CMS Identity Management (IDM) System UI

Tier I Help Desk Training & User Interface Overview for Non-Portal Applications

Presenter: Sarah Hangsleben, IDM Trainer

CMS IDM UI Training for Non-Portal Applications

INTRODUCTION

Presentation Roadmap

- URL and Help Desk Information
- UAT Testing
- Migration Information
- New User Registration
- Role Requests
- Self Service Functions
- Accessing the Help Desk UI
- User Search
- View User Details
- Account Unlock
- Password Reset
- View MFA Devices
- Updating a User's Email Address
- Updating a User's LOA
- Suspending/ Unsuspending Accounts
- Remove Roles and Attributes
- Cancel Pending Role Requests
- Approve Role Requests

CMS IDM UI Training for Non-Portal Applications

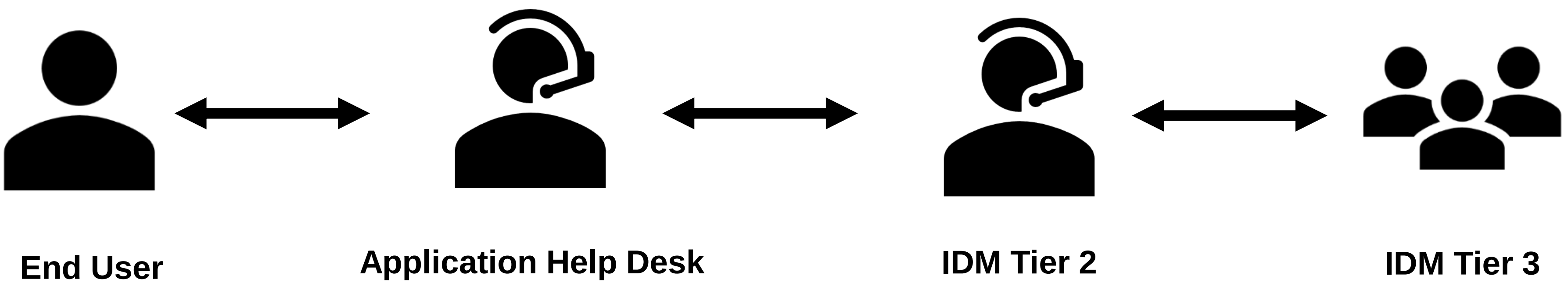
URL AND HELP DESK INFORMATION

URLs for Non-Portal Apps

Name	URL
TEST Environment	
Registration URL	https://test.reg.idm.cms.gov/registration.html?appid=cmsidm
Self Service URL	https://test.home.idm.cms.gov/selfservice/
IMPL/Val Environment	
Registration URL	https://impl.reg.idm.cms.gov/registration.html?appid=cmsidm
Self Service and Help Desk URL	https://impl.home.idm.cms.gov/selfservice/
PROD Environment	https://home.idm.cms.gov/signin/login.html

Contacting IDM Tier 2

- After Go-Live, issues that you cannot resolve will go to IDM Tier 2
- IDM Tier 2 does not work directly with end users
- End user must contact their application help desk for support and if the application help desk is not able to resolve the issue it will be escalated to IDM Tier 2
- Issues for advanced teams will still need to go through IDM Tier 2 first



Contacting IDM Tier 2 HD

IDM Tier 2 contact information is NOT to be shared with end users or outside of the Application Help Desks

By Phone

By Email

By Direct Assignment
Incident assigned via Service Now (SNOW)
Assignment Group: IDM Tier 2 Support

IDM Tier 2 is open 8:00 a.m. – 7:30 p.m. ET, Monday-Friday excluding Federal Holidays

Incidents and Service Requests

- If your application help desk uses Enterprise Service Now (SNOW), Incidents can be assigned directly to IDM Tier 2 Support
- The IDM Help Desk only works in Incident and Service Request modules within SNOW
  - ***Incidents/Problems*** – User or application receiving errors during standard processes, or the system not behaving as expected based on requirements. Other items that fall into this category include:
    - Requesting role approval for roles under IDM approval authority
    - Individual account inquiries such as account creation, auditing, or associated attributes
    - Role removal requests (when applicable)
    - User data modification requests (when applicable)
    - Account re-enable requests
  - ***Service Request*** – Requests for existing functionality within the system that is unrelated to an error. Examples include:
    - Creation of test accounts in the DEV or IMPL environments;
      - Individual testing accounts can be registered by the requester following the same process used in the PROD environment
    - Changes to application functionality, configuration, and role functionality
    - Changes to firewall rules and configurations
    - Generation of unique reports that are not included in the report UI
    - Add users to LDAP groups, such as Micro Strategy (MSTR) groups

Information for IDM Tier 2

- Before contacting IDM Tier 2, application help desks should have the following information ready:
  - URL the user is trying to access
  - Description of the issue
  - IDM environment incident occurred in
  - User ID
  - First & Last Name
  - E-mail address associated with the user's account
  - Steps taken by the user to receive the error
  - Screenshot of the error (whenever possible) including the URL
  - Approximate date and time when the error/issue occurred
  - Whether the error/issue occurs consistently or intermittently
  - Whether the issue is impacting a single user or group of users
  - Troubleshooting steps taken by the Application's Tier 1 Help Desk
  - Browser version/type that the user has attempted to use

User Guides

- User Guides for the IDM UI for non-portal applications can be found CMS.gov

- The title of the user guide is IDM User Guide

- This user guide goes into greater detail for end users, how to manage your own account, and includes help desk actions

First Login for Non-Portal Users

- Users logging into the IDM UI for the first time, will use their existing user ID and password

- If their account requires an MFA code, it will be defaulted to the email on their profile

- After successfully logging in, users can navigate to their profile and add additional MFA devices or change their security question and answer

New MFA options

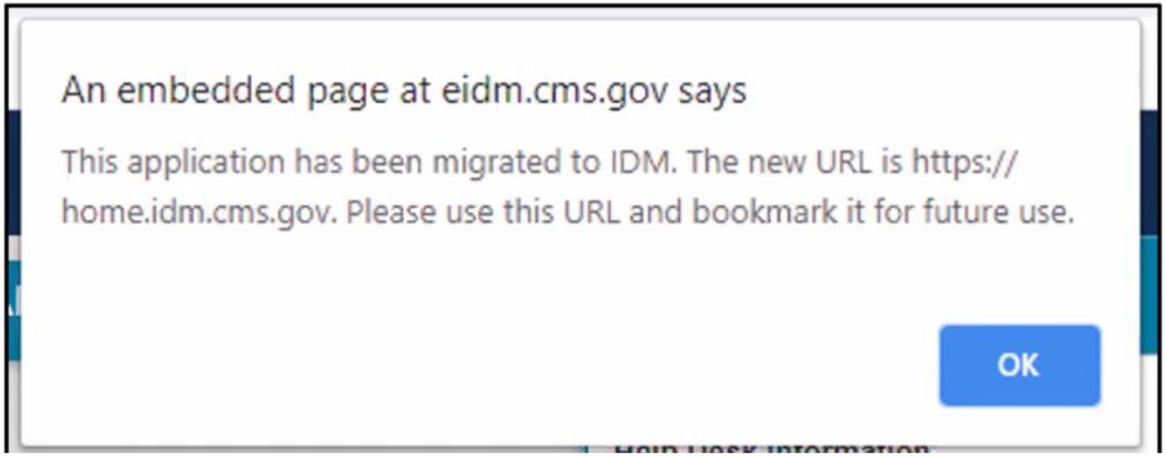
- With the new UI, MFA devices (other than the default email) will not migrate over

- New MFA options include:
  - Interactive Voice Response (IVR)
  - Google Authenticator
  - Okta Verify
  - Short Message Service (SMS) Text Message
  - YubiKey

Notifications for Migrated Applications

- If a user signs into EIDM and attempts to access an application that has been migrated to the non-portal they will get a notification informing them the application has moved and provide the link

- If a user signs into the IDM UI and attempts to access a Portal application, they will also receive an error stating to sign into EIDM (or IDM Portal post 2/2021)



Syncing between EIDM and IDM UI

- The EIDM and IDM UI for non-portal applications will have some syncing during the phased migration

- This only matters for users who need to access applications within both systems

