Office of the Chief Information Officer

Identity, Credential, and Access Management Program (ICAM)

MobileLinc Guide for Agency IT Support Sending a Push Notification

June 2023

Document Revision and History

***TABLE 1**: Document Revision and Version Information*

VERSION NO.	DATE	DESCRIPTION	AUTHOR/APPROVAL
1.0	5/2019	Initial Release	J.G.
1.0	5/2019	Branding, 508 Compliant	G.R.
1.1	12/2019	Updated screenshots for new website	J.G.
1.1	01/2020	Review, 508 Compliant	G.R.
1.2	01/2022	Updated screenshots, Other user guidance	K.K.
1.3	05/2022	Update Entrust App screenshots	K.K.
1.4	06/2023	Updated Alt Text and URLs	C.S.

Table of Contents

1. Introduction

1.0 Document Purpose

This document is a reference guide for using the MobileLinc admin role capabilities. This document provides detailed instructions for:

- Logging into the MobileLinc Admin interface
- Viewing the end user's MobileLinc credentials
- Sending a Push Notification to the user's MobileLinc credential(s)/ mobile device(s).

This document demonstrates how an IT Support Specialist can look up a user's record in IdentityGuard and send a push notification to the user's MobileLinc credential(s) on their mobile device(s). The purpose is to test that the MobileLinc service is working if the user has experienced issues. The root cause of the issue could be related to mobile device connectivity.

1.2 Audience

This document is intended for Agency IT Support Specialists that provision and support USDA mobile devices for end users.

1.3 Scope

This document provides information on MobileLinc administrative role capabilities that are assigned to Agency IT Support Specialists. This document is not a comprehensive guide for all MobileLinc administrative functionality. This document should be used by those meeting the "Audience" description and is not intended for dissemination to end-users.

1.4 ICAM Program Information

For more information on the ICAM program, visit our ICAM Customer Portal at URL:

