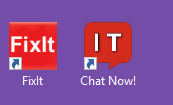
**Document Description:** This document will provide user instructions on how to connect to a virtual desktop.

1. **Install the Citrix Workspace App onto your computer:**

**CSAA Domain-Joined Laptop**

If your laptop has the below icons located on the desktop, it is a CSAA domain-joined laptop. Please refer to the Addendum of this document: *“HOW TO INSTALL THE CITRIX WORKSPACE APP ON A CSAA domain-joined ASSET” (See Page 5-6)*



**CSAA Non-Domain Joined Laptop or BYOD (Bring your own Device)**

If your CSAA laptop does not have the above icons located anywhere on the desktop, it is a non-domain joined laptop and you can download and install the Workspace App using the below method. This also applies to BYOD laptops:

Download/install the Workspace App from the below website:

Windows: <https://www.citrix.com/downloads/workspace-app/windows/workspace-app-for-windows-latest.html>

Mac: [https://www.citrix.com/downloads/workspace-app/mac/workspace-app-for-mac-latest.html](https://www.citrix.com/downloads/workspace-app/windows/workspace-app-for-windows-latest.html)

1. **Are you a new employee and haven’t logged into the CSAA Network before?**

If you answered “YES” to this question and you were given a temporary password, please reset your ENT password via SamReset.. You will need to do this before you attempt to login to your virtual desktop. If you need assistance with resetting your password, please call the IT Service Desk (ITSD) at 1-877-554-2911.  
  
**URL for SamReset:**

[https://csaa-insurance.aaa.com/b2ereset/hipm/#2](https://csaa-insurance.aaa.com/b2ereset/hipm/" \l "2)

1. **Setup Okta Multi-Factor Authentication (MFA) on Your Mobile Device:**

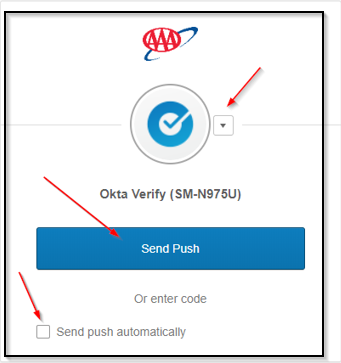
The first time you login to the CSAA VDI Portal you will need to register your device with Okta. This will provide an additional layer of security when connecting to your virtual desktop in the future. Please refer to the Addendum of this document: *“How to Configure your Mobile Device for Multi-Factor Authentication”. (See Page 7-10). You cannot skip to step 4 until you complete this first time Okta configuration on your mobile device.*

1. **Access the CSAA VDI Portal:**

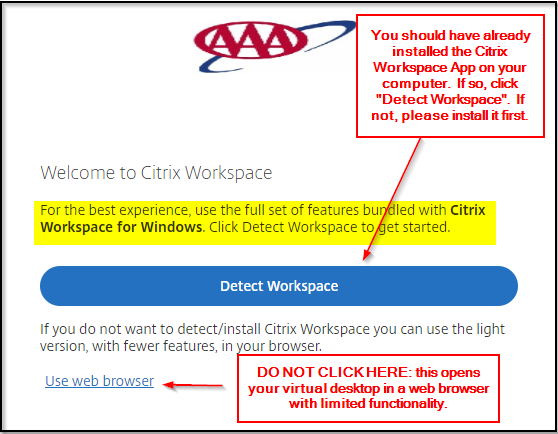
Open a browser and type this URL: <https://csaaig.cloud.com>.

Authenticate using your CSAA credentials (sometimes referred as your g-id)

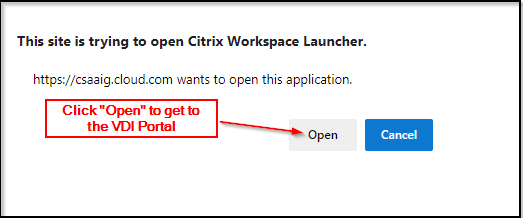
After entering your authentication credentials, you will click “Send Push” to have the Okta two-factor confirmation sent to the device you registered Okta with. When you receive the message on your device, click the ‘Yes, it’s me” button.



