



CoECS Horizon Virtual Desktop Guide

This guide will help you connect to the Omnissa Horizon Virtual Desktop for the students in the College of Engineering and Computer Science (CoECS).

Students can securely access a Virtual Windows PC 24/7 from anywhere with an internet connection. These cloud desktops are preloaded with essential software used in your courses, such as MATLAB, SolidWorks, and Ansys, and include access to your shared drives. You'll have reliable access to the tools you need—ready to go, anytime.

You can visit <https://www.fau.edu/engineering/tsg/instructional-resources/omnissa/> and follow the setup instructions, or simply follow the step-by-step guide provided in this document.

What's in This Guide: To make connecting to your Virtual Desktop as easy as possible, we've organized this guide into these sections:

1. **Microsoft Authenticator Mobile Setup** – Secure your account with two-factor authentication
2. **Accessing Virtual Desktops** – Connect using the web browser or desktop client
3. **Maintaining Virtual Desktops** – Sign out properly to avoid access issues
4. **Troubleshooting MFA Access Issues** – Resolve login, MFA, and synchronization problems
5. **Troubleshooting Web Login Service** – Stale Request Error (Horizon Desktop Client)
6. **Troubleshooting MacOS Horizon Client Login Issues** – Auto Login Enabled
7. **Mapping Shared Drives** – Access your network and course-related files
8. **Transferring Images to the Virtual Desktop** (Web Client) – Upload screenshots and photos into your VM

After following the steps below, if you're still having issues accessing your virtual desktop or shared drives, you can reach out to the TSG team:

- Email: help@eng.fau.edu
- Support Form: <https://tsg.eng.fau.edu>



STEP 1: MICROSOFT AUTHENTICATOR MOBILE SETUP

First, Download and install the Microsoft Authenticator Application On your mobile device:

- Open the Apple App Store or Google Play Store
- Search for Microsoft Authenticator
- Install the application
- (Optional) You may scan the QR codes provided on this page:
<https://helpdesk.fau.edu/TDClient/2061/Portal/KB/ArticleDet?ID=158414>

Linking your FAU account to the app will occur during enrollment in the next section.

Second, Enroll in Microsoft Entra MFA

- Open the Microsoft Authenticator app on your phone.
- When prompted “Ready to add an account?”, tap Add account.
- If it asks for the type of account, select ‘Work or School Account’.
- Enter your FAU email in the format:
- Standard accounts: NetID@fau.edu
- Follow the on-screen enrollment steps.
- Approve any sign-in requests on your device to complete the setup.

If you need assistance with installing and configuring Microsoft Authenticator on your phone, please call the FAU helpdesk at 561-297-3999. They will be able to help you to ensure that the application is installed and configured properly.

****** For more information and instructions on how to install and configure Microsoft Authenticator, please visit this FAU pages:

<https://www.fau.edu/oit/services/accounts/accounts-authentication/>

<https://helpdesk.fau.edu/TDClient/2061/Portal/KB/?CategoryID=13459>



STEP 2: ACCESSING VIRTUAL DESKTOPS

Ensure you have completed the MFA setup on the previous page, and you can connect to the MyFAU or Canvas application using your FAU username and password by using the MFA approve sign-in method.

There are two methods to access Virtual Desktops:

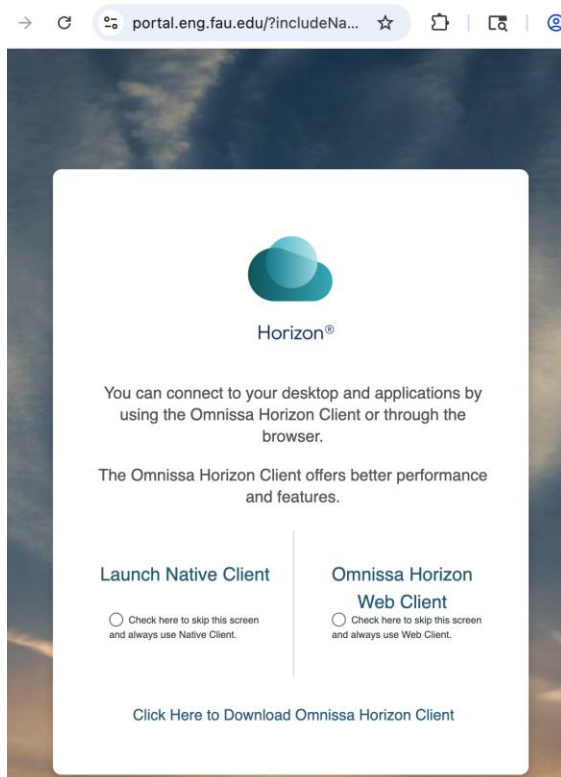
- Using a web browser: **Omnissa Horizon Web Client**
- Download and install a desktop application: **Omnissa Horizon Client**

Method 1: OMNISSA Horizon WEB CLIENT

Using this method, you do not need to install an application. You will use a web browser to connect to virtual desktops.