Password resets and account unlocks

IDM UI ⟷ EIDM

Profile Changes like updating email

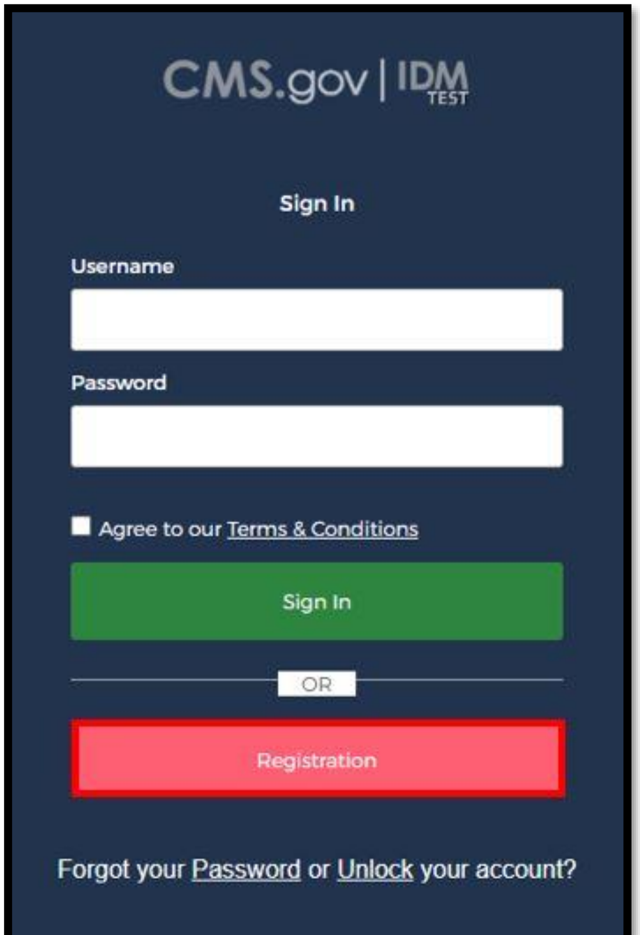
IDM UI ⟵ EIDM

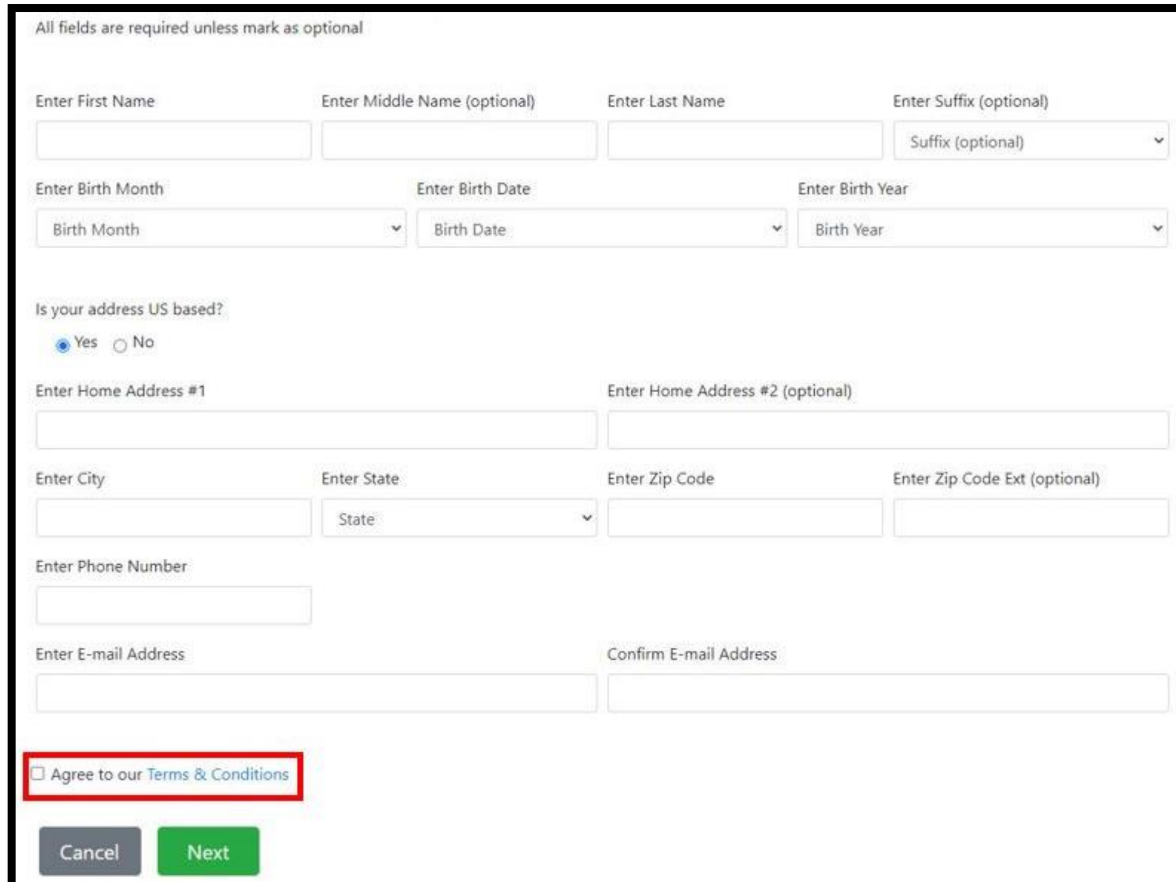
IDM UI ~~⟶~~ EIDM

CMS IDM UI Training for Non-Portal Applications

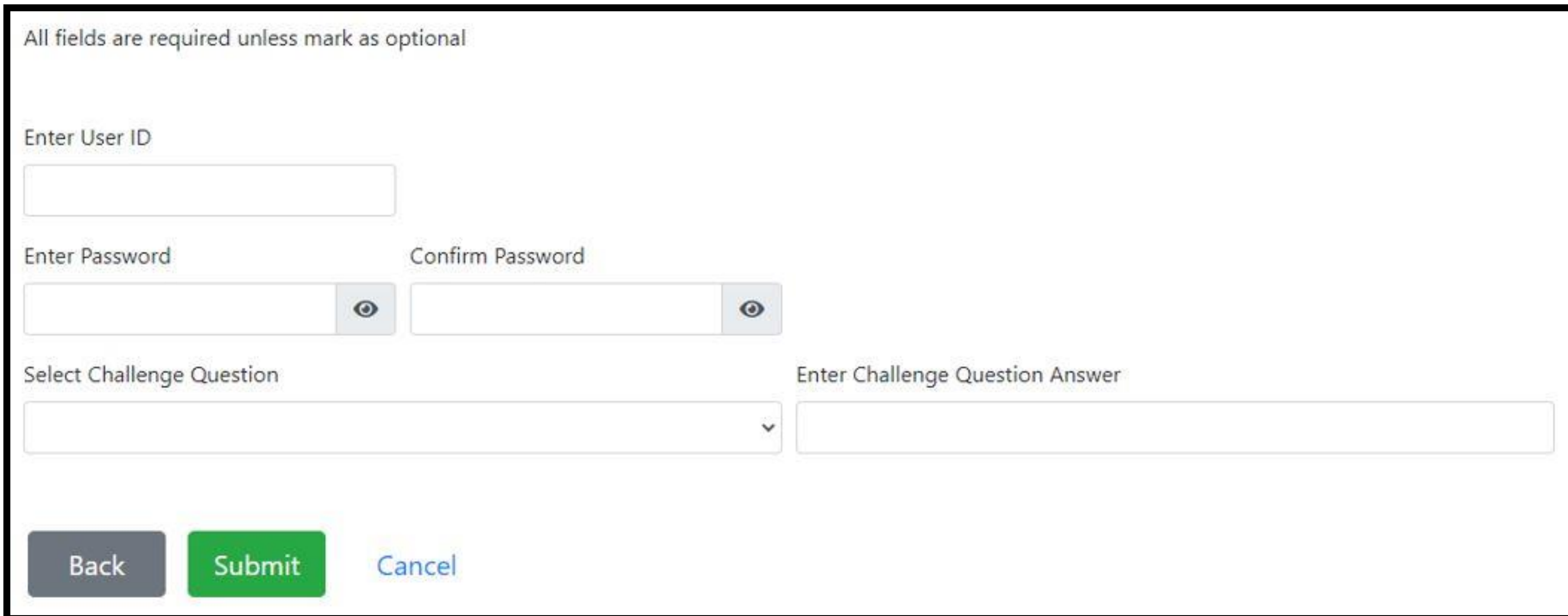
NEW USER REGISTRATION

New User Registration





New User Registration

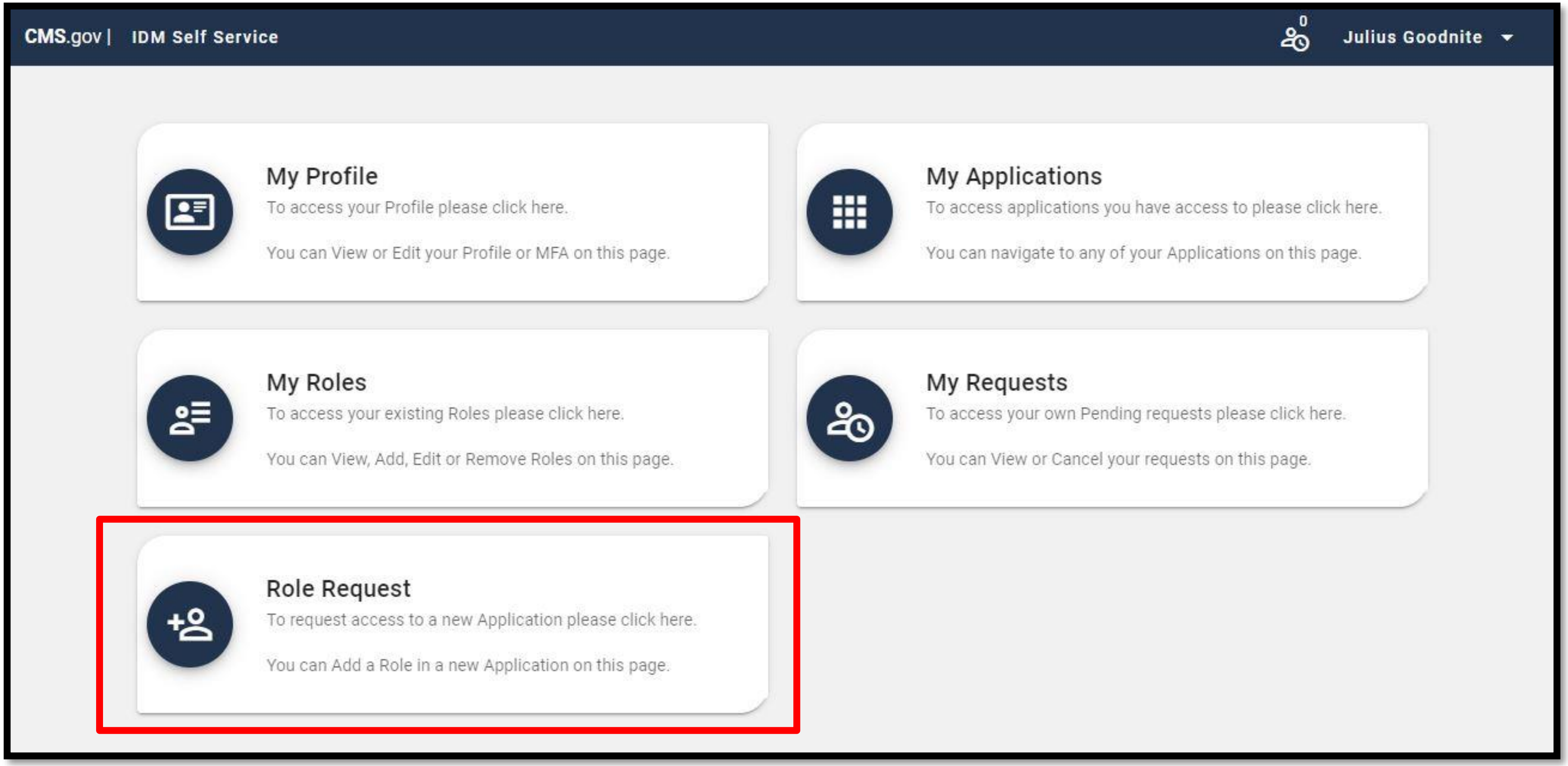


Users will not be able to create a new account if the combination of the first name, last name, and email matches an existing account

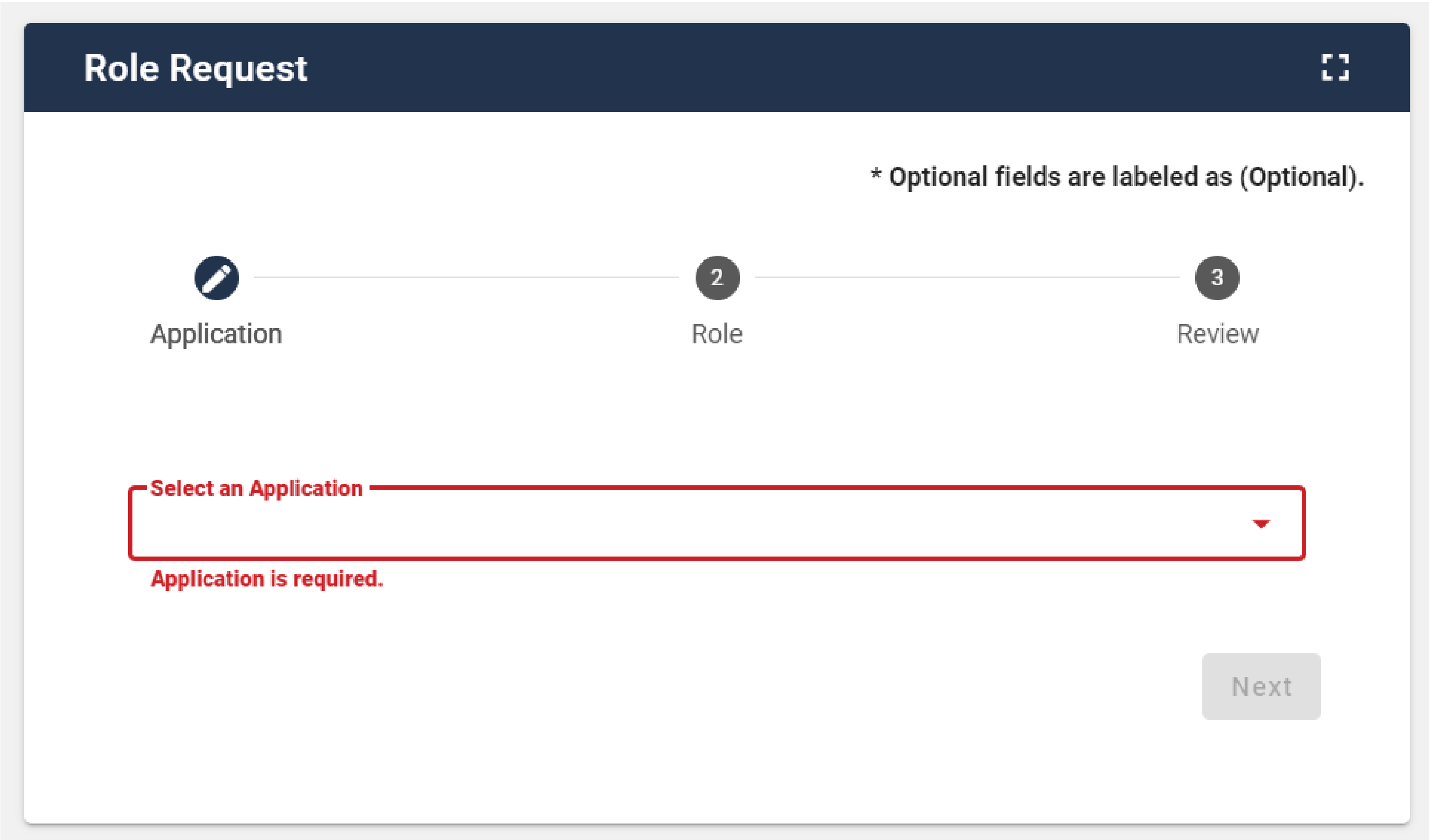
CMS IDM UI Training for Non-Portal Applications

REQUEST ROLES

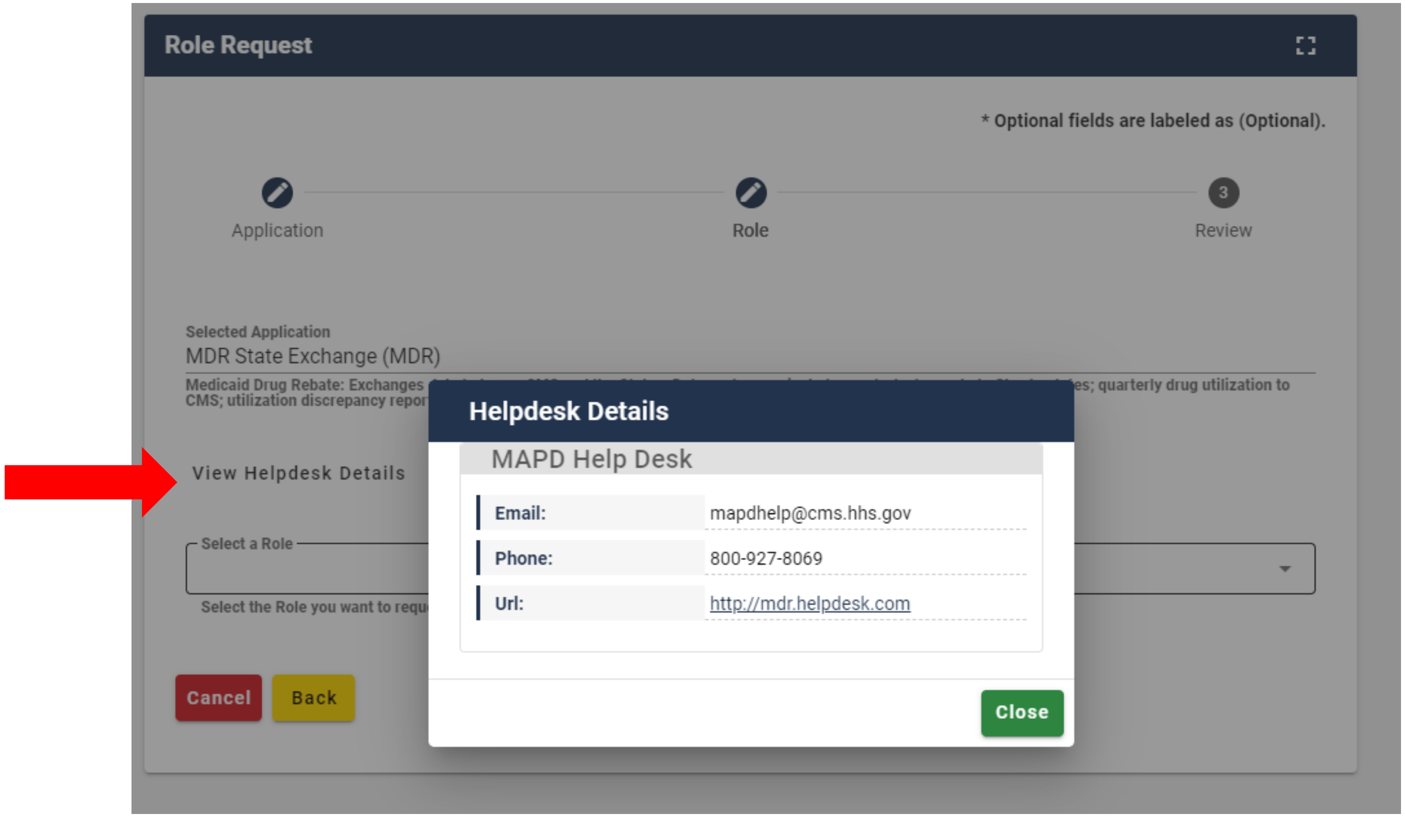
Requesting a Role



Requesting a Role



Help Desk Contact



Remote Identity Proofing

- If a user is at an LOA 1 and requests a role that requires an LOA 3, they must complete remote identity proofing (RIDP)
- IDM's RIDP is done through Experian
- During a role request, if the user needs to complete RIDP, it will automatically direct them to the proofing questions on the screen
- If a user cannot pass, the role request will not be submitted
- Users have the option to call Experian and attempt verification over the phone or attempt RIDP online again

Manual Proofing

- Manual Identity Proofing (IDP) can be established within an application.
  - Manual IDP allows applications to step up the LOA of a user who fails Experian's online and phone verification protocols
  - Manual identity proofing is not recommended under most circumstances, and should be avoided if at all possible
    - Scenarios exist where Manual IDP is warranted (User does not have the necessary credit history to complete RIDP, but has been issued a CMS PIV card)
- The Application's Business Owner determines whether or not to implement a manual identity proofing process.
  - Manual LOA step-up is always done through the application T1 helpdesk role.
- IDM can provide an approved manual process template, however manual IDP is not dictated or managed by IDM.
  - The application is responsible for creating and maintaining the manual proofing process if it's decided they want one.
- If Manual IDP is implemented for the application, it is the responsibility of the application to vet and validate user PII and step up the user's LOA through the Help Desk UI.
- IDM Tier 2 Support will not perform manual LOA Step Up in PROD

My Pending Requests

My Profile
To access your Profile please click here.
You can View or Edit your Profile or MFA on this page.

Role Request
To request access to a new Application please click here.
You can Add a Role in a new Application on this page.

Manage My Roles
To access your existing Roles please click here.
You can View, Add, Edit or Remove Roles on this page.

My Requests
To access your own Pending requests please click here.
You can View or Cancel your requests on this page.

