

E911 Cloud Solutions & Single Sign-On Interface Control Document

Version 1.2 | June 23, 2023

© 2023 by RedSky Technologies, Inc., All rights reserved.



Copyright © 2023 by RedSky Technologies, Inc.

All rights reserved. No part of this publication may be reproduced, distributed, or transmitted in any form or by any means, including photocopying, recording, or other electronic or mechanical methods, without the prior written permission of RedSky Technologies, Inc., except in the case of brief quotations embodied in critical reviews and certain other noncommercial uses permitted by copyright law. For permission requests, write to RedSky Technologies, Inc., addressed "Attention: Permissions Coordinator," at the address below.

RedSky Technologies, Inc. 333 North Michigan Avenue, Suite 1600 Chicago, IL 60601 www.redskye911.com

E911 Anywhere<sup>®</sup>, Horizon Mobility<sup>®</sup>, MyE911<sup>®</sup>, and HELD+<sup>®</sup> are registered trademarks of RedSky Technologies, Inc.



#### **Revision History**

Date	Version	Revision	Made By
05/30/2023	0.1	Initial Draft	Katrina Vlasich
06/06/2023	1.0	Adjusted wording in Section 4.1 and 4.2 based on feedback, mitigating possible confusion.	Katrina Vlasich
06/08/2023	1.1	Updated URLs and added disclaimer statement.	Katrina Vlasich
06/23/2023	1.2	Added important information about SSO not being supported on the EON client.	Katrina Vlasich



# Table of Contents

Introdu	ction	. 2
1	Requirements	. 3
2	Building the Application Integration	. 4
2.1	RedSky: Determine API Name	. 4
2.2	RedSky: Share Assertion and Audience URLs with Organization	. 4
2.3	Organization: Create Application Integration	. 5
3	Application Configuration Information	. 7
3.2	Security Hash Algorithm	. 8
4	E911 Anywhere®/Horizon Mobility® Configuration	10
4.1	Organization Level SSO Configuration	10
4.2	Organization Administrator SSO Configuration	11
5	Testing	13
5.1	RedSky/Organization Administrator SSO User Login	13
5.2	RedSky/Organization Administrator Local-User Login	14



# Introduction

RedSky has introduced the ability for users of the E911 Anywhere®/Horizon Mobility® admin portals to login using their identity provider's SSO service. This integration allows for a higher level of security and provides users of the admin portal with an improved UX by making the login process much smoother.

System level, Service Provider, Reseller/Business Partner, and Customer level administrators can use the integration if the organization (including System) and administrators are correctly configured.

This document covers what information will be needed and what steps must be taken by RedSky and a customer, for integration to be successful.



# 1 Requirements

To complete the integration steps outlined below, some perquisites must be met:

- 1. The organization is using and is familiar with configuring application integrations on the admin console of their identity provider (IdP).
- 2. The identity provider (IdP) supports SAML 2.0 protocols. (e.g., Okta or OneLogin)
- 3. The organization has been onboarded onto the E911 Anywhere®/Horizon Mobility® platform.

**\*\*** DISCLAIMER: RedSky Support will not have the ability to support the configuration of an IdP application integration. IdP configuration questions should be directed to the IdP itself. **\*\*** 



# 2 Building the Application Integration

An organization wanting to use the Single Sign-On (SSO) service, provided by their IdP, to log in to the E911 Anywhere®/Horizon Mobility® portals will need to create an application integration based on some information they get from RedSky. This section covers what that information is and some examples of where it would be used.

### 2.1 RedSky: Determine API Name

RedSky will need to determine a unique API Name for the organization. The recommendation is that the API Name is a variation on the Organization Name given during onboarding.

Some important considerations when determining the API Name for an organization:

- 1. Spaces in the API Name are not supported,
- 2. Special characters, outside of dashes and under-scores, are strongly discouraged.
- 3. It is suggested that API Name should be all lower-case.

