

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**

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	К.К.
1.3	05/2022	Update Entrust App screenshots	К.К.
1.4	06/2023	Updated Alt Text and URLs	C.S.

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

### **Table of Contents**

1.	Inti	roduction	
	1.0	Document Purpose	4
	1.2	Audience	4
	1.3	Scope	4
	1.4	Terms & Definitions	4
2.	Log	; into MobileLinc	4
	2.0	Access the MobileLinc Admin Interface	4
	2.1	Sending the Push Notification	5
3.	Sup	pport1	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 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: <u>https://mobilelinc.icam.usda.gov/home</u>

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

Identity, Credential, and Access Management (ICAM) MobileLinc User Guide for Sending Push Notification

FIGURE 1: MobileLinc Self Service Module

USDA MobileLinc	RICULTURE	
HOME CONTACT US MOBIL	ELINC HELP	
Welcome to US MobileLinc Cred	dential Portal	
MobileLinc c	ss From your Mobile Device with Fewer Par edentials (PIV-derived) are issued for use on USDA a rither secure mobile devices by eliminating the need	uthorized mobile devices. The use of MobileLinc
	rward Process to get you on your way d guided process to issue or revoke MobileLinc cred	entials.
Convenier MobileLinc c	ce edentials can be issued and managed by you 24/7 fr	om your USDA workstation.
Return to top		
Quick Links Issue a Credential MobileLinc Help	Administrative Links MobileLincAdmin Portal	Other Links Accessibility Statement Privacy Policy Non-Discrimination Statement USDA.gov USA.gov

### 2.2 Sending the Push Notification

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

Ouser 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.	Mana
Tokens	0

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

Page | 5

Identity, Credential, and Access Management (ICAM)
MobileLinc User Guide for Sending Push Notification

FIGURE 3a: Accessing a User's Account

A Home	<b>O</b> User Accounts	Cards	Tokens	Biometrics	Certificat	es 🗧 Smart Credentials	Groups
	ccount Create Acc	count Delete	Account	Find Accounts			
Search C	puons						
Acces	ss a user's account						
Enter	a User Name or Alia	s, along with a	n optional G	roup, to go to a sp	ecific user's ac	count.	
				* User Nam	e or Alias:		
					Group:	NA 🗸	
					G	o To Account	
					pillenenen		

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

Go To Account	Create Account	Delete Account	Find Accounts			
Search Options						
Find existing u	user accounts					
Please specify	the properties of t	the user account o	r accounts vou're loo	oking for. If	f vou don't specify anything	, then all user accounts will be returned.
			,		· · · · · · · · · · · · · · · · · · ·	
			User Name N	Matches:		7
					Consider aliases as we	
			the sele faill blocks a			
			User's Full Name N	Matches:	*Ky*	
			Groups	s Include:	01 🔺	
					02	
					03	
					07	
					• 80	
			User	Account:	Active or Suspender	1

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

#### Identity, Credential, and Access Management (ICAM) MobileLinc User Guide for Sending Push Notification

		FIC	GURE 3c: Access	ing a User's	Account		
Go To Account	Create Account	Delete Account	Find Accounts				
Search Options	Search Res	ults					
Accounts For	und :: Total of 2 User Nam	e	Group	Admin	Locked Out	Available	Has PIN
		28C84B	т	Yes	No	Yes	No
	/	A7D6FA	ІТ	Yes	No	Yes	No
Ly Delete	Account Unloc	k 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 S	Smart Credential
--------------------------	------------------

Home 🖲 User Accounts 🌐 Cards 🎞 Tokens 🖗 Biometrics 😯		
Go To Account         Create Account         Delete Account         Find Accounts           Search Options         Image: Search Results         View Account		
Account Information		
User Name		
Group	IT	
Repository	default	
User's Full Name		
Aliases		
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 (Admi	inistrator, Help-D
Contact Information	Email:	
Shared Secrets	com.entru	st.identityGuard.
Last Successful Authentication Time	Mon Jan 1	10, 2022 09:14
Last Successful Authentication Type	Certificate	9
Lockout Mode	Lock User	(Authenticator C
Login Attempts Remaining	3 ⊞ Additi	ional Details
🍰 Edit Account 🛛 🥒 Change Roles 🛛 🐣 Delete Accour	nt 🛛 🛈 Suspend Account	t 💿 Viev
Authentication Types		
Smart Credentials		
Smart Credential ID Smart	t Credential Name	State
ML2991115 Cert_1-6		Active
Edit Smart Credential Unapprove Smart Credential Seal Smart C	Credential Clone Smart Cre	dential Deliv
Ear onan oredential onapprove on an oredential Sear Shart o		Delly

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.