1. Visit: <https://portal.eng.fau.edu>.

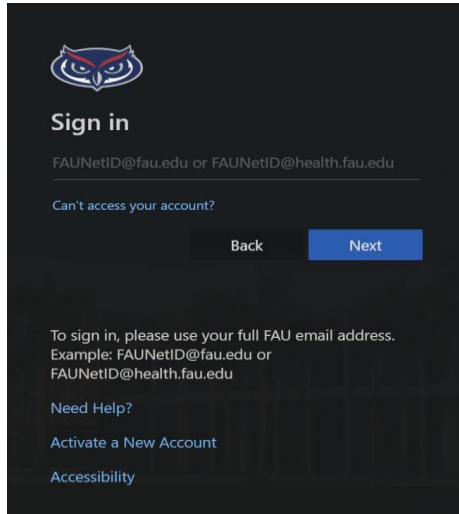
2. Select **Omnissa Horizon Web Client**, and it will redirect to the new screen if the browser doesn't have an authentication cookie and needs to complete a first-time login.





College of Engineering & Computer Science Technical Services Group (TSG)

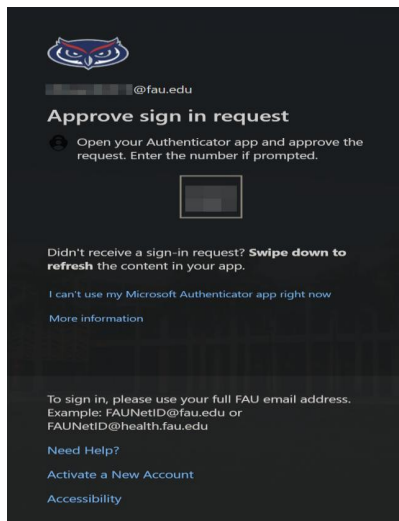
3. When prompted, enter your full **FAU email address**, click Next, enter your **password** on the next screen, and then click **Sign In**.



The image shows a 'Sign in' screen with a dark background. At the top is the FAU owl logo. Below it, the text 'Sign in' is displayed. A text input field contains the placeholder 'FAUNetID@fau.edu or FAUNetID@health.fau.edu'. Below the input field is a link that says 'Can't access your account?'. There are two buttons: 'Back' and 'Next'. Below the buttons, there is instructional text: 'To sign in, please use your full FAU email address. Example: FAUNetID@fau.edu or FAUNetID@health.fau.edu'. At the bottom, there are three links: 'Need Help?', 'Activate a New Account', and 'Accessibility'.

4. You will see a screen asking you to approve the sign-in SSO login request.

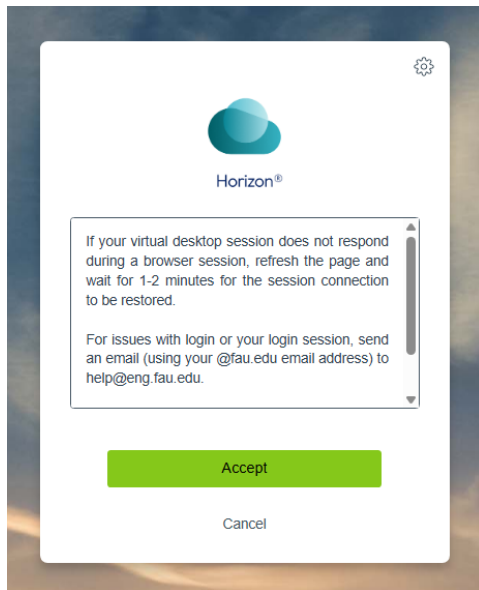
- Open the Microsoft Authenticator app on your mobile device
- Approve the sign-in request
- Enter the number shown on the screen if prompted