https://usdagcc.sharepoint.com/sites/ICAM

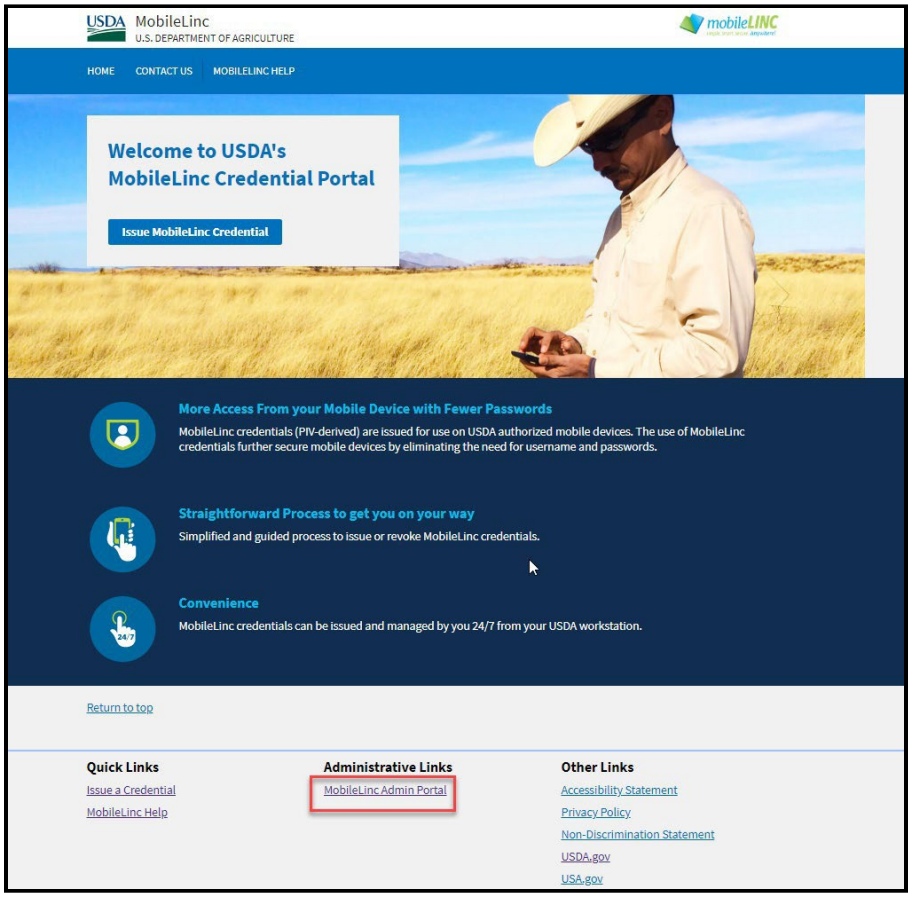
2. Log into MobileLinc

2.1 Access the MobileLinc Admin Interface

To access the MobileLinc Admin interface, go to the following URL:
https://mobilelinc.icam.usda.gov/home

Select the **MobileLinc Admin Portal** and log in with your LincPass.

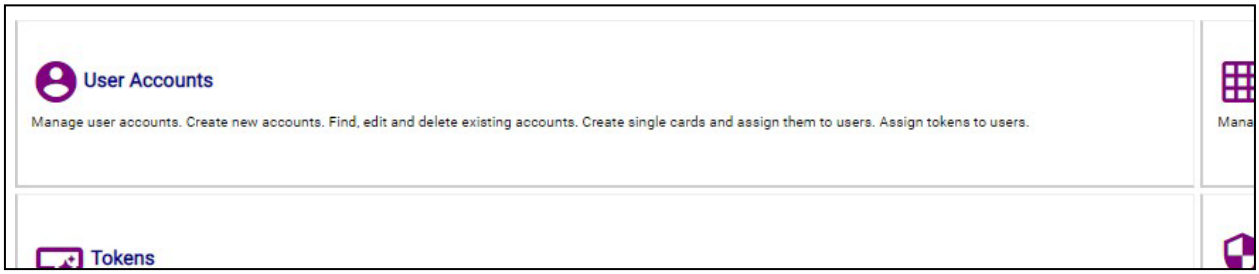
FIGURE 1: MobileLinc Self Service Module



2.2 Sending the Push Notification

After logging into the MobileLinc Admin Portal with your LincPass, select **User Accounts.**

