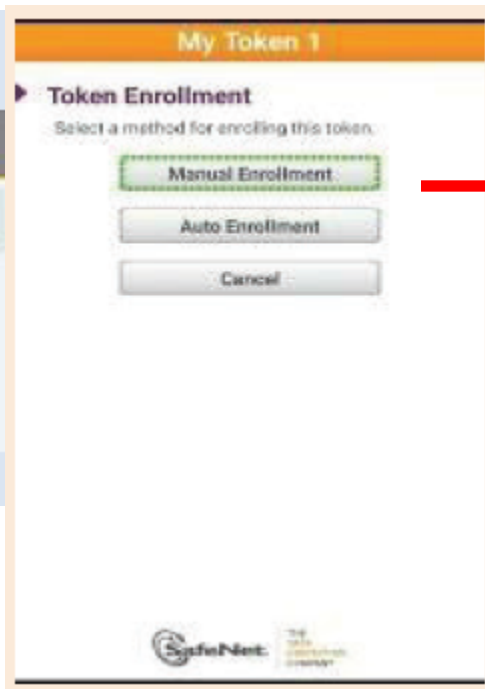
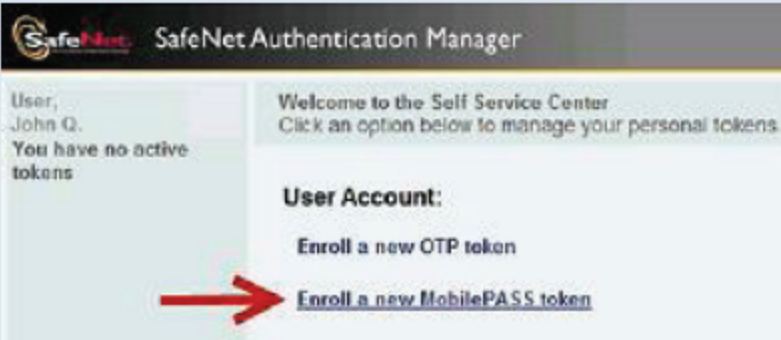


Nitty-gritty of MobilePASS setup - 2

On the PC, you choose to Enroll a new MobilePASS token

On the phone's MobilePASS app, you tap the "Manual Enrollment" button, and then enter the VA's "Policy String", which is 75816999

Step 5.1: Start MobilePASS



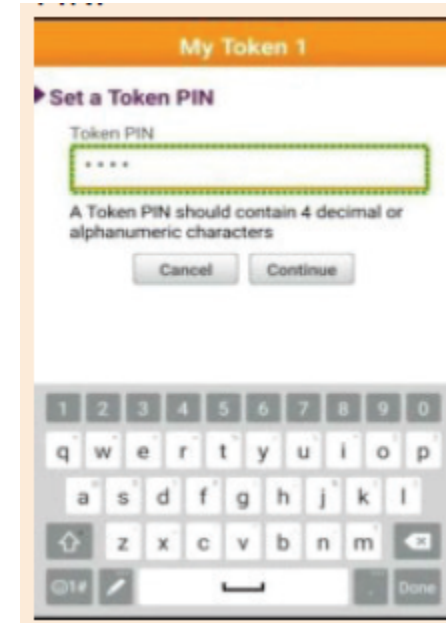
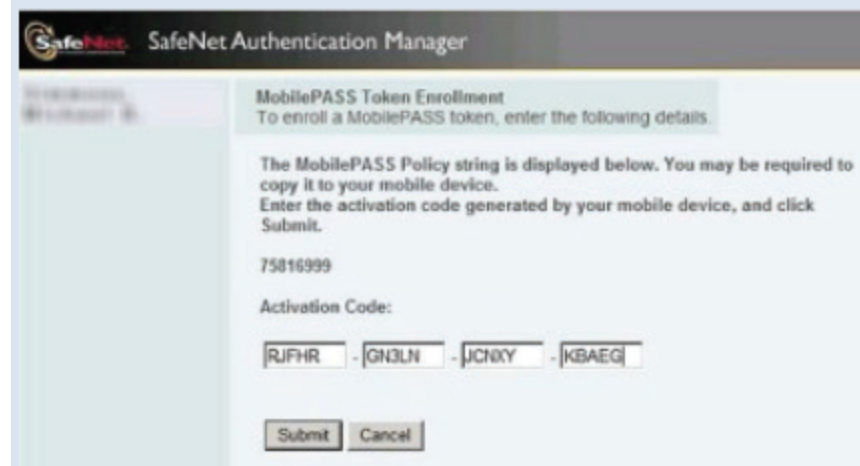
Nitty-gritty of MobilePASS setup - 3

