Single Sign On (SSO)
End User FAQs
Project: IAM

Document Control

Revision	Date	Changes	Updated By
0.1	28/09/2021	Initial draft	Lou Aloi

Table of Contents

Using this document

The purpose of this document is to provide a list of frequently asked questions (FAQs) related to using Single Sign On (SSO) in Western Health.

This document covers general Okta FAQs as well as information on Single Sign-On and Multi-Factor Authentication FAQs.

1. General Background Information

1.1. Can I authenticate using my mobile device?

Yes. You can use the Okta Verify or Google Authenticator mobile apps. Okta Verifyis recommended. from your app store.

1.2. Who do I contact in case of issues with SSO or MFA?

Contact the Western Health service desk for any issues related to SSO or MFA.

Phone:	03 8345 6777
Email:	servicedesk@wh.org.au
Internet:	https://servicedesk.wh.org.au/

2. Accessing the Okta Dashboard FAQs

2.1. How do I sign into Okta?

The dashboard can be access via **apps.wh.org.au/.**

3. Navigating the Okta Dashboard FAQs

3.1. What is a plugin?

Plugins are browser applications that can be easily installed and are used as a part of a web browser. They're sometimes called Browser Extensions (Chrome) or AddOns (Mozilla Firefox).

3.2. Do I have to use the Okta plugin?

The Okta plugin should already be installed in your web browser. We recommend that you use the Okta plugin because it can help you get to your apps faster than through the web Dashboard, you can add your apps to Okta on the fly, and it also comes with security benefits.

3.3. Why does my session expire when some apps are still open?

When you're logged out of your Okta session, Okta doesn't automatically log you out of your applications. Your apps have their own session lifetime which they determine, or you can manually log out of them when you're finished.

4. Managing Passwords/Accounts FAQs

4.1. How do I unlock my account?

If you're locked out of your account (but still remember your password), click the **Need help signing in?** link at the bottom of the sign-in page. Then click **Unlock account** to unlock it. If that doesn't work, call the Service Desk.

4.2. What do I do if I forgot my password?

If you've forgotten your password, click the **Need help signing in?** link at the bottom of the sign-in page. Then click **Forgot password** to reset it. If that doesn't work, call the Service Desk.

5. What is Single Sign-On (SSO)?

SSO lets you use a single username and password to access all your apps. No more remembering all your different password and username combinations to get to the apps that you need to get your work done.

5.1. How does SSO work?

With SSO, you sign in to Western Health's Okta Dashboard. From there, you can launch any of your web apps without having to enter any other additional credentials. Okta manages all your application credentials and securely logs you into your apps. Sometimes, you might not even know what your username and password are for certain apps because your IT team will manage all of that for you in the background.

5.2. How does Okta keep my username and password secure?

Okta provides rigorous security measures and controls to protect your information. This includes securing and verifying all communications with Okta, encrypting customer data, and ensuring that only the right people in your organization can control the Okta service. These controls are audited regularly.

5.3. What is my username and password for Okta?

Your username and password are a pair of credentials that you use to log in to the Okta dashboard. If you don't know your username, contact the Service Desk. If you've forgotten your password, click the **Need help signing in?** link at the bottom of the sign-in page. Then click **Forgot password** to reset it. If you don't see these options, contact the Service Desk.

6. General MFA Background FAQs

6.1. What is Multi-Factor Authentication (MFA)?

Multi-Factor Authentication is a security practice that requires more than one method of authentication, using independent categories of credentials to verify a user's identity. For example, you may log in to a system using your password ("what you know") and then verifying a separate six-digit number that is sent to your phone ("what you have"). By combining "what you know" and "what you have" verification, the hackers will have harder time breaking into our systems as they may not have both your password and your phone.
When you log in to an account or application, you're asked for a password so you can prove you are who you say you are. You may then be asked for a second factor.

6.2. What is a security "factor"?

The "factor" in MFA refers to a method of verifying your identity. Security factors used in Western Health are The Okta Verify Mobile App, Google Authenticator mobile app or SMS.

6.3. 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 actually who they claim to be.

6.4. What's wrong with just passwords?

● One set of login credentials (such as username and password) is not solving important access challenges.
● Passwords, in addition to being difficult to manage, are vulnerable to a variety of attacks like phishing, social engineering, etc.
● By boiling all applications down to one username and password, security strength is only as strong as that one set of credentials. If it's a bad password, your security situation hasn't improved.
● 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 or mission-critical data.

6.5. What are the benefits of MFA?

● Lower the chances of end-user identities (and, subsequently, their IT resources) becoming compromised.
● Even if hackers have a user's password, we can stop them by adding a personal, time-sensitive factor to the authentication process.
● Peace of mind for enterprise, knowing that users' sensitive 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 tight identity security.

7. Okta-Specific MFA Product FAQs

7.1. How does Okta keep MFA factors secure?

Okta encrypts your user credentials using two different software locks called keys. It stores user data and the keys used to unlock that data in separate databases. For extra security, it then encrypts the keys in three different ways for even stronger protection. No one person at Okta can access the encrypted master key, and Okta maintains an audit trail to show how it manages the keys.

7.2. Which MFA factors are supported in Western Health?

Western Health supports a number of factors: passwords, login codes sent via mobile apps or SMS, push notifications (Okta Verify with Push, Google Authenticator).

7.3. What is Okta Verify?

Okta Verify is a mobile application from Okta that can be used to verify a user for MFA purposes. You receive a push notification on your mobile to confirm the second factor after the factor is set up.

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

No. Once done or configured, you need not set up a factor again.

7.5. Different ways users can access Okta-integrated applications

There are two ways users can log in:

- Users can go to https://apps.wh.org.au/ and log in first, and then they can choose the application they want to access.
- Users can directly go to the application they want to access using application URL, and then the application may or may not redirect the user to Okta login page depending on whether they have a valid session or not.

7.6. Can users register two devices for MFA?

No, with push notification enabled, you cannot register two devices for a single account.

8. Okta-Specific MFA Product How-To/Troubleshooting FAQs

8.1. How do I set up and register my MFA?

Refer to the registration links that can be found at the bottom of the flowing webpage:
https://www.westernhealth.org.au/AboutUs/staff/SSO/Pages/default.aspx

8.2. How do I register a new device for MFA?

To register a new device you need to reset your MFA and then set it up again with the new device.

8.3. How do I reset my MFA?

1. Go to your Okta Dashboard, where you'll be redirected to the Okta login page
2. Submit your username and password
3. If prompted, add your second factor for authentication
4. Once you're logged in, go to the **Settings** page, and click on **Edit Profile**
5. For security, you'll be prompted to provide your password and/or second factor
6. Click **Remove** for factor to reset
7. Click on **Set up** for factor you wish to reset

8.4. What can I do if I am stuck on the "Enrolling Your Device" screen?

If you get stuck in a loop when attempting to register, 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, you need to reset MFA from your account, uninstall Okta Verify on the device, install it again, and then set up the MFA again.

8.5. 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.

2) *Policy configuration*: Your Okta administrator sets how often they want MFA challenge prompts to appear. If they have set that window to every eight hours or 24 hours, you'll see MFA prompts again after that window, even if you've selected the "Do not challenge me on this device again" checkbox.

3) *Exempted action*: Certain actions, like editing your account profile, will always trigger an MFA prompt as an additional layer of security.