



Virtual Desktop for AAA-ICDR Arbitrators

Welcome Guide

Contents

Getting started with your CaseShield virtual desktop	3
Recommended/Compatible Hardware.....	3
What to expect during the initial onboarding process	4
Technical Support	4
Prerequisites / Software needed on your physical laptop or desktop	5
Duo Mobile application needed on your mobile device.....	5
First time logging into your virtual desktop.....	7
Toolbar on top of virtual desktop screen.....	10
Changing your Password.....	12
Applications installed on the virtual desktop	13
Using OneDrive for transfer, storage, and back-up of your files and documents	14
Sharing Files Securely with OneDrive	15
Using your new caseshield.com email address with Outlook	16
Adding your CaseShield email to your mobile device.....	16
Accessing your Microsoft Office 365 account from outside the virtual desktop	17
Using Zoom	20
Appendix	21
Ensuring emails from CaseShield get delivered to your inbox	21
Setting a forward from your existing email to the new CaseShield email.....	23
Exporting existing email content/contacts and importing into CaseShield email.....	23
Adjusting the Screen Resolution of the CaseShield Virtual Desktop	24
Using “Dragon Naturally Speaking” Software with the CaseShield Virtual Desktop	25
Security benefits of using the CaseShield email address and virtual desktop.....	26

Getting started with your CaseShield virtual desktop

CaseShield by AAA-ICDRSM is a new initiative to enhance the cybersecurity of AAA-ICDR arbitrators. CaseShield is a virtual desktop, which is a computer running in the cloud. You can connect to this cloud-based virtual desktop from any physical personal computer including Windows, Apple, or Chromebook. Along with the virtual desktop, a new email account – @caseshield.com – is included for each arbitrator with CaseShield. Using this virtual desktop and email provides several “enterprise grade” technology and security solutions that are difficult to acquire, install, and maintain on an individual or consumer level. Some of these enterprise grade security protections include firewalls, email spam filtering, web content filtering, anti-virus/anti-malware software, and two-factor authentication. These are just some of the features that in conjunction will help protect important case data when using CaseShield.

The AAA is partnering with [dinCloud](#), who is a leading provider in the “Desktop-as-a-Service” market. dinCloud is providing the infrastructure where the virtual desktops are hosted. Technical support for CaseShield will be provided by the AAA-ICDR.

Recommended/Compatible Hardware

The CaseShield virtual desktop will work on any currently supported computer operating system. You can use a desktop or laptop computer with Windows 10, MacOS Mojave (or later), or a Google Chromebook. We recommend using the latest versions of the operating systems for any of these and to make sure automatic updates are enabled to continue to get the latest supported versions and all important security patches. A stable internet connection is also required to connect to your CaseShield virtual desktop. At a minimum your computer should have at least the following hardware resources:

- CPU: 1.5 GHz or better processor speed
- RAM: 4GB or more of memory
- Disk: 32 GB or more of disk space

These are minimum requirements, and going above these minimums could increase the performance of both the physical computer and using the CaseShield virtual desktop.

You can also use the CaseShield virtual desktop on a mobile device like an iPad, Android tablet, or an iPhone or Android phone, but the smaller screen size and fewer hardware resources may be less effective, and result in lower performance, than using a laptop or desktop computer with larger or multiple monitors.

What to expect during the initial onboarding process

You'll receive an email from CaseShield Support (support@caseshield.com) with a subject line of "Welcome to CaseShield". This email will go to your existing email account. **If you don't see the email in your Inbox, check your spam folder as it may be there. In the Appendix of this document, we provide steps you can take in Gmail to ensure emails from CaseShield Support get delivered to your Inbox and not the Spam folder.** In this welcome email from support@caseshield.com you'll see the CaseShield logo, as well as the website URL to access your CaseShield virtual desktop (<https://caseshield.dincloud.com/>) and your username to log in to your virtual desktop. A separate email from CaseShield support will be sent with your initial password, which you'll be prompted to change after the first time you log in.

After you receive these initial emails, you can use the information in the emails from CaseShield support and this guide to log in to your virtual desktop. If you are unable to complete the onboarding yourself, you can work with the CaseShield support team, see 'Technical Support' section below. If a support call is needed, a CaseShield support engineer may use Zoom to view your computer screen, and walk you through accessing your CaseShield virtual desktop to make sure you can log in and access everything you need. The typical initial onboarding call with CaseShield support should take 30 – 40 minutes, but can take longer depending on additional questions you may have for the support engineer.

Technical Support

For any issues with the CaseShield virtual desktop, technical support is provided by the AAA-ICDR's CaseShield Support team.

Support is available via email and phone from 7am EST to 8pm EST Monday - Friday. Emailing support@caseshield.com is the preferred method for opening a new support ticket. Emailing automatically creates a ticket and a support engineer will respond to your email promptly via email or phone call during support hours.

You can also call CaseShield support at 1-800-507-5578. You can leave a voicemail at this number if calling outside these hours, or if support engineers are unavailable due to helping other customers at the time of your call. However we recommend you initiate a technical support issue by emailing support@caseshield.com for the quickest response.

After opening a ticket with CaseShield support (either by email or phone) the support engineer may send you an email with a meeting invite link using Zoom. Clicking on the Zoom link will bring you to a meeting with the CaseShield support engineer who will then be able to see your screen. If needed, the support engineer may request control of your computer to troubleshoot or resolve an issue. You will have to confirm and give consent before the support engineer can do this.

Prerequisites / Software needed on your physical laptop or desktop

Whatever personal device you are using to connect to the CaseShield virtual desktop will need the Citrix Workspace App installed prior to the first time connecting to the virtual desktop. You can install the Citrix Workspace App on multiple devices and access your CaseShield virtual desktop from multiple devices, but not simultaneously. This Citrix Workspace app is one-time installation from each personal device you use, and will allow the full functionality of the virtual desktop. You'll be prompted to download the Citrix Workspace App the first time you log on to your CaseShield virtual desktop at <https://caseshield.dincloud.com/>. You can also download the Citrix Workspace App for your type of computer from the Citrix website here: <https://www.citrix.com/downloads/workspace-app/>. Once on this site, choose the Workspace app for your type of device (Windows, Mac, etc.)

In order to use Zoom on the virtual desktop, you'll also need a Zoom plugin for Citrix Workspace installed on your physical computer. This will allow the webcam and microphone on your physical computer to be used by Zoom on the virtual desktop. The Zoom plugin for Citrix Workspace can be downloaded at the link below. Choose the plugin for your type of device (Windows, Mac, etc.)

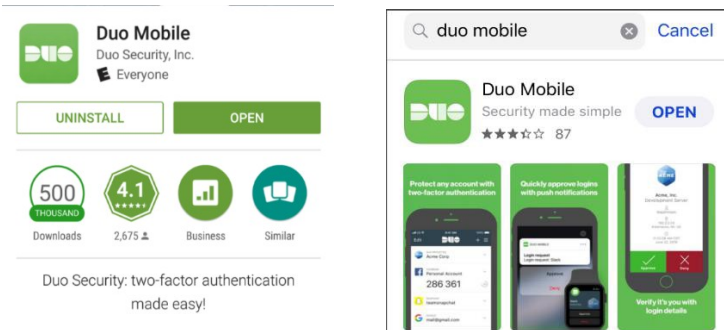
<https://support.zoom.us/hc/en-us/articles/360041602711-VDI-downloads-and-backwards-compatibility>

Both the Citrix workspace App and the Zoom plugin for Citrix Workspace that are installed on your physical computer will need an account with local administrative rights to complete the install.