Examples of valid API Names:

- acme-widget-company
- mr\_donut
- orion

# 2.2 RedSky: Share Assertion and Audience URLs with Organization

The combination of an environment URL, "/sso/saml/", and API Name becomes the Assertion URL, which will need to be sent to the organization, so that they can create the application integration for E911 Anywhere®/Horizon Mobility®. Here are some valid examples of Assertion URLs:

- https://api.anywhere.e911cloud.com/sso/saml/acme-widget-company
- https://api.primelab.e911cloud.com/sso/saml/mr\_donut
- https://api.horizon.e911cloud.com/sso/saml/orion

The Audience URL is the combination of the environment URL and the API Name. Here are some valid examples:

- https://api.anywhere.e911cloud.com/acme-widget-company
- https://api.primelab.e911cloud.com/mr\_donut
- https://api.horizon.e911cloud.com/orion



### 2.3 Organization: Create Application Integration

The organization will need to create the SSO application integration on the IdP admin console, using the information RedSky sent them. The following requirements need to be met:

• SAML Initiator is configured as Service Provider and Email address is configured as the SAML name identifier. Below are a couple examples of where this is configured for reference:

ڭ okta			Q. Search for people, apps and groups			0		ahyamasoods okta-dev-788	54729
Dashboard	~		SAML Settings	Edit	E .				
Directory	~		GENERAL						
Customizations	~		Single Sign On URL	https://api.primelabdev01.e911cloud.com/sso/saml/ApiNam	ne				
Applications	^		Recipient URL	https://api.primelabdev01.e911cloud.com/sso/saml/ApiNam	пе				
Applications			Destination URL	https://api.orimelabdev01.e911cloud.com/sso/saml/ApiNam	ne				
Self Service			Audiance Pertriction	https://api.primalabdeu01.e911claud.com/ApiNama					
API Service Integration	ins		Default Dalay State	https://api.printelaucevoites/hcioud.com/wpirvanie					
Security	~		Default Relay State						
Workflow	~		Name ID Format	EmailAddress					
Reports	~		Response	Signed					
Cattings			Assertion Signature	Signed					
ootanga			Signature Algorithm	RSA_SHA256					
			Digest Algorithm	SHA256					
			Assertion Encryption	Unencrypted					
			SAML Single Logout	Disabled					
			SAML Signed Request	Disabled					
			authnContextClassRef	PasswordProtectedTransport					
			Honor Force Authentication	Yes					
			Assertion Inline Hook	None (disabled)					
	ara	lijostoss Autostijos	Assertion Inline Hook SAML Issuer ID	None (disabled) http://www.okta.com/\$(org.externalKey)					
onelogin use Applications / SAML Custorn Co	ers App onnector (	lications Devices Authentice 	Assertion Inline Hook SAML Issuer ID atlon Activity Security Settings	None (disabled) http://www.okta.com/\$(org.externalKey) : Developers Getting Started Guide			More	₽ Actions ▼	Yahya Save
onelogin use Applications / SAML Custom Co	ers App onnector (	Identions Devices Authentice Advanced)	Assertion Inline Hook SAML Issuer ID ation Activity Security Settings	None (disabled) http://www.okta.com/\$(org.externalKey) : Developers Centurg Stanled Gudor			More	A Actions 👻	Yahya Save
onelogin use Applications / SAML Custom Co Info	ers App onnector (	Incetions Devices Authentice Advanced) ① * Required - Specifies time period, in SAML not valid on or after	Assertion Inline Hook SAML Issuer ID atton Activity Security Settings minutes, the assertion is valid for.	None (disabled) http://www.okta.com/\$(org.externalKey) Powelopers Cetting Started Guide			More	A Actions 👻	Yahya Save
onelogin use Applications / SAML Custom Co Info Configuration Parameters	ers App onnector (	Incations Devices Authentics Advanced) ① *Required - Specifies time period, in SAML not valid on or after 2	Assertion Inline Hook SAML Issuer ID attion Activity Security Settings minutes, the assertion is valid for.	None (disabled) http://www.okta.com/\$(org.externalKey) 2 Developers Cetting Startied Guide			More	A actions +	Yahya Save
onelogin use Applications / SAML Custom Co Info Configuration Parameters Rules	ers App pnnector (	Devices         Authentice           Advanced)         ① * Required - Specifies time period, in           SAML not valid on or after         2           ① * Required - Specifies time period, in         2	Assertion Inline Hook: SAML Issuer ID atton Activity Security Settings in minutes, the assertion is will for.	None (disabled) http://www.okta.com/\$(org.externalKey) • Developers Cetting Started Guide			More	<b>▲</b> e Actions ▼	Yahya Save
onelogin use Applications / SANL Custom Col Info Configuration Parameters Rules SSO	ers App	Icctions         Devices         Authentic           Advanced)	Assertion Inline Hook: SAML Issuer ID atton Activity Security Settings mminutes, the assertion is valid for.	None (disabled) http://www.okta.com/\$(org.externalKey)			More	Actions 👻	Yahya Save
onelogin use Applications / SAML Custom Co Info Configuration Parameters Rules SSO Access	ers App onnector (	Icotions         Devices         Authentic           Advanced)	Assertion Inline Hook SAML Issuer ID ation Activity Security Settinger minutes, the assertion is valid for.	None (disabled) http://www.okta.com/\$(org.externalKey) Perelopers Cetting Stathed Guide			More	A Actions 👻	Yahya Save
onelogin use Appleations / SAML Custom Co Info   Configuration Parameters Rules SSO Access Users Devidences	ers App	Devices         Authentic           Advanced)	Assertion Inline Hook SAML Issuer ID ation Activity Security Settings minutes, the assertion is valid for.	None (disabled) http://www.okta.com/\$(org.extarnalKey)			More	A e Actions 👻	Yahya Save
