Office of the Chief Information Officer

Identity, Credential, and Access Management Program (ICAM)

MobileLinc Guide for Agency IT Support

June 2023

Document Revision and History

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

VERSION NO.	DATE	DESCRIPTION	AUTHOR/APPROVAL
1.0	05/2019	Initial Release	J.G.
1.0	05/2019	Branding, Review and 508 Compliant	G.R.
2.0	10/2019	Added section for PersonGuid	J.G.
2.0	10/2019	Branding, Review and 508 Compliant	G.R.
2.1	12/2019	Updated screenshots for new website	J.G.
2.1	01/2020	Review, 508 Compliant	G.R.
2.2	01/2022	Updated Screenshots, Other user	K.K.
2.3	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 record/MobileLinc credentials
- Checking the user's record in Mobile Iron console for the USDA-PersonGuid flag
- Revoking a user's MobileLinc credentials

This document demonstrates how an IT Support Specialist can review/revoke a user's MobileLinc credentials. MobileLinc user role qualifications are:

- The user has a USDA issued mobile device and
- The user has an active LincPass.

This document also demonstrates how an IT Support Specialist can determine root cause and escalate the issue of a user not being able to log into the MobileLinc website.

1.2 Audience

This document is intended for Agency IT Support Specialists that provision USDA mobile devices for end users. Agency IT Support Specialists manage USDA mobile devices and can wipe or retire a user's mobile device. They can also respond to and troubleshoot issues users have using their mobile device.

1.3 Scope

This document provides information on the 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

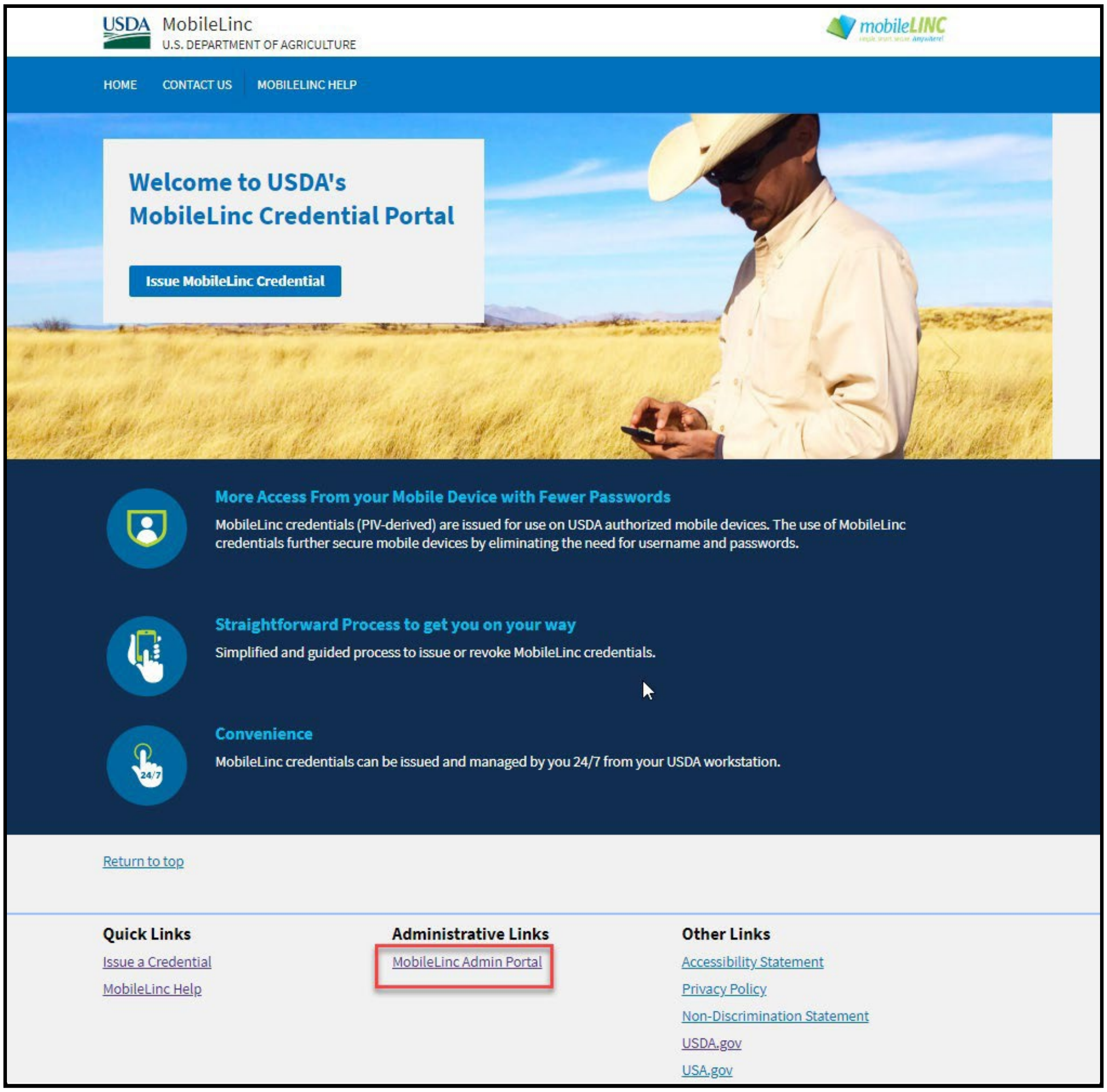
2. Logging into the MobileLinc Admin Interface