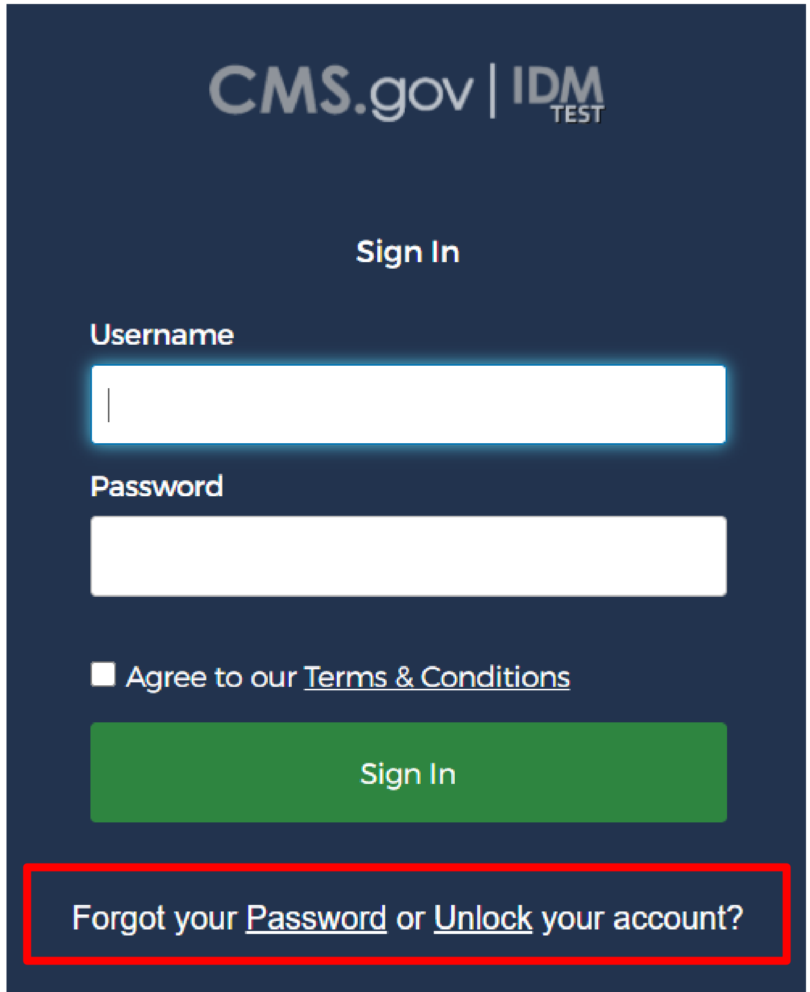
My Requests

Request ID	Application	Role	Submit Date	Expiration Date	Actions
71319	GENTRAN	End User	09/01/2020	09/02/2020	

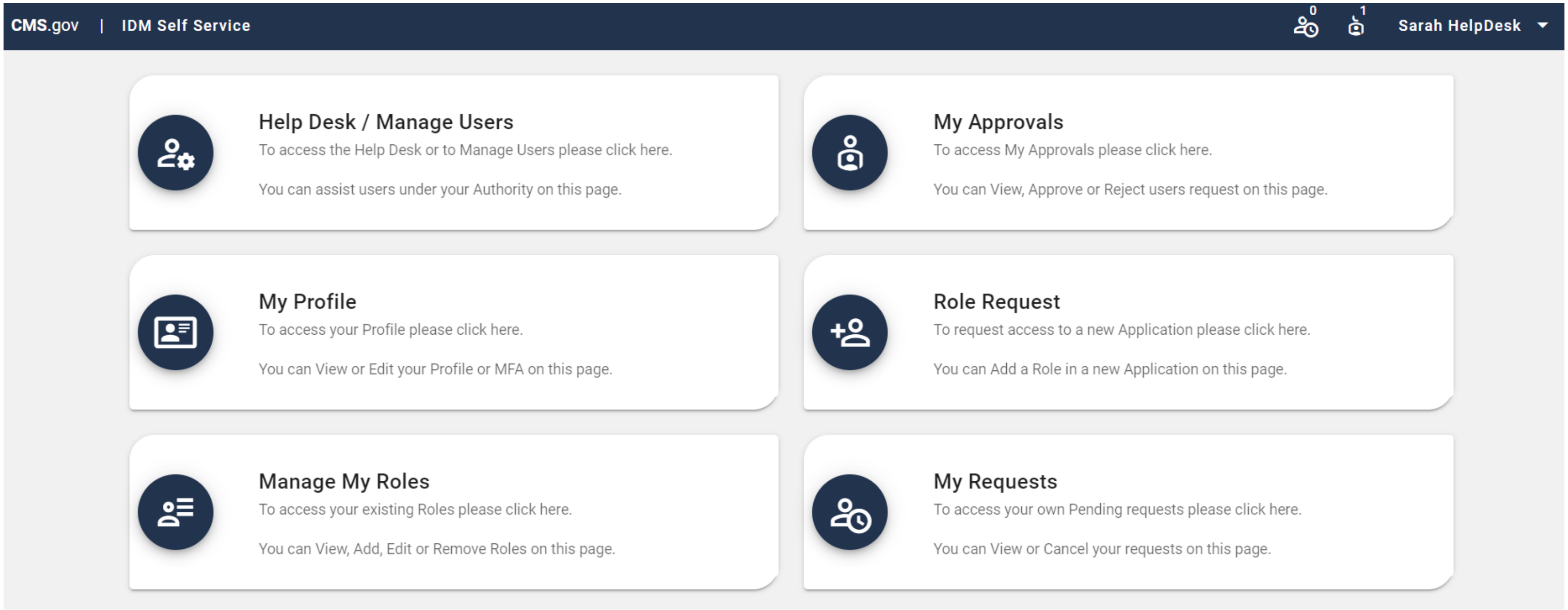
CMS IDM UI Training for Non-Portal Applications

SELF SERVICE FUNCTIONS

Home Page Self Service Functions

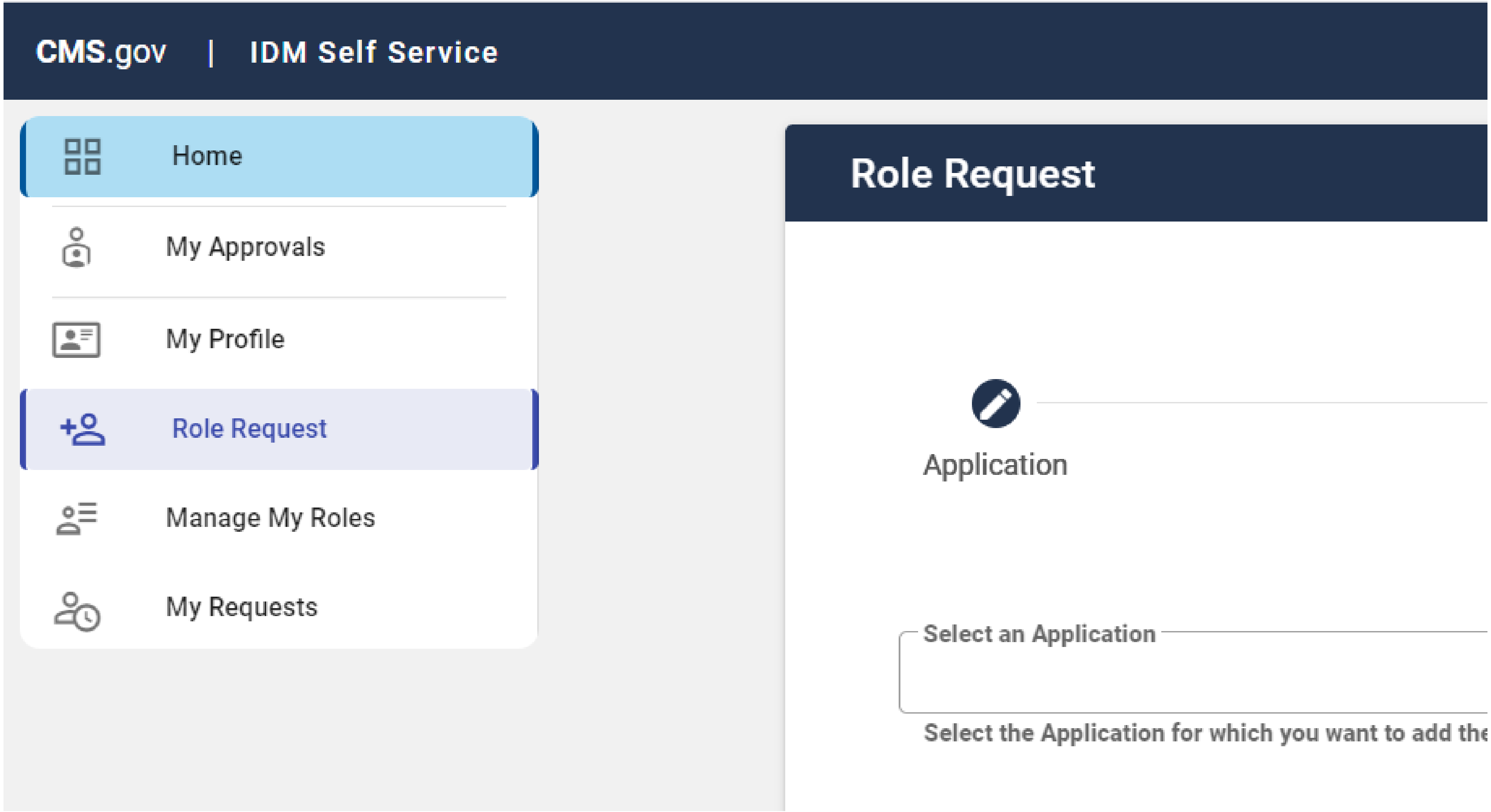


Self Service Page Icons



Help Desk/Manage Users and My Approvals tiles will only show up if that user has those functionalities based on their role(s).