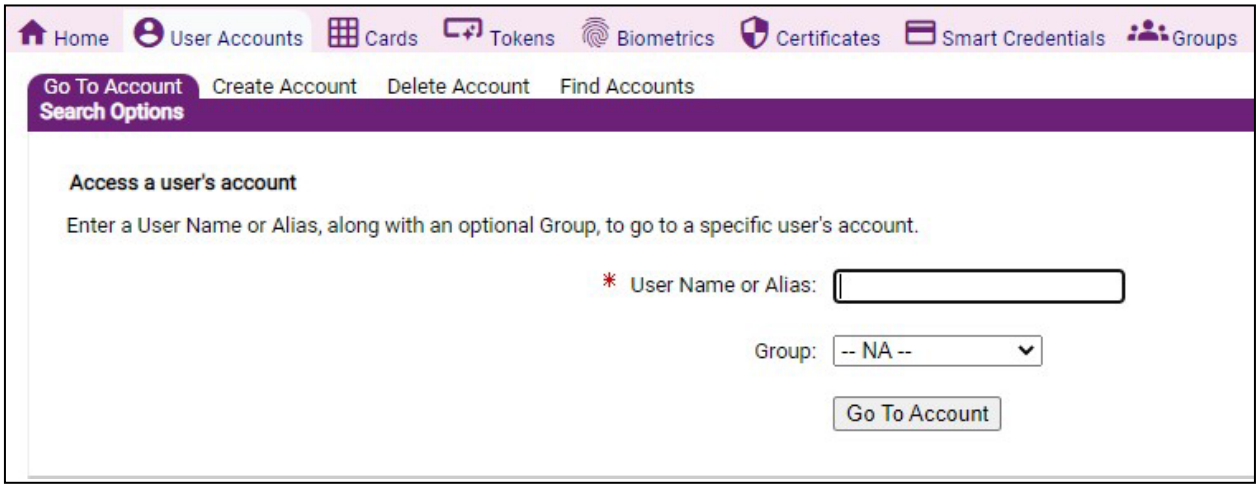
FIGURE 2: User Accounts



You can access a user's MobileLinc account by typing in their Alias, typically FirstName.LastName.

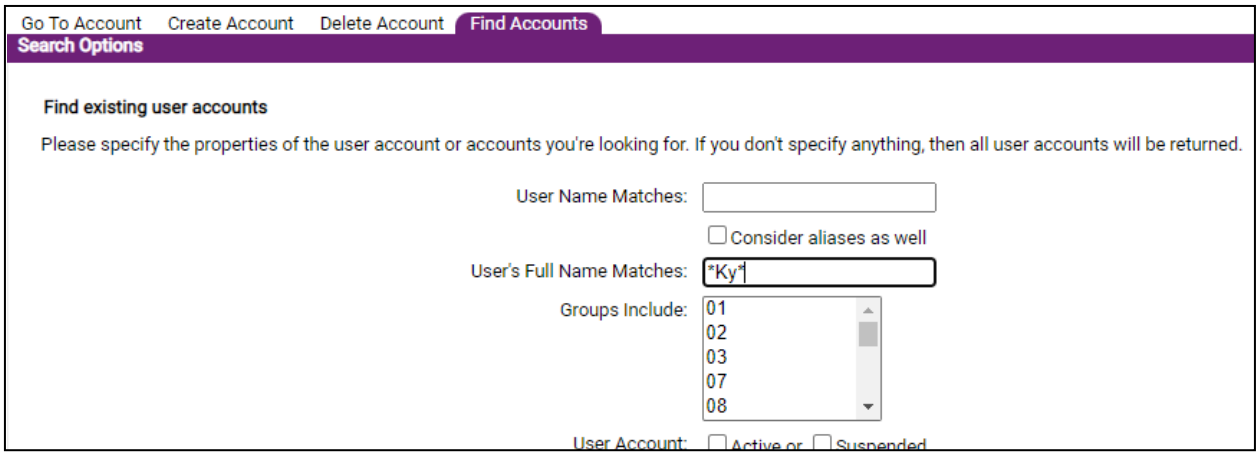
Do not enter a user's name, it does not map to their MobileLinc account

FIGURE 3a: Accessing a User's Account



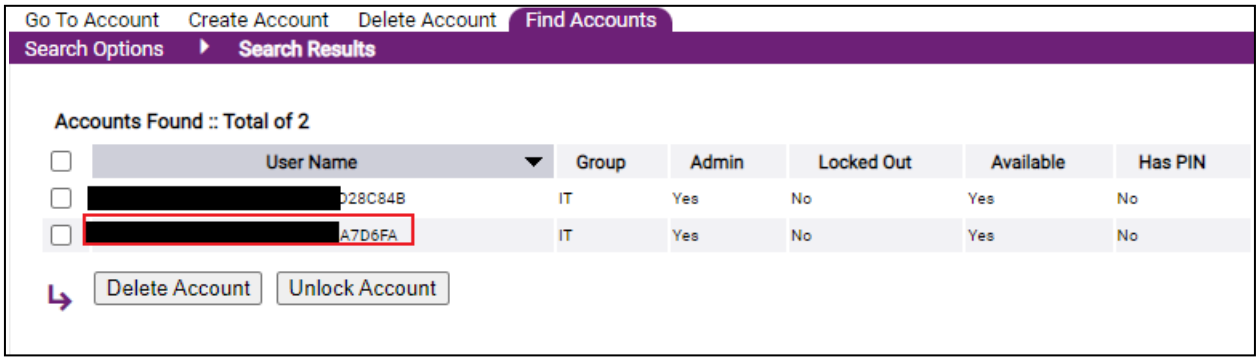
You can also select the **Find Accounts** tab and type a portion of their last name into the **User Full Name Matches** box. Use the * wildcard character before and after last name segment.

