CalSAWS |

CalSAWS Apps Teleworking User Guide (AWS AppStream 2.0)

April 6, 2020

CalSAWS APPS (AWS AppStream 2.0)

AppStream 2.0

- AppStream 2.0 is an Amazon Web Services (AWS) cloud product that provides a secure, easy-to-access portal for the applications you need while you support the County's mission as you work from home.

- We chose AWS AppStream because it allows you to be able to easily work from home using almost any type of computer, or even an iPad or Android tablet if necessary.

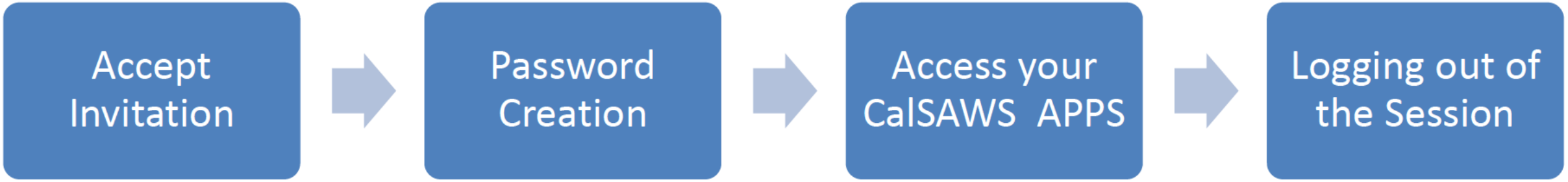
- AppStream is secure because it uses "multi-factor authentication", which means that in addition to a login and password, you also need to provide a secret code that will be emailed to you each time you log in. You can also use a number of apps to make this authentication easier. This security is necessary to protect our clients' data as there is more risk when working remotely.

- In addition, data security is ensured since all data in AppStream is encrypted in transit and at rest, and no data can be saved to your personal computer, iPad or tablet.

CalSAWS APPS (AWS AppStream 2.0)

User Registration

User Registration

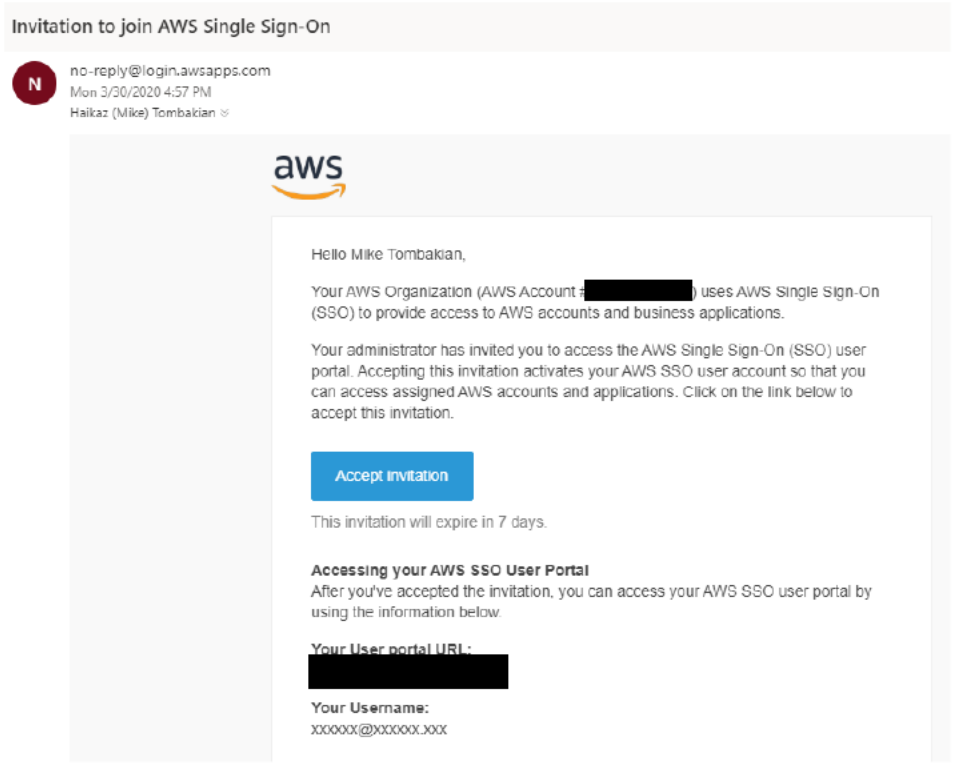


User Registration

Accept Invitation

- When a user is enrolled by their county to AppStream, an AWS (SSO) Single Sign-on invitation email is generated. To register, the user must accept the invitation by clicking on the **Accept invitation** button and create a password. *Note: The invitation will expire in 7 days.*

