



Office of the Chief Information Officer
Identity, Credential, and Access Management Program

MobileLinc Guide for Agency IT Support- Sending a Push Notification

December 2019

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.



Table of Contents

1. Introduction	4
1.0 Document Purpose	4
1.2 Audience	4
1.3 Scope	4
1.4 Terms & Definitions	4
2. Log into MobileLinc	4
2.1 Access the MobileLinc Admin Interface	4
2.2 Sending the Push Notification.....	5
3. Support	10

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 Terms & Definitions

For definitions see the [Identity, Credential, and Access Management \(ICAM\) Glossary](#) located on the [ICAM USDA Connect site](#).

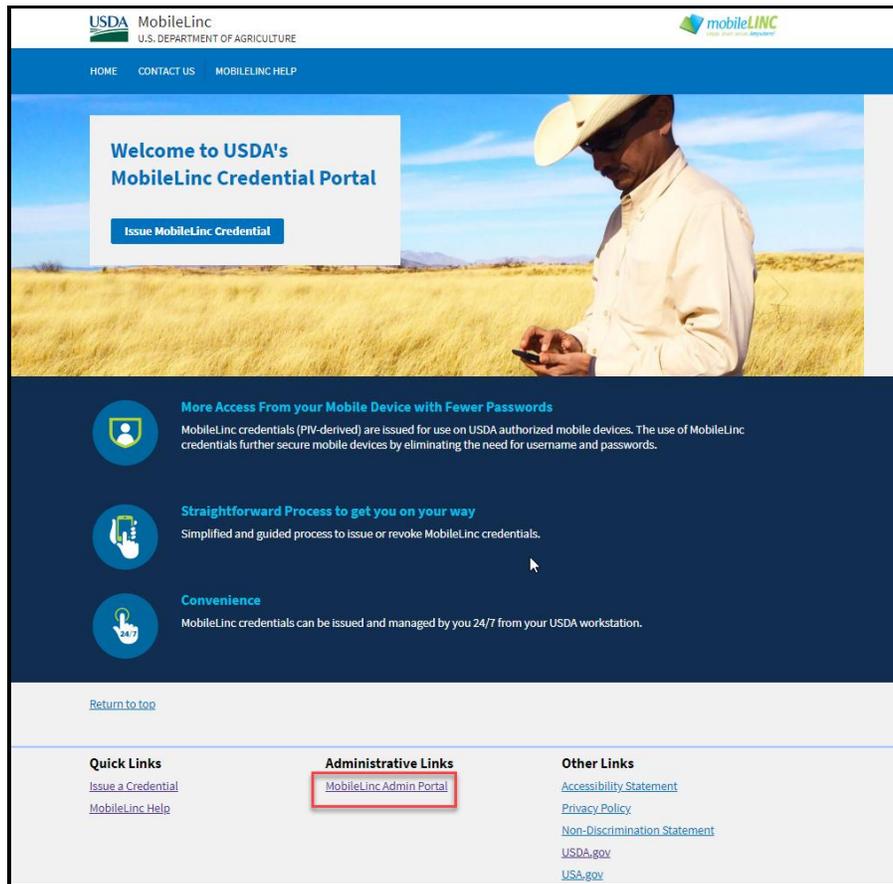
2. Log into MobileLinc

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

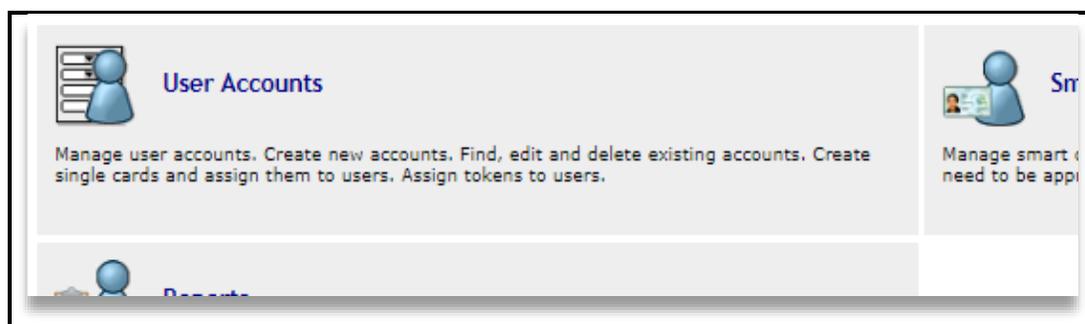
FIGURE 1: MobileLinc Self Service Module



