CAPPS Identity Access Management

1. CAPPS Identity Access Management

1.1 CAPPS IAM/TDIS

CAPPS Identity Access Management:

Texas Digital Identity Solution (TDIS)

1.2 Course Objectives

After completing this course, you will be able to:

- Complete the one-time enrollment through the TDIS Employee Portal.

- Log In/Out of CAPPS and the TDIS environments.

- Reset forgotten passwords.

- Understand how to unlock your account.

- Obtain assistance with CAPPS TDIS access.

1.3 Introduction

The Texas.gov Digital Identity Solution (TDIS) is being rolled out to your agency on June 7th.

1.4 Welcome Cont.

The Texas.gov Digital Identity Solution (TDIS) is a hosted Identity and Access Management (IAM) system that is being deployed for CAPPS applications and may be added to various state agency systems.

The IAM platform introduces a more rigorous authentication requirement while minimizing logins. This is accomplished through the use of multi-factor authentication (MFA) and single sign on (SSO) for all protected applications.

MFA (Slide Layer)

Multi Factor Authentication (MFA)

MFA is a way of verifying a user's identity with multiple pieces of evidence. When logging in, MFA requires that users provide a User ID and Password, plus a second method of authentication.

For example, when logging into CAPPS, you will first enter your user ID and password, and then you will be prompted to enter a one-time passcode (OTP) sent via text message, phone call or email.

SSO (Slide Layer)

Single Sign On (SSO)

SSO allows users to transition between different applications without requiring additional authentication.

For example, once logged in to CAPPS Financials, you can access any other application you have authorization to use, such as CAPPS HR/Payroll or CAPPS Business Objects without having to re-enter your user credentials. *

*Must use the same browser window when navigating.

1.5 Welcome Cont.

The TDIS platform will be used by all CAPPS agencies when attempting to log into any of the following production applications:

- CAPPS HR/Payroll, Financials, and Enterprise Learning Management

- Recruit

- Learn

- Business Objects

The TDIS platform is also used to access CAPPS non-production environments. Users who have assigned access to non-production environments must set up separate credentials for those environments (e.g. UAT, MNT, etc).

1.6 TDIS Enrollment

One Time Enrollment

Every CAPPS user must complete the one-time IAM/TDIS enrollment process before being able to access the CAPPS applications. IAM/TDIS is the only way to access these environments once implemented.

The enrollment process includes:

- Establishing your TDIS Password.

- Providing a mobile phone number for text messages and phone calls (optional)*.

- Setting up security questions (optional).

*Only mobile numbers can be used; land lines will not work for OTP.

1.7 Exercise

The following exercise provides step-by-step instructions on how to perform the following tasks :

- Complete initial enrollment process.

- Designate mobile phone to receive one-time passcodes.

- Set up security questions.

Scenario: How to Complete the One-Time TDIS Enrollment Process

When you are ready select this link **TDIS/IAM for CAPPS** and complete the following exercise: How to Complete the One-Time TDIS Enrollment Process

After completing the exercise, close the browser tab and return to the course.

1.8 Enrollment Completed

You have now completed your one-time enrollment and are in your TDIS Employee Dashboard. We will talk more about the dashboard in the next section.

1.9 Logging in to CAPPS

The URL for CAPPS does not change with the implementation of IAM/TDIS. Please continue to use your agency's existing links to access the CAPPS applications.

When logging in, enter your

1. TDIS user credentials, your primary agency email address or CAPPS 11-digit User ID and TDIS password

2. One-time passcode (OTP), i.e. the 6 digit passcode sent to you via

   - email to your agency email address

   - SMS/text to your mobile phone, if provided

   - phone call to your mobile phone, if provided

1.10 One-Time Passcode (OTP)

With MFA enabled, you must complete a second form of authentication when logging in.

The second form involves entering a one-time passcode (OTP), that is sent to you via email, text, or phone call.

This passcode is **valid for five minutes**. After five minutes, the passcode expires, and you will need to request a new one.