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



USDA MobileLinc
U.S. DEPARTMENT OF AGRICULTURE

Welcome to USDA's MobileLinc Credential Portal

More Access From your Mobile Device with Fewer Passwords

MobileLinc credentials (PIV-derived) are issued for use on USDA authorized mobile devices. The use of MobileLinc credentials further secure mobile devices by eliminating the need for username and passwords.

Straightforward Process to get you on your way

Simplified and guided process to issue or revoke MobileLinc credentials.

Convenience

MobileLinc credentials can be issued and managed by you 24/7 from your USDA workstation.

Return to top

Quick Links
Issue a Credential
MobileLinc Help

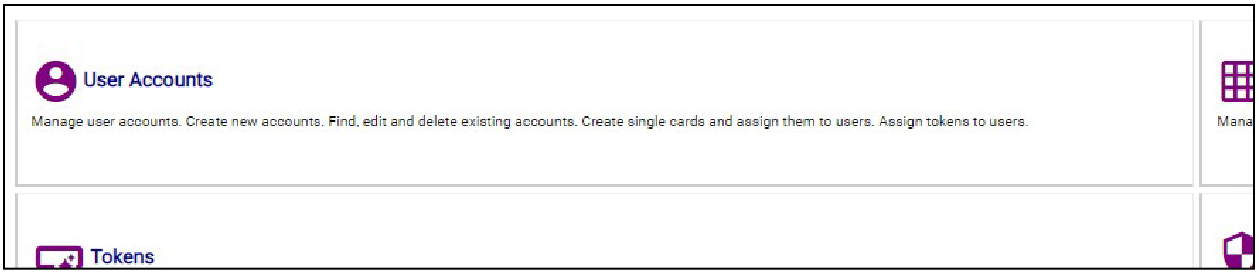
Administrative Links
MobileLinc Admin Portal

Other Links
Accessibility Statement
Privacy Policy
Non-Discrimination Statement
USDA.gov
USA.gov