FIGURE 3b: Accessing a User's Account



Accounts that match the search criteria will be returned. Be as specific as possible to reduce the number of accounts that match the search.

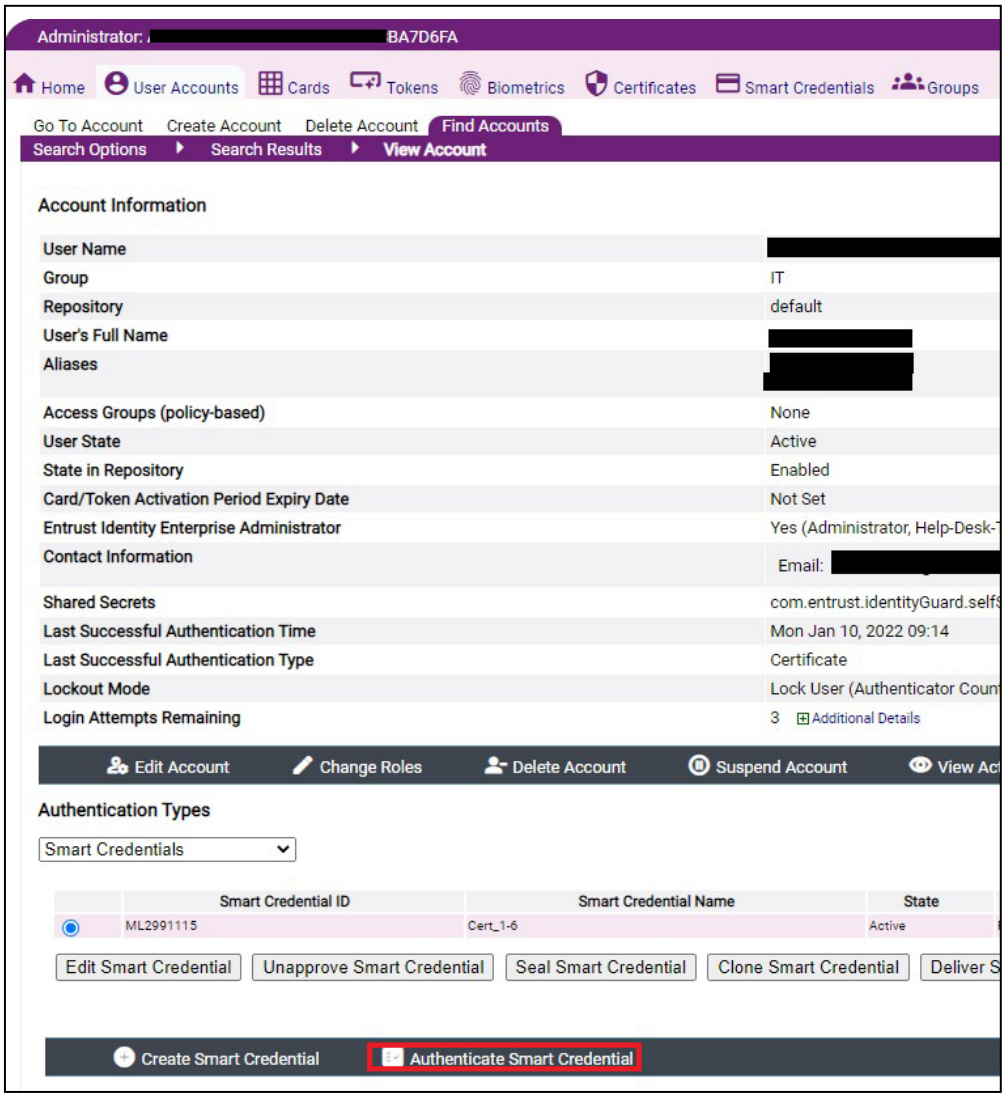
FIGURE 3c: Accessing a User's Account



Select the **User Name** (user's short PersonGUID) and the user's account information page will open.