1.11 Exercise

The following exercise provides step-by-step instructions on how to perform the following tasks :

   - Log in through the CAPPS System.

   - Navigate to the TDIS Employee Dashboard using a CAPPS tile.

Scenario: How to Log In from the CAPPS System

When you are ready select this link **TDIS/IAM for CAPPS** and complete the following exercise: How to Log In from the CAPPS System

After completing the exercise, close the browser tab and return to the course.

1.12 Session Time Out

Both, TDIS and CAPPS will time out after a period of inactivity.

- CAPPS environments time out after 30 minutes of inactivity.

- TDIS Employee portal times out after 4 hours of inactivity.

CAPPS is not aware of activity in TDIS and TDIS is not aware of activity in CAPPS.

- Timing out in CAPPS does not impact an active TDIS authentication.

- Timing out in TDIS does not impact an existing CAPPS session.

1.13 Session Timeout

Once timeout occurs you may be prompted to enter your primary agency email address, TDIS password and the OTP the next time you attempt to log into CAPPS.

Note: In addition to inactivity, closing your web browser ends the active session.

TDIS Single Sign On (SSO) feature

- If CAPPS times out, but TDIS Employee Portal is still active, then you can log back into CAPPS without entering your user credentials.

- If CAPPS times out and your TDIS Employee Portal times out, you must re-enter your user credentials and complete MFA.

Let's take a look at a few scenarios…

1.14 Question 1

Marie arrives at work at 8:00 am and logs into CAPPS using her TDIS credentials.

Once logged in, Marie has both an active CAPPS session and an active TDIS session running concurrently.

Marie continues to actively work in CAPPS Financials until 10:00 am when she stops for a break.

When Marie returns from her break at 10:15, assuming she did not close her browser, she

will need to enter her TDIS credentials to re-login before continuing to work in CAPPS.

will not need to enter her TDIS credentials and can proceed with working in CAPPS.

Feedback when correct:

That's right! Since CAPPS has only been inactive for less than 30 minutes (last used at 10:00) and TDIS has only been inactive for less than 4 hours (last used at 8:00) and the web browser used to initially log in at 8:00 is still active, then Marie WILL NOT need to enter her credentials.

Feedback when incorrect:

You did not select the correct response. Since CAPPS has been inactive for less than 30 minutes (last used at 10:00) and TDIS has been inactive for less than 4 hours (last used at 8:00) and the web browser used to initially log in at 8:00 is still active, then Marie will not need to enter her credentials.

1.15 Question 2

Marie continued to actively work in CAPPS Financials the remainder of the morning. At noon Marie decides to take lunch.

Once again, Marie, locks her computer and heads out for lunch.

Marie promptly returns from lunch at 1:00 and resumes working in CAPPS.

When Marie returns from her lunch at 1:00, assuming she did not close her browser, she

will need to enter her TDIS credentials to re-login before continuing to work in CAPPS.

will not need to enter her TDIS credentials and can proceed with working in CAPPS.

Feedback when correct:

That's right! Marie needs to enter her TDIS credentials to re-login before continuing to work in CAPPS. Since CAPPS has been inactive for more than 30 minutes (last used at noon) and TDIS has been inactive for more than 4 hours (last used at 8:00) then Marie will not need to re-enter her credentials.

Feedback when incorrect:

You did not select the correct response. Marie does need to enter her TDIS credentials and log back in before being able to work in CAPPS. Both her CAPPS (last used at noon) and TDIS session (last used at 8:00 when signing in) have been inactive for more than their allotted times.

1.16 Question 3

After Marie returns from lunch, she actively works in CAPPS until her team meeting at 3:00. The meeting is scheduled to last an hour.

Once again, Marie, locks her computer and heads out.

Marie returns from her meeting at 4:00 and plans on resuming her work in CAPPS.

When Marie returns from her meeting at 4:00, assuming she did not close her browser, she

will need to enter her TDIS credentials to re-login before continuing to work in CAPPS.

will not need to enter her TDIS credentials and can proceed with working in CAPPS.