Invitation email from AWS

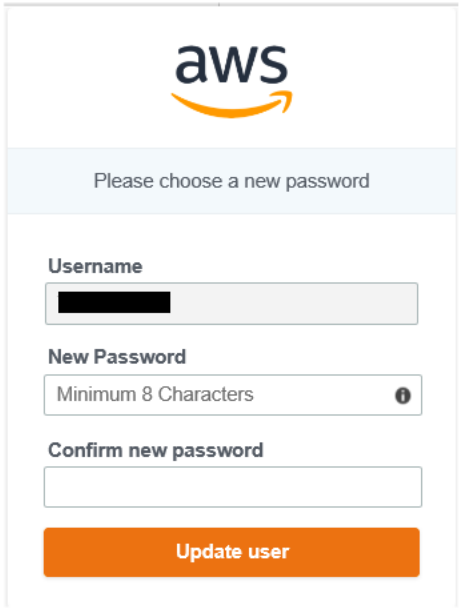


Password Creation

Register Single Sign-on account to access the CalSAWS AppStream 2.0 portal

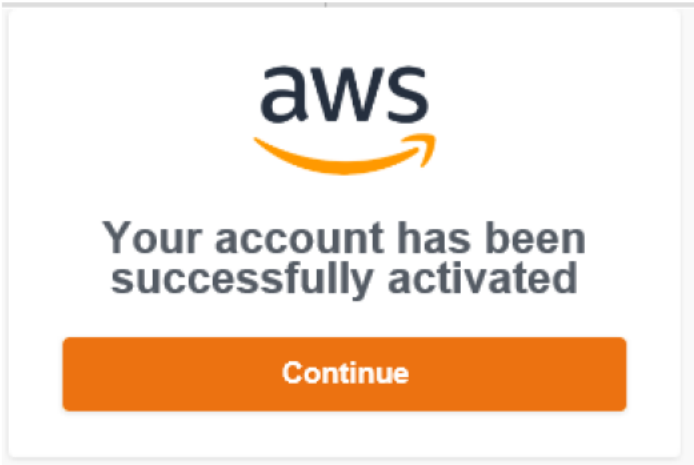
- After accepting the invitation, create a password for the CalSAWS AppStream Portal.

Enter a new password and click **Update user**



Users will see this image when successfully activated.

Click on **Continue** to immediately log into the CalSAWS APPS Portal.



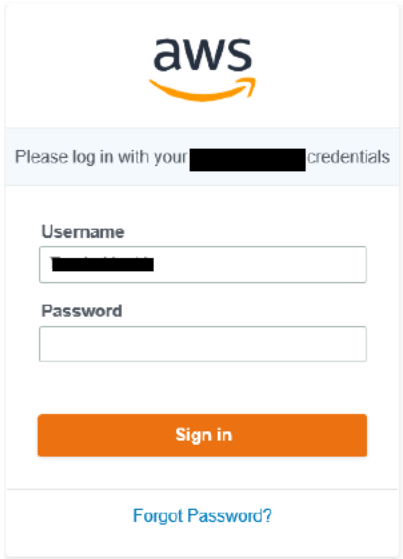
- The password must be 8 Characters and must meet security policy guidelines.

Access your CalSAWS APPS

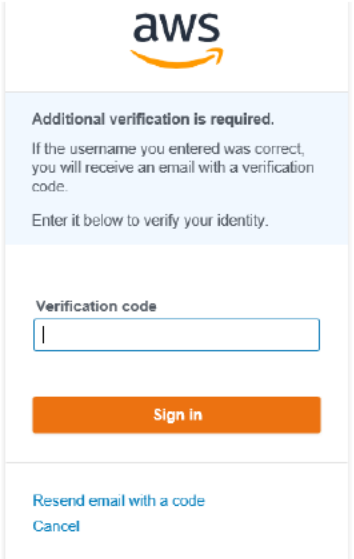
Logging into AppStream and Multi-factor Authentication (MFA)

- To log into AWS AppStream, users will need to enter their username and password. As a security measure, once credentials are entered, users will receive a 6 digit code in their email which must be entered to log into the AppStream. A unique Verification code email will generate each time a user attempts to log into the AppStream portal.