Before getting to the main VDI portal page you will need to click “Detect Workspace”



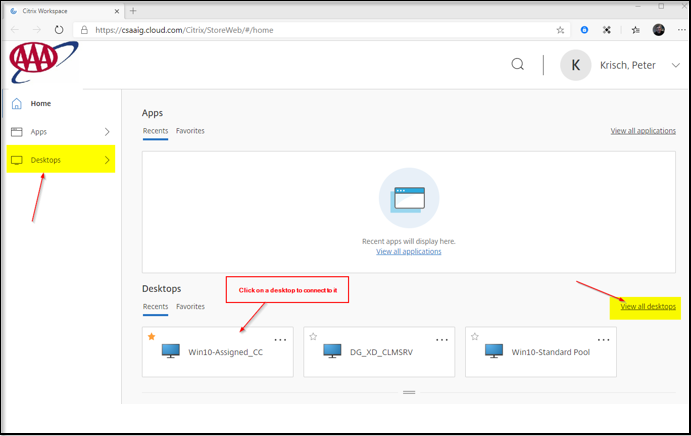
…and then on “Open”.



1. **Broker your Virtual Desktop or Published App:**

Once you are successfully authenticated and logged into the VDI Portal, go to the “Desktops” tab in the left column and then click “View All Desktops”. You will then see an icon that represents your virtual desktop. The name next to it will vary, but expect to see your virtual desktop computer name appear at some point down the road (i.e. ‘VDDXCSAAXXX”).

Click on the desktop icon and your virtual desktop should attempt to connect and open. **Please note:** *For users accessing their virtual desktop for the first time, it may take a couple minutes for it to totally appear, as Windows is doing a first-time setup. If the screen goes black, please don’t be alarmed. Let it sit there for a few minutes while it is configuring.*



**OTHER HELPFUL INFORMATION:**

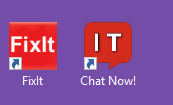
* If you have setup several methods of MFA authentication, you can click the drop-down arrow to choose the one you want to use….Okta Verify is recommended.
* If you are going to use a bookmark, please make sure you bookmark the correct page: <https://csaaig.cloud.com>. We’ve seen users that would bookmark the Okta URL.
* For users accessing their virtual desktop for the first time, it may take a couple minutes to totally appear, as Windows is doing a first-time setup. If the screen goes black, please don’t be alarmed. Let it sit there for a few minutes while it is configuring.
* For first-time users, when you open Outlook, it may take a while for email to appear in your mailbox. It is caching all your mail locally from the main server. After a minute, you will see mail starting to appear.
* It is very important that you keep plenty of free disk space available on your C: drive. If your virtual desktop C: Drive becomes low or runs out of space, your virtual desktop will perform very slowly, or freeze, especially at login. You also might not be able to successfully broker it and/or have a black screen.
* You should NOT be saving files to the Virtual Desktop C: Drive as this drive is NOT backed up and cannot be restored. Just like a physical laptop, if any OS corruption occurs, a new virtual desktop will need to be provisioned for you, and you WILL lose everything on the C: Drive. For this reason, you should be saving any files to your P: Drive.
* You should NEVER explicitly save or copy files and/or folders to your C:\Users\%User Id%\ folder location as that is reserved for profile data that synchronizes during login to a Network location. If large files or subdirectories are copied into this location, logging into your virtual desktop could take a very long time or appear frozen. If you insist on saving files to your virtual desktop rather than to your P: Drive, save documents to the “My Documents" folder. This location doesn’t save your documents to the virtual desktop as you would think, but rather redirects the files to a shared network profile location. (This does not apply to Developer VM’s in TENT). It’s recommended to use your P: Drive.
* You may experience a delay when logging into your Virtual Desktop for the very first time. This is due to the system building your new user profile.
* For security reasons, certain functions between your physical computer and the virtual desktop are prohibited (and are disabled). You will not be allowed to cut/paste clipboard data, copy/paste files, print and/or have local drive pass-thru capabilities.
* You should never share your ID with other users. This is a violation of Acceptable Use Policy.
* You must comply with the CSAA End User Device Standard and you agree to this when logging in to your session.
* Virtual Desktops are patched and automatically restarted twice a month. Watch your email for IT Service Alerts the day before and on those days it’s best to perform a full sign out of your virtual desktop at the EOD.

