Interior Health
IDENTITY & ACCESS MANAGEMENT

Multi-Factor Authentication (MFA) Project FAQs

What is Multi-Factor Authentication?

- Multi-Factor Authentication (MFA) is an authentication method in which a user is granted access after presenting two pieces of evidence (or factors). The first factor is "what you know" - this is your Interior Health (IH) username and password. The second factor is "what you have" - this is your mobile device with **Microsoft (MS) Authenticator** application installed.

Why should I use MFA?

- Using MFA helps to mitigate many of the cybersecurity threats IH faces every day. MFA also helps to minimize potential damage from phishing emails, credential stealing and malware attempts against IH systems.

Why is Digital Health retiring the existing legacy two-factor authentication (2FA) process?

- Implementing MS Authenticator as the primary MFA technology will ensure compliance with B.C. Ministry of Health security standards, and will align IH with other health authorities that already implemented this technology, which is considered the most secure method by today's standards.

- Enabling MS Authenticator will also increase security for IH by ensuring only registered and authenticated users are accessing IH systems remotely. This project is considered a foundational building block for future initiatives, including Microsoft self-service password reset process.

Multi-Factor Authentication (MFA) Project FAQs

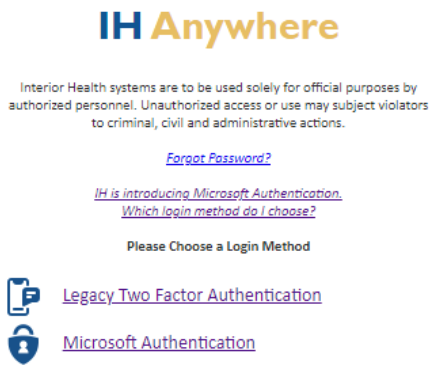
Who will be affected by this change?

- All Interior Health staff and medical staff using IH applications and systems remotely will be impacted by this change. “Remote use” means accessing applications from outside the IH network.
- It’s important to highlight that working from home using IH-provided device (e.g., a laptop) in conjunction with Check Point Mobile VPN solution is considered working within our secured IH network. Therefore, staff using this technology to access IH systems and applications will not be impacted by the MFA process.
- The list of applications protected by MFA when accessed externally continues to grow as Digital Health is migrating more and more applications to use MFA technology. Currently, the list of popular or frequently used IH applications protected by MFA includes:
    - i-Site
    - MS Teams (mobile)
    - Webmail
    - IH Anywhere
    - Infor / WFM
    - ACE hub
    - Covid hub

When will MFA roll out start?

- Effective Nov. 21, 2022 staff accessing applications remotely will be presented with two options for login: **Legacy Two Factor Authentication** and new **Microsoft Authenticator**.

Multi-Factor Authentication (MFA) Project FAQs



- This soft launch approach will ensure that staff have plenty of time to seamlessly transition to the new way of logging in. While the old method will continue to work for sometime in the future, staff are strongly encouraged to register for MS Authenticator as soon as possible, so that Digital Health can discontinue use of 2FA.

What actions should impacted employees take?

- If you are impacted by this change and have not yet registered for the MS Authenticator, please be sure to follow simple registration process.

  NOTE: The initial registration needs to be completed while your IH workstation (e.g., laptop) is connected to IH network. This means using IH-provided workstation at an IH facility while connected to the IH network, or via Check Point Mobile VPN on an IH laptop.

- For IH staff already registered with MS Authenticator, continue to use the new login process without interruption.

Is it acceptable to borrow a smartphone, or install MS Authenticator on mobile device I don't own?

- It is not acceptable to use a mobile device not exclusively owned by you. This is required for compliance with the Interior Health Acceptable Use of Information Systems Policy (AR0100) that applies to accessing information from mobile devices.

I do not have an Interior Health email address but use current 2FA login method. Will this change impact me?

- No, this change does not impact you. Please continue to use the existing 2FA authentication method.

Multi-Factor Authentication (MFA) Project FAQs

I am currently working remotely with limited access to an internal IH facility or ability to connect to IH network to complete the one-time registration process. What are my options?

- The current setup necessitates performing the initial registration while connected to the IH network. We are working towards a solution that will accommodate these unique situations and will have an update on this in the future.

What training and support resources are available to staff?

- We have several training and support resources available to assist with the initial registration and login process:
    - Step by step instructions
    - Instructional video
- For more information please visit InsideNet Projects & Initiatives page Multi-Factor Authentication

Who can I contact for technical issues with the registration or login process?

- For technical issues, please contact the Service Desk at 1-855-242-1300 or ServiceDesk@Interiorhealth.ca

Who can I contact with questions about this project?

- If you have questions about this project or would like additional information please contact the Service Desk at 1-855-242-1300 or ServiceDesk@Interiorhealth.ca. Indicate that your query is related to the **Multi-Factor Authentication (MFA)** project.