capps

Identity Access Management

IAM/TDIS Frequently Asked Questions

IAM/TDIS Overview

A new identity and access management (IAM) platform for CAPPS will be implemented in conjunction with the Department of Information Resources (DIR). In 2020, DIR implemented a new security solution designed to make access to state of Texas business systems more secure, consistent and easier to manage. The Texas.gov Digital Identity Solution (TDIS) is a hosted identity and access management system that will be offered for various state government systems. IAM is the CAPPS-specific implementation of TDIS for the CAPPS environments.

What are the benefits?

The TDIS/IAM solution delivers a more rigorous authentication while also minimizing logins. It does this by adding multi-factor authentication (MFA) to the authentication process and enabling single sign-on (SSO) for all protected applications. If your agency currently has an MFA option in place, CAPPS IAM will not replace your agency's current MFA but will serve as an additional layer of security. Agencies using MFA will have two logins when logging in to CAPPS: their current MFA login and their CAPPS IAM login.

When is this being implemented?

User acceptance testing (UAT) is scheduled to begin April 12, and the go-live date is June 7, 2021.

How do CAPPS users set up user access?

All current CAPPS users will receive an email to complete their registration in the Texas.gov Employee Portal. Once IAM goes live, a registration email will be generated when new users are added to CAPPS.

Does this mean that everyone using CAPPS will get a new username/password?

Everyone will be required to set up a new password for their TDIS account. The username is no longer required to be the CAPPS ID; an email address is the preferred username. In CAPPS, the user's CAPPS ID is unchanged.

Do users have to set up the security Q&A options during initial enrollment?

No, users have the option to skip that step during the initial setup. Users can go back into their Employee Dashboard and set up their security questions later. The purpose of these security questions is to facilitate the user self-service password reset option for the "Forgot Password" feature. If a user never sets up these questions, their self-service password options will be limited to the other MFA secondary factors that have been set up – either email or mobile phone.

What secondary factors are allowed for MFA functionality?

Options for secondary authentication include SMS (text message) or a one-time passcode sent to the user's email address. Email address is a required attribute while mobile phone is not. If a user chooses to not set up a mobile phone, the email address will be the only option for MFA.

If a user wants to select their phone number for secondary authentication, does it need to be entered into CAPPS first?

No. This is a standalone feature that is offered during MFA. The phone number in CAPPS stays in CAPPS and is used for contact information. The phone number used to log in with MFA is separate.

Will users have a way to update their phone numbers for MFA if the number changes?

Yes. Users will be able to edit (update) their phone number through the TDIS Employee Portal.

Can users opt out of MFA?

No. Use of the TDIS/IAM login will be required to access the system. Once implemented, IAM will be the only option for users to log in to CAPPS.

Will you need to sign in separately to Financials, HR/Payroll and ELM?

No. IAM enables SSO, which provides access across the production environments with a single authentication; this includes Financials, HR/Payroll, ELM, Business Objects, Learn and Recruit. The only separate sign-on will be for the non-production UAT environment, which includes UAT and MNT.

How often will users need to change their password now?

Users must change passwords every 60 days.

What is the turnaround time on password resets with IAM?

Password resets occur in real time.

Will password requirements be different with IAM than they are in CAPPS today?

Yes. The TDIS Employee Portal requires passwords to meet specific criteria. This information is available in the TDIS desk aids.

Will bookmarks and favorites reroute to the TDIS login page?

Yes. Existing bookmarks or favorites will redirect to the login page.

How will the new login impact the use of VPN and whitelisted URLs?

The IAM login for the HR/Payroll (HCM) tower will be accessible without connecting via agency VPNs. However, the Financials tower will still require whitelisted IP addresses and connection via VPN.

Is this mobile friendly?

Yes. The sign-on screen is mobile friendly.

Will CAPPS favorites still be active after TDIS is implemented?

Yes. CAPPS functionality, including user favorites, will not be affected by this implementation. IAM is the new way to sign into CAPPS but does not impact CAPPS itself.

Will non-production environments still have the red banner?

Yes. Once a user is logged into CAPPS, non-production environments will still show the red banner. However, the sign-on screen will not have the red designation.

Will terminated employees still be able to access their accounts?

Yes. They will still have access to their accounts for two years, as it is today. They will need to set up their account in the TDIS Employee Portal using their personal email. Agencies will need to create a plan to communicate the new process to former employees who are still eligible for CAPPS access.

How does this impact HUB agencies?

Hub agencies are out of scope for the IAM project. CAPPS modifications were made to facilitate the TDIS deployment. Some of those are part of a third-party software product and will not be delivered to Hubs. The IAM-related code changes that will be included in Texas Baseline will be categorized as discretionary. Also, some of the changed functionality is governed by a configuration switch that enables/disables the IAM-related logic; the CAPPS support team will provide more information closer to the implementation date. If the baseline has generic data, it will not be covered by the IAM solution.

Will agencies still be responsible for password resets and issues with MFA?

Yes. Agencies will maintain this responsibility. IAM is geared toward employee self-service. CAPPS users can reset their own passwords using the TDIS Employee Portal. If self-service reset is not successful, users will be able to contact their agency's delegated admins for help.

What is the delegated administrator (DA) role?

Delegated admins are the users at each agency who are given the role to reset employee passwords, unlock user accounts and initiate TDIS enrollment emails. The DA role is a new role for CAPPS users and must be requested by an agency's security coordinator through the Security Request System. DAs will use a DA console to complete their tasks.

How will IAM/TDIS impact the current password reset role?

Users who currently have the TX_SC_AGY_RESET_PASSWORD to access the TX_ADHOC_PWD_RESET page in CAPPS will retain their access to that page. However, the role is being updated to view-only access. These users will be able to see the security roles assigned to their agency's users. The password reset function is moving to TDIS and will be available to users who have the new delegated admin role.

Will the Comptroller's office distribute job aids or training materials?

Supporting documentation and tools will be provided to agencies before go-live. This may include materials such as FAQs, job aids, email templates and training documents.

How can I get more information?

CAPPS IAM project updates will be provided during the monthly CAPPS User Group meetings, as well as via the CAPPS page on the Fiscal Management website (FMX) and the News & Articles tile on the CAPPS landing page.