onelogin use Applications / SAML Custom Co Info Configuration Parameters Rules SSO Access Users Privileges Setup	ers App onnector	Devices         Authentic           Advanced)              • * inequired - Specifies time period, in            SAML not valid on or after               2            • * inequired - Specifies time period, in               service Provider            SAML not valid on or after               service Provider            SAML not wall format               Email	Assertion Inline Hook SAML Issuer ID ation Activity Security Settings minutes, the assertion is valid for.	None (disabled) http://www.okta.com/\$(org.externalKey)			More	A e Actions 👻	Yahya Save
onelogin use Appleations / SAML Custom Co Info Configuration Parameters Rules SSO Access Users Privileges Setup	ers App onnector (	Identions Devices Authentice Advanced)	Assertion Inline Hook: SAML Issuer ID attor Activity Security Settings minutes, the assertion is valid for:	None (disabled) http://www.okta.com/\$(org.externalKey) Developers Centrog Started Gude			More	Actions -	Save
onelogin use Applications / SAML Custom Col Info Configuration Parameters Rules SSO Access Users Privileges Setup	Approximation of the second seco	Devices         Authentical           Advanced)              • *Required - Specifies time period, in            SAML not valid on or after               2            • *Required - Specifies time period, in               Secure - Specifies time period, in            SAML initiator              Service Provider               Service Provider            SAML initiator              Service Provider               Setwice Type            SML initiator              Service Provider               Setwice Type            SML initiator              Service Provider              SML initiator               Service Provider                SML initiator               Service Type               Specific               SAML signature element	Assertion Inline Hook: SAML Issuer ID ation Activity Security Settings minutes, the assertion is valid for.	None (disabled) http://www.okta.com/\$(org.externalKey)  Pevelopers			More	A e Actions 👻	C Yahya Save
onelogin use Applications / SAML Custom Col info Configuration Parameters Rules SSO Access Users Privileges Setup	Mrs App prinnector	Actions Divices Authentics Advanced)	Assertion Inline Hook: SAML Issuer ID ation Activity Security Sattings mminutes, the assertion is valid for.	None (disabled) http://www.okta.com/\$(org.externalKey)  Developers Cetting Started Gude			More	▲ #Actions ◄	Save
onelogin use Applications / SAML Custom Co Info Configuration Parameters Rules SSO Access Users Privileges Setup	ere App	Devices         Authentics           Advanced)         Image: Comparison of the stree period, in the streep st	Assertion Inline Hook: SAML Issuer ID atton Activity Security Settings in minutes, the assertion is valid for.	None (disabled) http://www.okta.com/\$(org.externalKey)  Perelopers Cetting Status Guods			More	Actions ▼	Q Yabya Save
onelogin use Appleations / SAML Custom Co Info Configuration Parameters Rules SSO Access Users Privileges Setup	App Ponnector (	Devices         Authentics           Advanced)         Authentics           Advanced)         Image: Specifies time period, in           SAML not valid on a siter         Image: Specifies time period, in           2         Image: Specifies time period, in           SAML initiator         Service Provider           SAML initiator         Specifie           SAML initiator         Specifie           SAML isorature element         Emerging           SAML signature element         Response           SAML seportion method         Science of the second of th	Assertion Inline Hook: SAML Issuer ID atton Activity Security Settings mminutes, the assertion is will for.	None (disabled) http://www.okta.com/\$(org.externalKey)  Perelopers Cetting Statted Gudos			More	Actions ✓	Q Yabya Save
onelogin use Appleations / SAML Custom Co Info Configuration Parameters Rules SSO Access Users Privileges Setup	Approximation of the second se	Designs         Authentics           Advanced)         Authentics           Advanced)         Image: Specifies time period, in           SAML not valid on a siter         Image: Specifies time period, in           2         Image: Specifies time period, in           SAML not valid on a siter         Image: Specifies time period, in           SAML initiator         Service Provider           SAML initiator         Specific           SAML isourt type         Specific           SAML isourt type         Specific           SAML signature element         Response           Encrypt assertion         SAML eccyption method           TRPLEDES CBC         Image: Specific size size size size size size size size	Assertion Inline Hook: SAML Issuer ID atton Activity Security Settings mminutes, the assertion is will for.	None (disabled) http://www.okta.com/\$(org.externalKey)  Perelopers Cetting Statled Guds			More	Actions ◄	Save
onelogin use Appleations / SAML Custom Co. Info Parameters Rules SSO Access Users Privileges Setup	App Dinnector I	Devices         Authentice           Advanced)         • Required - Specifies time period, in           SAML not valid on or after         2           • Required - Specifies time period, in         5           SAML initiator         5           Service Provider         5           SAML initiator         5           Service Provider         5           SAML initiator         5           Specific         5           SAML signature element         7           Response         5           SAML encryption method         7           TRPL Dig C 80         5	Assertion Inline Hook: SAML Issuer ID ation Activity Security Settings an initiate, the assertion is valid for:	None (disabled)         http://www.okta.com/\$(org.externalKey)			More	A e Actions -	Save



