## Revision History

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author(s)</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.0</td>
<td>6/10/2013</td>
<td>VA NSOC (ENSTT)</td>
<td>Re-build of CAG Connection Guide</td>
</tr>
</tbody>
</table>
Table of Contents

1. Scope ..................................................................................................................... 1
2. Requesting Access ............................................................................................... 1
3. System Requirements .......................................................................................... 1
4. Connection Process ............................................................................................. 2
  4.1 Browser Configuration ..................................................................................... 2
    4.1.1 IE ........................................................................................................... 2
    4.1.2 Mozilla.................................................................................................... 4
  4.2 Two-Factor with CAG ...................................................................................... 5
  4.3 Connection to CAG .......................................................................................... 6
  4.4 Receiver Installation ........................................................................................ 8
  4.5 Launching Applications/Desktops .................................................................. 10
  4.6 Logging Off .................................................................................................... 11
5. Un-Installing Receiver ........................................................................................ 12
6. Password Change via CAG ................................................................................ 12
7. Troubleshooting .................................................................................................. 15
8. Requesting Support ............................................................................................ 17
1. **Scope**

This document provides information on how to connect a device to the Veterans Affairs (VA) Citrix Access Gateway (CAG) remote access solution. This guide is for devices using Windows Operating Systems.

For assistance with using CAG on another operating system, refer to the VA RESCUE media site.

2. **Requesting Access**

Before accessing the external CAG, CAG access must be enabled by the Information Security Officer (ISO). If access is not currently enabled, use the VPN self-service portal (available only from inside the VA network) to request access: https://vpnportal.vansoc.va.gov/SelfService/. This site can be used to check what remote access methods have been approved by the ISO. Once approved review the welcome letter to see which systems are authorized; if CAG is not listed in the welcome letter contact the ISO to specifically request CAG access also be allowed.

3. **System Requirements**

The CAG provides support for the following systems:

- **Operating Systems**
  - Windows XP, Vista, 7 and 8

- **Browser Support**
  - Internet Explorer (IE) 6 - 10
  - Safari
  - Firefox Mozilla
  - Google Chrome
4. Connection Process

4.1 Browser Configuration

Several browsers are supported for working with CAG. These browsers may require configuration changes to function properly with the VA CAG infrastructure.

4.1.1 IE

IE requires certain Internet Options to be configured. Use the following procedure to ensure that these settings are configured properly.

1. Click the Start button.
2. Select the Control Panel to open it.
3. From the top address bar, click the arrow next to the words Control Panel. Select All Control Panel Items.

4. Click the Internet Options icon.
5. Click the Advanced tab at the top of the window.
6. Ensure that Do not save encrypted pages to disk is not checked or greyed out.
7. If the Use TLS 1.0 checkbox is not checked, then check it.
8. If the Use TLS 1.1 and Use TLS 1.2 checkboxes are available, make sure Use TLS 1.1 is checked and Use TLS 1.2 is unchecked.

9. Click **Apply** to accept the changes.
10. Select the **Security** tab.
11. Click **Trusted Sites**, and then click **Sites**.

12. In the **Add this website to the zone** field enter [https://*.va.gov](https://*.va.gov), and click **Add**.

13. Click **Close** after adding the site.
14. Click **OK** to accept the changes.
15. If any IE browsers are open, close them and then re-open for the change to take effect.

### 4.1.2 Mozilla

Mozilla Firefox requires certain Options to be configured. Use the following procedure to ensure that these settings are configured properly.

1. Open the **Mozilla** browser.
2. Select the **Firefox** drop down.
3. Click **Options**.
4. In the Options pop-up, select the **Advanced** tab.
5. Select the sub-tab **Encryption**.
6. Ensure that **Use TLS 1.0** checkbox is checked.
7. Click **OK** to accept.

![Advanced tab with Encryption sub-tab selected](image)

**4.2 Two-Factor with CAG**

The use of a Personally Identifiable Information (PIV) smart card with CAG launched applications is supported.

1. The appropriate smartcard middleware (ActivClient) needs to be installed and a compatible smartcard reader device attached to the endpoint.
2. Before connecting to CAG:
   a. Insert the PIV card in the reader
   b. Connect the CAG
   c. Launch the application requiring the PIV

   **NOTE:** This is **NOT** for authentication into CAG.

The use of Universal Serial Bus (USB) tokens is also supported when the eToken PRO software is installed on the local device. Use the same process as PIV to use the USB token.