If you need help with this, you can contact CaseShield support, and they can help you install these apps if needed.

Duo Mobile application needed on your mobile device

On your mobile device, you'll need an app called Duo Mobile. This can be found in the [Apple App Store](#) for iPhone and the [Google Play store](#) for Android. Duo is used for two-factor authentication and greatly increases the security of your account and virtual desktop. Duo will be used as a second factor of authentication to log in to your CaseShield virtual desktop, and also to access your Microsoft account for your CaseShield email and OneDrive.



To install Duo, please follow these steps:

- 1) On your computer, open a new Internet Browser (Internet Explorer, Google Chrome, Mozilla Firefox etc.)
- 2) Go to website <https://caseshield.dincloud.com/>
- 3) Enter your username in the **User Name** field. Refer to the welcome email from CaseShield support for your username.
- 4) Enter your password in the **Password** field.
- 5) Click **Log On**.
- 6) Click Start Setup
- 7) Select the type of device you are adding (Mobile phone, Tablet etc.)
- 8) Click **Continue**
- 9) Enter your mobile number.
- 10) Click **Continue**.
- 11) Click **Continue** to Login on the next screen, a QR code will then appear on the computer screen.
- 12) Download the **Duo Mobile** app for your phone (App Store for iPhone and Play Store for Android).
- 13) Once the app is installed, open the app on your phone and press the + sign located on the top of the screen.
- 14) Use the Duo Mobile App on your phone to scan the QR code displayed on your computer screen for enrollment. Once enrolment is completed, a prompt will appear on computer screen informing you about the two-factor authentication.
- 15) Click **Send Duo Push** on the next screen on your computer. A notification appears in the Duo Mobile app on your phone.
- 16) Click **Approve** in the Duo app on your phone to authenticate.
- 17) Once authentication is complete, the dinCloud website redirects you to your virtual desktop.


Once the initial Duo setup is completed, you'll use the Duo app each time you login to the virtual desktop.

After you enter your username and password at <https://caseshield.dincloud.com/> you'll see a Duo prompt on the screen and can select from "Duo Push", "Call Me", or "Passcode". The easiest and recommended option is the "Duo Push" which will send a notification to your mobile device with the Duo app installed. After you open the Duo notification on your mobile device and tap the "Approve" button, you'll complete the login.

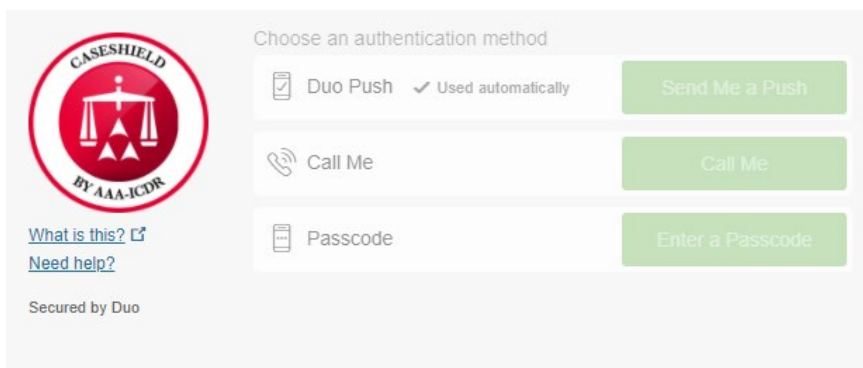
First time logging into your virtual desktop

You can access your virtual desktop at <https://caseshield.dincloud.com/>. Make sure to “bookmark” this site on your preferred web browser on your physical computer so you can easily access it again.

- 1) Login at <https://caseshield.dincloud.com/> with the username and password in the emails provided by CaseShield support.

The image shows the CaseShield login page. At the top is the CaseShield logo with the text "by AAA-ICDR". Below the logo, it says "Please log on". There are two input fields: "User name" and "Password". Below the password field is a red button labeled "LOG ON". The entire login form is centered on a light gray background, which is itself centered within a red border.

- 2) After you enter your username and password, complete the Duo two-factor authentication

The image shows the Duo two-factor authentication page. On the left is the CaseShield logo with the text "BY AAA-ICDR". Below the logo are links for "What is this?" and "Need help?". At the bottom left, it says "Secured by Duo". On the right, there is a section titled "Choose an authentication method". It contains three rows: "Duo Push" with a checkmark and "Used automatically" (with a "Send Me a Push" button), "Call Me" (with a "Call Me" button), and "Passcode" (with an "Enter a Passcode" button).

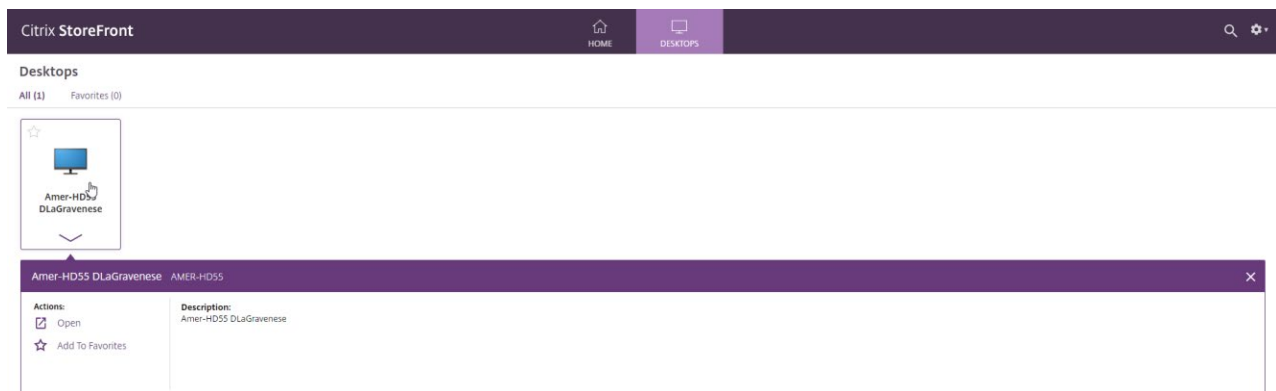
- 3) You'll arrive at a website that says "Citrix StoreFront" and "Welcome *your name*". The website will look like this:

Welcome Drew LaGravenese!