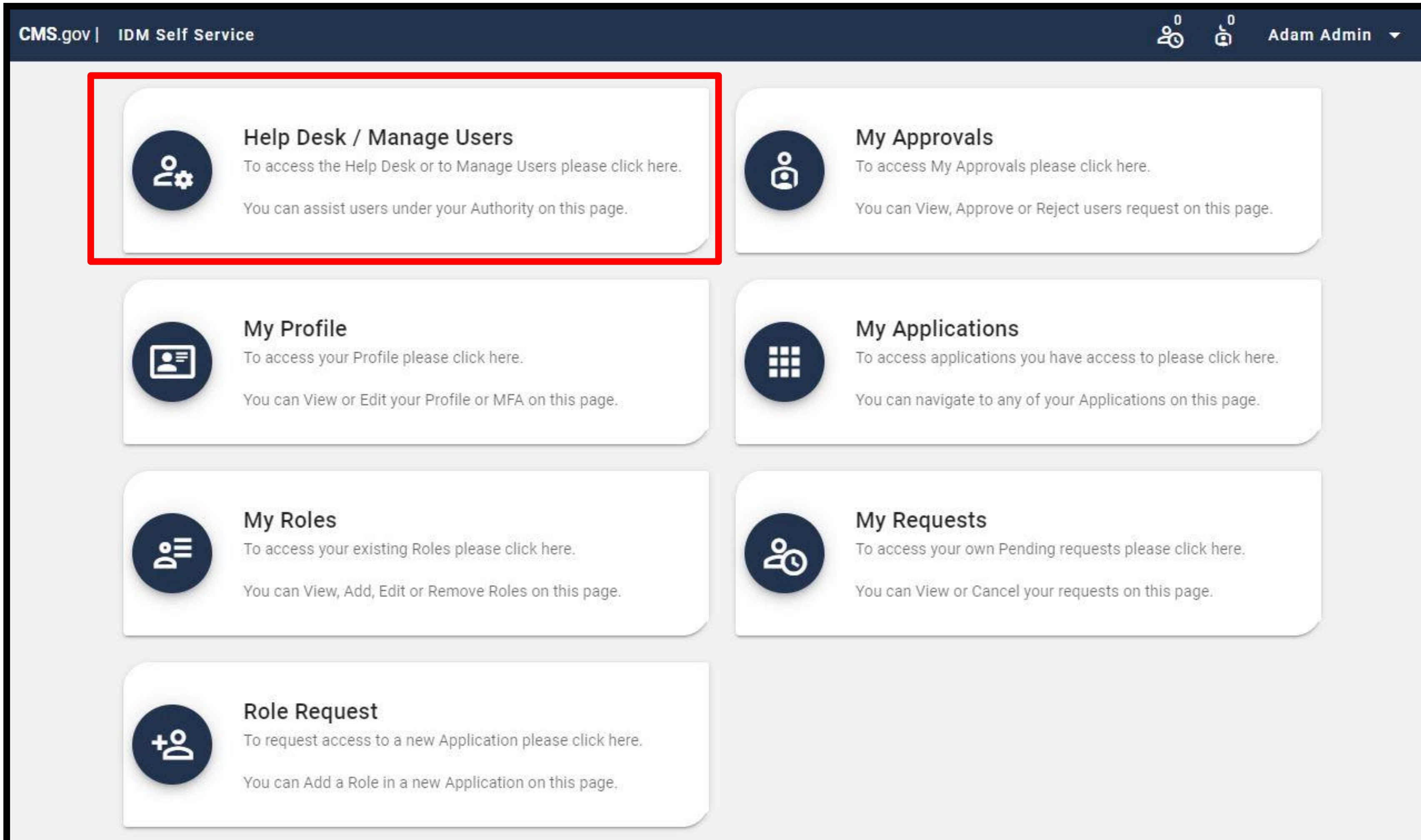
Self Service Page Icons



CMS IDM UI Training for Non-Portal Applications

ACCESSING THE HELP DESK UI

Self Service look for Help Desks



CMS IDM UI Training for Non-Portal Applications

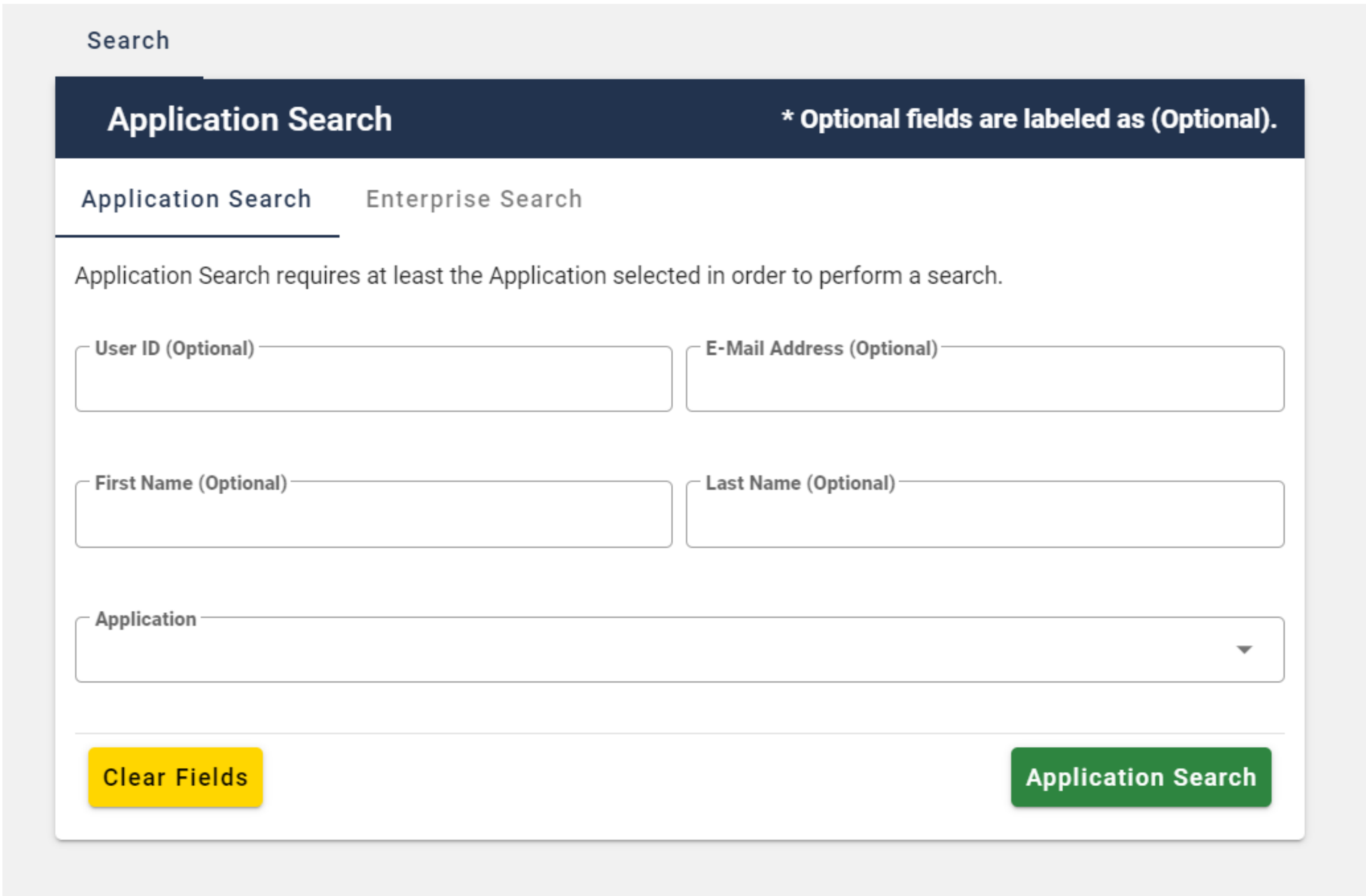
USER SEARCH

Application vs Enterprise Search

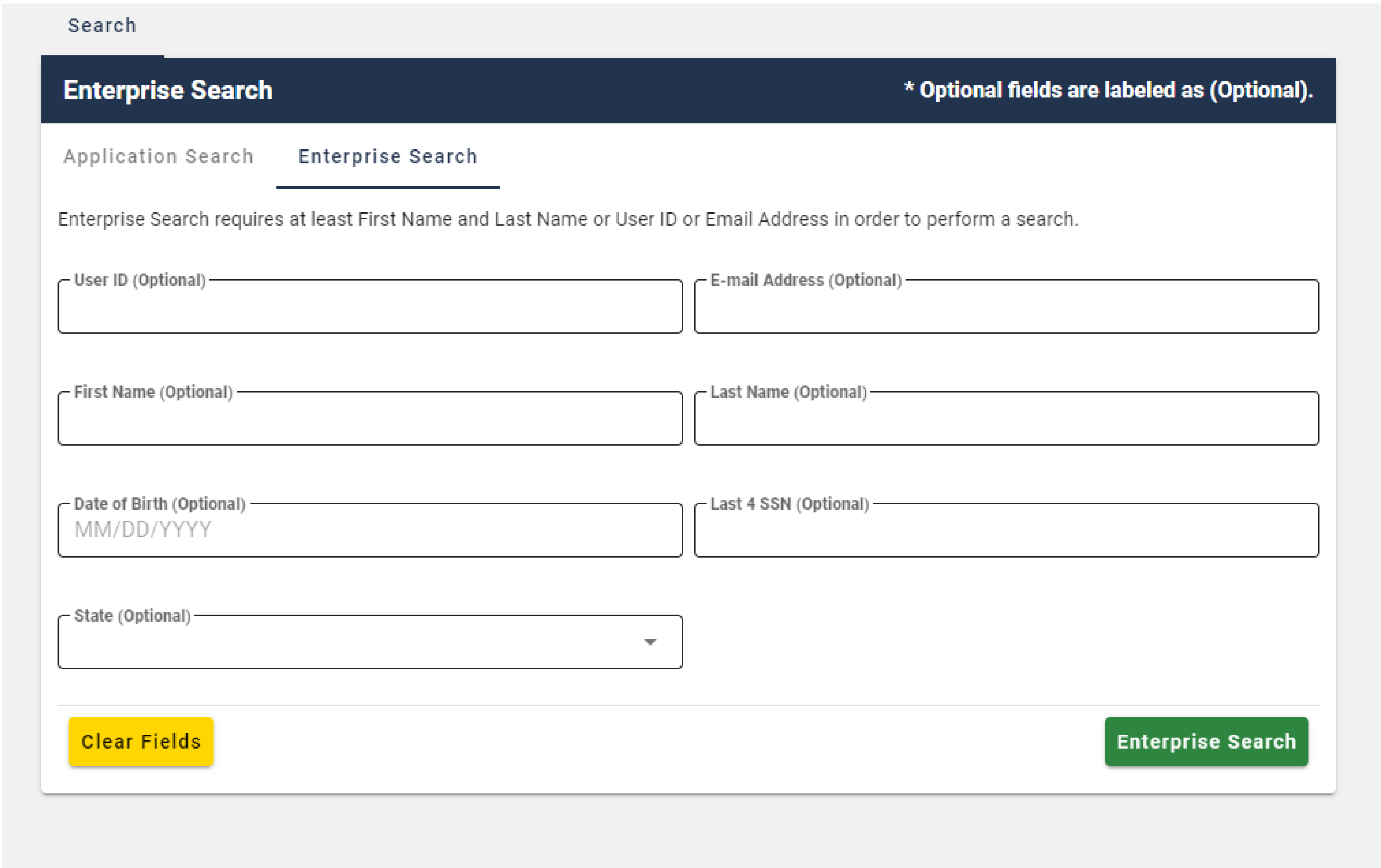
- Users with an Application Help Desk role will have the ability to use two different search functions – Application and Enterprise

	Application	Enterprise
Limitations	Only searches user within an application you have access to	Searches users across system
Search Options	User ID, Email, First Name, Last Name, Application, Role	User ID, Email, First Name, Last Name, DOB, Last 4 SSN, State
Search requirements	All fields optional except for application	-Partial First AND Last Name (min. 1 character) -Partial Email (min. 2 characters) -Partial User ID (min. 2 characters)
Max number of searches	50	5

Application Search



Enterprise Search



CMS IDM UI Training for Non-Portal Applications

VIEW USER DETAILS

Search Results

Search | Results

Search Results

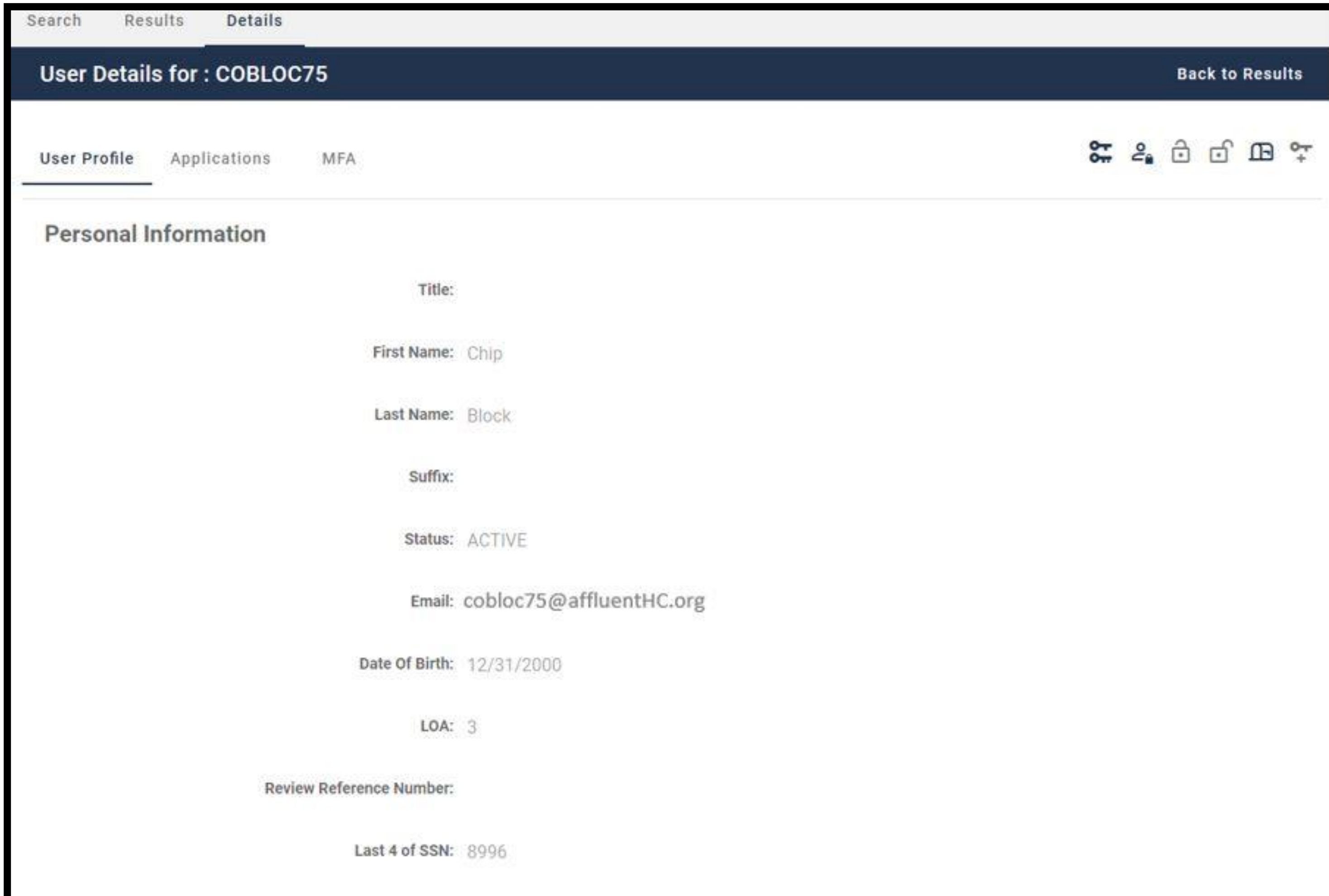
Back to Search

Total Results: 1

Filter

User ID	Name	E-mail Address	Status	Last Login	State	Source	Actions
MXE	FakeFirst FakeLast	@gdit.hcqis.org	ACTIVE		Virginia	eidm	

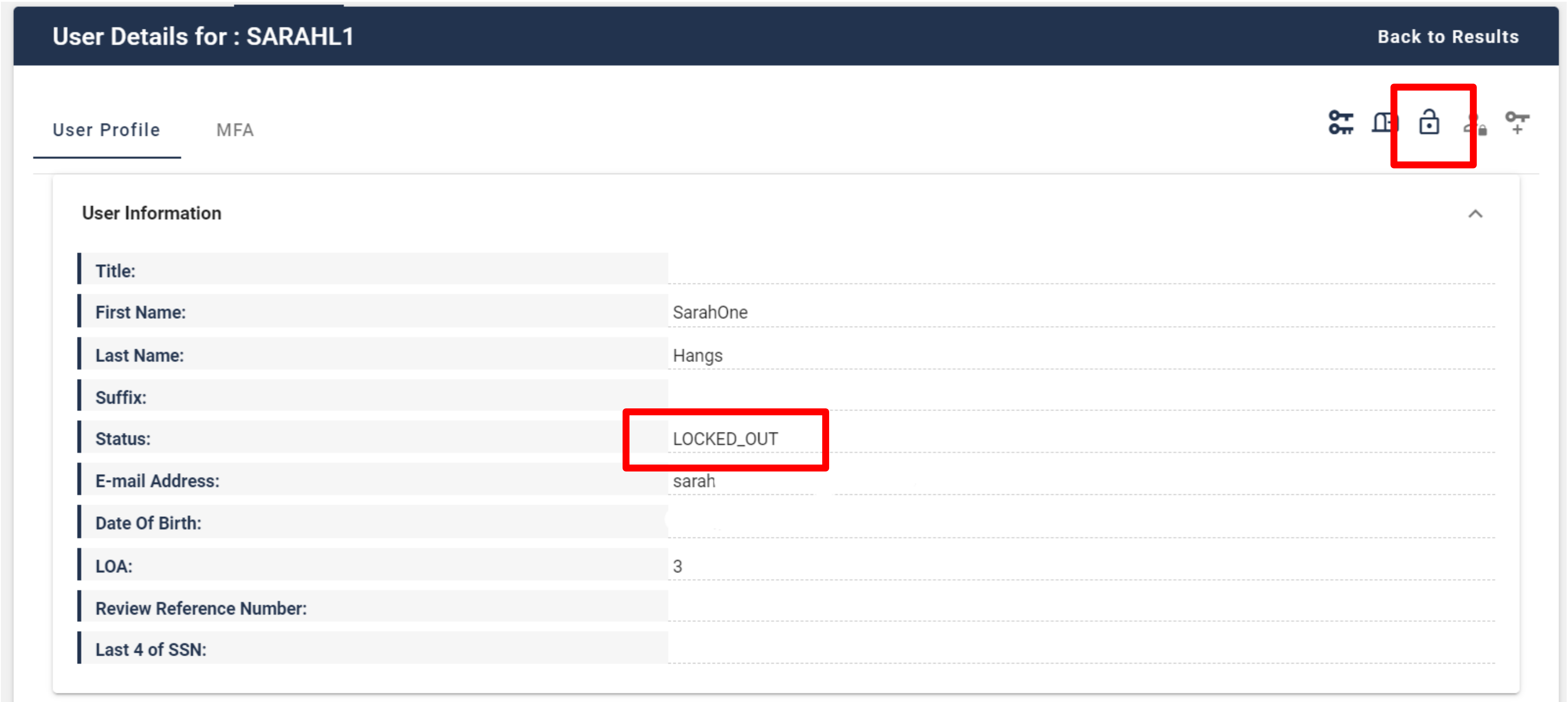
User Details Page



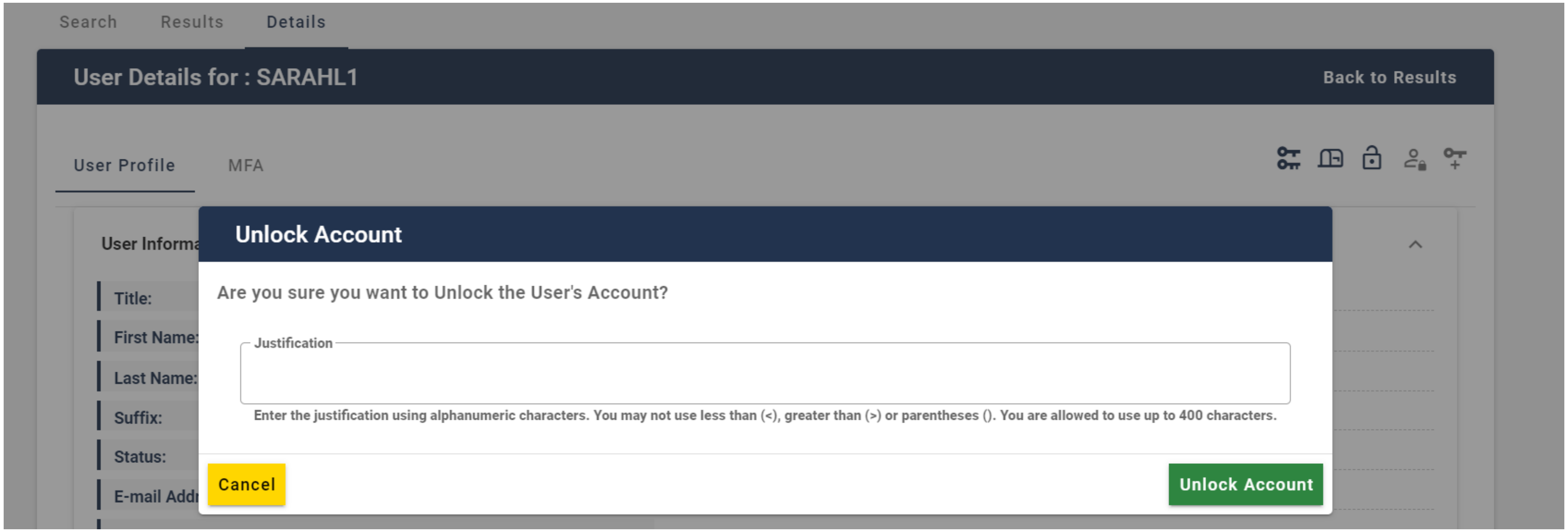
CMS IDM UI Training for Non-Portal Applications