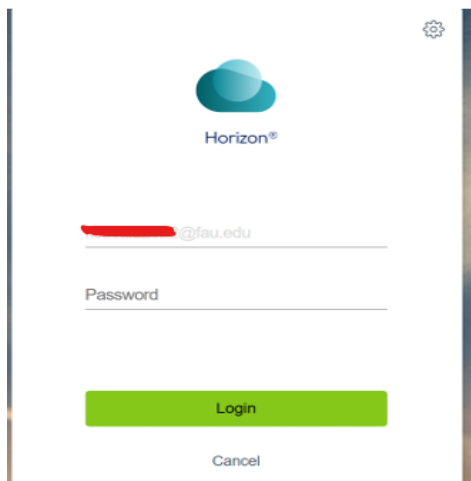
The image shows an 'Approve sign in request' screen with a dark background. At the top is the FAU owl logo. Below it, there is a partially obscured email address ending in '@fau.edu'. The title 'Approve sign in request' is followed by an instruction: 'Open your Authenticator app and approve the request. Enter the number if prompted.' Below this is a small rectangular box representing the authenticator app. Further down, there is text: 'Didn't receive a sign-in request? **Swipe down to refresh** the content in your app.' Below that is a link: 'I can't use my Microsoft Authenticator app right now' and another link: 'More information'. At the bottom, there is instructional text: 'To sign in, please use your full FAU email address. Example: FAUNetID@fau.edu or FAUNetID@health.fau.edu'. At the very bottom, there are three links: 'Need Help?', 'Activate a New Account', and 'Accessibility'.



5. Click or tap the **Accept** button to proceed to the login form.



6. Enter the **FAU Net ID password for the second time** and click on Login.



7. Select **Engineering Desktops**.

8. It will connect to your virtual desktop session. Please wait for the desktop and applications to load completely, then your virtual desktop is ready for use.

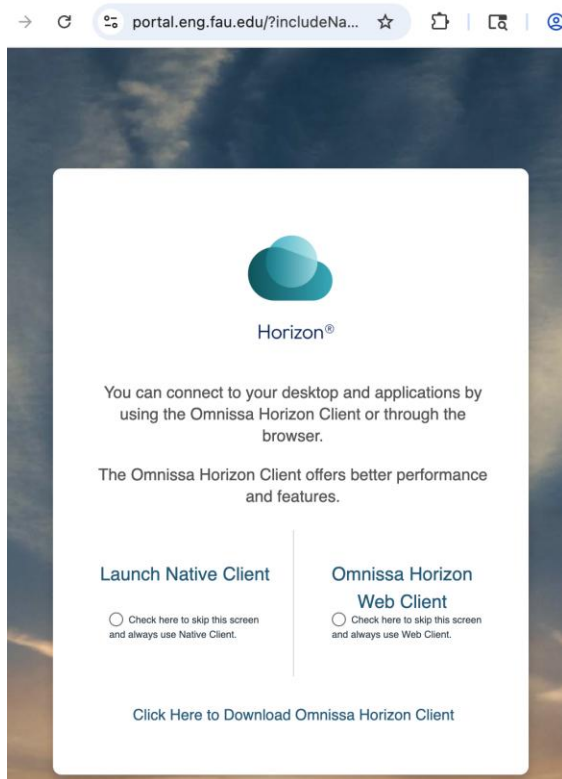
9. While connecting, you may be prompted to choose between full-screen or dual-screen mode. Select the option that best fits your setup and preferences.



Method 2: OMNISSA Horizon Client

Using this method, you will download, install, and set up a desktop application to connect to virtual desktops.

1. Visit: <https://portal.eng.fau.edu>
2. Choose to **click here to download the Omnissa Horizon Client**.



3. If your computer is a **Windows PC**, click **Go to Downloads** under **Omnissa Horizon Client for Windows** and click Download.

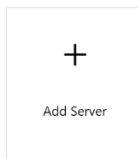
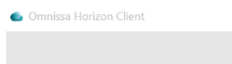
Product Downloads			Drivers & Tools	Open Source	Custom ISOs	OEM Addons
Product	Release Date					
▼ Omnissa Horizon Client for Windows						
Omnissa Horizon Client for Windows	2025-04-15		GO TO DOWNLOADS			
▼ Omnissa Horizon Client for macOS						
Omnissa Horizon Client for macOS	2025-04-15		GO TO DOWNLOADS			



4. If your computer is Apple and has **MacOS**, click **Go to Downloads** under **Omnissa Horizon Client for Mac** and click download.