The eToken PRO driver is available for download on the RESCUE media site [https://rescue.vpn.va.gov](https://rescue.vpn.va.gov). Once on the RESCUE media site go to **Citrix > Media**; there is a set of install instructions and the software is available for download.
4.3 Connection to CAG

CAG is a web-based application that uses an approved web browser and encrypts data using Secure Socket Layer (SSL).

1. Open an Internet browser.
2. In the address bar, enter one of the URLs shown below based on Region. If unsure, of which region, then use the closest geographical connection point based on the section of the country.

(Example: Current location is Houston, TX then connect to https://varsouth.vpn.va.gov)

Region 1
- https://varwest.vpn.va.gov
- https://varsouth.vpn.va.gov

Region 2
- https://varnorth.vpn.va.gov
- https://varsouth.vpn.va.gov

Region 3
- https://vareast.vpn.va.gov
- https://varnorth.vpn.va.gov

Region 4
- https://varnorth.vpn.va.gov
- https://vareast.vpn.va.gov
3. Login using `<domain\username>` (ie. vha01\jsmith01) and `<password>`.

4. Click **Logon**.

5. The first connection attempt for Windows and Macintosh will provide the ability to download and install the Receiver client.

   **NOTE:** For information on other Receivers see the RESCUE media site [https://rescue.vpn.va.gov](https://rescue.vpn.va.gov).
4.4 Receiver Installation

The Citrix Receiver client must be installed on the device to support the launching of applications. Use the procedures below to install the necessary client.

1. Login to one of the CAGs, and the screen below will appear if the Citrix Receiver has not yet been installed or needs to be updated.
2. Check the I agree with the Citrix license agreement checkbox.
3. Click the green INSTALL button.
4. Click Run, and the software will download to a temporary folder.
5. The Citrix Receiver Setup screen appears. Click **Install**.

6. The Installer Progress screen appears. This screen closes when the installation completes.

7. If any messages appear in the browser pertaining to Citrix Systems, **Accept** them.

8. Use **Section 4.5, Launching Applications/Desktops** to continue.
4.5 Launching Applications/Desktops

1. During the logon the screen below will appear, this screen may be displayed for a while. The system is loading applications based on permissions.

2. Applications Folders or Applications are presented. A Desktops tab may be available based on permissions.

3. Click the appropriate <application folder>.
   
   **NOTE:** Based on Region and VISN different folders and applications are displayed.
4. Click the `<application>` to launch.

5. A message indicating the application is starting should appear, wait after clicking as the application can take an extended time to load the first time.

### 4.6 Logging Off

**WARNING:** Click on **LOG OFF** before closing the internet browser. Without doing so, multiple sessions on different servers can be stuck or corrupted and prevent applications from working properly. Logging off properly will ensure that all previous sessions, including the corrupted & idle sessions are released.

1. Close all applications windows.
2. In the web browser, click **Log Off**.
3. Close the browser window or tab.
5. Un-Installing Receiver

1. Close all applications that were opened through Citrix.
2. Open the Control Panel.
3. Select Programs and Features.
4. Scroll through the list of applications and click Citrix Receiver.
5. Click Uninstall.

6. Follow the prompts to uninstall the application.
7. Reboot the computer to ensure all components have been removed

   NOTE: It is important to reboot before attempting to re-install the application.

6. Password Change via CAG

Use this procedure to change a VA Active Directory (AD) password when using a Windows device. In order to successfully change the password the account cannot be:

- Expired
- Disabled
- Locked out
- Set to change password at next login

To change the password:

1. Login to CAG.
2. Launch an <application>.
3. Once the application launches, click the window to ensure it is active.
4. Press Ctrl+F1.
5. The *Windows Logon* page displays.
6. Click the **Change a password...** link.
7. Enter the current `<password>`.
8. Then enter the new `<password>`.
9. Click the Blue arrow to confirm the change.
## 7. Troubleshooting