2.2 Sending the Push Notification

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

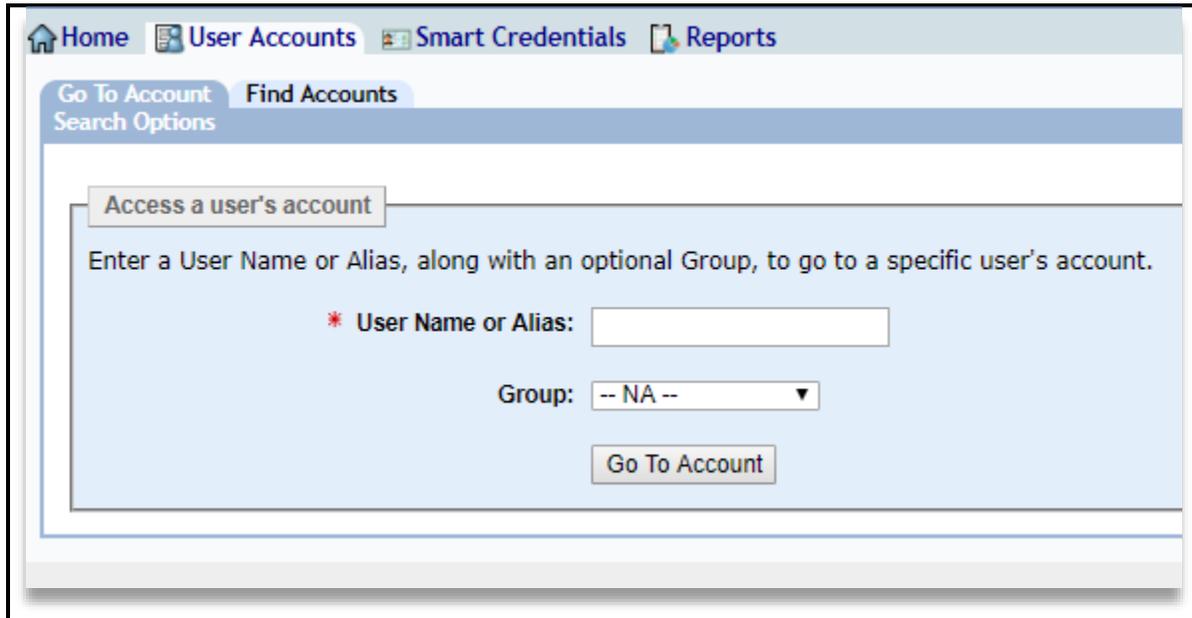
FIGURE 2: User Accounts



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

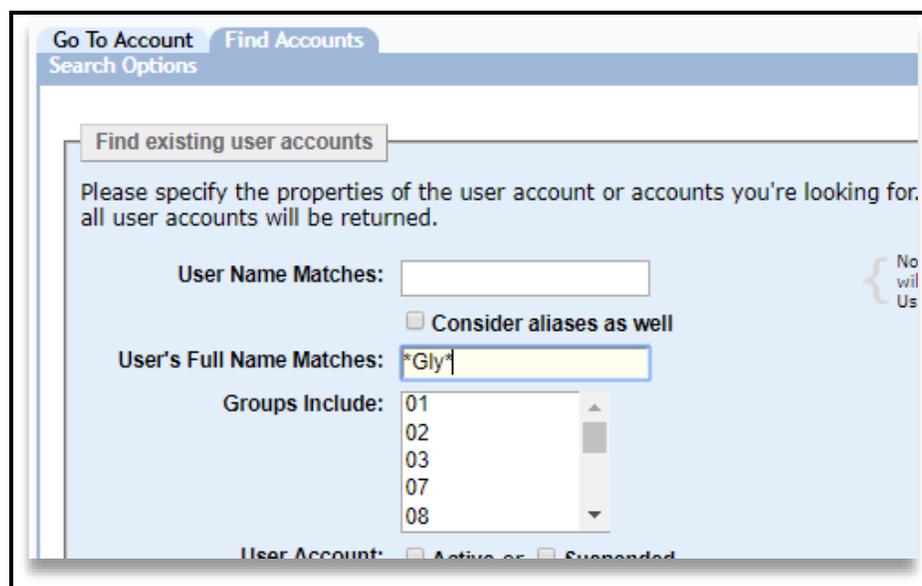
FIGURE 3a: Accessing a User's Account



The screenshot shows the 'Go To Account' form in the ICAM interface. The navigation bar includes 'Home', 'User Accounts', 'Smart Credentials', and 'Reports'. Below the navigation bar, there are tabs for 'Go To Account' and 'Find Accounts'. The 'Go To Account' tab is active, and the 'Search Options' section is visible. The form contains a title 'Access a user's account', a description 'Enter a User Name or Alias, along with an optional Group, to go to a specific user's account.', a required text input field for 'User Name or Alias', a dropdown menu for 'Group' with the value '-- NA --', and a 'Go To Account' button.