Product Downloads			Drivers & Tools	Open Source	Custom ISOs	OEM Addons
Product	Release Date					
▼ Omnissa Horizon Client for Windows						
Omnissa Horizon Client for Windows	2025-04-15	GO TO DOWNLOADS				
▼ Omnissa Horizon Client for macOS						
Omnissa Horizon Client for macOS	2025-04-15	GO TO DOWNLOADS				

5. Double-click on the installation file and **install** the application.
6. The installation will put the Omnissa client on the **Desktop** for **Windows** and in **Applications** for **MAC**.
7. Open the **Omnissa Horizon Client**.
8. The first time you run the client, it will ask you to “**Add Server**”.



9. Click **Add Server** and enter the name of our server: **portal.eng.fau.edu**

Name of the Connection Server

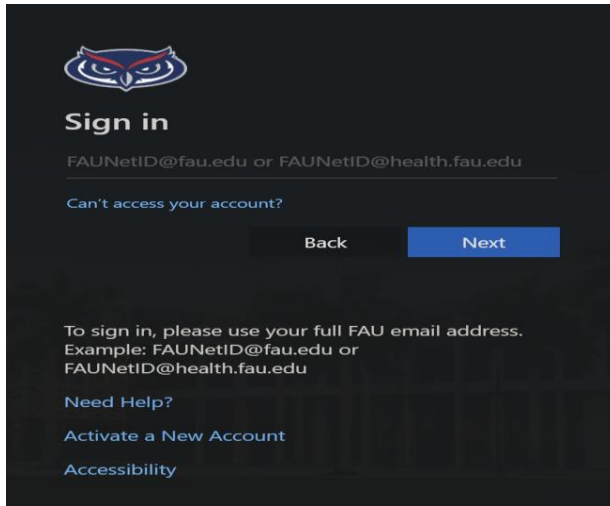
×

CancelConnect



College of Engineering & Computer Science Technical Services Group (TSG)

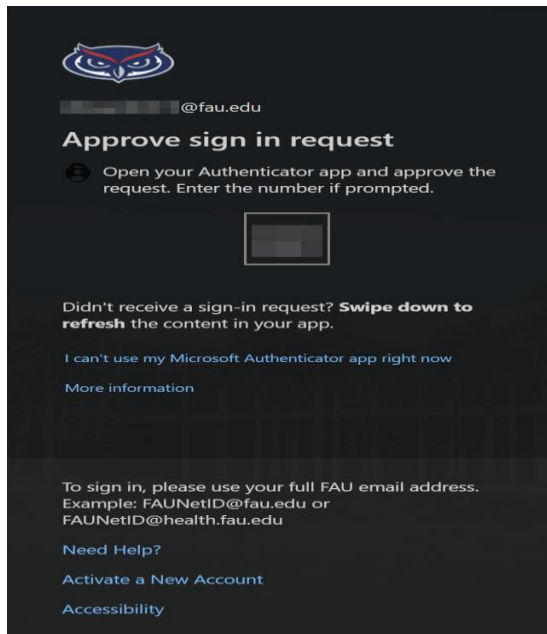
10. After clicking on the **connect**, it will be redirected to the MFA sign-in page, Enter the full FAU email address, click Next, enter your password on the next screen, and then click Sign In.



The image shows the FAU Sign in screen. At the top is the FAU Owl logo. Below it, the text "Sign in" is displayed. Underneath, there is a text input field with the placeholder "FAUNetID@fau.edu or FAUNetID@health.fau.edu". Below the input field is a link that says "Can't access your account?". There are two buttons: "Back" and "Next". Below these buttons, there is a message: "To sign in, please use your full FAU email address. Example: FAUNetID@fau.edu or FAUNetID@health.fau.edu". At the bottom, there are three links: "Need Help?", "Activate a New Account", and "Accessibility".

