Multi-factor Authentication FAQs for Users

1 Document Purpose and Use

The purpose of this document is to provide a list of frequently asked questions (FAQs) that HealtheConnections' customers may have regarding Multi-Factor Authentication. This document can be used as a reference for the internal team to communicate with customers.

2 General

General Okta Background FAQs

What is Okta?

Okta is a software company that helps businesses manage digital security.

Managing Passwords/Accounts FAQs

What if I forgot my password or am locked out of my account?

To change your myConnections password, click the "Reset password or unlock account" button on the portal sign in screen, or contact our Support Team by calling **315-671-2241 x5** or email **support@healtheconnections.org**

How do I re-enroll in myConnections?

Contact the HealtheConnections Support Team by calling **315-671-2241 x5** or email **support@healtheconnections.org**

`

3 Multi-Factor Authentication (MFA)

General MFA Background FAQs

What is Multi-Factor Authentication (MFA)?

Multi-factor authentication is an electronic authentication method requiring two sources of verification to gain access to a digital resource. Multi-factor authentication (MFA) is used to protect against hackers by ensuring that digital users are who they say they are.

Why is MFA required?

MFA is an effective way to provide enhanced security. Traditional usernames and passwords can be stolen, and they've become increasingly more vulnerable to malicious activity, and cyber-attacks like phishing or brute force attacks. MFA creates multiple layers of security to help increase the confidence that the user requesting access is who they claim to be.

Why isn't primary authentication enough, what's wrong with passwords?

- Passwords, in addition to being difficult to manage, are vulnerable to a variety of attacks like phishing, social engineering, etc.
- If hackers get a hold of a user's login credentials, they can access all of the user's resources. This is especially a threat if that user has access to privileged information

What are the benefits of MFA?

- Lowers the chances of your identity becoming compromised.
- Peace of mind knowing that sensitive patient data is made safer by an additional security layer.
- MFA also adds a sense of mindfulness to authentication. By taking the time to add their second factor, users are reminded of the importance of identity security.

MFA Factor FAQs

Which MFA factors does HealtheConnections support?

HealtheConnections supports the below MFA options:

- Okta Verify app
- Google Authenticator
- SMS authentication
- Email authentication
- Voice call authentication
- FIDO2 WebAuthn

`

[NOTE: instructions on how to set this up for each verification factor type is a separate document]

Do I need to set up MFA again if I registered previously?

No. Once you have configured MFA on your myConnections account, you do not need to set it again unless you are changing factors or need to reset your factors (i.e., get a new phone number/email address).

Can I turn off MFA?

No, you cannot choose to opt out. However, you can choose the best offered factor as mentioned above in MFA Factors FAQ.

Can I register more than one device for MFA?

No, you cannot register two devices, tokens, phone numbers, or email addresses for a single account. However, selecting two or more methods is acceptable.

MFA How-To/Troubleshooting FAQs

How do I set up and register my MFA?

1. User accesses myConnections
2. User is redirected to set up and register for MFA
3. User selects and submits MFA type/s
4. User is redirected to myConnections
5. User can then login with their myConnections credentials to resume portal use

How do I register a new device for MFA?

If you need to register a new device or change your MFA factor please contact the HealtheConnections Support Team by calling **315-671-2241 x5** or email **support@healtheconnections.org**

INTERNAL NOTE: It is essential that we implement good identification screening measures to ensure we do not allow someone disable MFA and get around simply by calling into to say they are on a new phone. They MUST prove they are who they are or this entire process is defeated if they can just call and ask us to turn it on and off again then bypass MFA

We will be using the Okta Admin functionality to reset MFA status when needed.

What can I do if I am stuck on the “Enrolling Your Device” screen on the phone I want to use for MFA?

If you get stuck in a loop when attempting to register via SMS or email, or you are not getting any code to enter or any push notification, it means your device may not have enrolled correctly. In this case, contact the HealtheConnections Support Team by calling **315-671-2241 x5** or email **support@healtheconnections.org**

Why do I keep seeing MFA prompts after I've selected "Do not challenge me on this device again"?

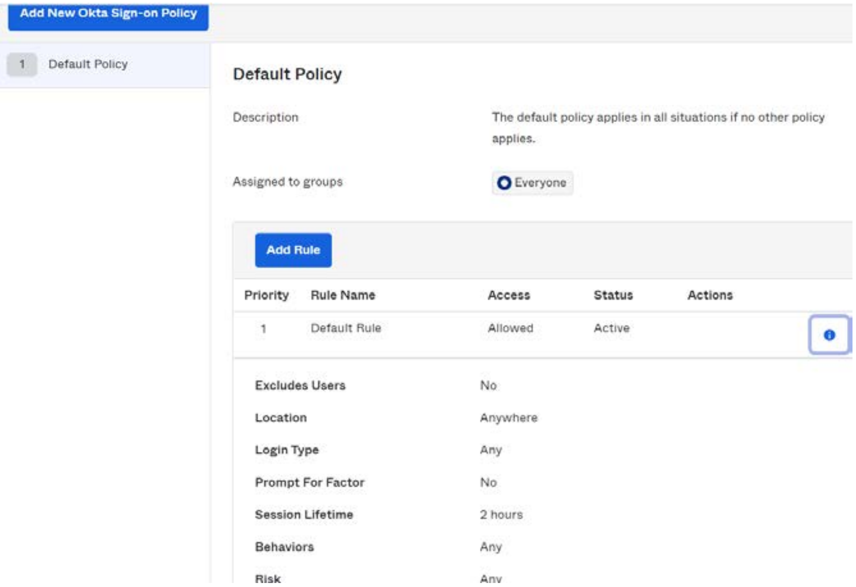
If you continue to see MFA prompts after selecting "Do not challenge me on this device again," it could be for a few different reasons:

1) *Cookie management*: The "Do not challenge me again" choice is captured in a browser cookie. If you've recently cleared your cookies, or are using a new browser (like Chrome, Internet Explorer, Mozilla Firefox), it won't remember the choice.

Additional Questions that still need answers:

Is there a session timeout?

Currently 2 hours per Okta, but myConnections tracks the session as well and I think provides some sort of feedback to Okta that the session is still active. We need to check this with ETG.



Default Policy

Description: The default policy applies in all situations if no other policy applies.

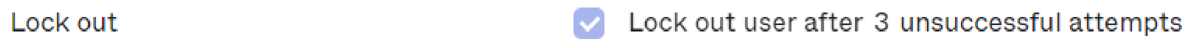
Assigned to groups: Everyone

Priority	Rule Name	Access	Status	Actions
1	Default Rule	Allowed	Active	

Excludes Users	No
Location	Anywhere
Login Type	Any
Prompt For Factor	No
Session Lifetime	2 hours
Behaviors	Any
Risk	Any

After a certain number of tries, can the end user be locked out?

Yes, after 3 tries.



Lock out ☑ Lock out user after 3 unsuccessful attempts

How do I register a new device for MFA?

`

Participants cannot reset their MFA settings. Please contact the support team.