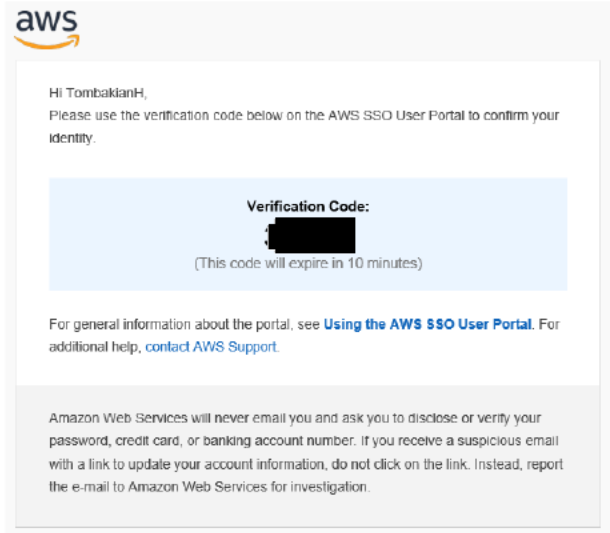
Enter your username and password and click **Sign In**



Immediately an email is generated from AWS and the Verification code is required.



Sample of Verification code sent to email.



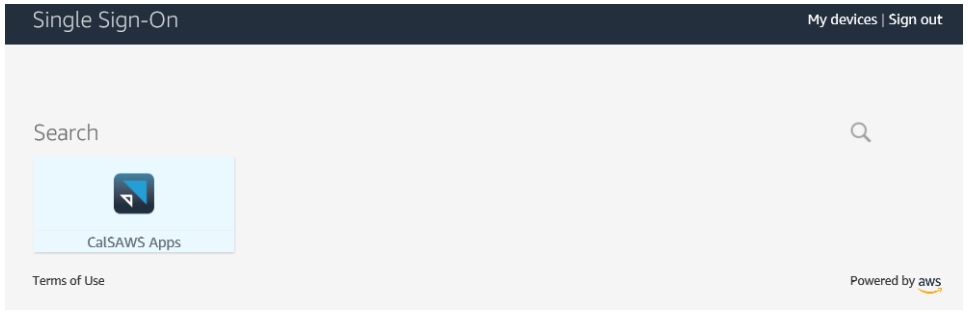
- *Note: Users can setup their own MFA tool, the FAQ section has additional details on available MFA methods.*

Access your CalSAWS APPS

Accessing available applications

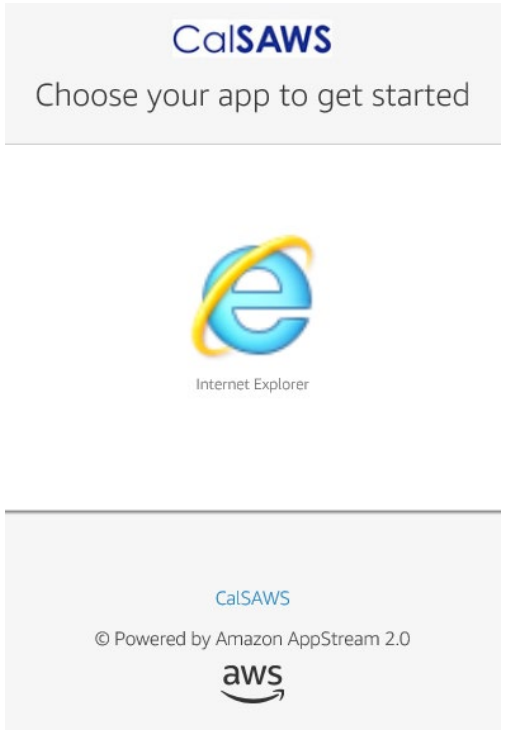
- Logging into the Portal and opening the Internet Explorer App will allow users to access the C-IV and LRS links.

