TrustFLEX AWS demonstration account setup instructions

In order to run the AWS TrustFLEX demo an AWS account is required. This document describes the steps required to obtain and configure an AWS account for the demo.

Amazon Web Services (AWS) provides computing services for a fee. Some are offered for free on a trial or small-scale basis. By signing up for your own AWS account, you are establishing an account to gain access to a wide range of computing services.

Think of your AWS account as your root account to AWS services. It is very powerful and gives you complete access. Be sure to protect your username and password.

You control access to your AWS account by creating individual users and groups using the Identity and Access Management (IAM) Console. From the IAM Console, you also assign policies (permissions) to the group.

Create your own AWS account

1. Create AWS account
   a. Go to https://aws.amazon.com/ and follow instructions to create your own AWS account. Additional details can be found at https://aws.amazon.com/premiumsupport/knowledge-center/create-and-activate-aws-account/

2. Secure root account with MFA (multi-factor authentication)

   This is an important step to better secure your root account against attackers. Anyone logging in not only needs to know the password, but also a constantly changing code generated by an MFA device.

   AWS recommends a number of MFA device options at the following link: https://aws.amazon.com/iam/details/mfa/

   The quickest solution is a virtual MFA device running on a phone. These apps provide the ability to scan the QR code AWS will generate to set up the MFA device.

   a. Return to https://aws.amazon.com/ and click the “Sign In to the Console”

b. If it asks for an IAM user name and password, select the "Sign-in using root account credentials" link.
c. Enter the email and password for your AWS account.
d. Under "**Find Services**" search for **IAM** and select it to bring up the Identity and Access Management options.
e. Click on "**Activate MFA (Multi-factor Authentication) on your root account**"

3. Create an admin IAM user

   AWS best practices recommend **not** using your root account for standard administrative tasks, but to create a special admin user for those tasks. See https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#lock-away-credentials

   a. Follow the instructions at https://docs.aws.amazon.com/IAM/latest/UserGuide/getting-started_create-admin-group.html for creating an admin user.
   b. Enable MFA (multi-factor authentication) for the admin user. See https://docs.aws.amazon.com/IAM/latest/UserGuide/best-practices.html#enable-mfa-for-privileged-users

Configuring the account using CloudFormation Templates

The usage of a custom PKI with TrustFLEX devices uses the Just-In-Time Registration (JITR) feature of AWS IoT Core. This feature requires a number of resources setup with an AWS account to work. The creation of these resources is automated through the AWS CloudFormation service.

1. Sign into the AWS console (https://aws.amazon.com/) using the admin user created in the previous section.
2. Change to region to **US East (Ohio)** (a.k.a. us-east-2). This is done from a dropdown in the top right of the console webpage after logging in.
3. Under "**Find Services**" search for **CloudFormation** and select it to bring up that service.
4. Click "**Create Stack**" button.
5. Select "**Upload a template file**" from the page of the stack creation.
6. Click "**Choose file**" and upload the "**aws-zero-touch-full-setup.yaml**" file. Note, if running from a China region, you'll need to select the "aws-zero-touch-full-setup-cn.yaml" instead.
7. Click "**Next**" to move on to the stack details.
8. Enter "**TrustFLEX**" as the stack name. Actual name isn't important, just has to be unique.
9. Enter a password for the user that will be created to run the demo under "**UserPassword**".
10. Click "**Next**" to move on to the stack options. Nothing needs to be changed here.
11. Click "**Next**" to move on to the stack review.
12. Check the acknowledgement box regarding IAM resources at the bottom of the page.
13. Click "**Create Stack**" to start the resource creation.
14. Wait until the stack creation completes. This can take a few minutes. Once done, the stack your created will show as **CREATE_COMPLETE**.

15. Save demo credentials. Click the "**Outputs**" tab for the stack to see the credentials to be saved.

    Save the credentials to CSV file (docs/AWS_test_account_credentials.csv) in Trust Platform files.