2.2 View a User’s Account

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

FIGURE 2: User Accounts

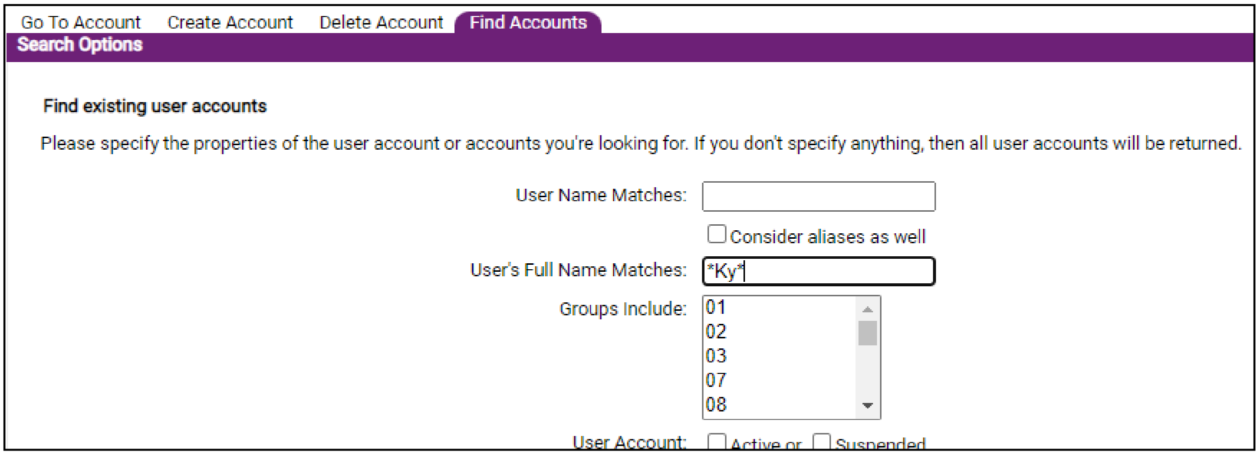


User Accounts

Manage user accounts. Create new accounts. Find, edit and delete existing accounts. Create single cards and assign them to users. Assign tokens to users.

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 3: Accessing a User’s Account



Search Options

Find existing user accounts

Please specify the properties of the user account or accounts you're looking for. If you don't specify anything, then all user accounts will be returned.

User Name Matches:

□ Consider aliases as well

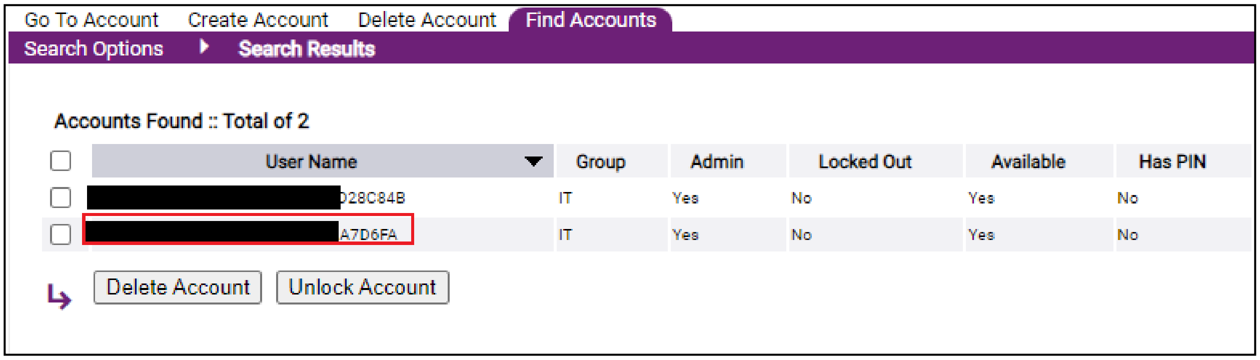
User's Full Name Matches: *Ky*

Groups Include: 01 02 03 07 08

User Account: □ Active or □ 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. If a large number of records are returned as in when the last name is a common name, you have the alternate method of looking up the users record in EEMS and putting their usdaShortPersonGUID into the User Name Matches box. That will return only one record.