At the bottom of the screen select the **Authenticate Smart Credential** button.

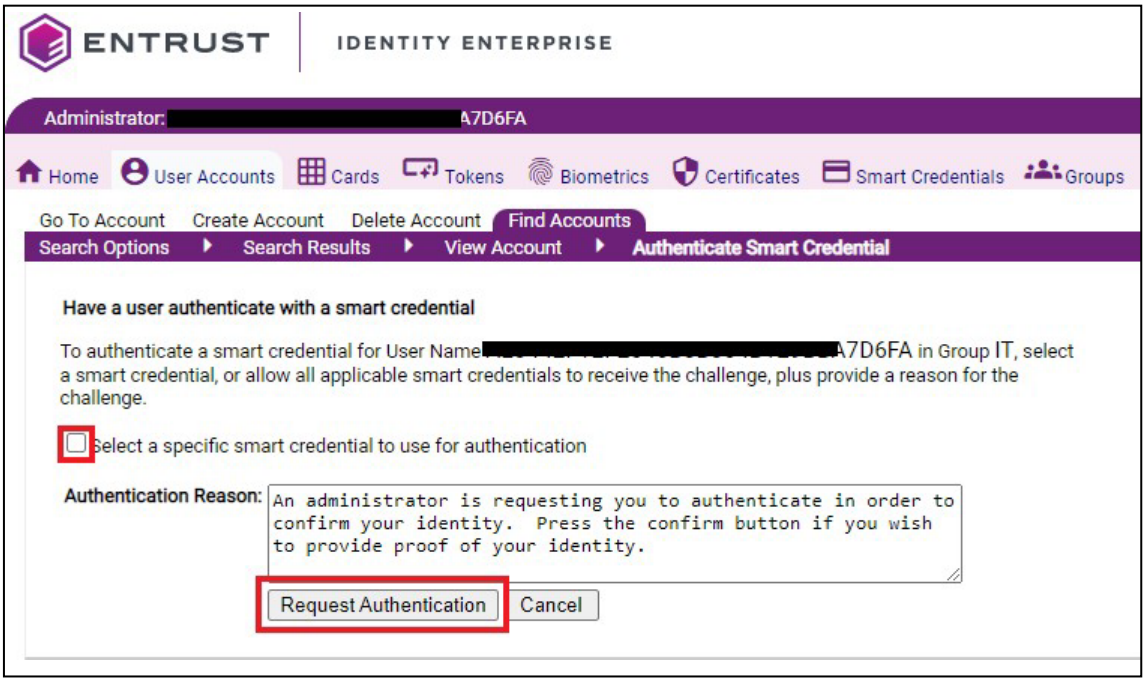
FIGURE 4: Authenticate Smart Credential



You can select a specific smart credential you wish to send a challenge to or if you leave the box unchecked all the user's credentials will receive an authentication challenge.