The phone's MobilePASS app will now generate an Activation Code.

On the PC, you now enter that Activation Code into the little boxes and click the "Submit" button.

Back on the phone's MobilePASS app, you now enter a 4-digit PIN that you will use every time you open the MobilePASS app in the future. When you do, the app will start displaying 6-digit numbers to you every 30 seconds.

(But you are NOT Done yet!)



Nitty-gritty of MobilePASS setup - 4

On the PC, you must return to the Main Menu to finalize the connection by choosing to “Validate the OTP token”. Getting the “Validate OTP Token” box can take a few minutes so can be frustrating.

The phone’s MobilePASS app will keep generating 6-digit numbers. When the PC Validate Box is ready, you now enter the 6-digit number you see into the box on the PC. If you miss the 30-second deadline, you must try the next number from the app.

Now you are done.

The screenshot displays the SafeNet Authentication Manager interface. At the top, a green checkmark icon and the text "The MobilePASS token is successfully enrolled" indicate completion. A red circle highlights the "Back to main menu" button. To the right, a "Selected Token:" menu lists several options: "Temporarily disable the token", "Report the token as lost or damaged", "Validate the OTP token" (highlighted with a red box), and "Unassign the token". A red arrow points from the "Validate the OTP token" button to the "Validate OTP Token" dialog box at the bottom. This dialog box contains the instruction "Use your token to generate an OTP passcode. Copy the OTP passcode generated by the OTP token to the OTP Passcode field below, and click Submit." Below the instruction is an "OTP Passcode:" input field with six dots, and "Submit" and "Cancel" buttons. To the left of the main interface, a separate window titled "My Token 1" shows a "Your Passcode" of "441048" and a note "Next Passcode in 20 seconds." A red arrow points from this passcode to the input field in the "Validate OTP Token" dialog.

Two-factor authentication on CAG

Requires one of two options:

1. Use of PIV card *instead of* your vha21\vhafcxxxxxx domain name and password, or;
2. Use of a “One Time Password” (a six-digit number generated by the MobilePASS App) *in addition to* your vha21\vhafcxxxxxx credentials
3. Best URL is citrixaccess.va.gov; other options are vacagwest.vpn.va.gov, vacageast.vpn.va.gov, vacagnorth.vpn.va.gov, vacagsouth.vpn.va.gov
4. Your Mac/PC/tablet must have Citrix Receiver installed (www.citrix.com)
For Mac, Safari is the best browser

VA Citrix Remote Access

When logging into this system you agree to the following:

You are accessing a U.S. Government information system, which includes:

- (1) this computer,
- (2) this computer network,
- (3) all computers connected to this network, and
- (4) all devices and storage media attached to this network or to a computer on this network.

This information system is provided for U.S. Government-authorized use only. Unauthorized or improper use of this system may result in disciplinary action, as well as civil and criminal penalties. By using this information system, you understand and consent to the following:

You have no reasonable expectation of privacy regarding any communications or data transiting or stored on this information system. At any time, the government may for any lawful government purpose monitor, intercept, search and seize any communication or data transiting or stored on this information system. Any communications or data transiting or stored on this information system may be disclosed or used for any lawful government purpose.