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.

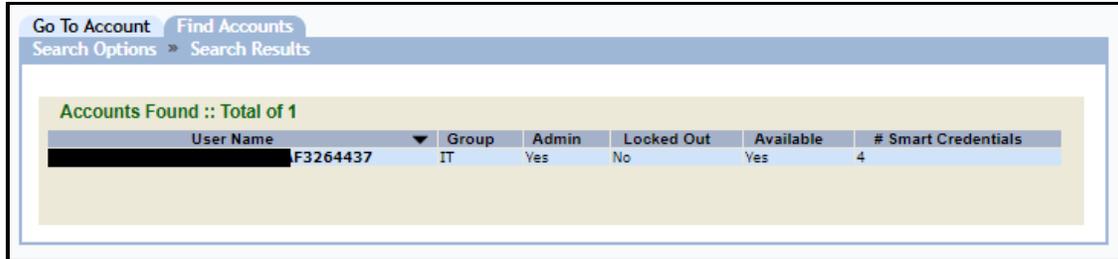
FIGURE 3b: Accessing a User's Account



The screenshot shows the 'Find Accounts' form in the ICAM interface. The navigation bar includes 'Home', 'User Accounts', 'Smart Credentials', and 'Reports'. Below the navigation bar, there are tabs for 'Go To Account' and 'Find Accounts'. The 'Find Accounts' tab is active, and the 'Search Options' section is visible. The form contains a title 'Find existing user accounts', a description 'Please specify the properties of the user account or accounts you're looking for; all user accounts will be returned.', a text input field for 'User Name Matches', a checkbox for 'Consider aliases as well', a text input field for 'User's Full Name Matches' with the value '*Gly*', a list box for 'Groups Include' with values 01, 02, 03, 07, and 08, and a 'User Account' section with checkboxes for 'Active or' and 'Suspended'.

