REQUESTING VA REMOTE ACCESS

CREATED BY: Michael H. Richardson
DATE: 07JUL2021
VERSION: 1.0

Purpose: To describe, in brief, the different types of VA remote access, the general VA request process, helpful links and training resources.

TYPES OF VA REMOTE ACCESS:

1. Citrix Access Gateway (CAG) https://raportal.vpn.va.gov/Main1//CAGOverview.aspx
    a. CAG is the recommended remote access solution for users without VA Government Furnished and managed Equipment (GFE); other equipment (OE), may include personally owned equipment (POE), other organizational equipment, such as university, contractor, other federal/state/local government systems, and other VA affiliate company devices. It provides a method for the VA to grant secure access to systems and applications from OE devices for approved users and device types.
    b. Citrix technology offers connectivity from almost every client and browser; However, due to VA smartcard authentication and security limitation of devices we have for testing and documentation - we only support accessing VA Citrix from specific operating systems and browsers.
    c. VA supported Operating Systems: current vendor supported and maintained Windows and Macintosh devices and operating system version, as well as VA GFE iOS devices.
    d. VA supported Browsers: MS Edge, Google Chrome, Internet Explorer, and/or Safari.
        i. NOTE: VA recommends Google Chrome for the most seamless experience for both Windows and Macintosh devices and Safari for VA GFE iOS devices.
    e. VA CAG presents both individual published applications as well as full published desktops.
    f. Various features such as file upload/download, printing, and client clipboard are restricted by default with this remote access type. Additional features related to microphone and camera use may not be allowed depending on the application and how accessed, but audio output is allowed and should work. For more information on features and limitations and/or troubleshooting audio and video cameras, please see the ServiceNow (yourIT) Knowledge Article titled "VA Citrix: Tips and Tricks for using VA Citrix" * https://yourit.va.gov/va can be accessed from within a launched Citrix session (Chrome/Edge browser published application or full desktop).
    g. CAG should not be utilized on GFE devices unless a specific application and/or access need has been specified, or unless in an emergency as it is unnecessary for normal business needs. It may cause connection, access and/or other system problems if inappropriately utilized. Please utilize RESCUE-GFE for GFE VA devices.
2. RESCUE-GFE https://raportal.vpn.va.gov/Main1//RescueOverview.aspx
    a. This solution is designed and recommended to be the sole VPN solution for GFE devices. RESCUE GFE provides a security posture check and ensures VA data is encrypted from the end device into the VA trusted network. Prior to the device connecting and being allowed onto the VA trusted network the system is checked for multiple security baselines. Once the system has been determined to have met the requirements an encrypted SSL VPN tunnel from the endpoint to the VA network is established. The user has access to all allocated resources just the same as if they were sitting inside of the VA network. This software is installed on all GFE laptops prior to being provided to the user. Currently RESCUE GFE supports Windows 7, Windows 8, Windows 10 and MAC OSX.
    b. RESCUE-GFE is unnecessary in the facility and CBOC/Outbuilding areas that have VA network access. Only utilize this access method when outside of the VA facilities to prevent system problems.
3. Windows Virtual Desktop (WVD) https://raportal.vpn.va.gov/Main1//WVDOverview.aspx
    a. WVD is a cloud Desktop-As-A-Service (DaaS) platform. It provides authorized users connecting with VA-issued or privately-owned Windows 10 computers access to a standardized VA desktop. Two-factor authentication is required to log in.
4. GFE MOBILE https://raportal.vpn.va.gov/Main1//GFEMobileOverview.aspx
    a. GFE Mobile was developed as a solution to support remote users with government furnished Apple iOS and Android tablets and smartphones. This solution enables users with approved government furnished mobile devices to connect remotely to the VA Network. Cisco AnyConnect Client is utilized to create a full VPN tunnel back to the VA trusted network. The system integrates with Mobile Device Management systems to apply profiles to the end devices. The profiles are used to apply policy to the device. The applications on the device are authorized and downloaded by the VA store which ensures that all the application data being stored is encrypted on the device.
5. VA Virtual Office (VAVO) https://raportal.vpn.va.gov/Main1//VAVOOverview.aspx
    a. The VA Virtual Office (VAVO) remote access solution is a hardware (router) technology refresh for existing End of Life (EOL) VA Small Office/Home Office (SOHO) routers. The VAVO remote access solution includes an upgrade to the Trusted Internet Connection (TIC) gateway architecture, new end user devices, and integration with the Remote Access Portal (RAP).
    b. VAVO remote access is a highly scalable solution which provides teleworkers, small offices, and mobile users with office-like experiences combining voice, video, wireless (upcoming), and real-time data applications in a secure environment.

c. Due to the associated costs of VAVO, the Remote Enterprise Security Compliance Update Environment (RESCUE) solution remains the primary remote access method for users with VA-issued Windows and Macintosh computers. VAVO is an alternative remote access solution that may be discussed between a user and their supervisor if RESCUE fails to meet the user's remote access needs.

d. For more information, please see VAVO bulletin (accessible only via the internal VA network).