FIGURE 4: Accessing a User’s Account



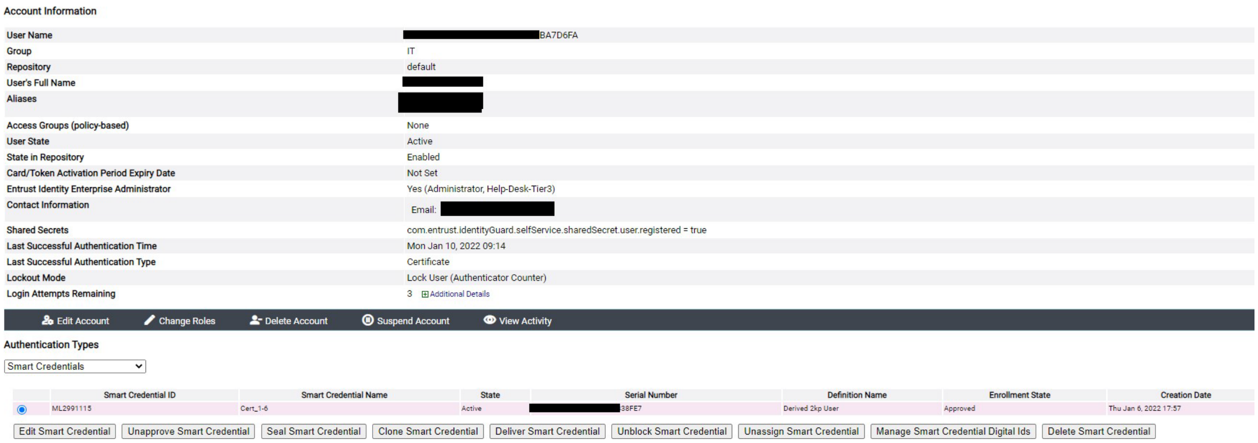
Accounts Found :: Total of 2

☐	User Name	Group	Admin	Locked Out	Available	Has PIN
☐	[redacted]D28C84B	IT	Yes	No	Yes	No
☐	[redacted]A7D6FA	IT	Yes	No	Yes	No

Once you have the user record, select the **User Name** (USDA ShortPersonGUID) and the user's account will open.

A quick check of the health of a user's account would be that the **User State** is Active, **Login Attempts Remaining** is greater than zero, and if the user has a Smart Credential listed, the **State** is Active, there is a **Serial Number**, and the **Enrollment State** is Approved.

FIGURE 5: User Account Information


Account Information

User Name	[redacted]BA7D6FA
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 Identity Enterprise Administrator	Yes (Administrator, Help-Desk-Tier3)
Contact Information	Email: [redacted]
Shared Secrets	com.entrust.identityGuard.selfService.sharedSecret.user.registered = true
Last Successful Authentication Time	Mon Jan 10, 2022 09:14
Last Successful Authentication Type	Certificate
Lockout Mode	Lock User (Authenticator Counter)
Login Attempts Remaining	3 ⊞ Additional Details

Authentication Types

Smart Credentials

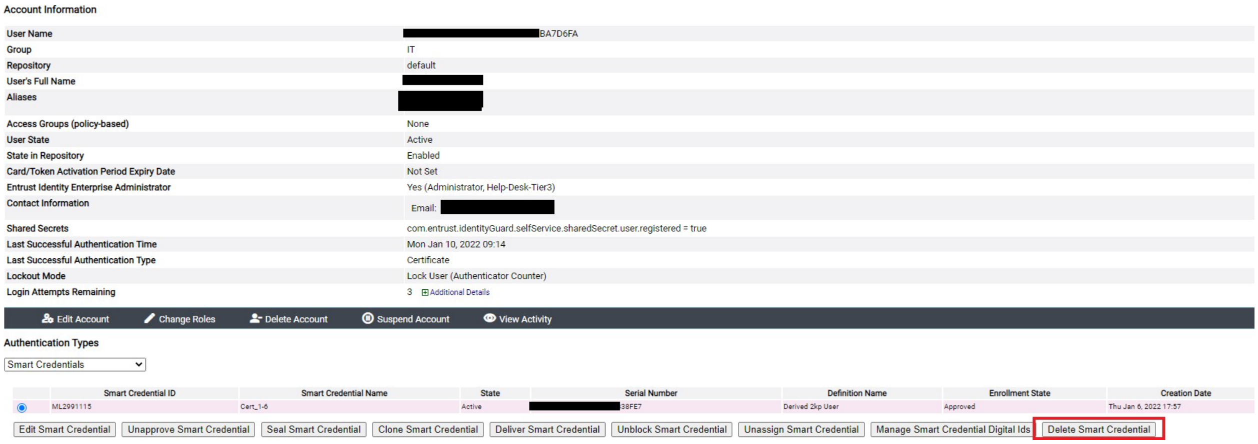
	Smart Credential ID	Smart Credential Name	State	Serial Number	Definition Name	Enrollment State	Creation Date
●	ML2991115	Cert_1-6	Active	[redacted]38FE7	Derived 2kp User	Approved	Thu Jan 6, 2022 17:57

2.3 Revoking a User's MobileLinc Credential

Revoking a MobileLinc credential is a self-service action the user can do by themselves, however if a user seeks assistance from the Help Desk, the IT Specialist can revoke the user's credential(s) after logging into the MobileLinc Admin portal.