If you have any further questions regarding Citrix Remote Access and associated resources, please contact the VA Service Desk at 1-855-NSD-HELP (1-855-673-4357) Option 6, Option 1 or via email at NSD.VPNSecurity@va.gov

Domain\Username:

Domain Password:

Logon

Click here to use PIV:

Click here to use OTP Token:

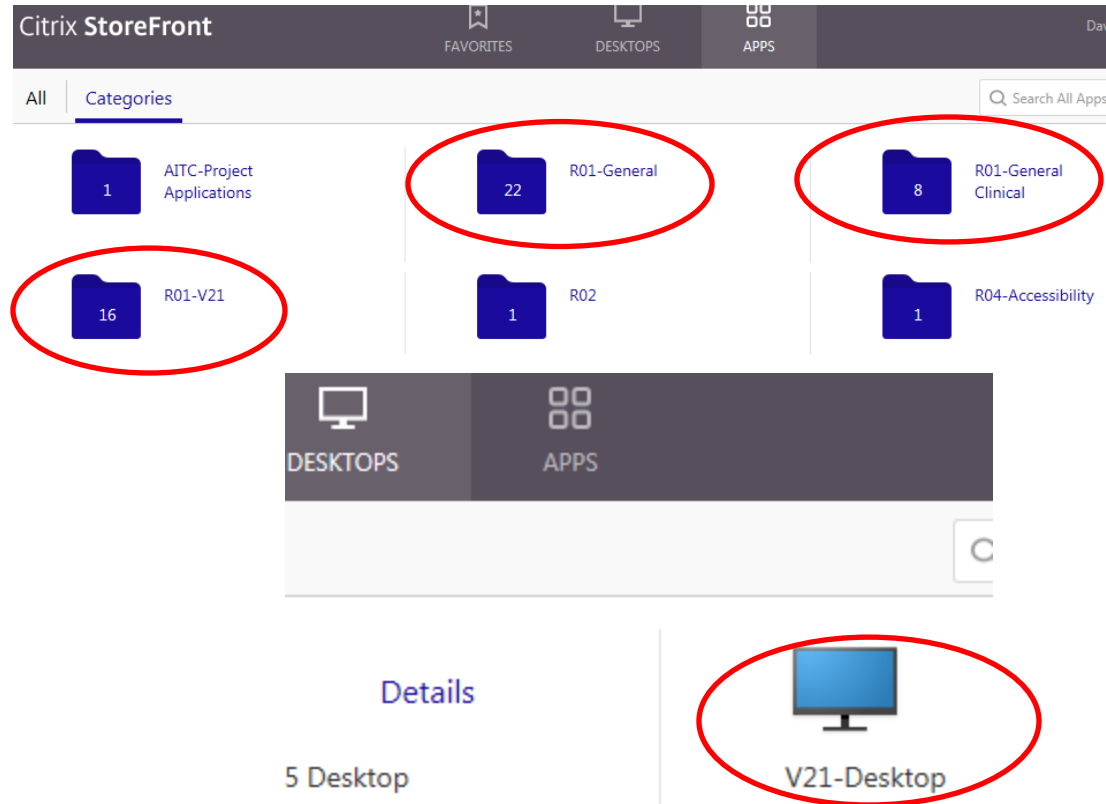
Citrix Gateway (CAG) Navigation - 1

- After login, the Main StoreFront Apps window lets you choose from 3 folders. In *R01-General* you will find Outlook, Internet Explorer, Word, PowerPoint, etc;

In *R01-General Clinical* you will find basic CPRS and VistAWeb, but you have to choose vista.sanfrancisco.med.va.gov as the server for this version of CPRS;

In *R01-V21* you will find the *SFC* folder that contains CPRS, Vista Imaging, and iSite Radiology specific to San Francisco. **If you see no relevant apps, your account is not yet active!** [check the self-service site in slide 2].

- You may also choose a “Desktop” instead of an individual App. If you want to use CPRS and Outlook at the same time, choose the V21-Desktop. While Outlook is in the menu bar, CPRS is hidden in the “VA Shortcuts” folder (V21>SFC>Local>CPRS Alternate).
For easier future use, drag the CPRS Alternate link over to the Start menu on the V21-Desktop. It will create the shortcut inside a new ‘quick link folder’ with your name on it.