• The integration uses the Assertion and Audience URLs sent. Below are some examples of where the Assertion and Audience URLs are configured for reference:

‡ oktα		Q. Search for people, apps and groups		⑦ 器 · ·
Dashboard	~	General Settings	2 Configure SAML	3 Feedback
Directory	~			
Customizations	~	A SAML Settings		
Applications	~	General		What does this form do?
Security	~	Single sign on LIDL		for the app's SAML request.
Workflow	~	Single agriculture of	<ul> <li>s://api.primelabdev01.e911cloud.com/sso/saml/ApiN</li> <li>Use this for Recipient URL and Destination URL</li> </ul>	Where do I find the info this form
Reports	~	Audience URI (SP Entity ID)	http://www.insignalabdou.01.c011-land.com/Aciblema	The app you're trying to integrate with
Settings	~		https://api.primeiabdevol.e51icioda.com/Apirvame	should have its own documentation on using SAML. You'll need to find that
		Default RelayState 🛛 🕲		doc, and it should outline what information you need to specify in this
			If no value is set, a blank HelayState is sent	form.
		Name ID format 🔘	EmailAddress v	
		Application username	Okta username v	
		Update application username on	Create and undate	
			Create and update	
			Show Advanced Se	attings
		Attribute Statements (optional)	LEARN	IMORE
onelogin Use	rs Applications Devices Authentic	ation Activity Security Settings	Developers Getting Started Guide	
Applications / SAML Custom Co	nnector (Advanced)			More Actions 👻 Save
Info	Application details			
Configuration	RelayState			
Parameters				
Rules	Audience (EntityID)			
SSO	https://api.cirrus1.e911cloud.com/A	piName		
Access	Recipient https://api.cirrus1.e911cloud.com/s	so/saml/ApiName		
Users	ACS (Consumer) URL Validator*			
Setup	https://api.cirrus1.e911cloud.com/s	so/saml/ApiName		
	③ *Required.			
	ACS (Consumer) URL*			
	https://api.cirrus1.e911cloud.com/s	so/saml/ApiName		
	(i) *Required			
	Single Logout URL			
	Login URI			