ACCOUNT UNLOCK

User Details Page



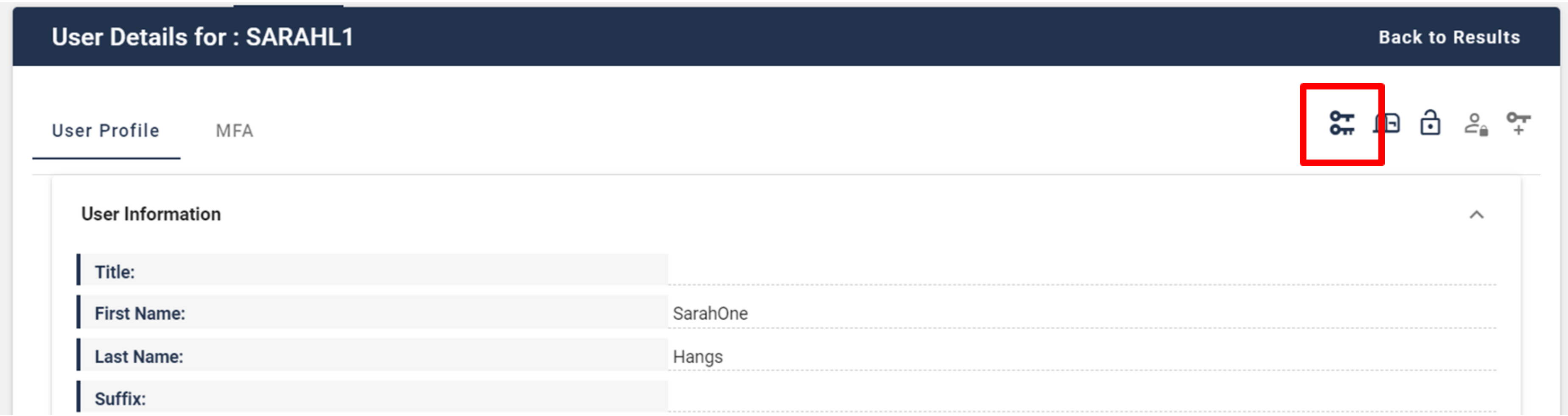
Unlock Confirmation



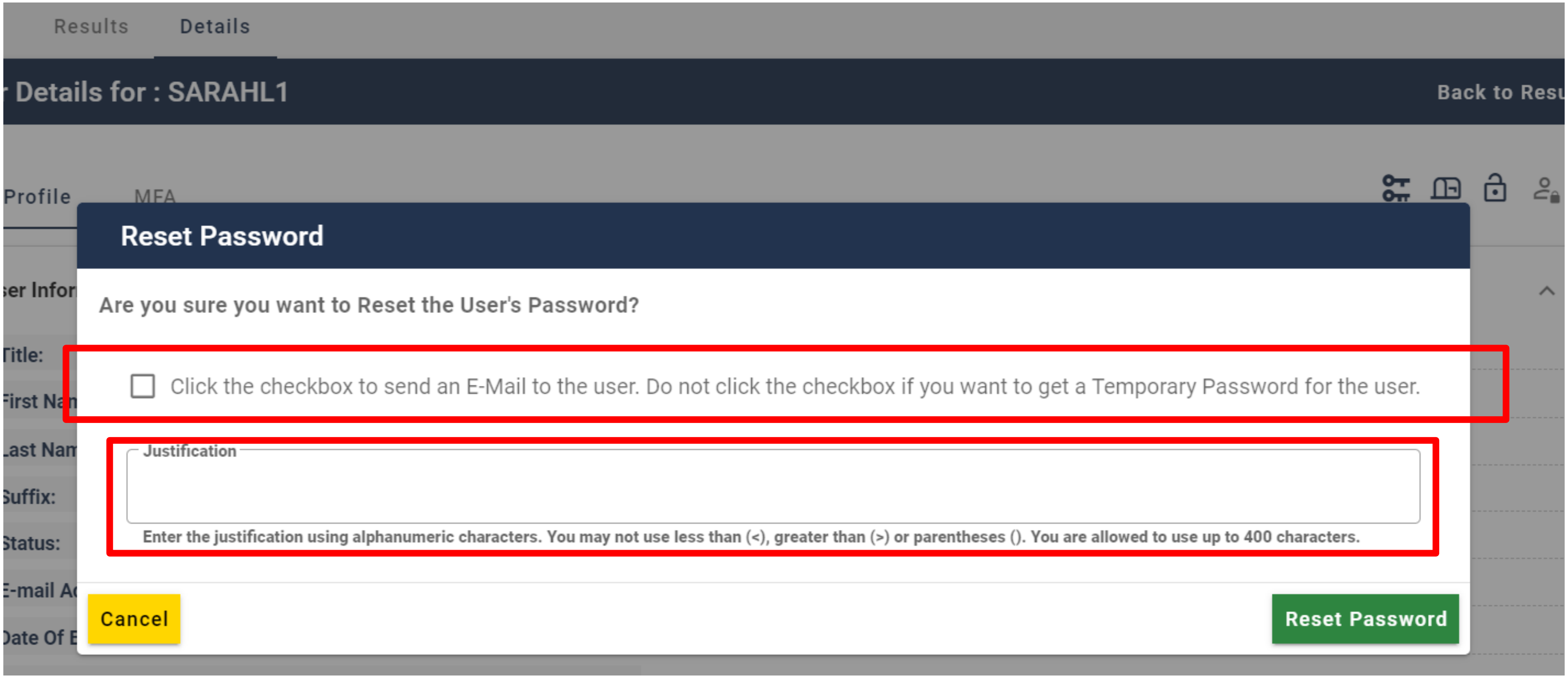
CMS IDM UI Training for Non-Portal Applications

PASSWORD RESET

Password Reset



Email Password Reset



Email Password Reset

[EXTERNAL]Help Desk Assisted Password Reset (CMS IDM IMPL)

IA

IDM Auto Response <no-reply@impl.idp.idm.cms.gov>

To

If there are problems with how this message is displayed, click here to view it in a web browser.

Help Desk Assisted Password Reset

CMS.gov
Centers for Medicare & Medicaid Services

CMS Identity Management System (IDM) - IMPL Environment

Dear SarahApp Hangs,

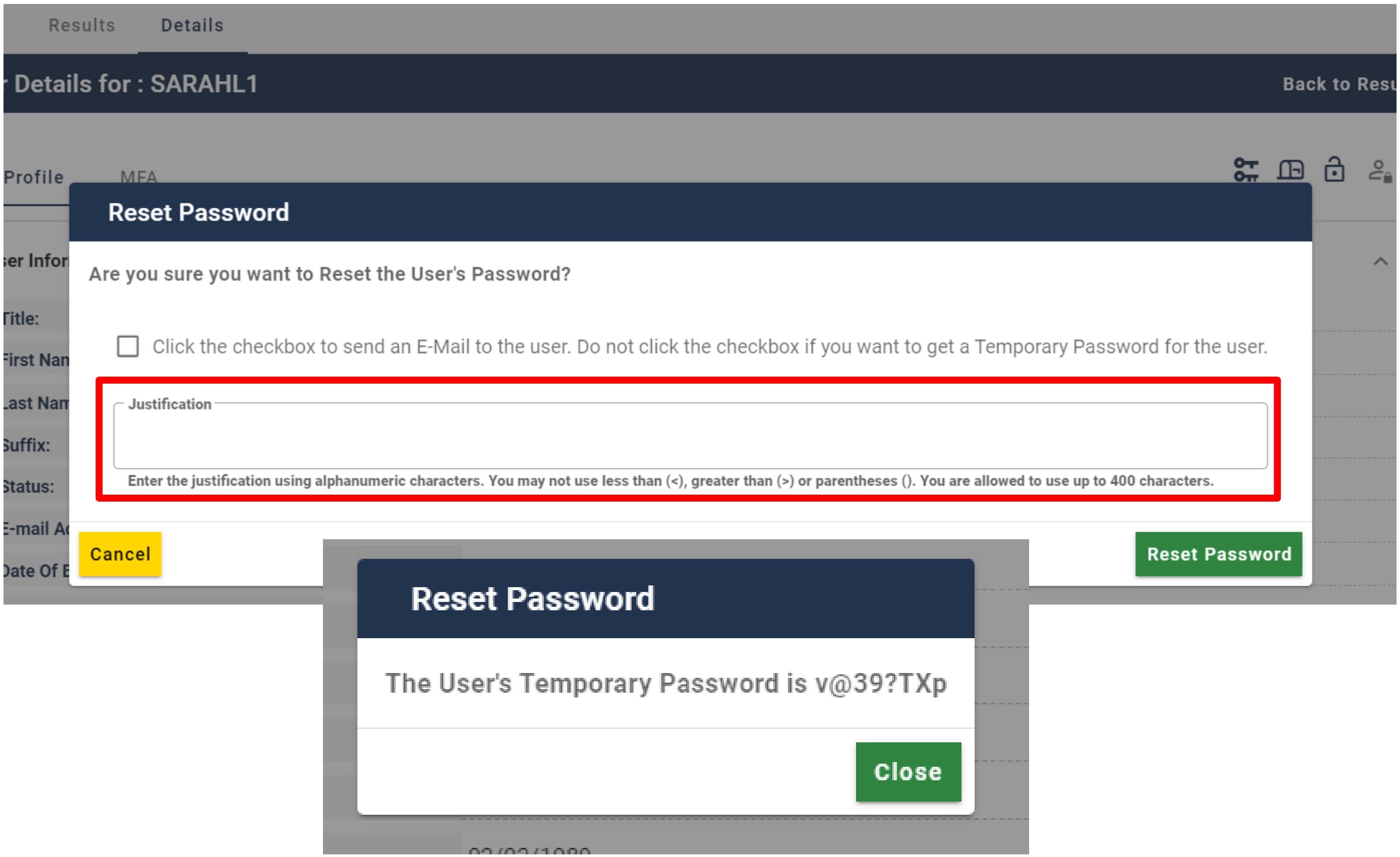
A password reset for your CMS IDM account has been initiated by your CMS application help desk. If you did not make this request, please contact your application help desk immediately.

Click the link below to reset the password for your username, SarahApp2:

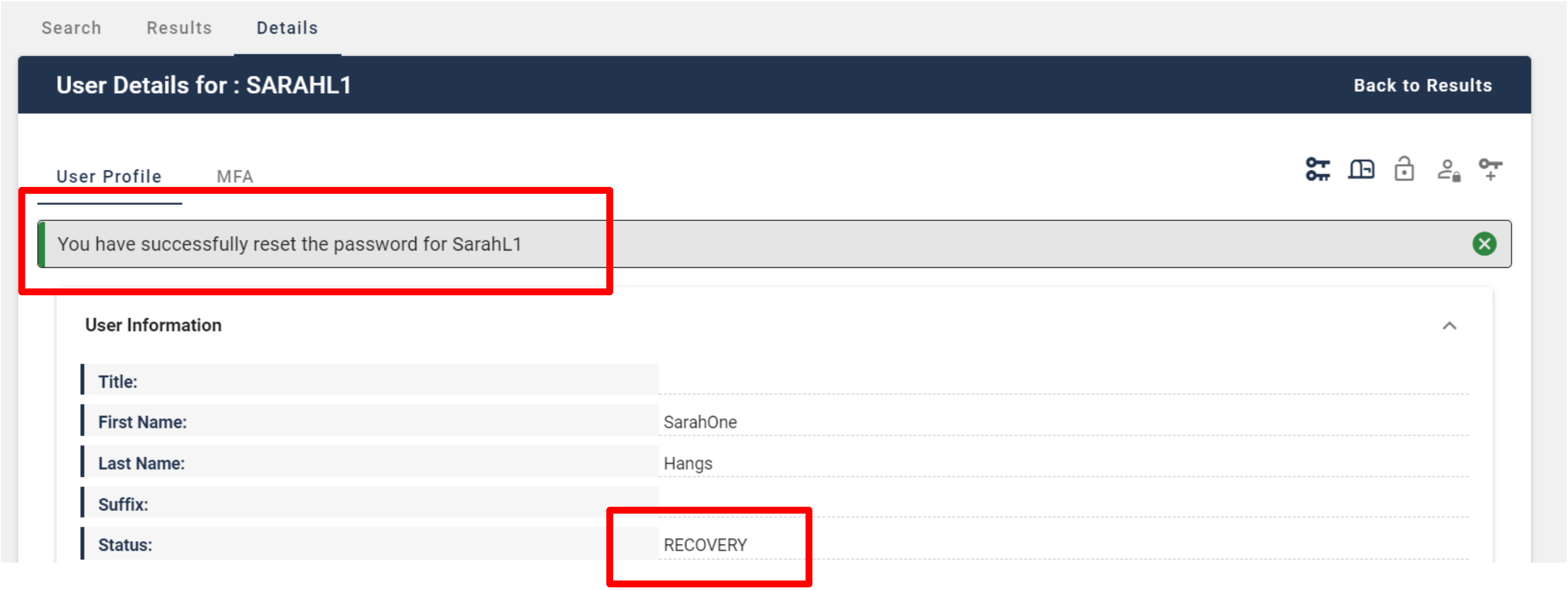
Reset Password

This link expires in 4 hours.