REQUESTING A RAP PROFILE: (RESCUE, CAG, GFE Mobile, WVD) VIDEO LINK: https://youtu.be/izUjlt8KjUs

1. Navigate to the RAP (REMOTE ACCESS PORTAL) Self Service Portal. (Only accessible within the VA network)
2. If you are a new VA Employee, you will automatically be placed into registration. (If you do not have a VA profile in existence)
3. Click into the "Self Service Portal" tab area.
4. Under the "Remote Access User Menu" choose the area for "Request Access".
5. Verify that your information, which was pulled from Active Directory, is correct. Add a secondary email and/or phone number if you wish, click "Next". (RAP emails will be sent to both the primary and secondary email addresses).
6. Enter a justification for the account and click "Next". (IMPORTANT! See your Service Line ADPAC and/or Supervisor with any questions/clarifications on the verbiage you need to place here for proper justification to prevent any delays in approval.)
7. Select your assigned State and Facility from the specific drop-down areas and click "Next".
8. Select your appropriate employment status, "Contractor" or "VA Employee" and click "Next".
9. If selecting "Contractor", select the specific company from the drop-down list. NOTE: If you do not see the company in the drop-down list, you will need to add the company via the "Manage Companies" link under the Quick Menu.
10. Select your appropriate "Approving Official" and click "Next". (This is usually your Supervisor but confirm with your Service Line ADPAC and/or Supervisor to ensure the correct individual is selected and so that there is no delay in approvals.)
11. Review your "Profile Summary" for accuracy and click "Next".
12. The profile has now been created and will go through the approval process.

REQUEST SPECIFIC ACCESS: (RESCUE, CAG, GFE Mobile, WVD) VIDEO LINK: https://youtu.be/izUjlt8KjUs

1. Once your RAP Profile has been initially created you will be able to select specific access. The request process is similar to below for all four types. Watch the video for a detailed visual walkthrough of the request process. VIDEO LINK: https://youtu.be/izUjlt8KjUs
2. Navigate to the RAP (REMOTE ACCESS PORTAL) Self Service Portal. (Only accessible within the VA network)
3. Click into the "Self Service Portal" tab area.
4. Under the "Remote Access User Menu" choose the area for "Request Access".
5. You will be given two radio button options "RESCUE/CAG/GFE MOBILE" and "VA Virtual Office (VAVO). Choose the appropriate request option and click on "Submit".
6. Scroll down to the section "Rescue Access, Access Type) Drop-down the list, then choose the appropriate selection and click "Next".
7. Accept the "Terms and Conditions" by checking the box for "I Accept" and click "Next".
8. A pop-up will then display specifying that "Your request has been submitted successfully". You can choose to "Request another Remote Access Type" or "Back to Account Details".
9. Your request is now pending approval by your approving official. Reach out to them with any further questions and/or view the approval process in the RAP Quick Menu "Access Request Details" which will show "Pending and "Completed" requests.

LINKS:

REMOTE ACCESS PORTAL: https://vaww.ramp.vansoc.va.gov/Pages/Dashboard.aspx
CITRIX ACCESS (CAG): https://citrixaccess.va.gov
VA | Remote Access Information and Media Portal: https://raportal.vpn.va.gov/Main1//CAGMedia.aspx
REQUESTING VA REMOTE ACCESS - VIDEO LINK: https://youtu.be/izUjlt8KjUs

ADDITIONAL SUPPORT:

For log on support, please contact the National Service Desk (NSD) at 1-855-NSD-HELP (1-855-673-4357) or by email at NSD.VPNSecurity@va.gov.

INFORMATION ON PIV CARD READERS AND (2FA)-TWO FACTOR AUTHENTICATION:

Two Factor Authentication (2FA)

2FA is required for authenticating remotely into VA systems. This means that a PIV card reader must be attached to the remote device or your VA Network Account must have a PIV Exemption to properly access VA Networks and Systems.

Where can I get a PIV card reader?

The distribution of PIV card readers is site-specific.

Currently, for the MIN AREA employee and other VA AREA Telework employees supported by MIN AREA OIT, they can visit VETMART in BM123 – LOGISTICS and request a card reader. Office of Information Technology/OIT – BV101 (Local OIT) does not provide this equipment for any type of employee.

What if I cannot get a PIV Card Reader? What if it does not work on my PC?

A temporary PIV exemption is needed. Contact ESD to request this exemption as per below contact information:
Contact: Enterprise Service Desk (ESD)
Toll Free Phone Number: 855-673-4357 (TTY: 844-224-6186)
You can also visit: YourIT Services (only available while on VA's internal network)

Other PIV Information:

Card readers for personally owned equipment:
-If CAG is being used on a personally owned device and your VA login/PIV is not classified as PIV exempt, a reader will be needed for the PIV card.
If a PIV reader is being purchased by your Service Line's office supplier or by yourself (available online: Amazon, Best Buy, MicroCenter, WalMart, etc.) it must be a FIPS compliant, Class 2 type reader.

Some common and approved PIV readers include:

- SCR3310 and SCR3500
- ACR39U, ACR39U-N1, ACR39U-UF, ACR39U-H1, and ACR39U-ND from ACS Corp are PocketMate series readers
- OMNIKEY 3021 and OMNIKEY 3021 with Base from HID Global

ADDITIONAL INFORMATION:

-You need to periodically login to your approved and active VA Remote Access areas, once a month and outside of the VA facility to keep your system access from inactivation for inactivity. A helpful way to ensure this takes place is to create a reoccurring Outlook calendar reminder for every 29 days or sooner. (In the event your reminder occurs on a day you cannot get logged in. Ideally, you should try to login every 2 weeks) In the event your access disables you will have to re-request access, which is not immediate and will cause a significant disruption for you and your service lines needs for your position.
-When in doubt, have any type of error or problem, it is best to reboot your PC, reseat your PIV and try again, before contacting any further help with your issue.