11. You will see a screen asking you to approve the sign-in SSO login request.

- Open the Microsoft Authenticator app on your mobile device
- Approve the sign-in request
- Enter the number shown on the screen if prompted

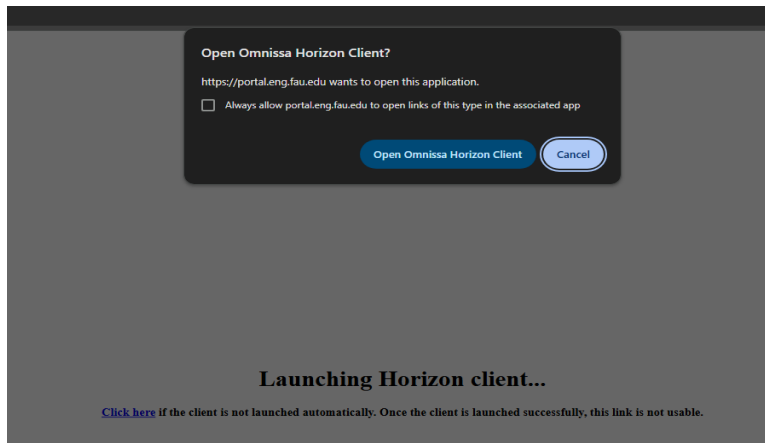


The image shows the FAU Approve sign in request screen. At the top is the FAU Owl logo. Below it, there is a text input field with the placeholder "@fau.edu". Underneath, the text "Approve sign in request" is displayed. Below this, there is a message: "Open your Authenticator app and approve the request. Enter the number if prompted." There is a small image of a smartphone screen showing a sign-in request. Below this, there is a message: "Didn't receive a sign-in request? **Swipe down to refresh** the content in your app." Below this, there is a link that says "I can't use my Microsoft Authenticator app right now". At the bottom, there is a link that says "More information". Below these links, there is a message: "To sign in, please use your full FAU email address. Example: FAUNetID@fau.edu or FAUNetID@health.fau.edu". At the bottom, there are three links: "Need Help?", "Activate a New Account", and "Accessibility".

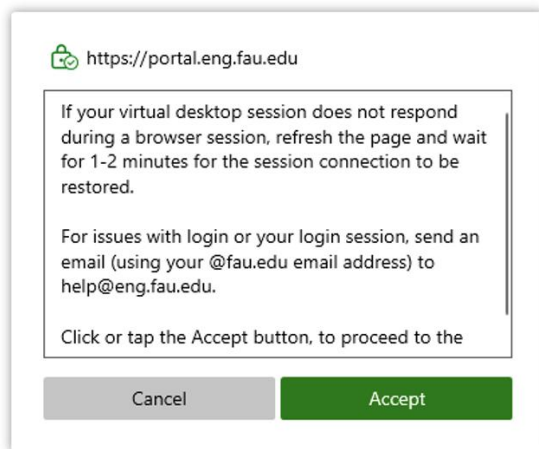


College of Engineering & Computer Science Technical Services Group (TSG)

12. After the MFA sign-in is approved on your phone, on the next screen, it will ask to launch the Horizon client, click Open Omnissa Horizon Client.



13. Click or tap the **Accept** button to proceed to the login form.



13. On the next screen, enter your **FAU password** and click on **login** for the second time.

14. Select **Engineering Desktops**.

15. It will connect to your virtual desktop session. Please wait for the desktop and applications to load completely, then your virtual desktop is ready for use.

16. While connecting, you may be prompted to choose between full-screen or dual-screen mode. Select the option that best fits your setup and preferences.

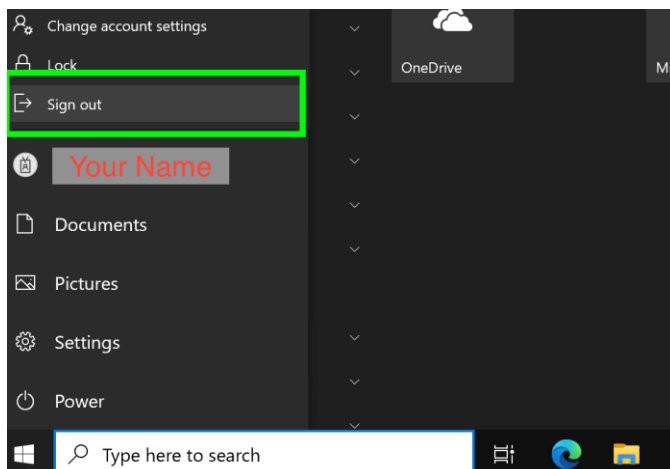
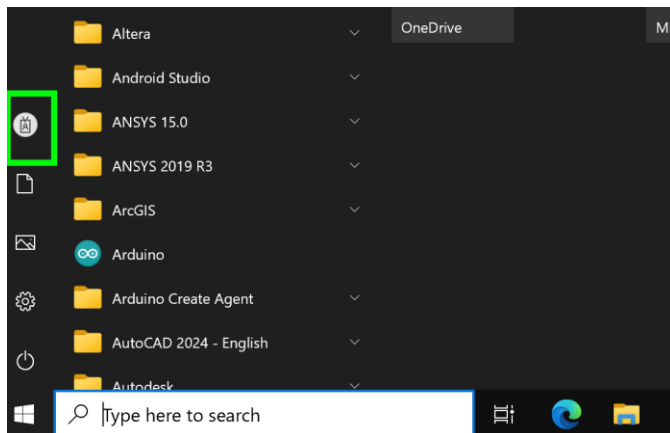