Feedback when correct:

That's right! Marie will not need to enter her TDIS credentials to re-login before continuing to work in CAPPS. Even though Marie was logged out of CAPPS due to inactivity (i.e. she was inactive more than 30 minutes), her TDIS session which was last active when she logged in after lunch at 1:00 has not been inactive for more than 4 hours.

Feedback when incorrect:

You did not select the correct response. Marie will not need to enter her TDIS credentials to re-login before continuing to work in CAPPS. Even though Marie was logged out of CAPPS due to inactivity (i.e. she was inactive more than 30 minutes), her TDIS session which was last active when she logged in after lunch at 1:00 has not been inactive for more than 4 hours.

1.17 Untitled Slide

So far you have learned how to:

- set up your new TDIS user credentials,

- access CAPPS using your new credentials, and

- recognize when CAPPS and TDIS become inactive and require you to log back in.

There are a few more topics to review before wrapping up the course.

1.18 Untitled Slide

During the final section, you will learn about:

- Forgot Passwords

- Application Lockout

- Expired Passwords

- Managing TDIS Credentials

1.19 Forgot Password

You can use the **Forgot Password** link to reset your password, if you forget it.

1.20 Account Lockout

Account lockout occurs after:

- 5 consecutive invalid password attempts.

    o Hint: Use Forgot Password to reset your password before exceeding the 5 attempts

- 3 consecutive invalid OTP entries.

- 3 consecutive security question failures.

Once locked out, you can

- attempt to log in again (or use forgot password) after 4 hours, or you can

- contact your Delegated Admin to request access sooner.

1.21 Expired Password

Passwords expire after 60 days and must be reset.

An email notification will be sent as an alert that your password needs reset.

1.22 Maintain TDIS User Credentials

TDIS User Credentials

At any time, you can edit your TDIS credentials through the TDIS Employee Portal.

This includes adding/modifying your:

- Password

- Mobile Phone

- Security Question

- Can be added if not provided during enrollment.

1.23 Exercise

The following exercise provides step-by-step instructions on how to perform the following tasks:

- Reset Password

Scenario: How to Reset Password Using Forgot Password Link

When you are ready select this link **TDIS/IAM for CAPPS** and complete the following exercise: How to Reset Password Using Forgot Password Link

After completing the exercise, close the browser tab and return to the course.

1.24 TDIS Helpful Hints

TDIS is designed to allow users to address many of their own needs, reducing their dependency on support staff (i.e. Delegated Admins)

Tip 1: Be sure to set up your security questions.

Security questions can be set up during the one-time enrollment process, or after using the TDIS Employee Portal - Account Settings page.

Tip 2: Check your Spam folder if emails are not showing up in your Inbox.

Emails will come from: no-reply@myaccess.dir.texas.gov

Tip 3: Use the Password Reset link before getting locked out if you have trouble remembering your password.

Once locked out, you will either need to wait 4 hours for the lock to expire or contact your Delegated Admin for assistance.

Tip 4: If locked out, wait for the 4-hour lock out period to expire and then reset your password using the Password Reset link.

If you need immediate access then contact your Delegated Admin for assistance.

Tip 5: Complete your one-time enrollment within 72 hours of receiving your email notification.

Contact your Delegated Admin if you did not receive or cannot find the initial enrollment email.

1.25 Additional Help

TDIS Delegated Admin

- Have access to a Delegated Admin Console where they can manage users and perform certain administrative support tasks.

- Can help with the following:

    - Resend one-time enrollment emails for those who did not complete the process within 72 hours of the initial notification.

    - Initiate Password Reset emails.

    - Unlock user accounts.

    - Escalate access/account issues to the HR/Payroll CAPPS Help Desk.

1.26 Summary

Summary

Congratulations, you have completed this course. Today you learned the following IAM/TDIS features:

How to set up and maintain your CAPPS IAM/TDIS User Credentials.

How to recognize if sessions have timed out.

How to reset a forgotten password.

How to navigate to TDIS Employee Dashboard.

1.27 Conclusion

Congratulations, you have finished the CAPPS IAM/TDIS course!