# **3** Application Configuration Information

Once the customer has completed creating the application integration, they must provide the following information to RedSky, so that the SSO integration can be completed on the E911 Anywhere®/Horizon Mobility® side:

- 1. IdP Meta Data
- 2. Security Hash Algorithm
- 3. SAML Identity Location

Where this information is used will be covered in Section 4.

### 3.1 IdP Provider Metadata

IdP metadata is required to configure the SAML connection settings for the integration. The XML of the metadata can be downloaded or copy/pasted into a file from the admin console of the IdP.

Below are screenshots of the Okta and OneLogin admin consoles to help illustrate where this information can be gathered in the case that an organization may need some assistance in finding the information.:

🕻 okta		Q. Stearch for people, appa and groups
Dashboard	~	How to Configure SAML 2.0 for
Directory	~	Note: These setup instructions include certificate information for this app's most recently created SAML signing certificate. For users to get
Customizations	~	access to the app using these instructions, that certificate must be active.
Applications	^	The following is needed to configure
Applications		1 Identity Provider Single Sign-On URL:
Self Service		https://dwokta.com/app///soc/aaal
API Service Integrations		
Security	~	2 Identity Provider Issuer:
Workflow	~	http://www.ckta.com/won&errdow/Q0/w67507
Reports	~	
Settings	~	3 X.509 Cartificata:
		Bally Carrielone 
		Optional         Provide the following IDP metadata to your SP provider.         <2mil version="1.0" encoding="UTF-8";?><mdEntlyDescriptor ently/D="http://www.okta.com/</td>



onelogin Users	Applications Devices Authentication Activity Security Settings Developers Getting Started Guide	A (0)
Applications / SAML Custom Connec	tor (Advanced)	More Actions - Save
Info	Application details	Vendor Homepage Reapply entitlement mappings
Configuration	ReleyState	SAML Metadata 👦
Parameters		Delete
Rules	Audience (EntityID)	
SSO	https://api.cirrus1.e911cloud.com/ApiName	
Access	Recipient	
Users	https://api.cirrus1.e911cloud.com/sso/saml/ApiName	
Privileges	ACS (Consumer) URL Validator*	
Setup	https://api.cirrus1.e911cloud.com/sso/saml/ApiName	
	① *Required.	
	ACS (Consumer) URL*	
	https://api.cirrus1.e911cloud.com/sso/saml/ApiName	
	(j) "Required	
	Single Leaver LBL	
	aulita rolitori nur	

### 3.2 Security Hash Algorithm

The correct Security Hash Algorithm will be needed. This information is generally configured at the organization level at the IdP and can be accessed via the SAML 2.0 settings. Here are examples from both Okta and OneLogin:

🎇 okta		Q Search for people, apps and groups		yahyamasood93@g okta-dev-78854729
Dashboard	~	SAML Settings	Edit	
Directory	~	GENERAL		
Customizations	~	Single Sign On URL	https://api.primelabdev01.e911cloud.com/sso/saml/ApiName	
Applications	^	Recipient URL	https://api.primelabdev01.e911cloud.com/sso/saml/ApiName	
Applications		Destination URL	https://api.primelabdevO1.e911cloud.com/sso/saml/ApiName	
Self Service		Audience Restriction	https://api.primelabdev01.e911cloud.com/ApiName	
API Service Integrations		Default Relay State		
Security	~	Name ID Format	EmailAddress	
Workflow	~	Response	Signed	
Reports	~	Assertion Signature	Signed	
Settings	~	Signature Algorithm	RSA_SHA256	
		Digest Algorithm	SHA256	
		Assertion Encryption	Unencrypted	
		SAML Single Logout	Disabled	
		SAML Signed Request	Disabled	
		authnContextClassRef	PasswordProtectedTransport	
		Honor Force Authentication	Yes	
		Assertion Inline Hook	None (disabled)	
		SAML Issuer ID	http://www.okta.com/\${org.externalKey}	