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



Go To Account Find Accounts
Search Options » Search Results

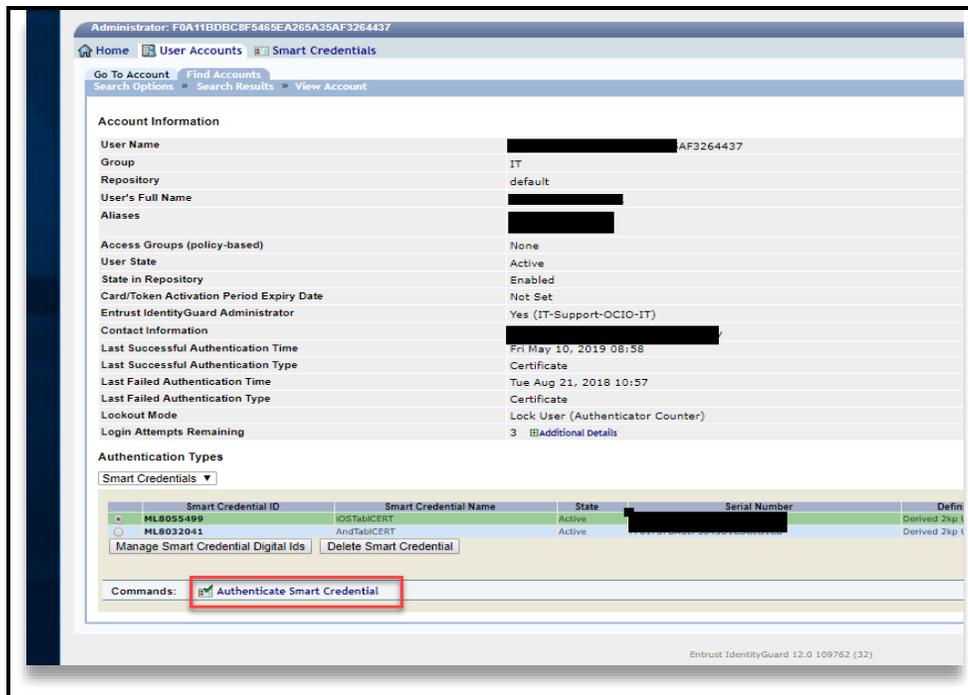
Accounts Found :: Total of 1

User Name	Group	Admin	Locked Out	Available	# Smart Credentials
[REDACTED] AF3264437	IT	Yes	No	Yes	4

Select the **User Name** (user's short person guid) 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



Administrator: F0A11BD8C8F5469EA265A35AF3264437

Home User Accounts Smart Credentials

Go To Account Find Accounts
Search Options » Search Results » View Account

Account Information

User Name [REDACTED] AF3264437

Group IT

Repository default

User's Full Name [REDACTED]

Aliases [REDACTED]

Access Groups (policy-based) None

User State Active

State in Repository Enabled

Card/Token Activation Period Expiry Date Not Set

Entrust IdentityGuard Administrator Yes (IT-Support-OCIO-IT)

Contact Information [REDACTED]

Last Successful Authentication Time Fri May 10, 2019 08:58

Last Successful Authentication Type Certificate

Last Failed Authentication Time Tue Aug 21, 2018 10:57

Last Failed Authentication Type Certificate

Lockout Mode Lock User (Authenticator Counter)

Login Attempts Remaining 3 [Additional Details](#)

Authentication Types

Smart Credentials

Smart Credential ID	Smart Credential Name	State	Serial Number	Defn
<input checked="" type="radio"/> MLB055499	iOSTabICERT	Active	[REDACTED]	Derived 256...
<input type="radio"/> MLB032041	AndTabICERT	Active	[REDACTED]	Derived 256...