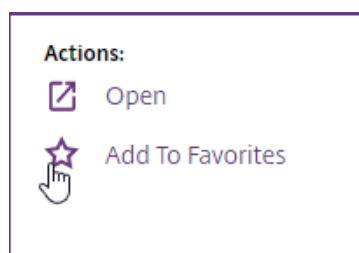


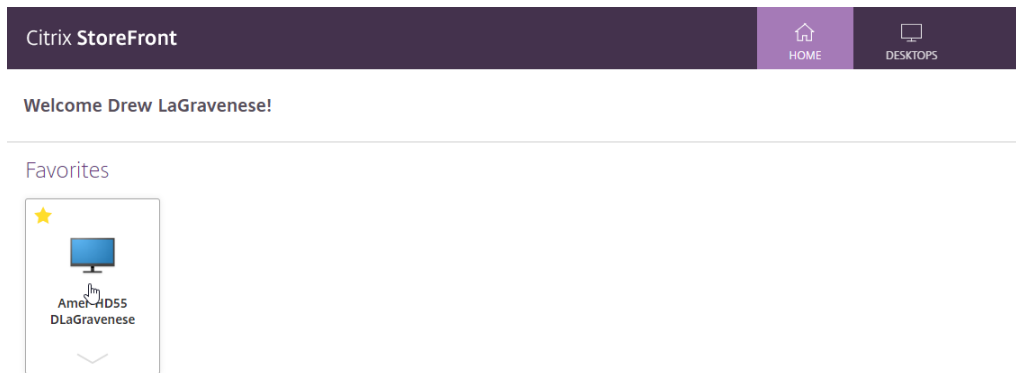
You do not have any favorite Desktops yet.
To get started, go to Desktops and click or tap the star to favorite an item.

- 4) At the top of the screen in the middle you'll see 'Home' is selected. Click on 'Desktops' and then you'll see your virtual desktop which you can click on that will launch your virtual desktop. Your virtual desktop will be named "Amer-hdxx *username*".

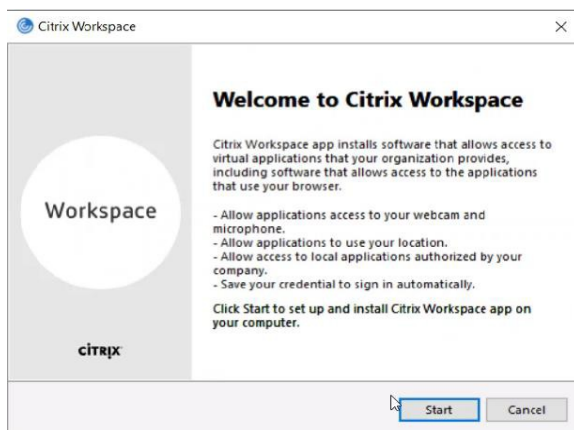


- 5) You can also click the 'Add to Favorites' star which will add your virtual desktop to your home screen.





- 6) After clicking on your virtual desktop for the first time, it will detect if the Citrix Workspace app is already installed. If not, you'll be prompted to download it. Once downloaded, click on the "CitrixWorkspaceApp.exe" to install. You'll see a popup like the below prompt. Click 'Start' and follow the prompts.



- 7) Click 'Finish' and 'restart' when installation is complete. Your physical computer will restart. You will only have to download and install the Citrix Workspace app the first time accessing your CaseShield virtual desktop. Subsequent times logging in clicking on your virtual desktop will log you right in.
- 8) Once your computer comes back on, go to the login website at <https://caseshield.dincloud.com> and login using your credentials and Duo verification.
- 9) Click on the virtual desktop icon to launch your cloud desktop. You will be logged in and see a new Windows 10 desktop with the CaseShield logo as the background picture. This CaseShield logo in the background will allow you to easily identify when you are working in the CaseShield virtual desktop vs. the desktop of your physical computer.



Toolbar on top of virtual desktop screen

When you are logged into the CaseShield virtual desktop, at the top center of the screen you'll notice a toolbar. Click the arrow to expand the toolbar. You'll see options that you'll need when working in the virtual desktop.



Home – Minimizes the desktop session. This is how you can toggle out of the virtual desktop and back to your regular desktop of your physical computer.

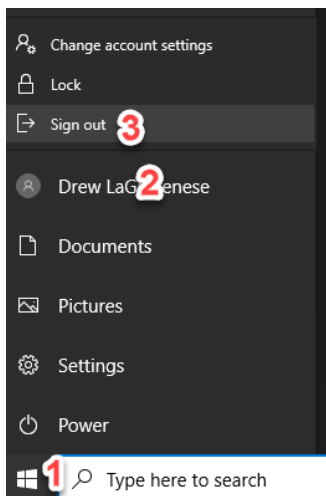
The Citrix Workspace App icon in the taskbar of your physical computer desktop is how you can maximize the virtual desktop session again.



Window – Changes the virtual desktop from full screen to a smaller window. Then you can drag the window with your mouse to adjust the size or move to a different monitor if you are using multiple monitors. If you want to use multiple monitors simultaneously, you can span the CaseShield virtual desktop across both monitors by dragging the CaseShield window to where it is partially showing on both screens and then click maximize (square) at the top right corner of the window.

Disconnect – Stops your virtual desktop session but does not properly log you out of the virtual desktop. As a best practice to avoid potential issues with the virtual desktop, it is recommended you follow the below steps to log out of the virtual desktop when you are done working.

- 1) Click the Windows icon in the lower left hand corner of the virtual desktop
- 2) Click on your name
- 3) Click 'Sign out'