onelogin Users	Applications Devices Authentication Activity	Security Settings Develop	Getting Started	Guide	👤 Yahya
Applications / SAML Custom Connec	or (Advanced)			More Actions 👻	Save
Info Configuration Parameters Rules <b>SSO</b> Access Users Privileges Setup	Enable SAML2.0 Sign on method SAML2.0 X.509 Certificate Standard Strength Certificate (2048-bit) Change View Details SAML Signature Algorithm SHA-256 Insuer OHL https://redskydevtest.onelogin.com/trust/sami2/http-post/sts SLO Endpoint (HTTP) https://redskydevtest.onelogin.com/trust/sami2/http-redirect	\$ a0-b88a-c9254eb541af sc/53836ee6-34af-4fa0-b88a-c9254eb54 t/sio/2198300	€ € €	there 💐 Any questions? (	
	Login Hint		can	help here!	- <u>                                    </u>





# 4 E911 Anywhere®/Horizon Mobility® Configuration

## 4.1 Organization Level SSO Configuration

Each organization, regardless of type, including System, must be configured before using SAML 2.0 SSO. Currently, this can only be done by a RedSky Administrator.

To integrate with an organization's IdP SSO service, the RedSky Administrator will navigate to the *Organization Management* page for the organization in question then complete the *SAML 2.0 Single Sign-On Settings* form. To complete the form, the API Name generated in Section 2.1 must be provided as well as the information outlined in Section 3, which should have been shared by the customer. Here is a screenshot of the form:

Organiza	tion Management
•	SAML 2.0 Single Sign-On Settings
	*API Name
	*Identity Provider Metadata:
	Security Hash Algorithm:
	<ul> <li>SHA-1</li> <li>SHA-256</li> </ul>
	SAML Identity Location:           Identity is in the NameIdentifier element of the Subject statement           Identity is in an Attribute element
	SAVE



▲	SAML 2.0 Single Sign-On Settings
	*API Name acme-widget-company
	*Identity Provider Metadata:
	UPLOAD XML FILE IdP_metadata.xml
	Security Hash Algorithm: SHA-1 SHA-256
	SAML Identity Location: <ul> <li>Identity is in the NameIdentifier element of the Subject statement</li> <li>Identity is in an Attribute element</li> </ul>
	SAVE

*Note:* As SAML 2.0 currently only supports Email as the name identifier, so the first radio button should stay selected for *SAML Identity Location*.

When the need arises the current SAML 2.0 SSO integration can be disabled and cleared at system/organization level by clicking the CLEAR button. Please note that any exiting RedSky/Organization Administrators configured as SSO users will stay SSO users and the log in process will fail unless another SAML 2.0 SSO integration is successfully configured. Those SSO Users can be converted to local-login users, which is covered in Section 4.2.

### 4.2 Organization Administrator SSO Configuration

Once an organization has been configured to use SSO, RedSky and Organization Administrators will need to be configured individually on the E911 Anywhere®/Horizon Mobility® platform to log in using SSO. This can be done by any RedSky/Organization Administrators that belong to the organization. Configuring a RedSky/Organization Administrator is as simple as turning ON/OFF a toggle on the Add/Edit Administrator modals.