**ADDENDUM**

**INSTALL THE CITRIX WORKSPACE APP ON A CSAA DOMAIN-JOINED LAPTOP**

*The Citrix Workspace App is necessary if you need to access a virtual desktop or published application.*

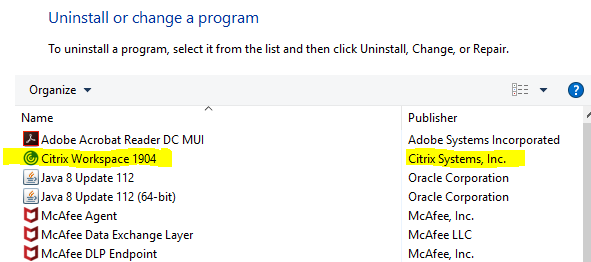
**Please note:** If you see these two icons on your desktop, you have a Domain-joined laptop:



The Workspace App may not have been included on your CSAA laptop. Since user’s don’t have local administrator rights to install applications, you will need to be on the CSAA Network to do this step. For that reason, you will need to use the VPN first to get on the Network. Once you are done with this step and you have the Citrix Workspace App installed on your laptop, you can EXIT the VPN and then just use your local internet.

* Before installing, confirm if you already have it installed. If it is installed, please skip this section all together. Here is how to confirm if it is installed already:

On your CSAA asset, right click on the Windows Start Button, choose Control Panel, then “Programs and Features”.



If you do not see Citrix Workspace in the Program list, you will be able to install it yourself. The App version # might be newer than above.

Here is how to install/reinstall the Citrix Workspace App (Reminder, if you are not on the CSAA Network, use VPN for this step or simply call the ITSD for assistance)

* Connect to the CSAA Network via VPN. Once you are connected, proceed to the next bullet
* Click the Windows Start button and type “Software Center”
* Under the Applications tab, you should see “Citrix Workspace xxxx” (“xxxx” representing the latest certified version).



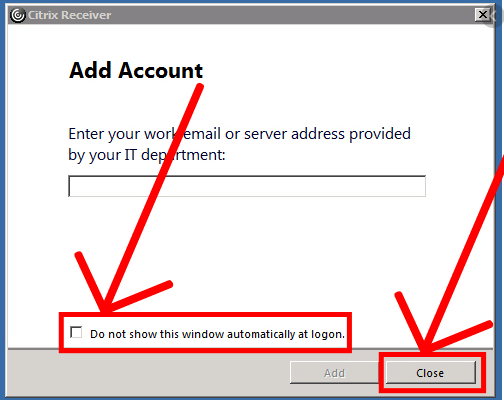
* If the version is newer than what is already installed on your CSAA Asset, click in the checkbox next to the Citrix Workspace icon and then click “Install Selected” in the upper right-hand corner.
* The package will take a minute or so to download and it should then install.
* Upon completion, you WILL need to restart your computer for the Citrix Workspace to be fully functional.

**Important Notes**:

After the Workspace App is installed you might receive the below Popup window…

**Do NOT enter your email or server address in the box.**

Just click the checkbox “Do not show this window automatically at logon” and then click “Close”. This popup window might also appear when you login to your virtual desktop and until you click the “Do not show” checkbox.

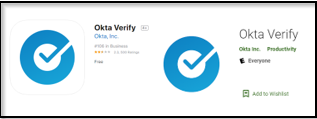
****

**HOW TO CONFIGURE YOUR MOBILE DEVICE FOR OKTA MULTI-FACTOR AUTHENTICATION**

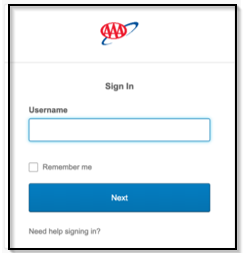
For Security purposes, we require an additional layer of security to connect to your virtual desktop. This is referred to as “two-factor” (or Multi-Factor Authentication-MFA). CSAA has decided to use Okta as the Enterprise MFA solution. Follow the below instructions to setup your Okta MFA account and register your mobile device.