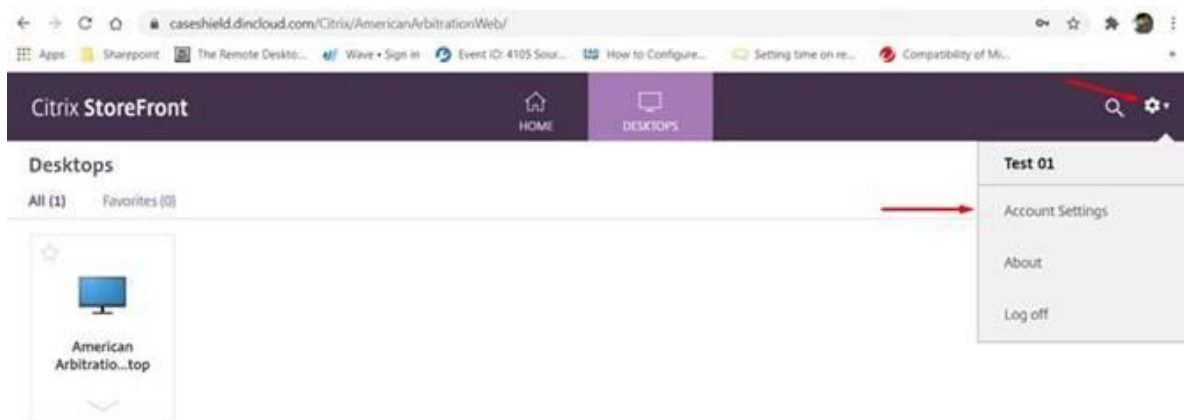


Changing your Password

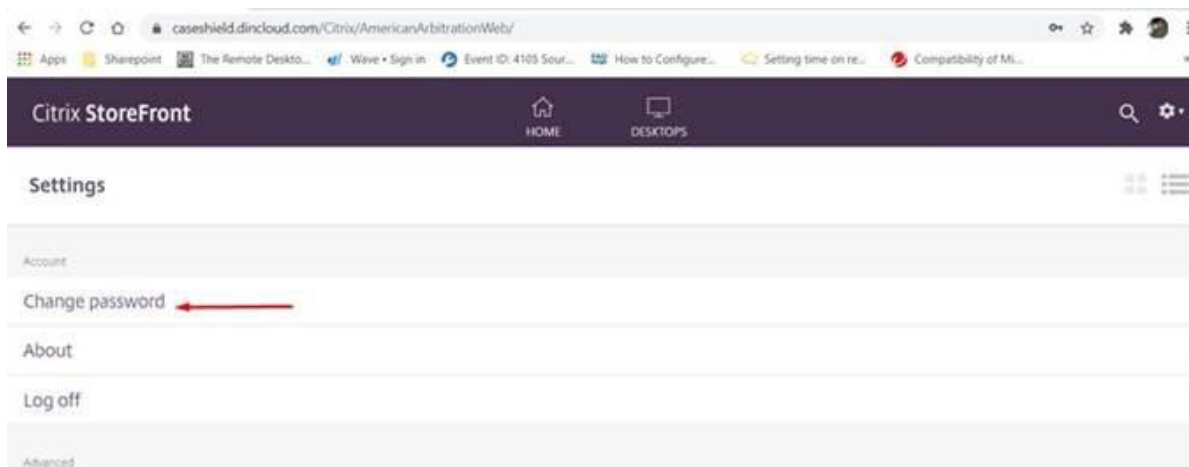
In your welcome email you receive from CaseShield support you'll receive your username and the URL to access your virtual desktop (<https://caseshield.dincloud.com/>). A separate email will be sent to you with your initial password. This username and password is used for both your virtual desktop and your Microsoft Office 365 account which includes your caseshield.com email address and OneDrive access. After logging in to <https://caseshield.dincloud.com/> the first time, you'll be required to change your password. If you need to change your password going forward follow the below steps.

**** Please note that when you change your password using this method, you'll also need to change your password on your mobile device if you have already set up your caseshield.com email address with your old password on the mobile device.*

- 1) Once logged in to <https://caseshield.dincloud.com/>, click on the gear settings button on the top right side of the screen and then click 'Account Settings'



- 2) Click on 'Change password'

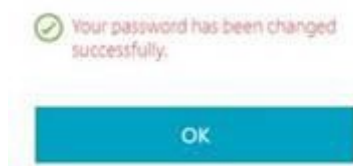


- 3) Enter your old password, a new password, and confirm the new password and click 'OK'



A screenshot of a 'Change Password' dialog box. It contains four input fields: 'User name:' with the text 'caseshield.local\test01', 'Old password:', 'New password:', and 'Confirm password:'. Each password field is masked with dots and has a small icon on the right. At the bottom, there are two buttons: 'OK' and 'Cancel'. A red arrow points to the 'OK' button.

You'll see that your password has been changed successfully. Use the new password to log in going forward.



Applications installed on the virtual desktop

Web browsers – Google Chrome and Microsoft Edge (updated version of Microsoft Internet Explorer)

Microsoft Office apps – Outlook (for your CaseShield email), Word, Excel, PowerPoint, OneNote

Meeting Tools – Zoom VDI (Zoom version needed on virtual desktops; VDI stands for Virtual Desktop Infrastructure; requires separate account/subscription with Zoom to use)

Adobe – Adobe reader to view PDFs, and Adobe Acrobat DC to edit PDFs (requires separate account/subscription with Adobe to use)

If there is other software that you typically use that is not on the virtual desktop initially, you can work with CaseShield support to get it installed on your virtual desktop. The software needs to be compatible with the Windows 10 virtual desktop.

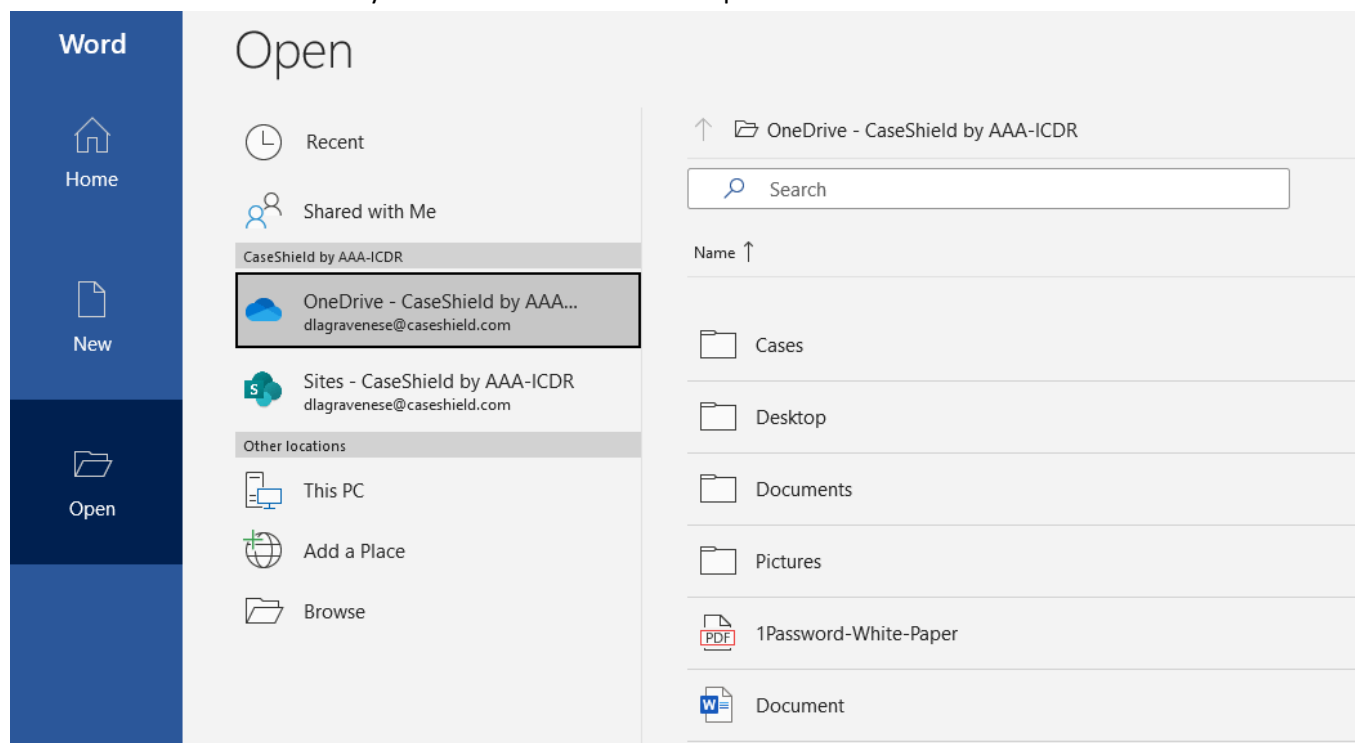
Using OneDrive for transfer, storage, and back-up of your files and documents

OneDrive is a tool in the Microsoft Office 365 suite of applications that is great for transferring, storing, and backing up your files and documents. OneDrive will allow you to copy the important files and documents you currently have stored on your physical laptop or desktop to use in your CaseShield virtual desktop. With OneDrive, you can store all your documents, the Microsoft Office 365 license allows for 1TB of space.

OneDrive is similar to DropBox or Google Drive, in that it is a cloud based tool you can access from any device. To access OneDrive to transfer and manage any documents, you can go to <https://portal.office.com> from inside or outside of the virtual desktop. You'll need your CaseShield username and password to log in (the same username and password when you log in to the virtual desktop) and you may also have to complete the Duo multi-factor authentication step.