Citrix Gateway Tips, Tricks, Oddities - 1

- **PC and Mac users:** Ensure your browser's encryption settings for "SSL 3.0" and "TLS 1.0" are both checked ON (IE Menu: Tools→Internet Options→Advanced; Firefox: Tools→Options→Advanced→Encryption; Mac Firefox: Preferences→Advanced→Encryption; Safari is auto-set to ON). Also be sure you have *installed* the Citrix Receiver client after you download it (installation is not automatic after download). **When in doubt, re-install the newest version from citrix.com.**
- Sometimes, an app will stop launching from your Citrix App window and a few tries will be needed.
- **FIREFOX issue:** Check preferences under Add-Ons→Plugins and set Citrix Plugin to "Always Activate". **AVOID Firefox on a Mac; use Safari instead.**
- **iPad Citrix Receiver users (should be similar for Android, but untested):**
 1. Read ALL of the Help items under the Settings menu in Citrix Receiver about how different finger swipes work, how the Citrix virtual keyboard can be brought up or down (learn the three-finger tap!), etc.
 2. Turn 'Caffeine' ON [Settings→Advanced] so Citrix won't 'sleep';
 3. You do not need to set up an account in Receiver to use Safari to connect to the CAG sites via https; when prompted what to do with the '.ica' file in Safari, use the Citrix default

Citrix Gateway Tips, Tricks, Oddities - 2

- **Security Certificate issues for all users (PC, Mac, iPad): IMPORTANT**
 - If the browser says the security certificate can't be verified, you must install new security certificates and ensure they are up to date and trusted. In fact, do this anytime there is any message about security certificates. Obtain the *Federal Common Policy Certificate* and any other required certificates from <https://raportal.vpn.va.gov> under General Media. Installation instructions are also on that site or contact Dr. Ben Davoren at ben.davoren@va.gov for info. There are 5 certificates as of March 2016– the first three here are key; install the last two if you wish to use Lync remotely (though that won't work on iPad).
1. For Mac OS X, the certificates are in the Utilities Folder→Keychain Access folder. (get there from either “Find” or the “Go” menu on the basic Mac desktop screen, but Firefox and Safari have their own quirks – review the site. You must select “Always Trust” for EACH certificate individually on a Mac in the Keychain Access application. If you are still prompted in Safari or Firefox, do not click the ‘continue’ button that appears. Instead, click “Show certificate” and trust *again* for that specific browser.
 2. In Windows 7, type “certmgr.msc” into the “Search...” box from the Start Menu.
 3. For iPad, iOS will download it into the correct folder.

Citrix Gateway Tips, Tricks, Oddities - 3

- **Citrix/CAG Limitations as of 2017:**

1. CPRS Tools Menu items *may* not work, e.g. VistAWeb/iMed Consent that depend on CPRS-set patient context. Use “classic” Remote Data Views in CPRS on the labs or reports tabs (blue Remote Data button at upper right) instead of VistAWeb, or ask for “Remote Desktop Connection” (RDC) to use Citrix to control your PC at work. **Starting** RDC is slow, and there are keyboard mapping issues with Citrix and iPad (in the RDC dialog on iPad, click on “Options” and be sure ‘apply windows key combinations’ is set to ‘local computer’ or ‘this computer’).
2. Copying, Pasting, and Printing are turned OFF by default in the CAG. That also means you can’t use Dragon / iOS dictation to enter text. Printing permission request form is at ISO SharePoint (2nd page this handout)
3. If your keyboard has no number pad, the “exit” command from VistA screens (e.g. leave requests) of “PF1+E” can’t be used because there is no PF1 (Num Lock on number pad). F1 may work; if not, the ASCII code for PF1 is “esc+O+P” (escape + capital O + capital P, so that “PF1+E” is “escape-capital O-capital P-E” in *sequence*).
4. To map a network drive via CAG (W: drive, etc.) use the MapMyDrives link on the V21 Desktop to V21-SFC and the drives you see at work will appear available to you.