<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Solution</th>
</tr>
</thead>
<tbody>
<tr>
<td>Unable to reach the CAG website.</td>
<td>• Try one of the other CAG websites.</td>
</tr>
<tr>
<td></td>
<td>• Clear the browser cache.</td>
</tr>
<tr>
<td></td>
<td>• Try using another web browser.</td>
</tr>
<tr>
<td></td>
<td>• Reboot the device.</td>
</tr>
<tr>
<td>Browser is giving a connection error.</td>
<td>Ensure that TLS 1.1 and 1.2 are enabled or supported by the browser.</td>
</tr>
<tr>
<td>Error message “The credentials you provided are either incorrect or you are not enabled for VA external Citrix access.”</td>
<td>• Check that the username and domain are spelled correctly.</td>
</tr>
<tr>
<td></td>
<td>• Ensure that the domain\username has been entered with the correct backslash “\” between the domain and username.</td>
</tr>
<tr>
<td></td>
<td>• Ensure that the requesting access process has been completed and a welcome letter from the ISO has been received before attempting to connect.</td>
</tr>
<tr>
<td>Did not receive a prompt to install the Citrix Receiver.</td>
<td>• The client may already be installed on the device.</td>
</tr>
<tr>
<td></td>
<td>• Go to the RESCUE media site to download and install the client. <a href="https://rescue.vpn.va.gov">https://rescue.vpn.va.gov</a></td>
</tr>
<tr>
<td>The Receiver is already installed but the install button is still showing.</td>
<td>• Check that this is not a software upgrade being pushed. From time to time, a newer receiver will be pushed out.</td>
</tr>
<tr>
<td></td>
<td>• Click the <strong>Skip to Log On</strong> link.</td>
</tr>
<tr>
<td>Browser is reporting a certificate error for the web site.</td>
<td>Try another browser to see if the error occurs again, if it does, do not proceed, contact the National Service Desk and report the error. If the error does not appear in the second browser then the previous browsers certificate store may need to be updated.</td>
</tr>
<tr>
<td>Applications are taking an extended time to launch.</td>
<td>• Ensure that the closest geo-graphical web interface is being connected successfully.</td>
</tr>
<tr>
<td></td>
<td>• When using an application for the first time it can take longer for it to start.</td>
</tr>
<tr>
<td>Applications are not being shown.</td>
<td>• Clear the browser cache.</td>
</tr>
<tr>
<td></td>
<td>• Try connecting via a different browser.</td>
</tr>
<tr>
<td></td>
<td>• Reboot the computer.</td>
</tr>
</tbody>
</table>
|                                                                        | • Contact the NSD and advise that expected applications are not showing. Advise if these applications were showing previously or if access to an application may
<table>
<thead>
<tr>
<th>Problem</th>
<th>Possible Solution</th>
</tr>
</thead>
</table>
| Applications are not launching.              | • Try another web browser.  
• Try another CAG web interface.  
• Un-install the Receiver, then restart and connect to CAG, and install the Receiver again.  
• Capture or record the error message that is being received and what application was tired when the error occurred. Refer to Section 8 Requesting Support for further instructions. |
| Why can I not copy and paste?                | • The copy and paste feature must be requested through the ISO.  
• If this worked previously, contact the NSD and have them verify the account settings. |
| Why can I not print?                         | • The printing feature must be requested through the ISO.  
• If this worked previously, contact the NSD and have them verify the account settings. |
| The Receiver is not un-installing.           | • Ensure all applications have been closed that were started via CAG.  
• Use task manager to verify the Citrix Receiver application is not running. Stop the process if it is still running.  
• Try to reboot the computer. |
| New user and not able to login via CAG.      | Prior to logging into CAG as a new user, the user must change the original password. If the account was just changed by an AD admin and has been set to change password at next login, then the password change feature does not work and CAG cannot be logged into. |
8. Requesting Support

If having difficulty installing or connecting with the Secure Mobility Client and need assistance contact:

Contact: National Service Desk (NSD)

Phone Number: 1-800-877-4328 (Option 1)

Email: NSD.VPNSecurity@va.gov

* Email should include the following details:
  - Login Name including domain
  - Date/Time any connection attempts were made
  - What URL(s) were tried
  - Computer Make/Model
  - Operating System (including service pack level)
  - Browser including version
  - Any additional information or screen captures of errors that may be helpful