Once you log in to OneDrive from your physical computer at <https://portal.office.com>, you can copy files to OneDrive, and then access them again from within the CaseShield virtual desktop. More info about this in the section below on "Accessing your Microsoft Office 365 account from outside the virtual desktop"

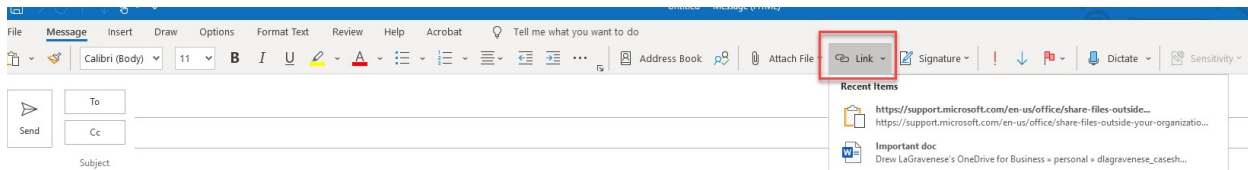
When you open Word in the CaseShield virtual desktop, you can open your OneDrive documents – you'll see 'OneDrive – CaseShield by AAA-ICDR' as a location to open documents from.



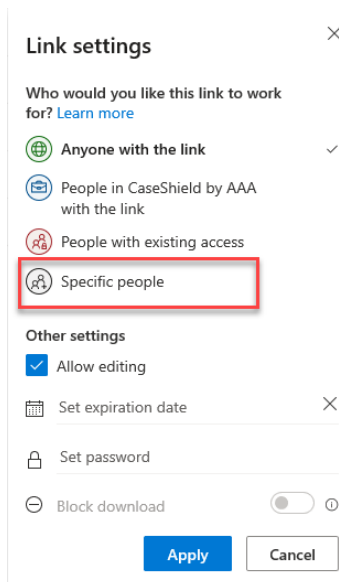
Sharing Files Securely with OneDrive

When you store files in OneDrive, you can securely share those files with specific people that need to view or edit them. There are multiple ways to do this. It can be managed through the web when you log in to <https://portal.office.com> and access your OneDrive. Here you can allow specific people to view or edit the file, and an email will be sent to them with the link to that file. You can also do this via Outlook in CaseShield by using the 'Link' button on the toolbar of a new email.

The 'Link' button in the Outlook toolbar of a new email:



Make sure you select specific people that can access the link/file. The default setting when sharing will allow “anyone with the link” to access it.



The below articles from Microsoft Support have more details about sharing files with OneDrive and using secure links to do so.

<https://support.microsoft.com/en-us/office/share-onedrive-files-and-folders-9fcc2f7d-de0c-4cec-93b0-a82024800c07>

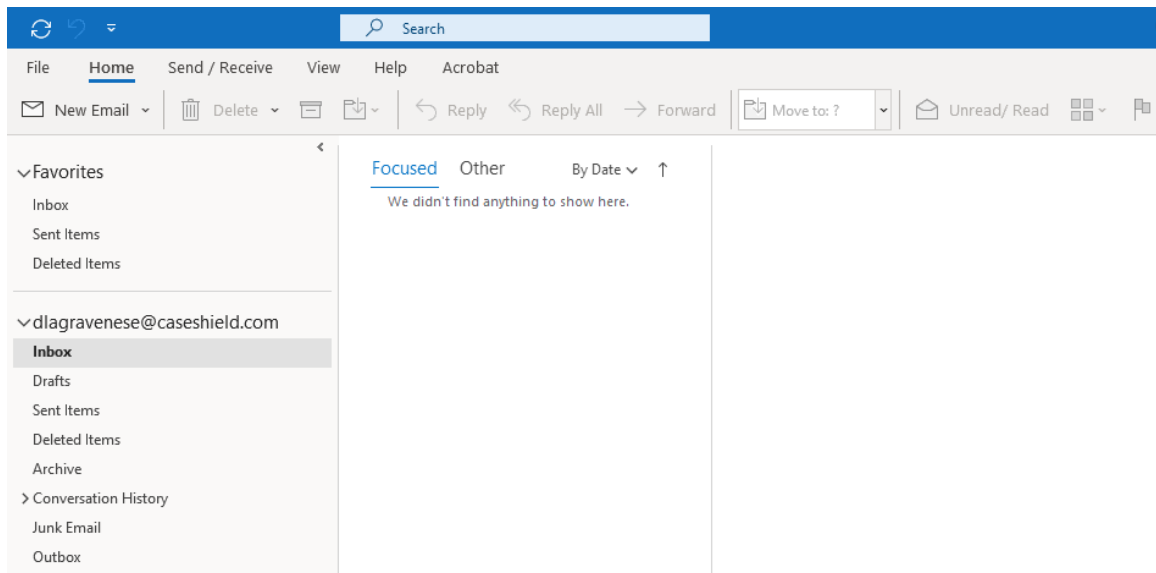
<https://support.microsoft.com/en-us/office/share-files-outside-your-organization-with-secure-links-7266f44e-3e06-4736-b9d3-0580c24bba34>

Using your new caseshield.com email address with Outlook

Once you are in your CaseShield virtual desktop for the first time, click on the Outlook icon on the desktop.



The first time opening Outlook, you'll see a pop up window with your new CaseShield email address populated. This pop up is an initial configuration screen and after this first time, clicking on the Outlook desktop icon will open Outlook immediately where you can use your new CaseShield email.



Adding your CaseShield email to your mobile device

There are two different ways to add your caseshield.com email to your mobile device.

If you use an iPhone or iPad, you can add your caseshield.com email to the default mail app on the iPhone or iPad. When adding the account, select “Microsoft Exchange” as the account types and follow the prompts to enter your CaseShield email address and password. The rest of the server settings will automatically apply.

You can also add your CaseShield email to your mobile device with the Microsoft Outlook mobile app. On your smart phone or tablet, you can use the app store to find the Outlook mobile app.

For Android devices on the Google Play store:

https://play.google.com/store/apps/details?id=com.microsoft.office.outlook&hl=en_US&gl=US

For Apple devices on the App store:

<https://apps.apple.com/sb/app/microsoft-outlook/id951937596>

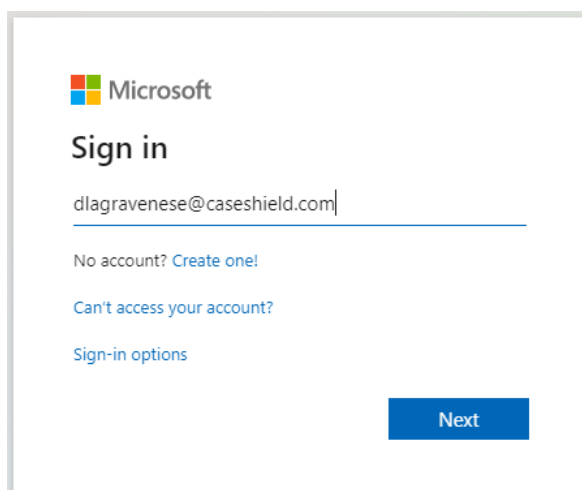


In order to add your CaseShield email to a mobile device like your phone or iPad, it is required the device have a password or passcode set of a minimum of 4 characters.