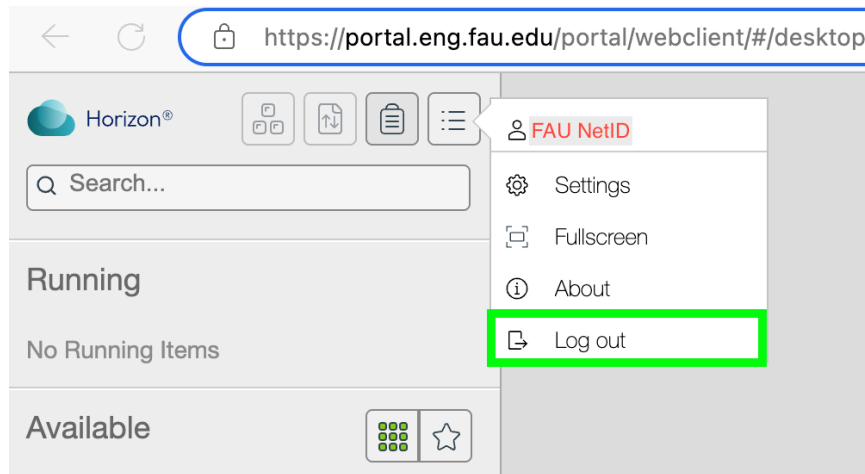
STEP 3: MAINTAINING VIRTUAL DESKTOPS

After completing your work on your Virtual Desktop, it is strongly recommended that you **sign out of your session** properly. This is to **ensure your session closes cleanly**, so you can reconnect **with no issues** later.

✓ How to Sign Out

- Inside the virtual desktop, click the Windows Start menu (bottom-left corner)
- Click your username/profile icon
- Select Sign Out from the menu
- Ensure to also log out from Omnissa Horizon





What Happens If You Don't Sign Out?

- The system will wait 15 minutes, then lock the virtual desktop screen.
- You can still reconnect to the same virtual desktop session during this time.
- If you do not return, the system waits another 20 minutes, then logs you out automatically.
- If you close your web browser or your computer goes to sleep (common on laptops when the lid is closed or on battery), your session will be immediately disconnected.

💡 Many laptops enter sleep mode after just 5–10 minutes of inactivity to save battery. To avoid unexpected disconnections, keep your device active or adjust your power settings.



STEP 4: TROUBLESHOOTING MFA ISSUES

Users may encounter problems during MFA authentication. Please follow the steps below to resolve the issue. Also, here is the link for more information:

<https://helpdesk.fau.edu/TDClient/2061/Portal/KB/ArticleDet?ID=159300>

1. Account Blocked Due to Suspicious Activity

If you attempt to sign in and receive a message stating that your account has been **blocked due to suspicious activity**, this indicates that Microsoft security has temporarily restricted access to protect your account.

How to Resolve the Issue

- Visit <https://accounts.fau.edu/>
- Select "Forgot Your Password"
- Complete the password reset process by following the on-screen steps
- After resetting your password, wait 5–10 minutes to allow full synchronization with Microsoft systems
- Attempt to sign in again — you should now be able to log in normally and receive MFA prompts