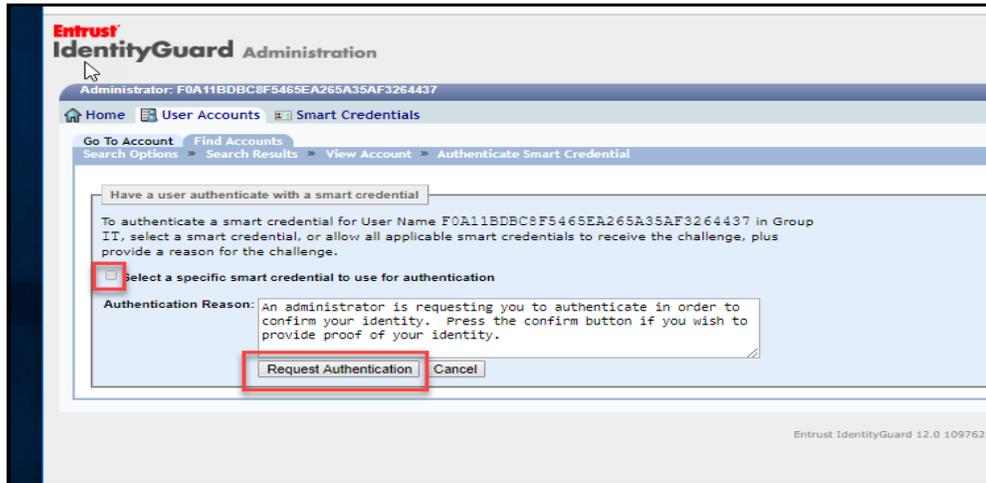
Manage Smart Credential Digital Ids Delete Smart Credential

Commands: Authenticate Smart Credential

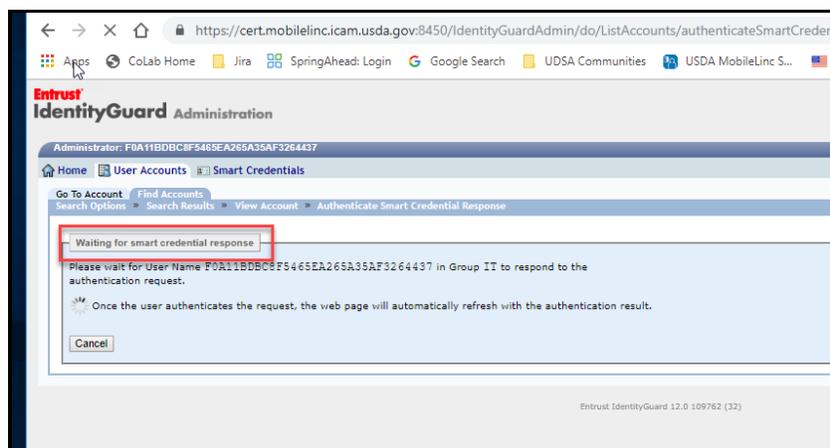
Entrust IdentityGuard 12.0.109762 (32)

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

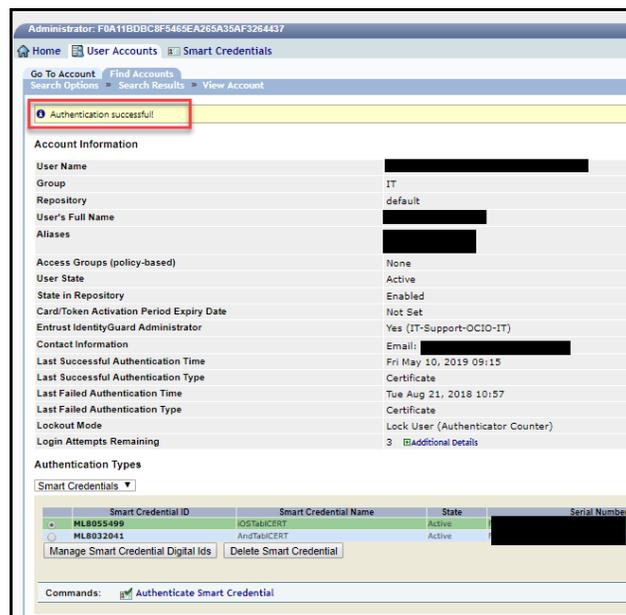
While you are waiting for the user to respond to the challenge you will get the following screen.

FIGURE 6: Waiting for Smart Credential Response

The user will receive an Entrust challenge on their mobile device. The user should respond to the challenge by confirming it in the Entrust app on their mobile device.

FIGURE 7: User Mobile Device Screens/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.