Accessing your Microsoft Office 365 account from outside the virtual desktop

You can access your Microsoft Office 365 account, and all the associated apps, like Outlook and OneDrive, from outside the virtual desktop. Accessing Office 365 from outside the virtual desktop requires two-factor authentication with the Duo Mobile app installed on your phone.

- 1) Use your web browser to navigate to <https://portal.office.com>. Type in your full CaseShield email address. So your username (first initial, last name) followed by '@caseshield.com' and click 'Next'.



- 2) You then get a Duo prompt. Enter your username (this time without the '@caseshield.com') and password. This is the same password you use to log in to your virtual desktop. Click 'Login'



Log in


Please enter your credentials to access Office 365.

Username
diagravenese

Password
[Redacted]

Log in

- 3) You'll get an option to select your authentication method. The 'Duo Push' is the easiest method and if selected you'll get a notification on the mobile device where you have the Duo Mobile app installed.



Choose an authentication method

☒ Duo Push ✓ Used automatically **Send Me a Push**

☐ Call Me **Call Me**

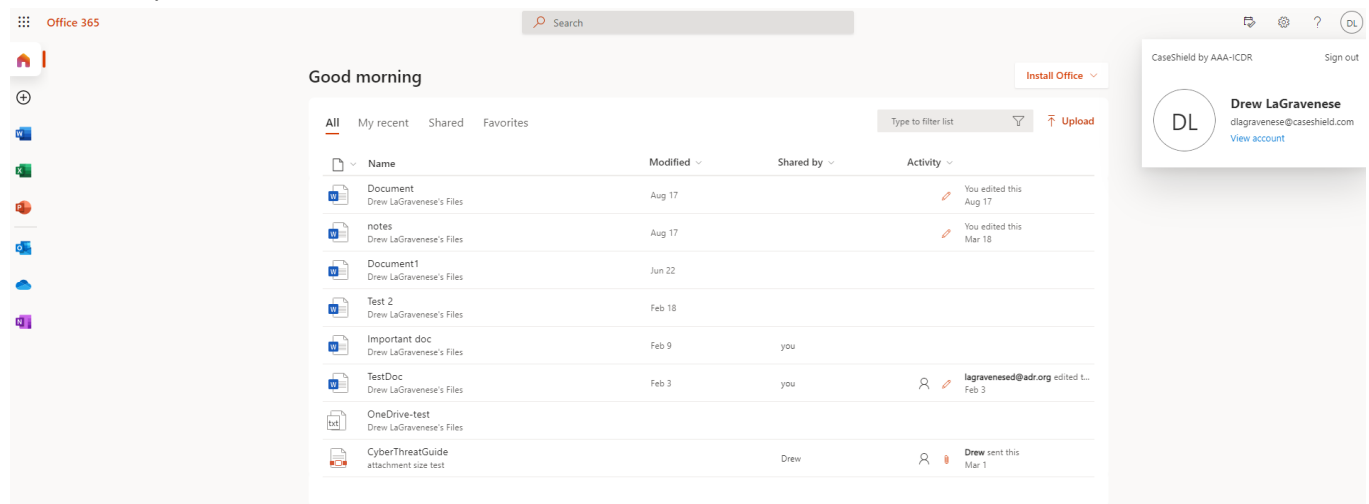
☐ Passcode **Enter a Passcode**

[What is this?](#) [Need help?](#)

Secured by Duo

Pushed a login request to your device... **Cancel**

- 4) Tap 'Approve' on the Duo Mobile app to complete the authentication. You'll now be logged in to your Microsoft Office 365 account and see a screen similar to this.



Office 365

Good morning

DL **Drew LaGravenese**
diagravenese@caseshield.com
[View account](#)

Document
Drew LaGravenese's Files
Aug 17
You edited this Aug 17

notes
Drew LaGravenese's Files
Aug 17
You edited this Mar 18

Document1
Drew LaGravenese's Files
Jun 22

Test 2
Drew LaGravenese's Files
Feb 18

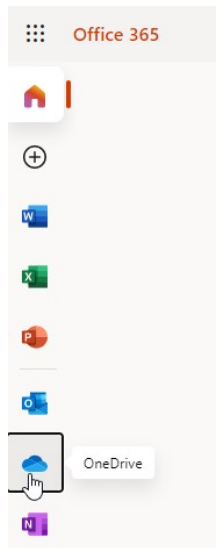
Important doc
Drew LaGravenese's Files
Feb 9
you

TestDoc
Drew LaGravenese's Files
Feb 3
you
lagravenese@adr.org edited L... Feb 3

OneDrive-test
Drew LaGravenese's Files

CyberThreatGuide
attachment size test
Drew
Drew sent this Mar 1

- 5) You can access the various apps from the left side menu. Click on the OneDrive icon to go to your OneDrive page where you can add/upload documents from your physical computer, and then access those same documents from within your virtual desktop.



- 6) Clicking the OneDrive button will open a new tab where you can manage your OneDrive files.

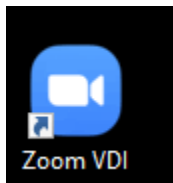
A screenshot of a web browser displaying the OneDrive interface. The browser's address bar shows the URL: caseshield-my.sharepoint.com/personal/dlagravenese_caseshield_com/_layouts/15/onedrive.aspx. The OneDrive interface has a blue header with the 'OneDrive' logo and a search bar. Below the header, there's a navigation pane on the left with 'My files' selected. The main area shows a list of files and folders. The list has columns for Name, Modified, Modified By, File size, and Sharing. The files listed are 'Cases', '1Password-White-Paper.pdf', 'Important doc.docx', 'notes.docx', 'OneDrive-test.txt', and 'TestDoc.docx'.

Name	Modified	Modified By	File size	Sharing
Cases	February 9	Drew LaGravenese	0 items	Private
1Password-White-Paper.pdf	November 16, 2020	Drew LaGravenese	523 KB	Private
Important doc.docx	February 9	Drew LaGravenese	11.6 KB	Shared
notes.docx	February 3	Drew LaGravenese	10.9 KB	Private
OneDrive-test.txt	November 5, 2020	Drew LaGravenese		Private
TestDoc.docx	February 3	lagravenesed@adr.org	13.7 KB	Shared

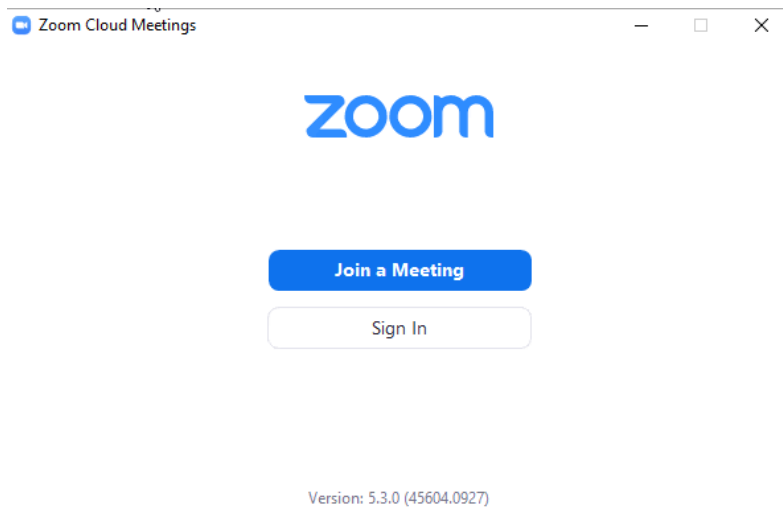
Using Zoom

You can use Zoom for meetings and virtual hearings on your virtual desktop just as you would on your physical computer. The Zoom client comes pre-installed on your virtual desktop, but an account/license is not included. You can go to <https://zoom.us> to create a free account or purchase a paid license if needed. There is also an application called Zoom plug-in for Citrix Workspace App that needs to be installed on your physical computer. This app on your physical computer is required to be able to use the webcam and microphone on your physical computer in Zoom on the virtual desktop.