2. Not Receiving Microsoft MFA Code Prompts or Push Notifications

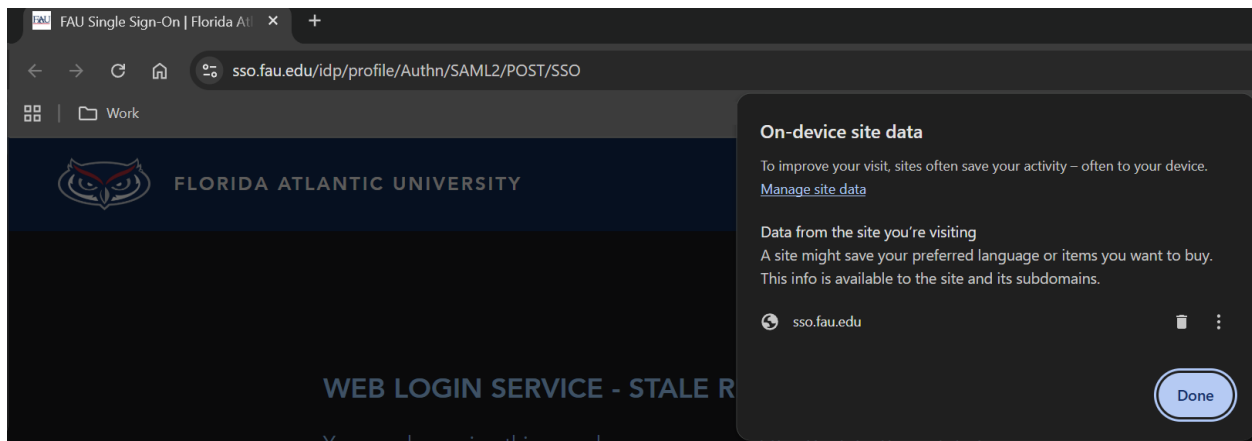
If you are attempting to sign in, but **no MFA push notification or verification code appears**, follow the troubleshooting steps below. Also, here is the link for more information: <https://helpdesk.fau.edu/TDClient/2061/Portal/KB/ArticleDet?ID=158654>

- Open the Microsoft Authenticator app and check if the incorrect FAU entry is present.
- On your phone, open Settings (not Authenticator settings).
- Go to Accounts and Backup > Manage Accounts.
- Find the @fau.edu Work Account and select Remove Account.
- Confirm removal if prompted by tapping OK.
- Reopen the Microsoft Authenticator app to ensure the account is deleted.
- Re-enroll your FAU account following the MFA setup instructions.



STEP 5: TROUBLESHOOTING “WEB LOGIN SERVICE – STALE REQUEST” ERROR (HORIZON DESKTOP CLIENT)

Some users may encounter the following error during login when using the **Omnissa Horizon Desktop Client**: “FAU Single Sign-On – Web Login Service – Stale Request.”



This error typically occurs due to cached browser data or stale authentication of cookies used during the SSO login process. First Attempt: Restart Login Session

1. Close all open web browsers on your computer.
2. Close the Omnissa Horizon Desktop Client completely.
3. Reopen the Omnissa Horizon Desktop Client.
4. Attempt to log in again at: portal.eng.fau.edu

If the error appears again, proceed to the steps below.

1. Clear the browser cache for the website
2. Close the Horizon Desktop Client
3. Re-open the Horizon Desktop Client and attempt to log into portal.eng.fau.edu

Here is the link for more information:

<https://helpdesk.fau.edu/TDClient/2061/Portal/KB/ArticleDet?ID=133474>



STEP 6: TROUBLESHOOTING Apple Mac HORIZON CLIENT LOGIN ISSUES (AUTOLOGIN ENABLED)

Some Apple Mac OS users may be unable to log in to the Omnissa Horizon Desktop Client if **Autologin was previously enabled** for the server (portal.eng.fau.edu). This issue is caused by cached Horizon preference (plist) files.

Follow the steps below to remove cached Horizon preference files and fully reset the Horizon client configuration.

1. Close all applications

- a. Quit the Omnissa Horizon Desktop Client
- b. Close all open web browsers

2. Open a Terminal session

- a. Go to Applications → Utilities → Terminal
- b. Or press Cmd + Space, type Terminal, and press Enter

3. Check for existing Horizon preference files

Run the following command:

```
ls -alh ~/Library/Preferences | grep horizon
```

4. Remove VMware / Omnissa Horizon plist files

Run: `rm ~/Library/Preferences/*horizon*`

5. Verify removal

Re-run the command from Step 3:

```
ls -alh ~/Library/Preferences | grep horizon
```

- No output confirms the files were successfully removed

• Restart the Horizon Client

- Open the **Omnissa Horizon Desktop Client**
- Click **Add Server**
- Enter: portal.eng.fau.edu
- Proceed through MFA and login normally



STEP 7: MAPPING SHARED DRIVES IN OMNISSA

Anytime you are using a Virtual Desktop or a computer connected to the FAU network, you will have access to "Network locations" in file explorer/finder. The drives you will see are:

- **H: J: K:** Drives – These are for homework submissions. DO NOT perform live work on files here. When you are ready to submit work, copy your files to this folder. Your instructor can see your files here.
Access to these drives is **based on registering for certain classes**. After registering for these classes, drives will be created, and you will have access.
- **Z:** Drive – This is your private storage space provided by the College of Engineering and Computer Science. Only you have access to this folder.
- **M:** Drive – Your general-purpose FAU storage with a 500MB limit. Access is private to you only.