Temporary Password



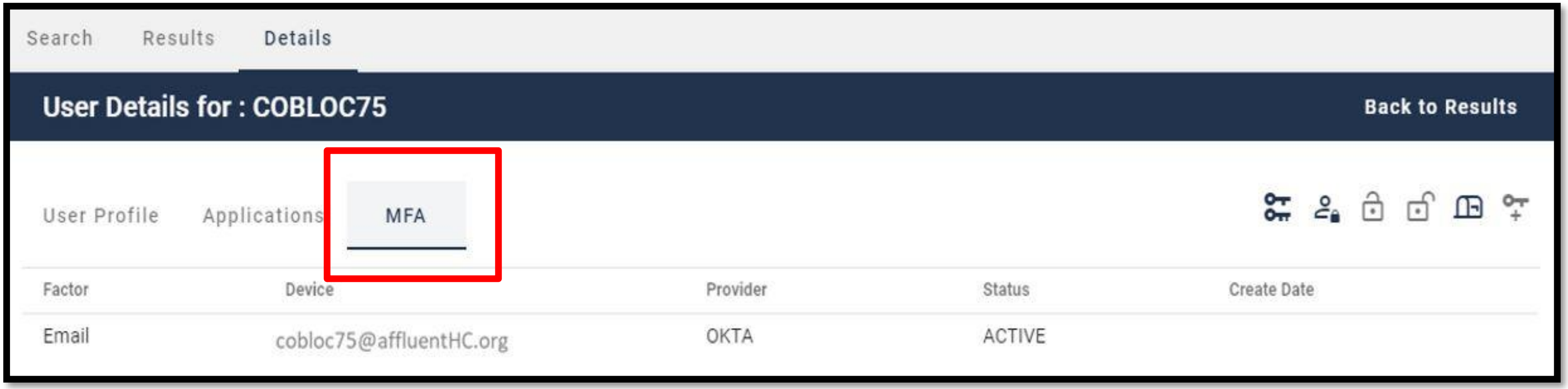
Password Reset Confirmation



CMS IDM UI Training for Non-Portal Applications

VIEW MFA DEVICE

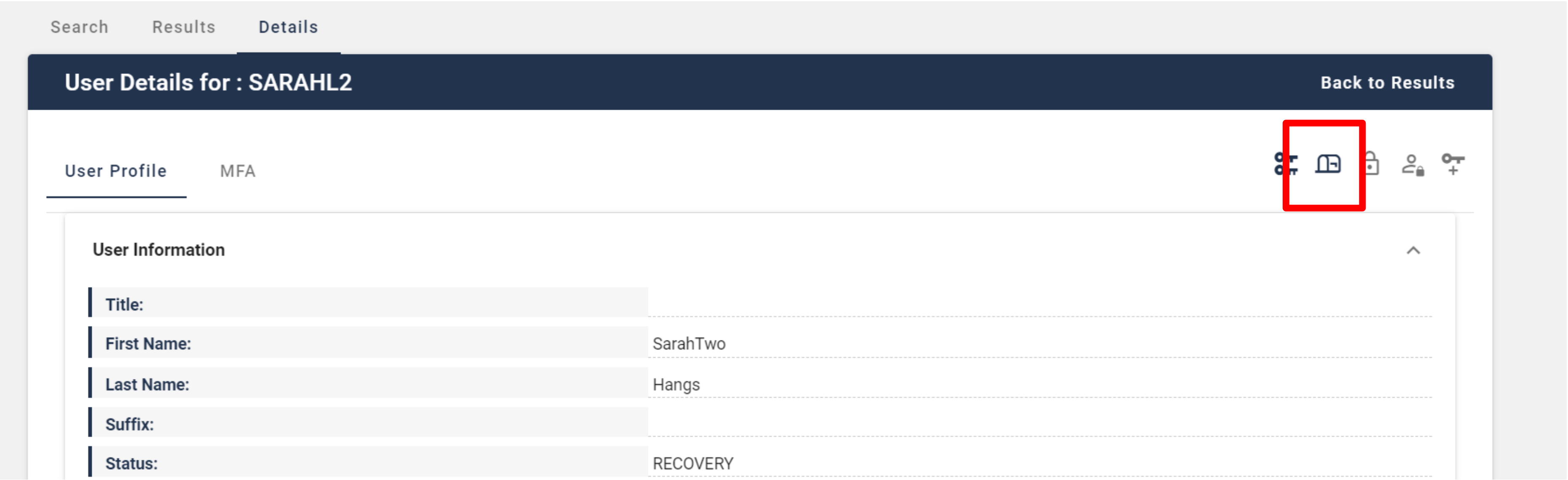
Viewing MFA devices



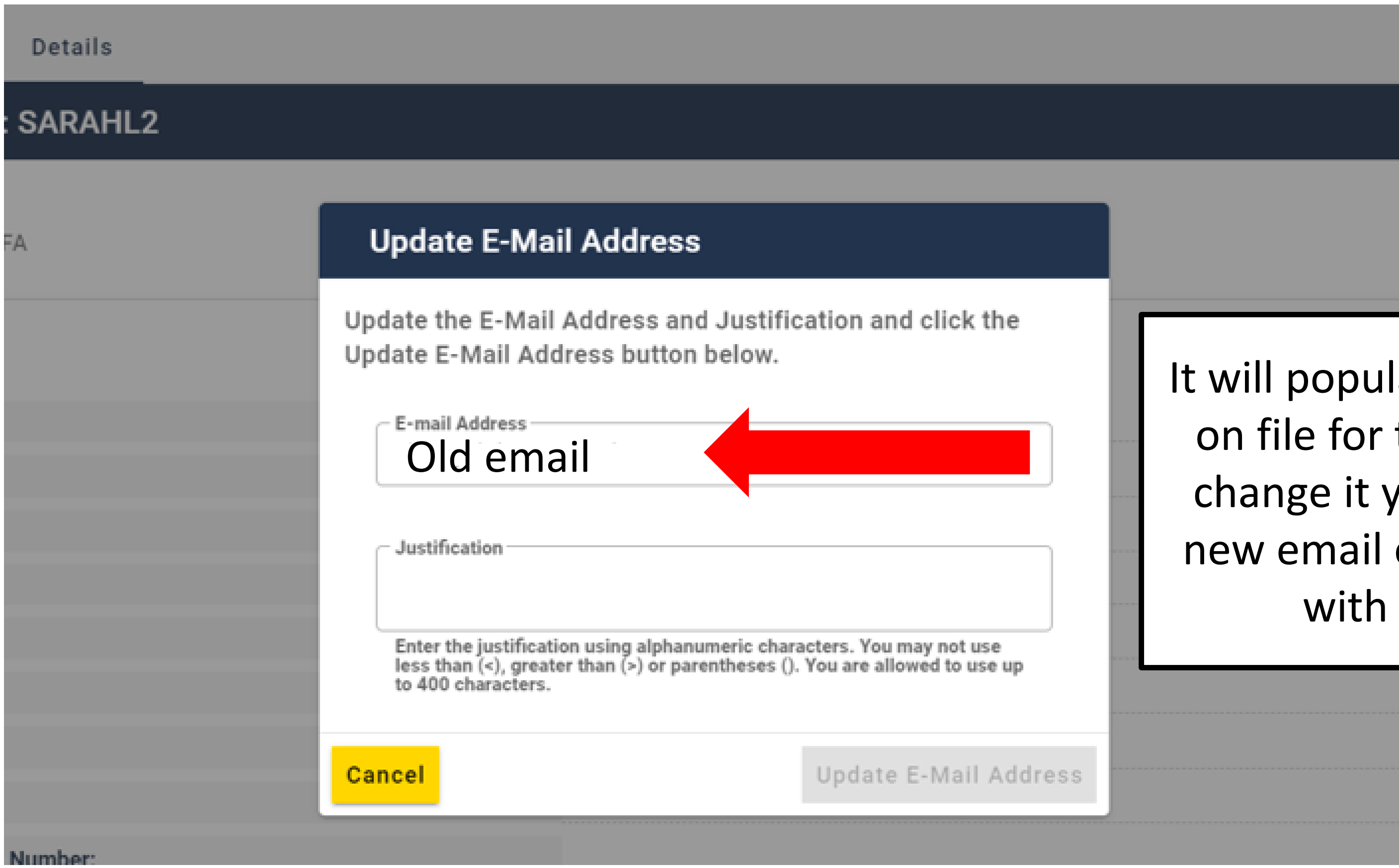
CMS IDM UI Training for Non-Portal Applications

UPDATING A USER'S EMAIL ADDRESS

User Details page



Update Email Pop up

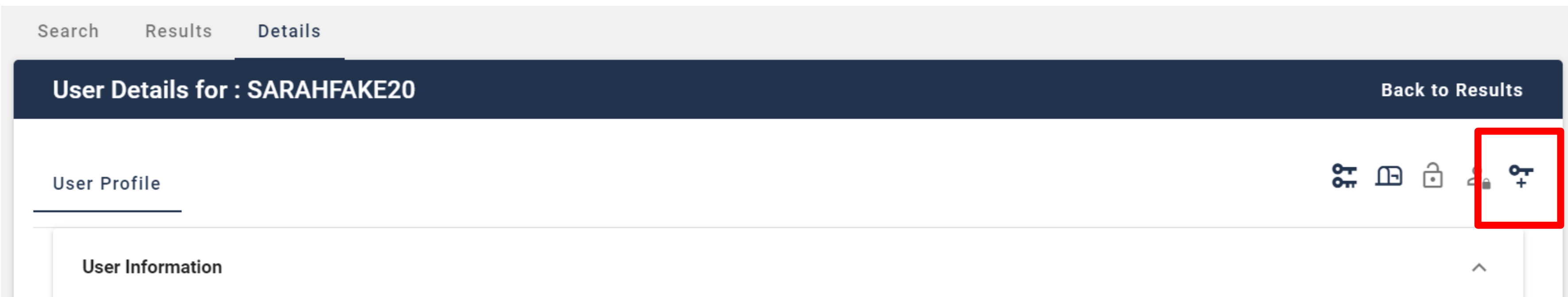


It will populate the current email on file for the user. In order to change it you must type in the new email on this pop up along with a justification.

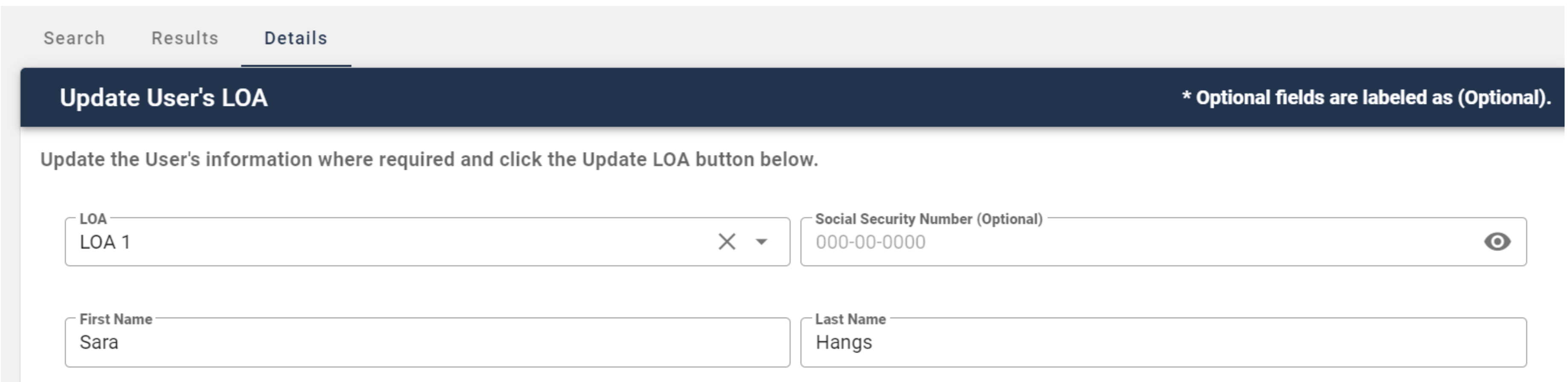
CMS IDM UI Training for Non-Portal Applications

UPDATING A USER'S LEVEL OF ASSURANCE (LOA)

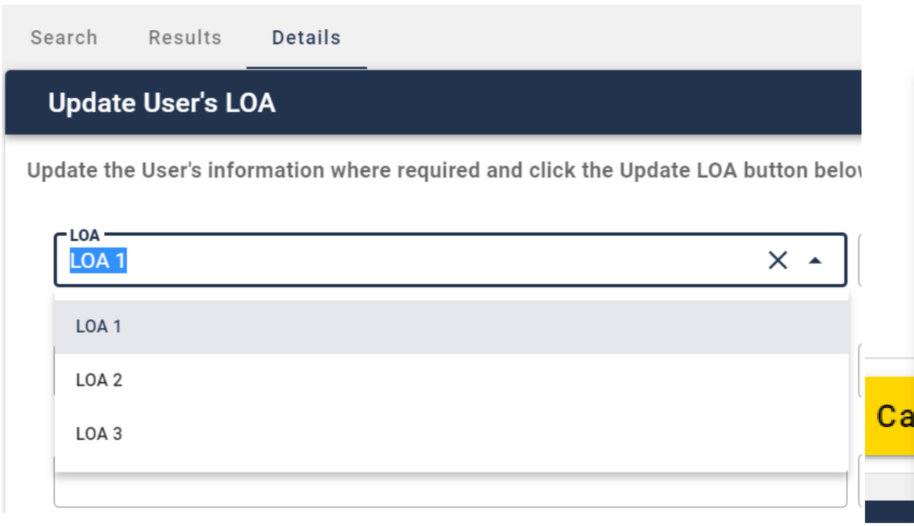
User Details Page

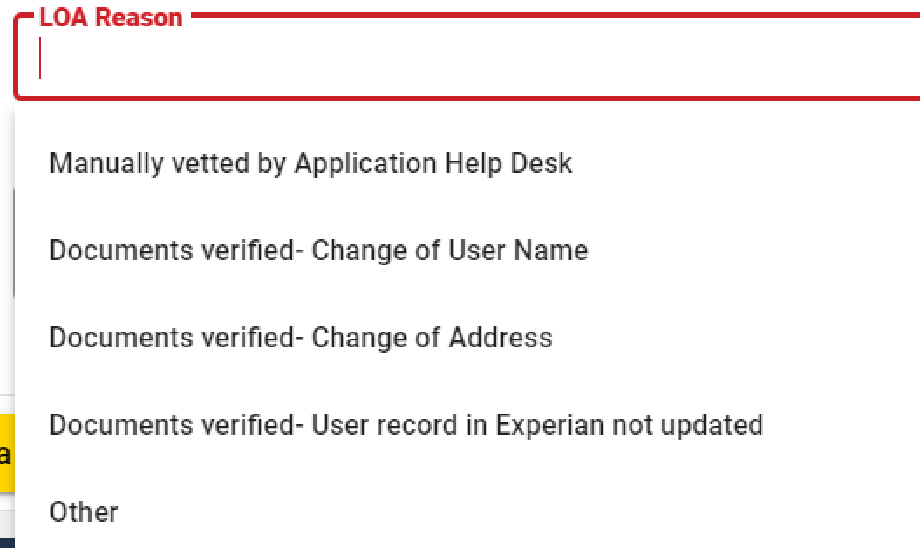


LOA Information Page



Note that SSN is optional for LOA 1 and LOA 2. When you select LOA 3 from the drop SSN changes to a required field



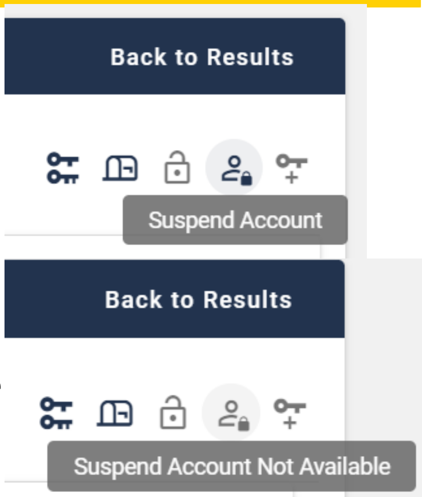


You will also be required to select an LOA reason from the drop down and justification before submitting