On your virtual desktop, you'll see an icon named Zoom VDI. This is a version of Zoom specifically for virtual desktops (VDI stands for Virtual Desktop Infrastructure).



After clicking this icon, you'll get the same initial zoom screen you typically see to sign in or join a meeting.

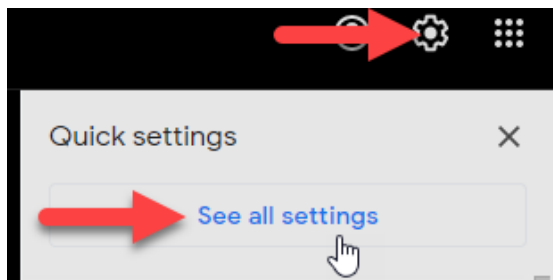


Appendix

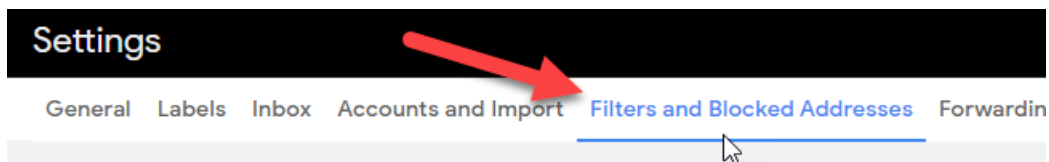
Ensuring emails from CaseShield get delivered to your inbox

We want to ensure that emails coming from CaseShield Support get delivered to your current email inbox and not in the spam folder. To do that in Gmail, you'll need to create a filter for emails coming from @caseshield.com to "never send it to Spam". Please follow the steps below to create this filter in Gmail. If you use a different email currently, the steps will be slightly different so you'll have to check the settings in that email platform.

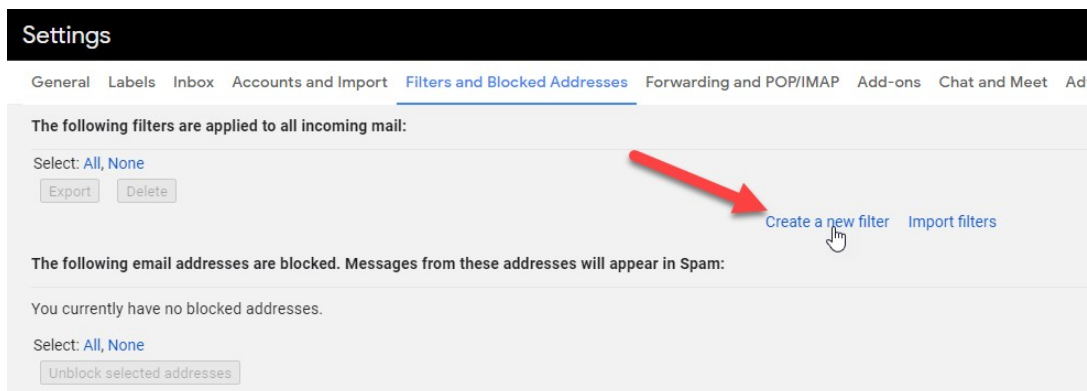
1) Login to Gmail, click on the gear icon in the top right side of the screen and select "See all settings":



2) Select "Filters and Blocked Addresses":



3) Click "Create a new filter":



- 4) In the pop up window that appears, type "@caseshield.com" in the "From" field and click "Create filter":

from:@caseshield.com

From @caseshield.com

To

Subject

Has the words

Doesn't have

Size greater than MB

☐ Has attachment ☐ Don't include chats

Create filter Search

- 5) Check the "Never send to spam" box and then click "Create filter". Now all emails from @caseshield.com will show up in your Gmail Inbox and not the Spam folder.

from:@caseshield.com

← When a message is an exact match for your search criteria:

☐ Skip the Inbox (Archive it)

☐ Mark as read

☐ Star it

☐ Apply the label: Choose label...

☐ Forward it [Add forwarding address](#)

☐ Delete it

☒ Never send it to Spam

☐ Always mark it as important

☐ Never mark it as important

☐ Categorize as: Choose category...

☐ Also apply filter to 0 matching conversations.

Note: filter will not be applied to old conversations in Spam or Trash

[? Learn more](#)

Create filter

Setting a forward from your existing email to the new CaseShield email

You may want to forward some or all of your incoming emails in your existing email account to your CaseShield email. To do that with Gmail, please follow the steps in the below support article from Google. If you use a different email currently, the steps will be slightly different so you'll have to check the settings in that email platform.

<https://support.google.com/mail/answer/10957?hl=en>

Exporting existing email content/contacts and importing into CaseShield email

There are multiple ways to get your existing email, calendar, and contacts into your CaseShield environment. Below are some of the most common ways to do it with Gmail. If you use a different email currently, the steps will be slightly different so you'll have to check the settings in that email platform.

- To add your Gmail email to Outlook in your CaseShield virtual desktop, please follow the steps in the support article from Microsoft:

<https://support.microsoft.com/en-us/office/import-gmail-to-outlook-20fdb8f2-fed8-4b14-baf0-bf04b9c44bf7?ui=en-US&rs=en-US&ad=US>

- To add your Gmail calendar to Outlook in your CaseShield virtual desktop, please follow the steps in the support article from Microsoft:

<https://support.microsoft.com/en-us/office/import-google-calendar-to-outlook-098ed60c-936b-41fb-83d6-7e3786437330?ui=en-US&rs=en-US&ad=US>

- To add your Gmail contacts to Outlook in your CaseShield virtual desktop, first you'll need to export your Gmail contacts by following the steps in this article from Google:
<https://support.google.com/contacts/answer/7199294?co=GENIE.Platform%3DDesktop&hl=en>

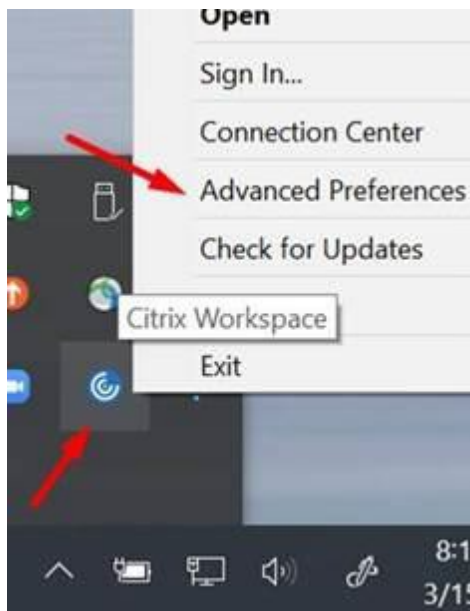
Then please follow the steps in the support article from Microsoft to import the contacts into Outlook:

<https://support.microsoft.com/en-us/office/import-contacts-to-outlook-bb796340-b58a-46c1-90c7-b549b8f3c5f8>

Adjusting the Screen Resolution of the CaseShield Virtual Desktop

It's possible that when first using your virtual desktop the screen resolution may not be optimized to for your physical computer and monitors, which can give a fuzzy, blurry, or unclear picture in the virtual desktop. If you are experiencing this, please follow the below steps to adjust the virtual desktop screen resolution to match the screen resolution of the physical computer you are using.

