

POC Manager Validation Authentication

Starting with the May 2026 version of Epic, which we took when upgrading to August 2026 on 9/16/2026, any Perimeter Authentication URL connection requires 2FA in order to log into the environment. Currently users are getting the message below when trying to log into the URL needed for manager validation.

Two-factor authentication is required to log in from the internet. Contact your system administrator to set up two-factor authentication for your account.

From discussions with Epic, when using the URL for Perimeter Authentication now, Epic will always treat that connection as an External connection over Public Internet.

Resolution:

Internal Users

For users that are on the UAB internal network, they will need to use the URL below in order to access Manager Validation and bypass the Perimeter Authentication URL.

URL: https://hsw-np.et1460.epichosted.com/HSWeb_POC

External Users

For users that are not on the UAB network, they would still have to go through the current Perimeter Authentication URL.

In order to get the URL to work, we would need to update our access settings in POC so allow for Public Access from Unregistered Clients. This was set to Inactive after discussions with UAB Information Security, SAM Team, and Epic on a call.

 **Public Network**

Active Inactive

☒ Allow All Activities 

Legacy:

Exclude Include

Analytics:

Exclude Include

Admin:

Exclude Include

Round Table

Exclude Include

☐ Prefer Hyperspace Desktop Client

☐ Allow downloads on Hyperspace for Windows 

☐ Restrict by user access groups?

 [Go to Category List Maintenance](#)

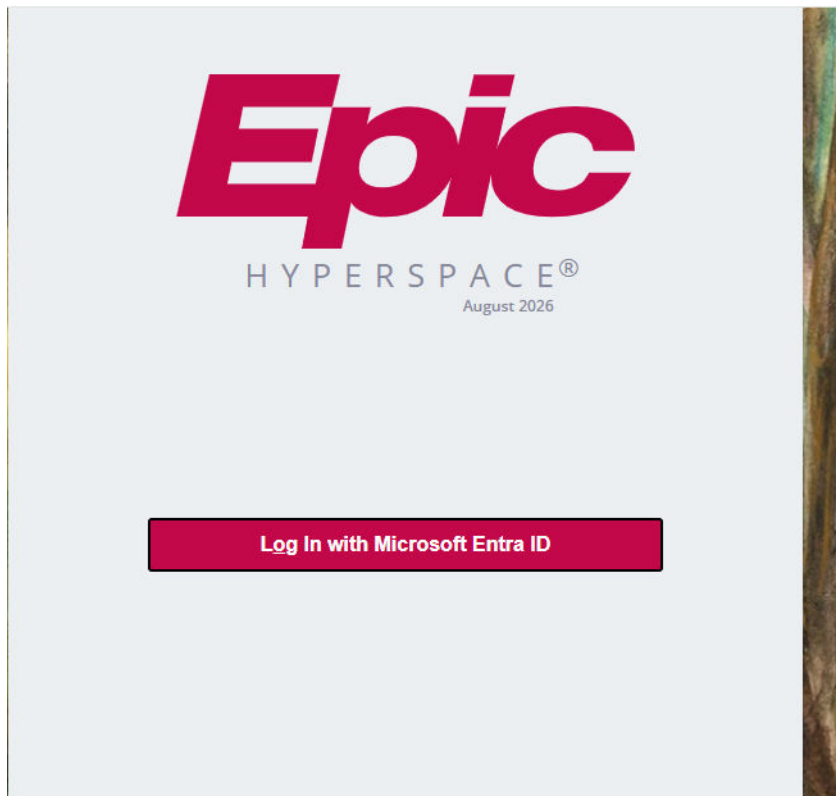
All Public connections to POC require that the user go through UAB MFA in order to authenticate into the environment so if they are not enrolled in UAB MFA they would not be able to get in.