	IDENTITY ENTERPRISE
Administrator:	47D6FA
	Cards Tokens Biometrics Certificates Smart Credentials Croups
	rch Results View Account Authenticate Smart Credential
a smart credential, or allo challenge.	redential for User Name The Select A7D6FA in Group IT, select wall applicable smart credentials to receive the challenge, plus provide a reason for the tredential to use for authentication
	An administrator is requesting you to authenticate in order to confirm your identity. Press the confirm button if you wish to provide proof of your identity. RequestAuthentication Cancel

#### 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

IDENTITY ENT	ERPRISE		
47D6F	FA		
		B Smart Credentials	Groups
A CONTRACTOR OF A CONTRACTOR O	and the second	Credential Response	
itial response			
ne	A7D6FA in Group I	T to respond to the	
enticates the request, the we	b page will automatically refresh w	ith the authentication resu	ult.
	A7D6 Cards Tokens coount Delete Account arch Results View Ac titial response	A7D6FA Cards Tokens Biometrics Certificates count Delete Account Find Accounts arch Results View Account Authenticate Smart ( tital response ne A7D6FA in Group I	A7D6FA Cards Tokens Biometrics Certificates Smart Credentials coount Delete Account Find Accounts arch Results View Account Authenticate Smart Credential Response tial 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.

9:54 🧐 🖪 🏟 🏭	ब्द्र 📲 🖗 पड	al 97% 🗎	41	9:54 📽 🖻 🅅 📳	cə 📢 💱	∝.⊪ 97%∎	
ACTIONS			÷	TRANSACTION			
Pull down to refresh			Entrust	e I			
EntrustID_Android Challenge 08 May 2022 21:54:15			>	An administrator is requesting you to authenticate in order to confirm your identity. Press the confirm button if you wish to provide proof of your identity.			
				Identity		EntrustID_Android	
				Date	08 M	ay 2022 21:54:10	
					Confirm		
Actions		50° 2°%	\$	Suspicious		Cancel	
III	O	<		111	0	<	

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

Administrator: 47D6FA							
Home OUser Accounts Cards Tokens	Biometrics 😯 Certificates	B Smart Credentials	Groups	B Policies	Roles	💠 System	Bulk
Go To Account Create Account Delete Account Fir Search Options View Account	nd Accounts						
Authentication successful!							
Account Information							
User Name				A7D6FA			
Group		IT					
Repository		default					
User's Full Name							
Aliases							
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 (Administra	tor, Help-Desk-	Tier3)			
Contact Information		Email:					
Shared Secrets		com.entrust.ide	ntityGuard.self	Service.share	dSecret.use	r.registered =	true
Last Successful Authentication Time		Mon Jan 10, 203	22 09:53				
Last Successful Authentication Type		Certificate					
Last Failed Authentication Time		Mon Jan 10, 20	22 09:30				
Last Failed Authentication Type		Certificate					
Lockout Mode		Lock User (Auth	enticator Cour	nter)			
Login Attempts Remaining		3   Additional D	etails				
🍰 Edit Account 🥒 Change Roles	🐣 Delete Account 🛛 🔘	Suspend Account	💿 View Ac	ctivity			
Authentication Types							
Smart Credentials							
Smart Credential ID	Smart Credential N	lama	State		Se	rial Number	
ML2991115	Cert_1-6	Act			38F		
Edit Smart Credential Unapprove Smart Creden	tial Seal Smart Credential	Clone Smart Credenti	al Deliver S	Smart Creden	tial Unb	lock Smart C	redential
🕂 Create Smart Credential 🛛 🔛 Authen	iticate Smart Credential						

### 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.