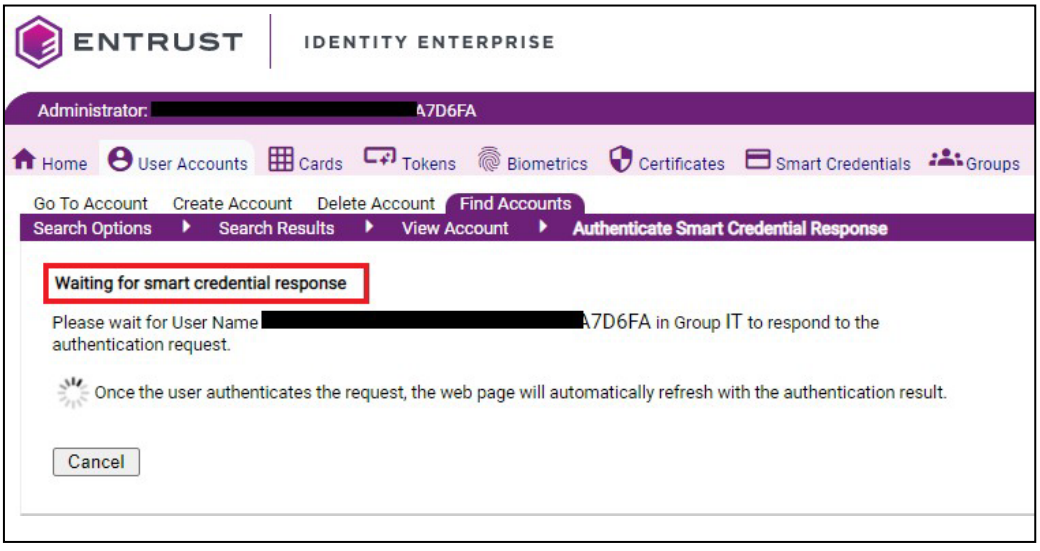
After making the choice of which credentials to issue a challenge to, select the **Request Authentication** button.

FIGURE 5: Request Authentication



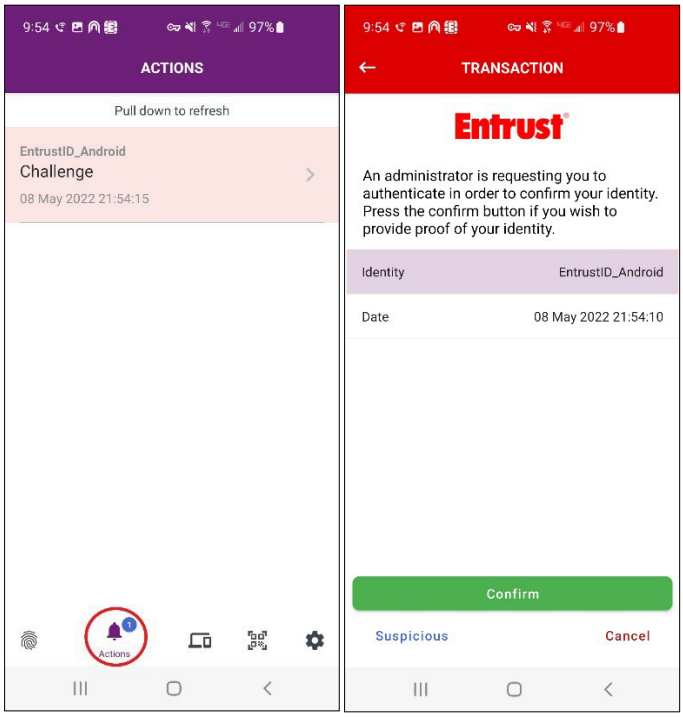
While you are waiting for the user to respond to the challenge you will get the following screen.