If your shared drives are not visible in your virtual desktop, you can follow these steps to map them and restore access to your network files.

✓ Step 1: Restart Your Virtual Desktop

- Sometimes, the shared Drives may not map correctly due to a temporary issue. Restart your virtual desktop session to refresh the connection between your virtual desktop and the network drive.
- Simply sign out of your virtual desktop (see step 3), wait a few minutes, and connect back
- After connecting back to your virtual desktop, check if your Drives are accessible

✓ Step 2: Mapping Shared Drivers Manually

- If the shared drive still doesn't appear after restarting, you can try manually mapping the drive. Please contact help@eng.fau.edu to get the actual network path.

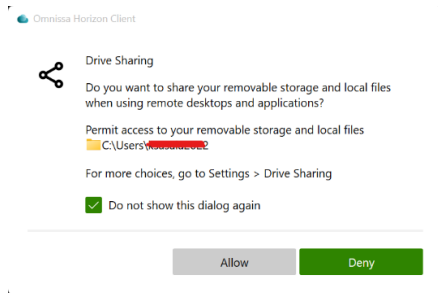
Open **File Explorer**, enter this network path in the address bar, and press Enter. This should allow you to access your network files

✓ Step 3: Check the Drive Sharing Dialog



College of Engineering & Computer Science Technical Services Group (TSG)

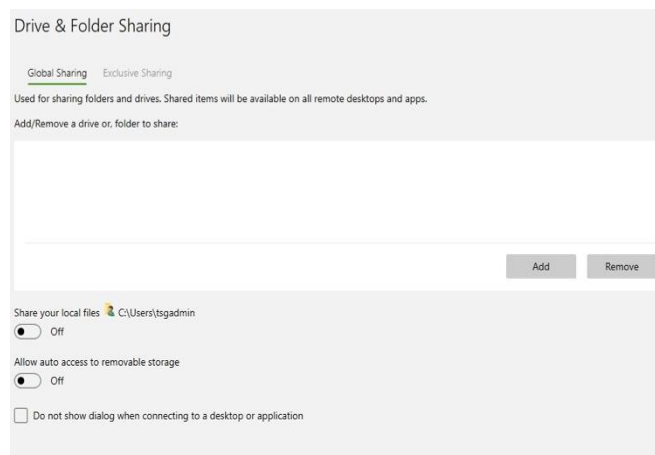
- Upon starting Horizon Omnissa, you may see the following "**Drive Sharing**" dialog (as shown below):



- This dialog asks if you want to share your local removable storage and files with Omnissa Horizon virtual desktop.
- Important:** Click Deny when prompted to share files with the virtual desktop. Allowing local storage sharing may cause conflicts and prevent the shared Drives from mapping correctly to your network files.

✓ Step 4: Check Your Omnissa Horizon Settings

- If the issue persists, ensure that file sharing settings are correctly configured: go to **Settings > Drive & Folder Sharing in Omnissa Horizon Client**.
- Ensure the correct settings are applied to access your network drives and avoid sharing local drives.





STEP 8: TRANSFER IMAGES FROM YOUR COMPUTER TO THE VIRTUAL DESKTOP (WEB CLIENT)

Use this when you're in the **Omnissa Horizon Web Client** and need to move screenshots or photos into the VM.

How to Upload (Web Client):

1. While connected to your virtual desktop in the browser, click the **Transfer Files** icon on the top toolbar



2. In the **Transfer Files** window, make sure the **Upload** tab is selected.
3. **Drag & drop** your image files into the window **or** click **Choose Files** and select them (JPG/PNG/BMP/GIF, etc.).
4. Wait for the upload to finish.
5. Your files will appear inside the VM in **My Documents** (path: C:\Users\<>your-FAU-NetID>\Documents or %USERPROFILE%\Documents).
6. Open the file from there in your app (e.g., insert into Word, SolidWorks, MATLAB, etc.).