Although there are several different methods available for MFA authentication, we highly recommended to virtual desktop users to utilize the “Okta Verify” method. This method consists of a “push” message being sent to your mobile device, followed by simple user validation. Here are the one-time configuration steps necessary:

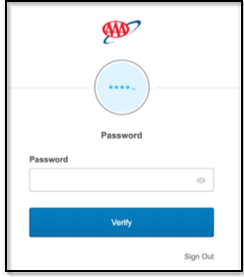
1. Download the Okta Verify app from the [Apple App Store](https://itunes.apple.com/ca/app/okta-verify/id490179405) or [Google Play](https://play.google.com/store/apps/details?id=com.okta.android.auth) onto your primary mobile device.



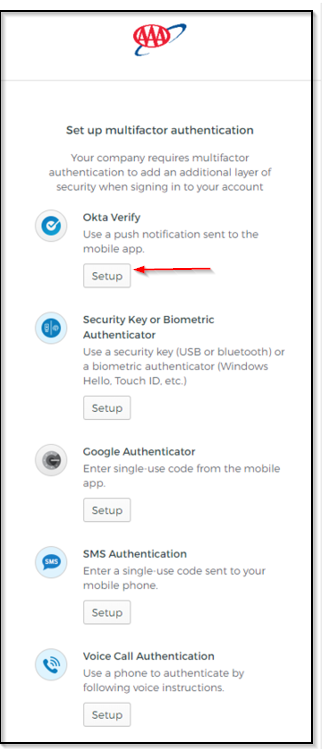
1. Using your computer’s browser, navigate to the new CSAA VDI Portal page: <https://csaaig.cloud.com> .
2. Enter your CSAA credentials to Sign In (g-id and password).
   1. Enter your g-id under username and click Next..



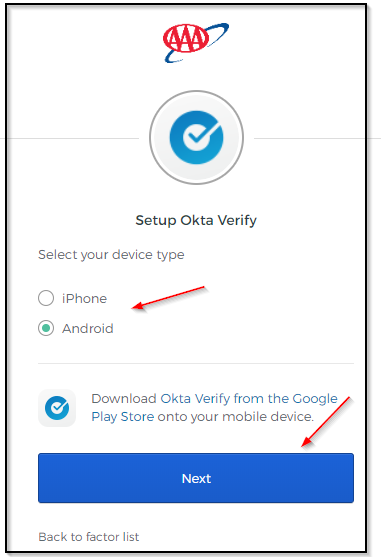
* 1. Enter your corresponding password and click ‘Verify’.



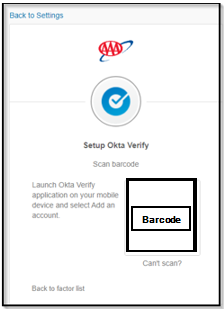
1. Choose “Setup” under the “Okta Verify” option:



1. Depending on what type of mobile device you have pick the appropriate option, followed by “Next”.



1. Open the Okta Verify app on your mobile device. Click the ‘+’ in the app to add an account. Point the mobile device at the barcode now shown on your monitor and center the barcode between the boxes shown on your device. If for some reason your device cannot scan the barcode, click the “Can’t scan” button under the barcode.



1. You are now complete with the initial configuration of Okta MFA. You will not have to perform these steps again unless you care to setup alternative options for two-factor authentication. Please proceed back to Page 2 to login to the CSAA VDI Portal and connect to your virtual desktop.

NOTE:

* You do not need to allow location access. CSAA is not using any location services with Okta.
* You should ‘**Allow Notifications’** for the Okta App on your mobile device, otherwise, you'll need to manually find and open Okta Verify each time you need to authenticate.
* You should **allow** access to the **camera** for the initial device registration. You can turn off camera use from "Settings" after the registration.

If you need further assistance or have a question regarding this process, please reach out to the IT Service Desk and they can assist…

**877-554-2911**