System Changes Needed:

1. Update Public Network for Unrecognized Clients to Active
2. Process all Wave 2 managers through the Epic External User ID Mapping tool to associate an ENTRA MFA Key to their EMP record in Epic so they will be prompted for MFA

User Experience:

When a user goes to the Perimeter Authentication URL after the above system changes are made, they would be prompted to log in using their Entra ID which will launch the UAB MFA sign in.



Sign in to your account - School - Microsoft Edge

https://login.microsoftonline.com/44784e6c-ffc6-4a36-8fd8-b99d8edc...

UAB MEDICINE.

Sign in

someone@uabmc.edu

[Can't access your account?](#)

Next

Please enter your uabmc ID in the form of "email@uabmc.edu".

 Sign-in options

[Terms of use](#) [Privacy & cookies](#) ...

Sign in to your account - School - Microsoft Edge

https://login.microsoftonline.com/44784e6c-ffc6-4a36-8fd8-b99d8edc...

UAB MEDICINE.

← mageorge@uabmc.edu

Enter password

Password

[Forgot my password](#)

[Use a certificate or smart card](#)

Sign in

Please enter your uabmc ID in the form of

Once the user enters their username and password, they should get a code sent to their phone via SMS Text, Duo, or Microsoft Authenticator depending on how they are enrolled.

Multifactor Authentication (MFA) Instructions

- [MFA enrollment instructions](#)

Important: You must be connected to the UAB Health System network to initially enroll in Microsoft MFA. Your best options to do this are to use a computer on the network, remotely via Citrix, or by connecting through our Virtual Private Network.

If using Citrix, look for the "MFA Enrollment" icon.

Please follow these steps to enroll in Microsoft MFA:

1. Using a web browser, go to <https://myprofile.microsoft.com>
2. You will be prompted for a login, enter your userID followed by @uabmc.edu (e.g. userid@uabmc.edu)
(Note: For Cooper Green employees use @cgmhs.org and for Legacy of Hope employees use @legacyofhope.org after your userid)
3. A green screen with "UAB Medicine" will appear prompting you for your password. Use the same password you use for email or Citrix
4. Once authenticated, you will then be presented with a profile management page. Click the "Update Info" located on the "Security Info" tile
5. You will be presented with a new screen titled "Security Info". Using this screen, click the "Add method" plus sign to add a new MFA method
6. You will have the option to choose either "Phone" or "Authenticator App" using a drop down menu

Option 1 - Phone

Using the phone option allows you to authenticate using a code received through either SMS text or a phone call. Follow these steps to complete the phone enrollment option. Go to Option 2 to use the Authenticator app on a smart device.

1. After choosing "phone" from the previous steps, click "Add"
2. A new screen will appear prompting you to enter the telephone number
3. Select the country code for your phone, enter the 10-digit number and choose how you prefer to receive the security code
4. After completing the fields and options, click Next
5. The system will then test your device by using the method you chose in the earlier step.
6. You will be prompted to enter the number you received through either an SMS text or by phone call
7. Enter the code and click Next

8. After entering the correct code, you will be shown a prompt stating the code has been verified. Click Done

Option 2 - Authenticator App

You can also use a mobile app called Microsoft Authenticator to approve sign ins. It's more convenient than texts because you can respond very quickly on your phone.

1. Choose Authenticator app from the dropdown menu and click Add
2. You will be shown a screen prompting you to download the authenticator app. Clicking
3. Download will take you to a website where you can be directed to the iPhone and
4. Android app stores, or you can just go directly to the store on your phone. Install the app on your mobile device, then click Next
5. The next screen notifies you that you will now configure the new app. Follow the instructions on this screen and click Next
6. On the following screen you'll see a QR code displayed on your screen along with some instructions. Leave this screen up and go to your phone and launch the new Authenticator app.
7. On your phone, tap the plus sign in the Authenticator app in the top right
8. After tapping the plus sign tap "Work or School account"
9. Now, using your phone, scan the QR code on your screen from step 4. This will complete the setup for the Authenticator app
10. Lastly, you will be walked through a test scenario to ensure the Authenticator app is working properly.