Single Sign-On Portal View



Click on the **CalSAWS Apps** icon to load the available applications.

Available Applications

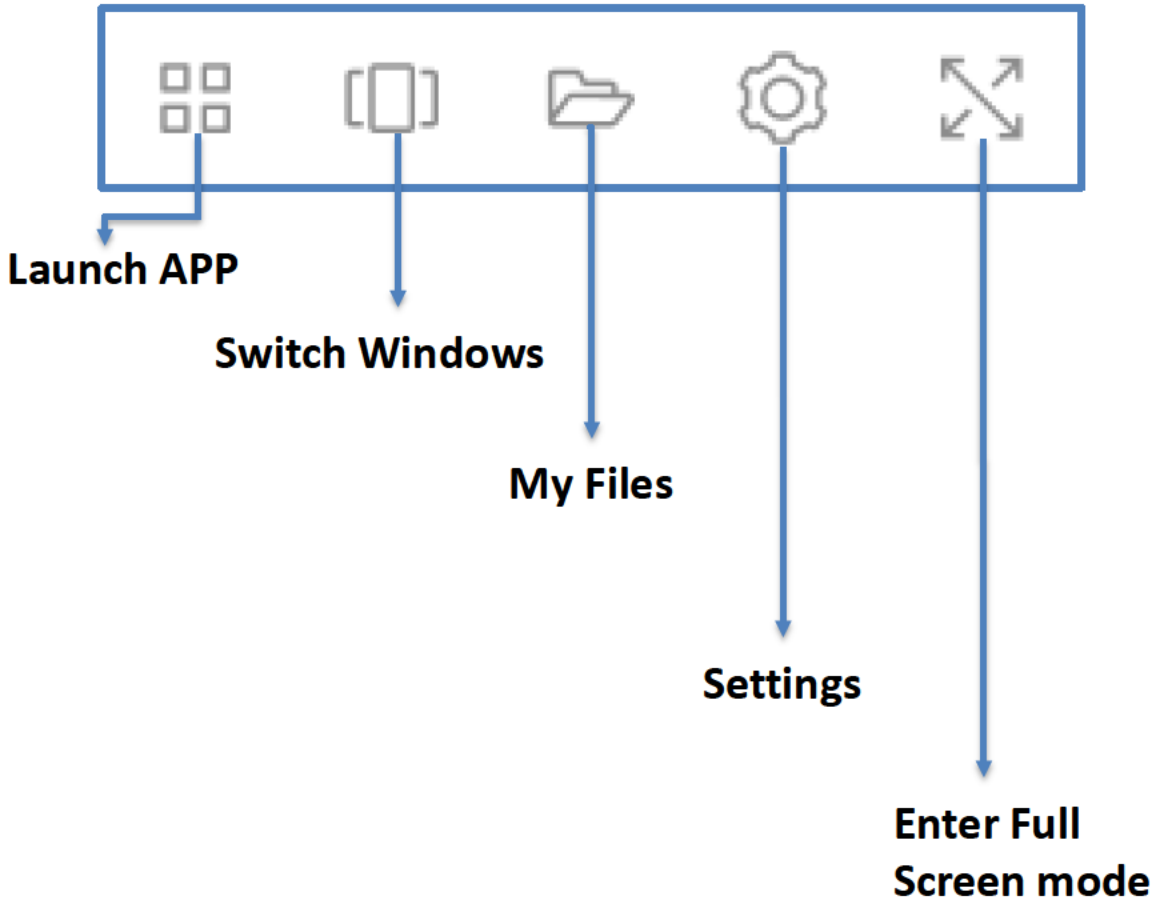


Click on **Internet Explorer** to launch the application and access your County C-IV or LRS link.
Note: Shortcuts to all unique county URLs are bookmarked on the IE home page.