FIGURE 6: Waiting for Smart Credential Response



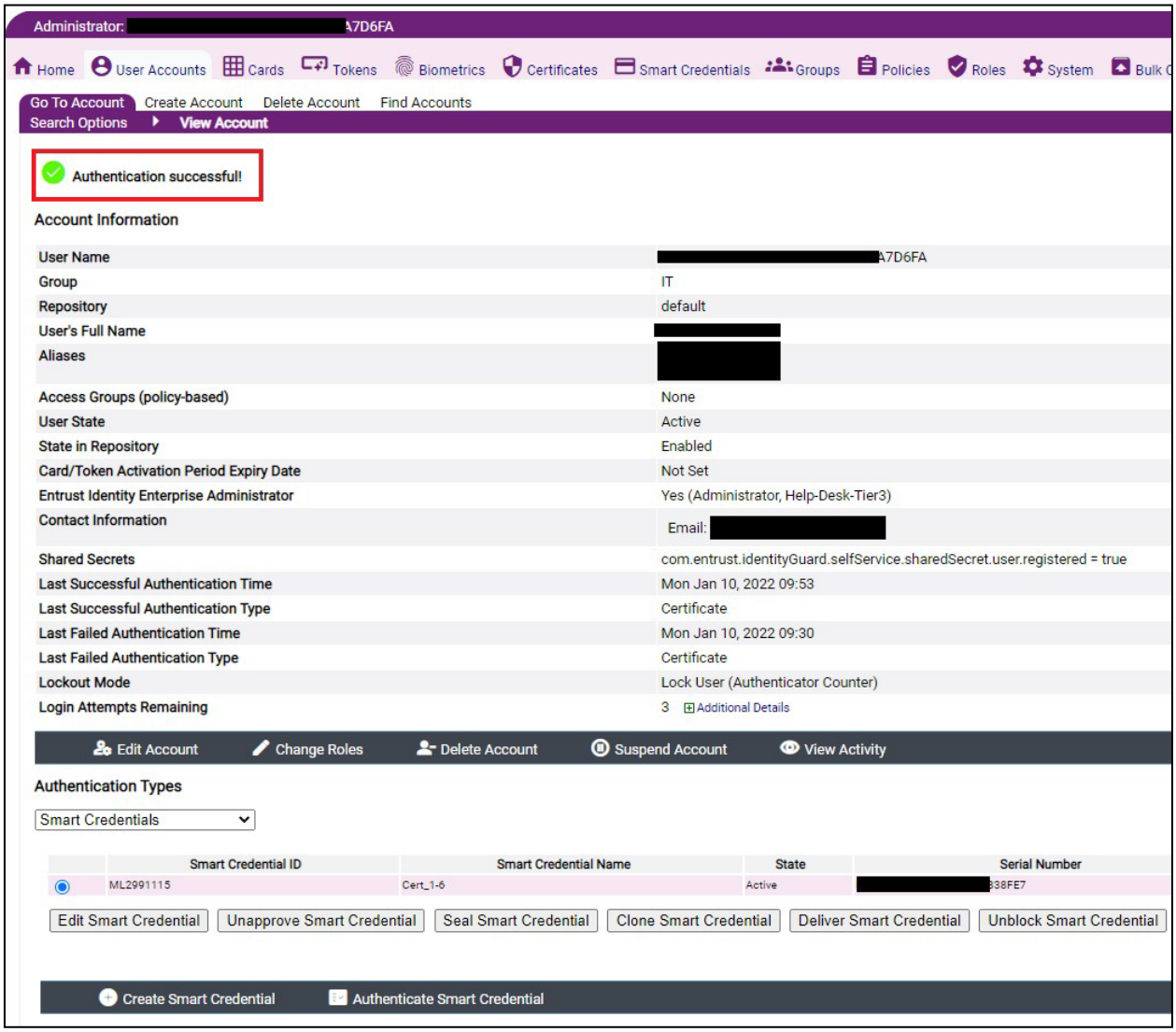
The user will receive a challenge within the Entrust Identity app under the "**Actions**" tab on their mobile device. The user should select the challenge and enter the pin, then respond to the challenge by confirming it in the Entrust Identity app on their mobile device.

FIGURE 7: Entrust Identity Action/Challenge Response



Once the user responds to the challenge, that will be indicated in the IDG admin portal.

FIGURE 8: Authentication Successful



3. Support

Escalate unresolved through your agencies Help Desk escalation process. Include the incident ID and details and results of all troubleshooting steps.

Important Note: Internal USDA workers listed in search results may not have a fully registered account for use in accessing eAuthentication-protected applications; however, roles can still be added to the user's record and then access will be permitted once they register. Also, users must use their LincPass to log on to MobileLinc Identity Guard.