#### E911 Cloud Solutions & SSO ICD

Administrators		Administrators	
Search Q		Edit Administrator	CLOSE
Add Administrator	CLOSE	Role* Organization Administrator	- ic
Role* Organization Administrator		Log in using SSO Email*	
Log in using SSO		First Name	
Email*	A	Last Name	
First Name	_	Please note that the user will need to click on the 'Forgot/Deset Password' link	
Last Name		on the log in page, before logging in for the first time.	
SAVE		SAVE	

By default, new RedSky/Organization Administrators will be set as SSO users. Simply toggle-off the *Log in using SSO* setting to make them local-login users.

Existing RedSky/Organization Administrators will stay configured as local-login users. Meaning they will use the email address and password configured on the E911 Anywhere®/Horizon Mobility platform. Simply toggle-on the *Log in using SSO* setting to make them SSO users.

As a reminder, if the SAML 2.0 SSO integration is disabled and cleared at system/organization level, any exiting RedSky/Organization Administrators configured as SSO users will stay SSO users and the log in process will fail unless another SAML 2.0 SSO integration is successfully configured. Those SSO Users can be converted to local-login users; however, those users would need to go through the process of setting the password if they have never set their password locally.

IMPORTANT NOTE: Any Organization Administrators that are set as SSO Users may no longer be able to log in to the EON desktop client because the EON client currently does not support SSO. Until it does, we strongly recommend that Organization Administrators needing access to the EON client not be configured as an SSO user, or if another email address is available, provision a separate EON user.



# 5.1 RedSky/Organization Administrator SSO User Login

To test if the SAML 2.0 SSO integration is working, an SSO user should be created at system level or the organization in question, and they should attempt to log in to the environment in question.

The following is the valid workflow for SSO user log in:

1. When a RedSky/Organization Administrator logs in, they will only be prompted for their email address at first.

	MOBILITY
Welco	ome to Horizon Mobility <sup>®</sup> Porta Please sign in below
Email	
	SIGN IN

- 2. Once the SIGN IN button is selected, the system will check if SSO integration is enabled at the system/organization level and what SSO provider is being used.
  - a. If SSO integration is not configured at the system/organization level, the RedSky/Organization Administrator will be prompted to provide their password on the system, as they did, prior to SSO integration.

HORIZON
Welcome to Horizon Mobility <sup>®</sup> Portal Please sign in below
Email
····
Password 🔤
SIGN IN
Forgot/Reset Password?

- b. If SSO integration is configured at the system/organization level, the system will do an additional check to see if the RedSky/Organization Administrator is configured as an SSO user.
  - i. If the RedSky/Organization Administrator is not configured as an SSO user, they will be prompted to provide their password on the system, as they did prior to SSO integration.





ii. If the RedSky/Organization Administrator is configured as an SSO user, they will be taken to the system's/organization's IdP login page, where they can provide their credentials.

Connecting to O
okta
Sign In
Password
<b>B</b>
Keep me signed in
Sign in
<u>Forgot password?</u> <u>Help</u>

## 5.2 RedSky/Organization Administrator Local-User Login

To test if a local-login user can still login using the credentials set on the E911 Anywhere®/Horizon mobility platform.

Below is the valid local-user login workflow:

1. When a RedSky/Organization Administrator logs in, they will only be prompted for their email address at first.



HORIZON
Welcome to Horizon Mobility <sup>®</sup> Portal Please sign in below
Email
SIGN IN

- 2. Once the SIGN IN button is selected, the system will check if SSO integration is enabled at the system/organization level and what SSO provider is being used.
  - a. If SSO integration is not configured at the system/organization level, the RedSky/Organization Administrator will be prompted to provide their password on the system, as they did, prior to SSO integration.

HORIZON
Welcome to Horizon Mobility <sup>®</sup> Portal Please sign in below
Email
Password
SIGN IN
Forgot/Reset Password?

- b. If SSO integration is configured at the system/organization level, the system will do an additional check to see if the RedSky/Organization Administrator is configured as an SSO user.
  - i. If the RedSky/Organization Administrator is not configured as an SSO user, they will be prompted to provide their password on the system, as they did prior to SSO integration.

HORIZON
Welcome to Horizon Mobility <sup>®</sup> Portal Please sign in below
Email
Password
SICN IN
Forgot/Reset Password?