To revoke a user's MobileLinc credential, open the user's account. If the user has active credentials there will be a **Delete Smart Credential** button at the bottom of the page. To revoke a credential, select the **radio button** to the left of the Smart Credential ID to be revoked then **select Delete Smart Credential**. You will be asked if you are sure you want to delete the smart credential. Select OK and the credential will be revoked. You can log out of the MobileLinc Admin portal.

FIGURE 6: Revoking a Credential



Account Information

User Name	[redacted]BA7D6FA
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 Identity Enterprise Administrator	Yes (Administrator, Help-Desk-Tier3)
Contact Information	Email: [redacted]
Shared Secrets	com.entrust.identityGuard.selfService.sharedSecret.user.registered = true
Last Successful Authentication Time	Mon Jan 10, 2022 09:14
Last Successful Authentication Type	Certificate
Lockout Mode	Lock User (Authenticator Counter)
Login Attempts Remaining	3 ⊞Additional Details

Authentication Types

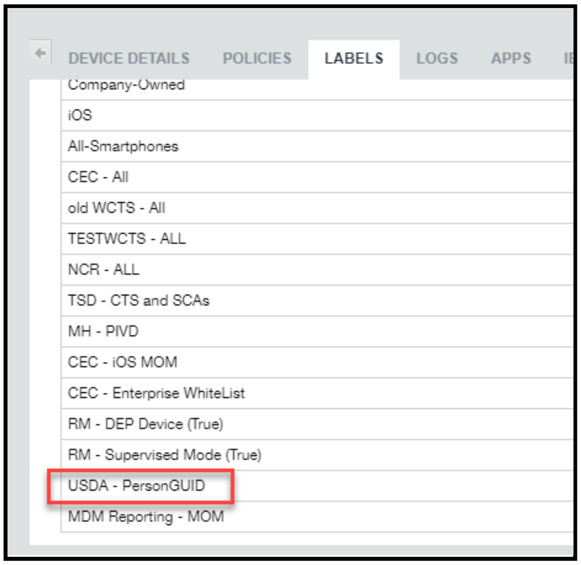
Smart Credentials

	Smart Credential ID	Smart Credential Name	State	Serial Number	Definition Name	Enrollment State	Creation Date
●	ML2991115	Cert_1-6	Active	[redacted]38FE7	Derived 2kp User	Approved	Thu Jan 6, 2022 17:57

2.4 User Cannot Log into the MobileLinc Website

MobileLinc User accounts are automatically created when the user gets a mobile device. If the user's MobileLinc account is not created, the user will get an "**Invalid LincPass**" message when trying to log into the MobileLinc website. A user's MobileLinc account will not be created if the user's PersonGUID has not been added to their AD account. The IT Specialist can check this by logging into the Mobile Iron console and look at the user's Mobile Iron record. If the PersonGUID has been added to the user's account, you will see the USDA-PersonGUID label as shown below. If the label is not present the PersonGUID must be added to the user's AD account.

FIGURE 7: USDA PersonGUID



Company-Owned
iOS
All-Smartphones
CEC - All
old WCTS - All
TESTWCTS - ALL
NCR - ALL
TSD - CTS and SCAs
MH - PIVD
CEC - iOS MOM
CEC - Enterprise WhiteList
RM - DEP Device (True)
RM - Supervised Mode (True)
USDA - PersonGUID
MDM Reporting - MOM

Once the user's Personguid has been added to the user's AD account, the user can do a "Force Device Check-in" on an Android or a "Check for Updates" on an Apple device, which will initiate the creation of their MobileLinc account. The actual time needed to create the account will depend on network connections and bandwidth.

2.5 MobileLinc Account Locked Out

If a user does not respond to an Entrust challenge and this occurs three times in a row the user's IDG account will be locked. When this happens, the user will not be able to log into the MobileLinc website. The account will automatically be unlocked after 15 minutes, but the flag that the account was locked will still be on the user's account. This will prevent an IT Support Specialist from doing a Push Notification from the user's IDG record when the IT Support Specialist has logged into the MobileLinc Admin Portal and has the user's IDG record open.

To clear the account locked out flag requires the user to respond to a Push Notification. The simplest way to do this is to provide the self-service Push Notification tool URL to the user. The URL is https://www.eauth.usda.gov/TestResources/USDA/LincPass_MobileLinc_Auth_Scheme/Protected.asp

Note: The User must be within the USDA domain to use the URL.

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.