CMS IDM UI Training for Non-Portal Applications

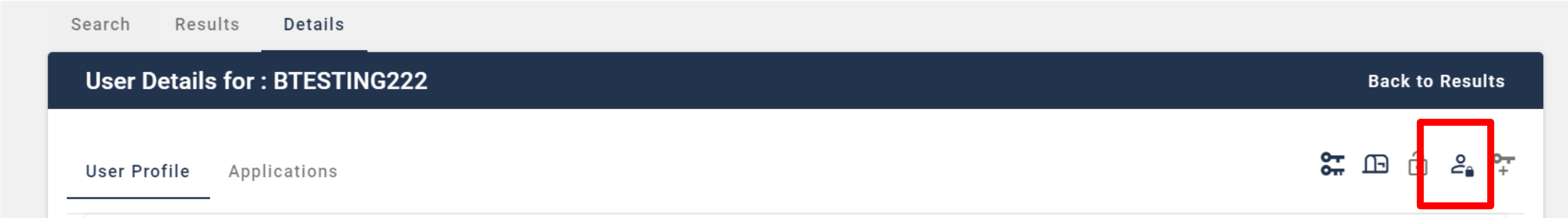
SUSPENDING / UNSUSPENDING USERS

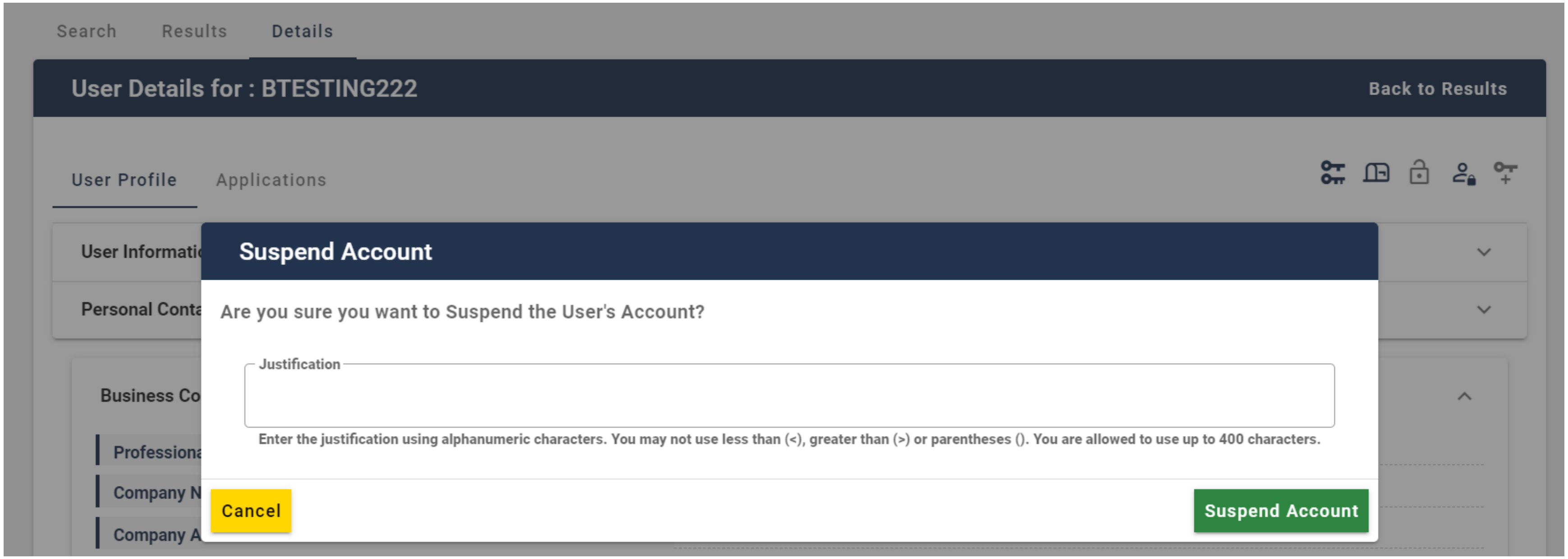
Suspending Accounts



- You can only suspend accounts of users associated with your application, otherwise the option will be greyed out
- Suspending accounts should only be used for when a user violates the system's user agreement
- Examples of user agreement violations include users sharing their account with another individual, using screen scraping software, and cases where the user's identity has been stolen and their account may be accessed fraudulently
- You should not suspend an account for someone who has left an organization or no longer needs access. Instead their roles they no longer need should be removed
- Suspended accounts will not be able to access the system at all, regardless of status with other system applications
- Applications should notify IDM Tier 2 when they have suspended a user by creating an Incident or sending an email and attaching the completed security form found on Confluence

Suspending Accounts





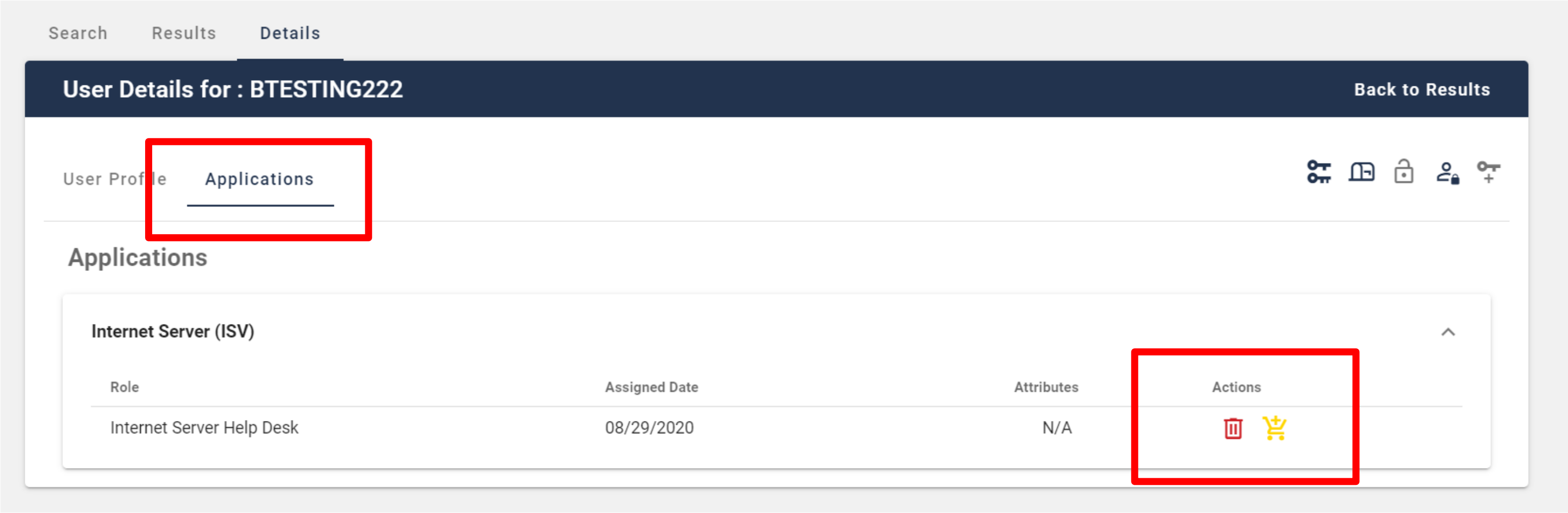
Unsuspending Accounts

- Application Help Desks do not have the ability to unsuspend user accounts
- If a user has taken the necessary steps to be reinstated, the application help desk will contact IDM Tier 2 and provide the user's information
- Please provide the original Incident number that the account was suspended under

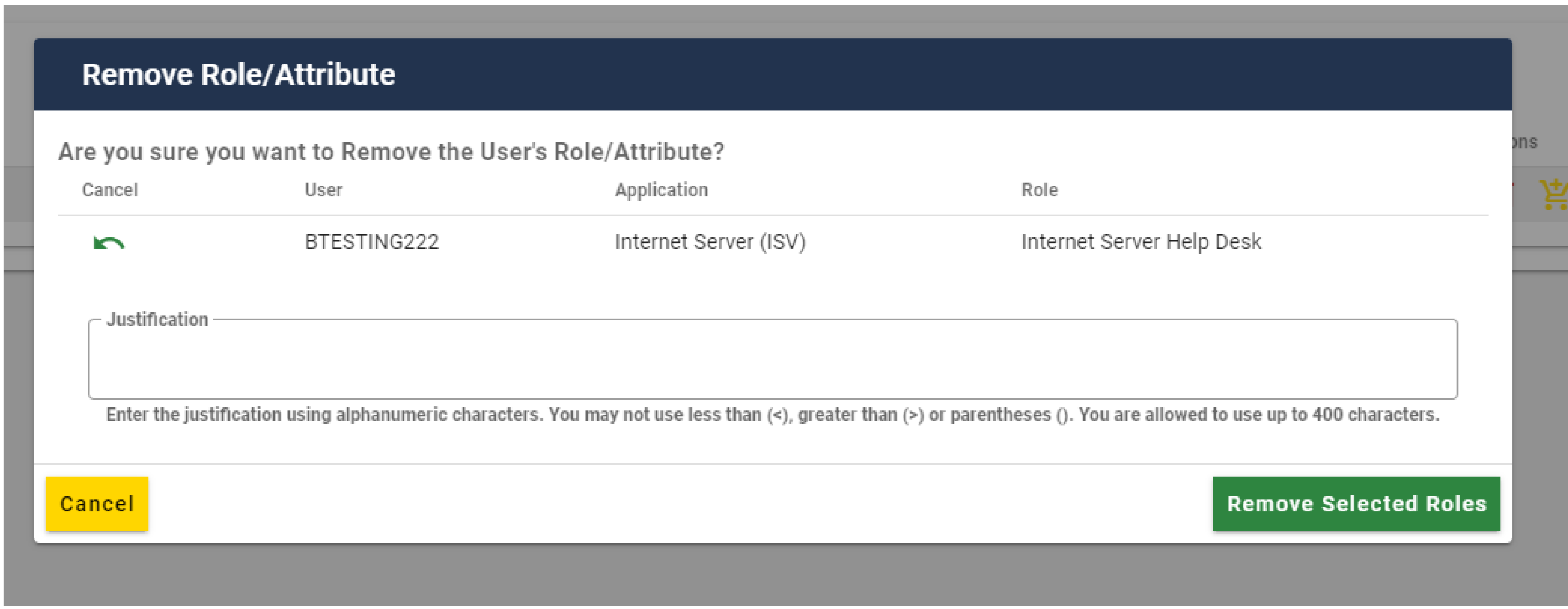
CMS IDM UI Training for Non-Portal Applications

REMOVE ROLES AND ATTRIBUTES

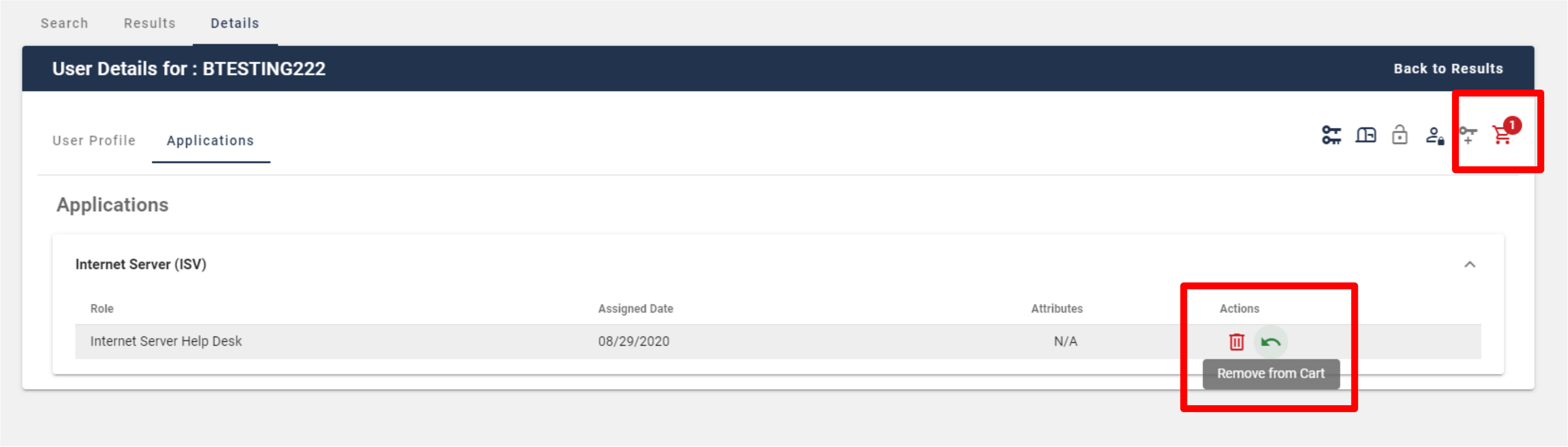
User Details



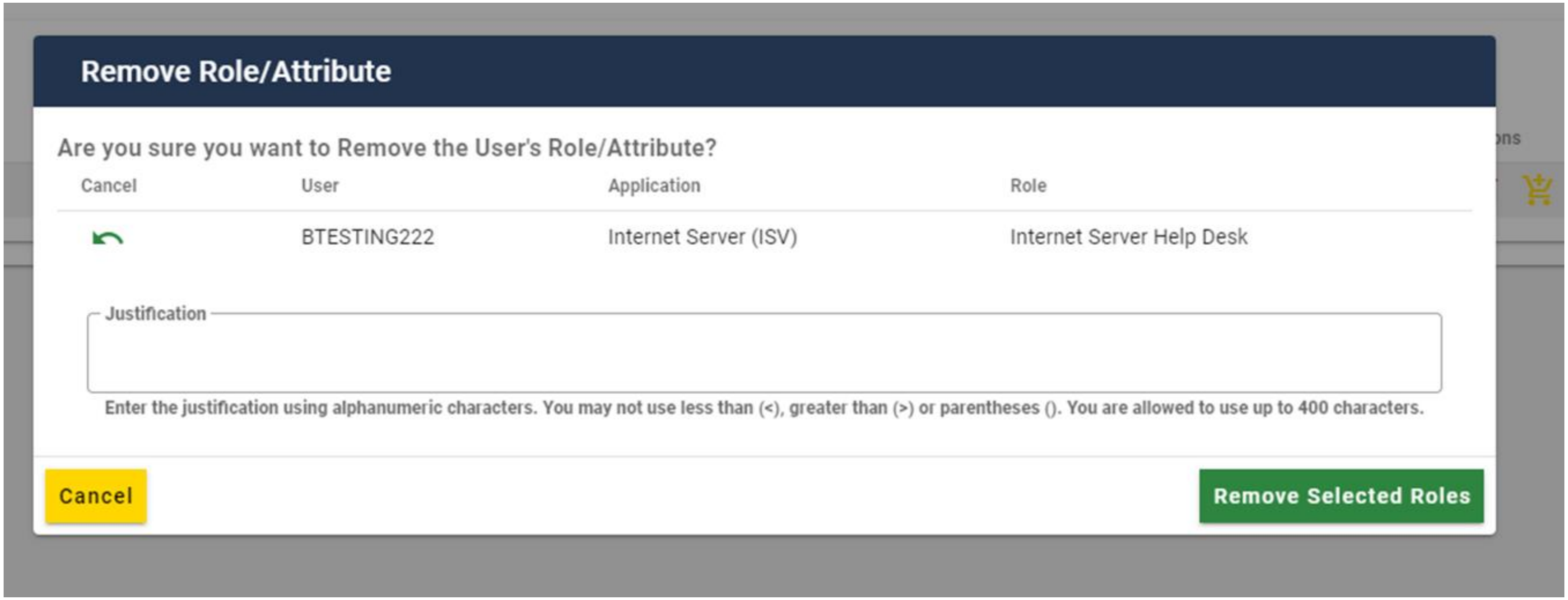
Remove Role Confirmation



Add to Cart


Search
Results
Details
User Details for : BTESTING222
Back to Results
User Profile
Applications
1
Applications
Internet Server (ISV)
Role
Assigned Date
Attributes
Actions
Internet Server Help Desk
08/29/2020
N/A
Remove from Cart