Access your CalSAWS APPS

Toolbars

- **The following tools are available after launching the application:**

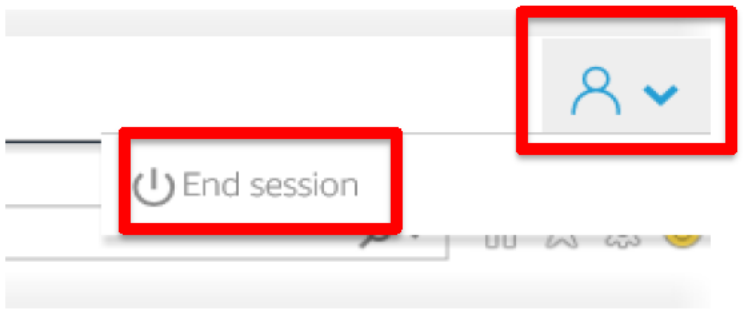


Logging out of the Session

Ending a Session

- End Session (when an application is launched)

In Session View



Click the **User** icon on the right side of the AppStream navigation bar and select **End session**.
Disconnected sessions (closing the web browser) will stay active for 30 minutes and idle sessions (no keyboard / mouse activity) will stay active for 20 minutes and then be automatically logged off. If you fail to reconnect or actively use your session before the 30-minute timeout ends, all your unsaved work will be lost and you will need to start over.
Note: The existing timeout for C-IV and LRS applications remain at 20mins of inactivity.

Support

Support

Support for CalSAWS AppStream 2.0

- **CalSAWS AWS AppStream Access/Environment issues:**
  - Email AppStream.Support@calsaws.org for support on registration or access to the CalSAWS AWS AppStream portal.
- **Password Resets for CalSAWS AWS AppStream portal:**
  - Go to [redacted] type in your User Name and click on **Forgot Password** and follow the steps to reset your password.
- **For C-IV and LRS application support follow your existing County process.**

Frequently Asked Questions (FAQs)

Frequently Asked Questions (FAQs)

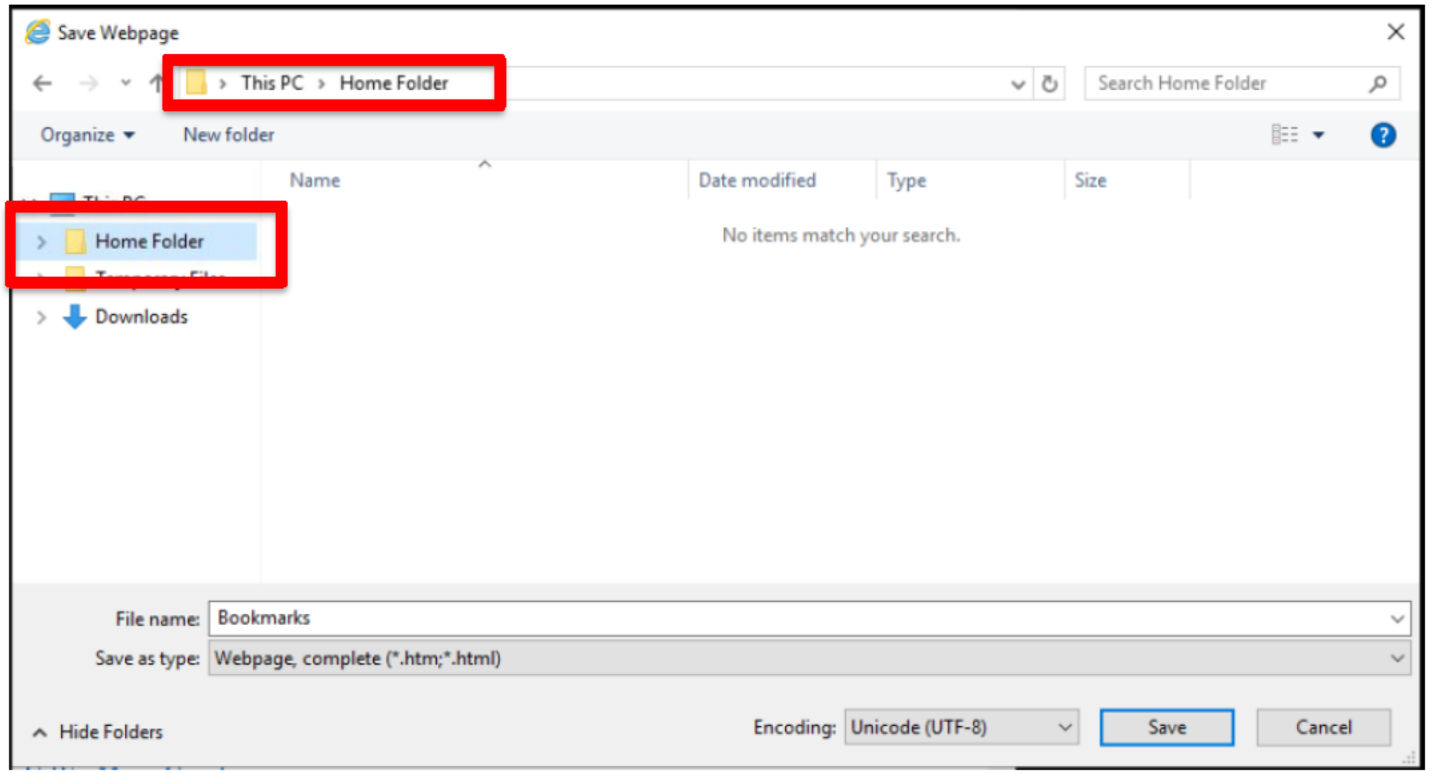
What are the CalSAWS Password complexity requirements?