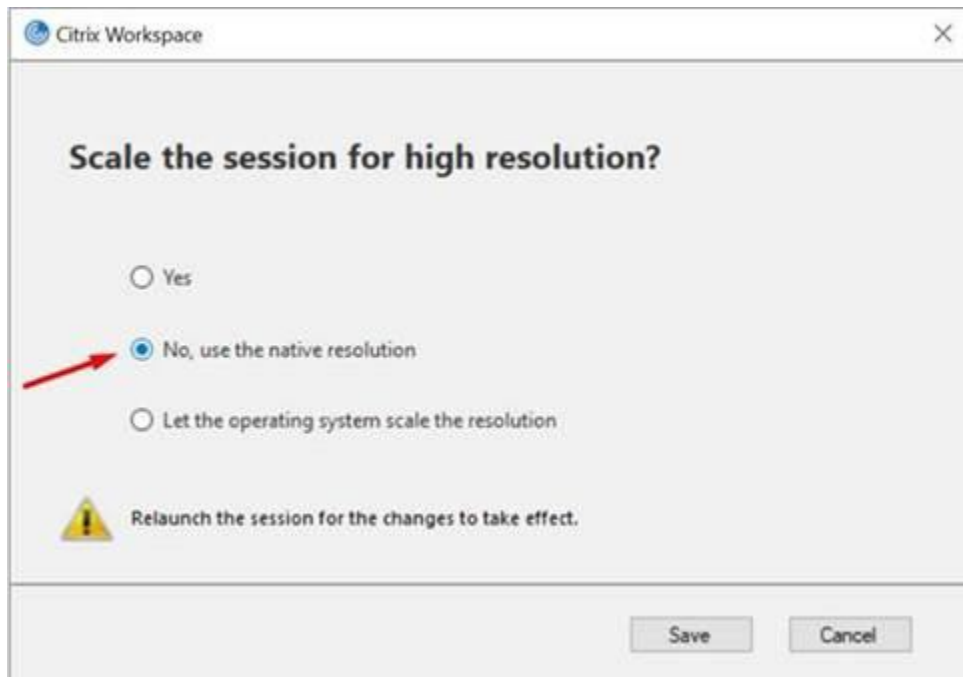
1. On your physical computer, right click on the Citrix Workspace icon in the tray (in the lower right hand side of your main monitor) and select "Advanced Preferences":



2. Click on "High DPI" in the Advanced Preferences window:



3. Select “No, use the native resolution” in the settings window, and click “Save”:



4. Sign out from the virtual desktop, and connect back in for the changes to take effect.

Using “Dragon Naturally Speaking” Software with the CaseShield Virtual Desktop

Dragon Naturally Speaking is a speech recognition and dictation software that many arbitrators use. We’ve found that installing Dragon on the virtual desktop does not always work as intended. Instead, Dragon can be used in the virtual desktop while still installed on your physical computer. If you use Dragon, please follow the below steps for the optimal way to use it with the CaseShield virtual desktop.

1. Install Dragon directly on the physical desktop/laptop that will be used to access CaseShield virtual desktop.
2. Configure Dragon with the microphone of choice.
3. Launch Dragon with Dragon Dock appearing at the top of the screen (usually large Microphone icon).
4. Connect to your CaseShield Virtual Desktop.
5. Launch Word in CaseShield.
6. Activate Dragon by clicking on the red mic (at the top of the screen).
7. Dictate text – uncheck “use this box for this application” at the bottom left of the Dragon Text box if it appears.
8. Dictate text with Word in the foreground as an active window – Dragon will put text in Word directly.

Security benefits of using the CaseShield email address and virtual desktop

A new Microsoft Office 365 based email – **@caseshield.com** – can be used by the arbitrators as their primary case work email address. It can be accessed through Outlook on the CaseShield virtual desktop, but also outside the virtual desktop, for example personal device, connecting through the web or mobile device – both would require logging in to the Microsoft account with Duo multi-factor authentication (MFA).

The naming convention for the email address is *first initial last name @caseshield.com* (e.g. `ddidia@caseshield.com`; `ddidia` would be the username to log into the virtual desktop and the first part of the email address prior to `@caseshield.com`).

The below info highlights some of the security benefits from using the CaseShield email platform. Using the `caseshield.com` email account on the virtual desktop provides four main protections that an arbitrator likely doesn't have when using a Gmail or other consumer grade email account on a consumer grade laptop.

A. Enterprise grade spam protection. Part of the Office 365 subscription. No spam protection tool will catch all potentially malicious emails but Microsoft's anti-spam protection through O365 will block more malicious emails that may be delivered to free/consumer mailboxes. Some phishing emails that arbitrators receive now may simply not show up in their new mailbox, which would lower the likelihood of clicking on a phishing link and compromising their email account or virtual desktop.

B. Enterprise grade web content filtering / proxy. The CaseShield virtual desktop has web content filtering that by default will block access to potentially malicious sites. If an arbitrator does get a phishing email and clicks on a link that attempts to take them to a potentially malicious website, the web filter, not 100% of the time, but more often than not would block access to the site. Compared to a consumer grade laptop with no web content filtering, this would certainly be a big improvement and reduces the risk of the arbitrators email account or virtual desktop becoming compromised.

C. Enterprise grade anti-virus/anti-malware. Each virtual desktop has Sophos anti-virus/anti-malware software installed that will help prevent the virtual desktop from getting infected with a virus, malware, or ransomware. In the event a phishing link is clicked or attachment opened by an arbitrator and a malicious file is downloaded, Sophos will be able to detect and block its execution more often than not. Certainly more often than on a consumer grade laptop that may not be running any local anti-virus/anti-malware protection, or a consumer grade one.

D. Multi-factor Authentication with Duo. In CaseShield, MFA with Duo is configured to access / log in to the virtual desktop. That same Duo MFA is turned on for the Microsoft O365 CaseShield account. Adding MFA to an email account significantly reduces the risk of an email account being compromised and taken over by a bad actor. MFA can be enabled in Gmail and other consumer email platforms, but in general, most users do not turn it on.

If an arbitrator still uses their existing Gmail or other free/consumer email in the virtual desktop, protections B and C above would still be in place, but not protection A, making it safer than using Gmail on their local laptop. We could also help with protection D by providing instructions to turn on the available MFA for Gmail. Most email platforms have the ability to use MFA but do not have them on by default.

Cybersecurity is about having layers of protection. So having all these protections in place together, or even 2 or 3 of them, significantly reduces the risk of a successful attacks, for example two common ones through email are phishing messages that delivers a ransomware payload or email account compromise which is further propagated by sending phishing emails to all contacts.