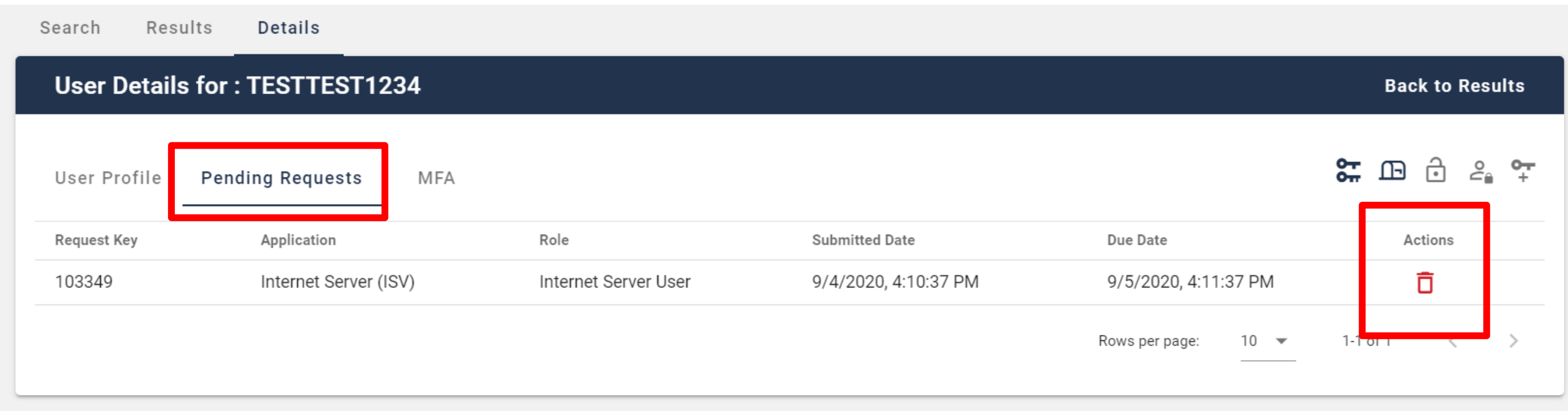
Add to Cart Icon



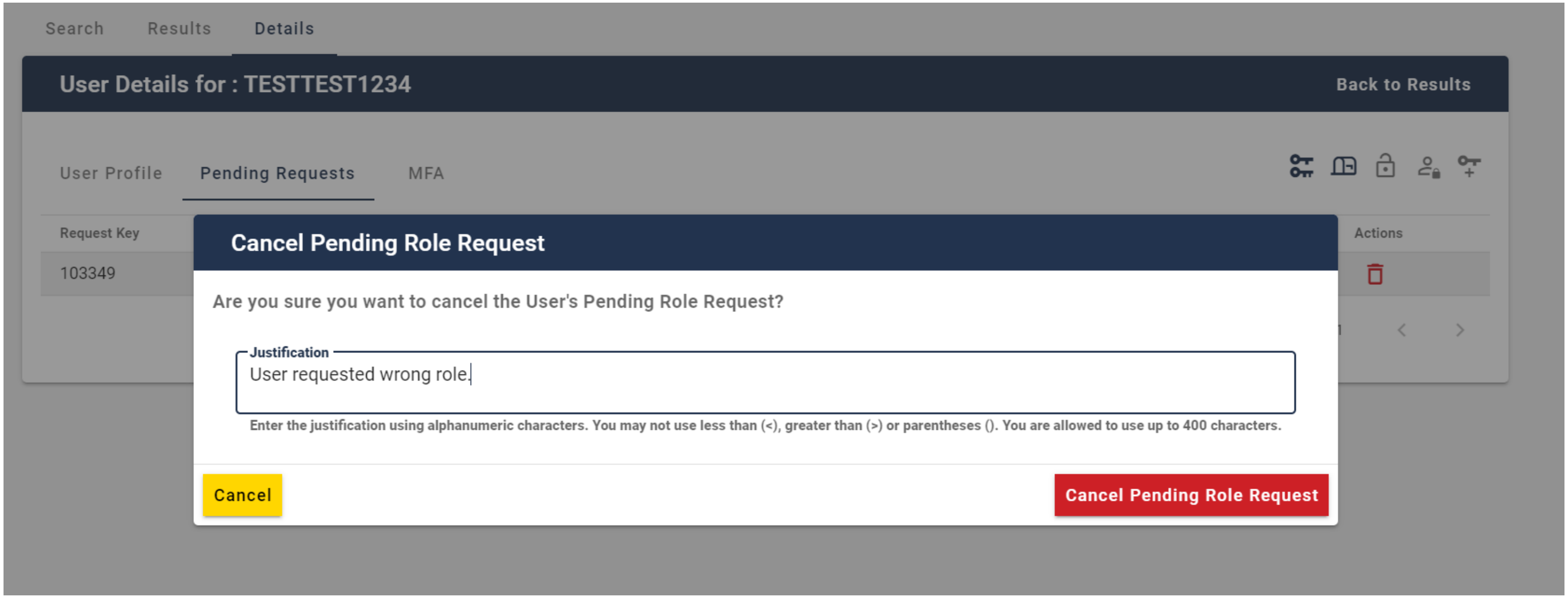
CMS IDM UI Training for Non-Portal Applications

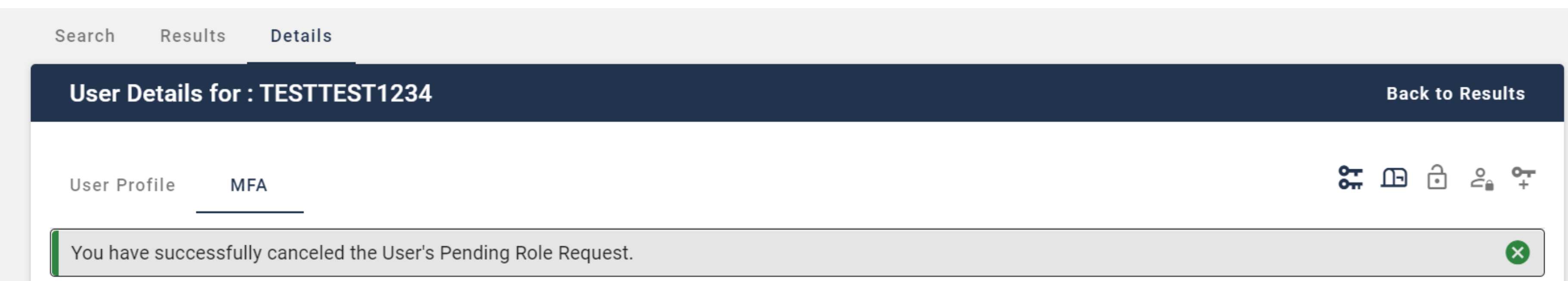
CANCEL PENDING ROLE REQUESTS

User Details



Justification and Confirmation





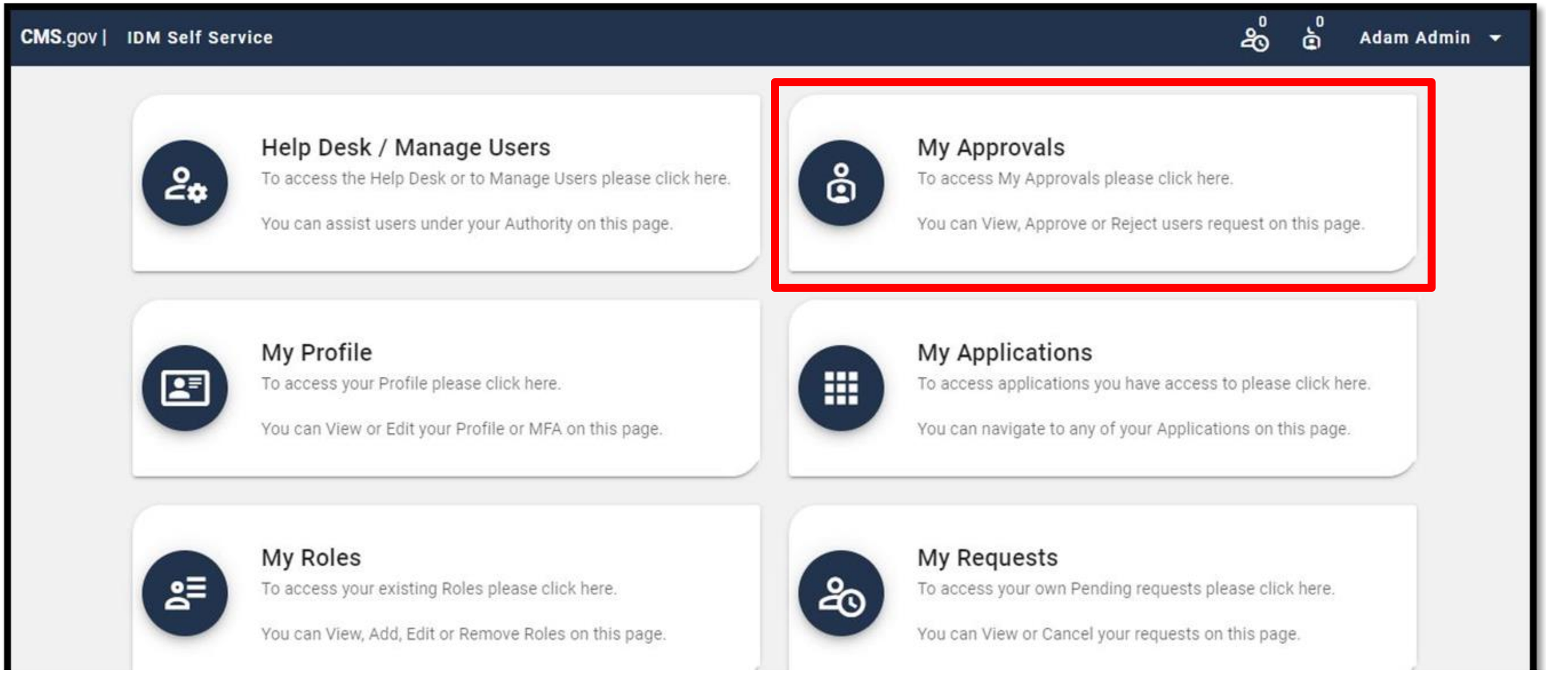
CMS IDM UI Training for Non-Portal Applications

APPROVE ROLE REQUESTS

My Approvals

- Some Application Help Desks also have the ability to approve/reject roles

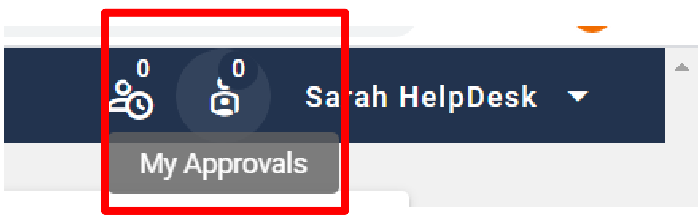
- If your help desk has that capability, you will see My Approvals when signing into the system



Notifications for Pending Request

- You will receive notifications and emails when a role under your authority has been requested

- Notifications in the system will be located in the top right corner by your name



TEST IDM Action Required: Pending Approvals

D donotreply-idm@cms.hhs.gov
To

The tracking number for this request is 220953.

Application: CPI API Onboarding
Role: CPI API Onboarding BOR

To review the pending approvals, go to https://test.home.idm.cms.gov

After logging into the system:

1. Select the 'Approvals' tile on "IDM Dashboard" page.
2. On the 'My Pending Approvals' page select a request(s).
3. Provide Justification in the text box
4. Click on "Approve Selected" or "Reject Selected" button for your decision

If you have questions or need assistance, please use the following information to contact the Application Help Desk:

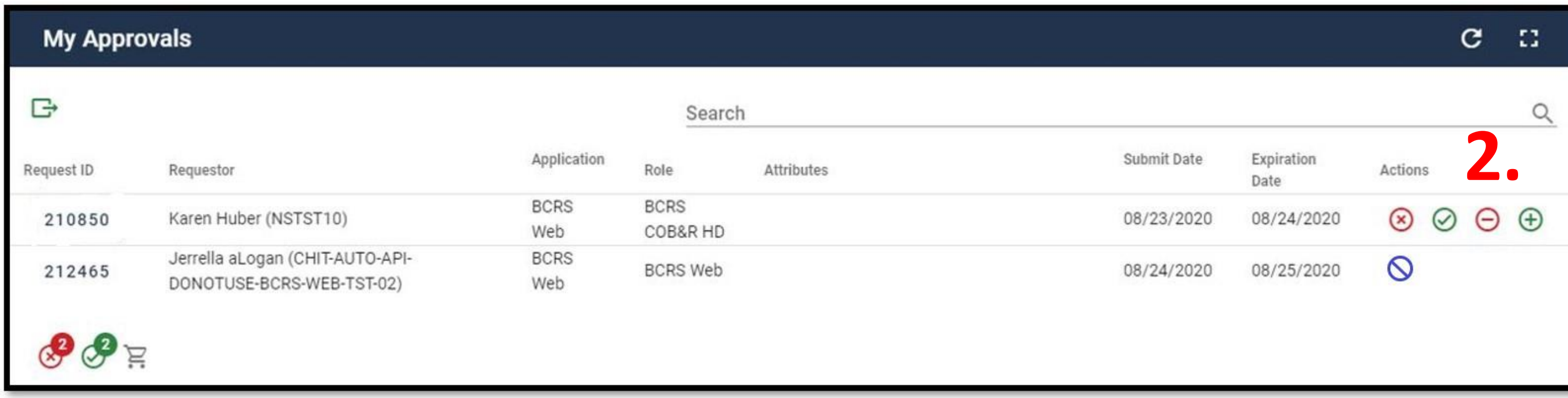
Support Desk
SampleTEST@test.com
123-456-7890

Thank you,
CMS Identity Management System

Please do not reply to this system generated email.

Approving Roles

1.

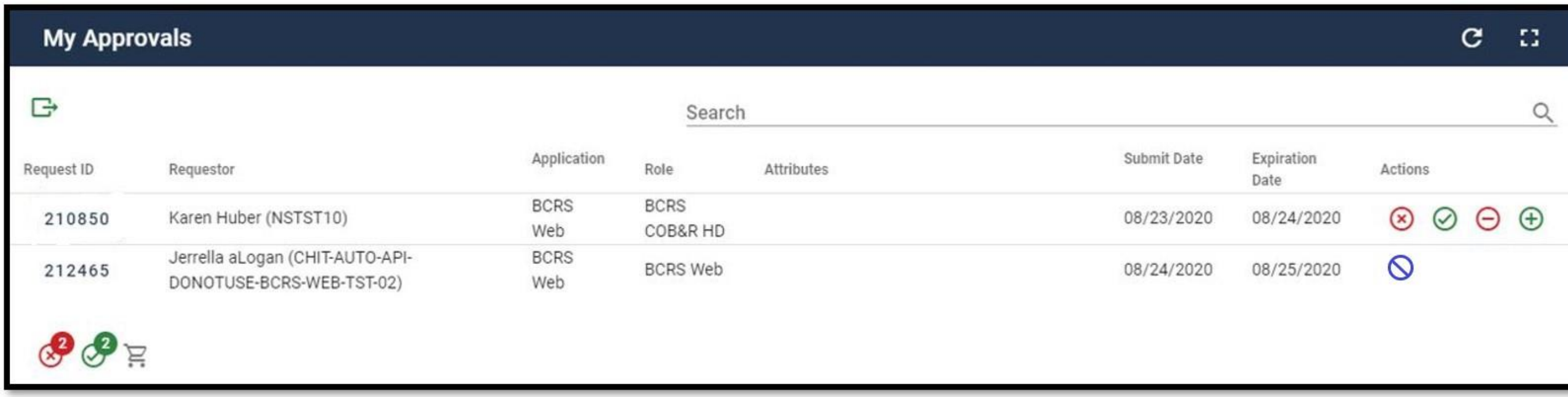


3.

1. Individual Request ID – you can click on the request ID to view more information about the request
2. Quick Action Buttons – (left – right) reject request, approve request, add to cart for rejection, add to cart for approval, the blue circle is to remove the request from the cart
3. Cart Buttons – (left – right) how many requests are rejected in the cart, how many requests are set to be approved in the cart, view cart

Approving Roles

4.



4. This green button allows you to export the list of requests

All requests whether approving or rejecting will require a justification