- Use a password that is easy to remember and complies with the following standards:
- Must not be the same as your last 5 passwords
- Exclude all or part of your Username
- Exclude keyboard patterns, keys listed next to each other vertically or horizontally on a standard keyboard
- Exclude commonly used words, or words written backwards or disguised with special characters
- Contain at least eight characters
- Contain at least four unique characters and each character must not be repeated more than three times
- Contain characters from all of the following four categories:
  - Upper Case characters
  - Lower Case characters
  - Numerals
  - Special Character (except the <,> characters are not accepted)

Frequently Asked Questions (FAQs)

Can I save a file to my AppStream local drive (c:____)?s

- To save a file during your AppStream session, use the HOME folder. It is the only folder that will retain your data.
- **Any files saved outside of the Home Folder will not be saved or be accessible after logging out of your session.**



Frequently Asked Questions (FAQs)

How to do I register my existing Multi-factor Authentication (MFA) application?

- Use the following procedure within the user portal to register your new device for multi-factor authentication (MFA).
- **Note**
- We recommend that you first download the appropriate Authenticator app onto your device before starting the steps in this procedure. For a list of apps that you can use for MFA devices, see Multi-Factor Authentication.
- **To register your device for use with MFA**
- Go to your user portal.
- Near the top-right of the page, choose **My devices**.
- On the **My devices** page, choose **Register MFA device**.
- **Note**
- If the **Register MFA device** option is grayed out, you will need to contact your administrator for assistance with registering your device.
- On the **Device name** page, enter a friendly name for the new MFA device. It is helpful to describe the device to make it easy to identify and remove if your device is lost or stolen. For example, you might enter "My iPhone X." Then choose **Next**. This name will be visible to your administrator.
- The **Device configuration** page displays some information for the new MFA device, including an obscured QR code. Using the physical MFA device, do the following:
- Open a compatible MFA authenticator app. (For a list of apps that you can use for hosting MFA devices, see Multi-Factor Authentication.) If you are not sure which app to download, contact your administrator. If the MFA app supports multiple accounts (multiple MFA devices), choose the option to create a new account (a new MFA device).
- Determine whether the MFA app supports QR codes, and then do one of the following on the **Device configuration** page:
- Wait until no one is looking over your shoulder, choose **Show QR code**, and then use the app to scan the QR code.
- Wait until no one is looking over your shoulder, choose **show secret key**, and then enter that secret key into your MFA app.
- On the "**Device configuration**" page, under "**An MFA code will be displayed on your device. Type that MFA code here.**", enter the one-time password that currently appears in the MFA app.
- **Important**
- Submit your request immediately after generating the code. If you generate the code and then wait too long to submit the request, the MFA device may become out of sync. This happens because time-based one-time passwords (TOTP) expire after a short period of time.
- Choose **Register MFA device**. Your new MFA device can now start generating one-time passwords and is now ready for use with AWS.

AWS Link: https://docs.aws.amazon.com/singlesignon/latest/userguide/user-device-registration.html

FAQs

Important Links/Email:

- AppStream Link: [redacted] or [redacted]
- CalSAWS AppStream Support Email: AppStream.Support@calsaws.org
- MFA setup for AWS AppStream: [redacted]