everbridge™ redsky

E911 Cloud Solutions & Single Sign-On Interface Control Document

Version 1.2 | June 23, 2023

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

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

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

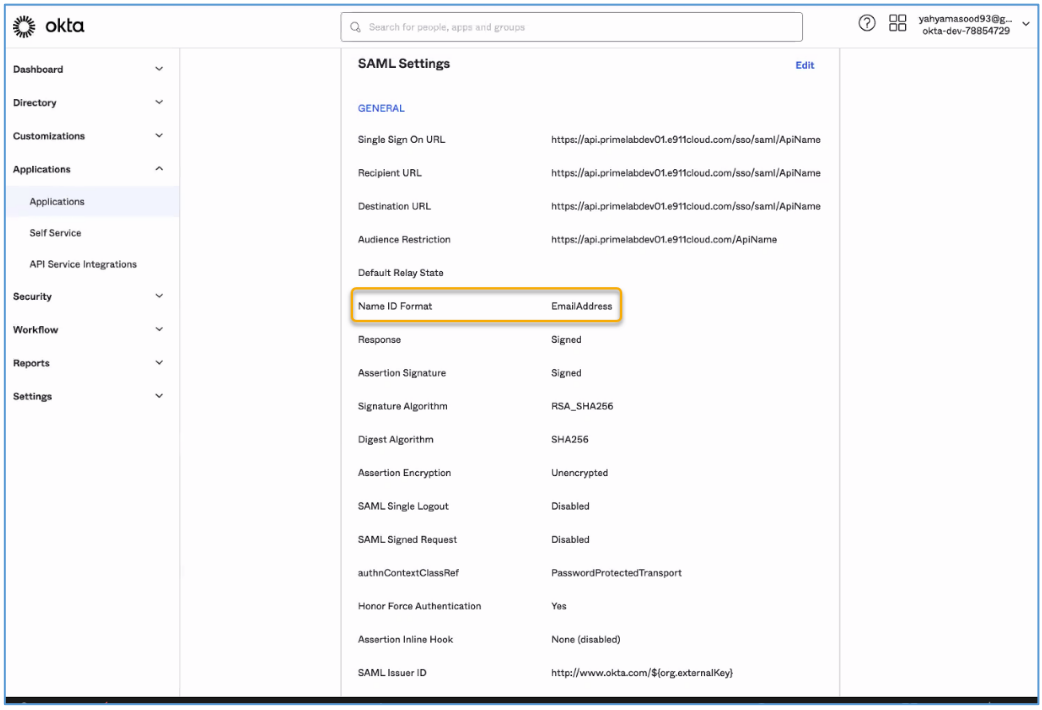
The Audience URL is the combination of the environment URL and the API Name. Here are some valid examples:

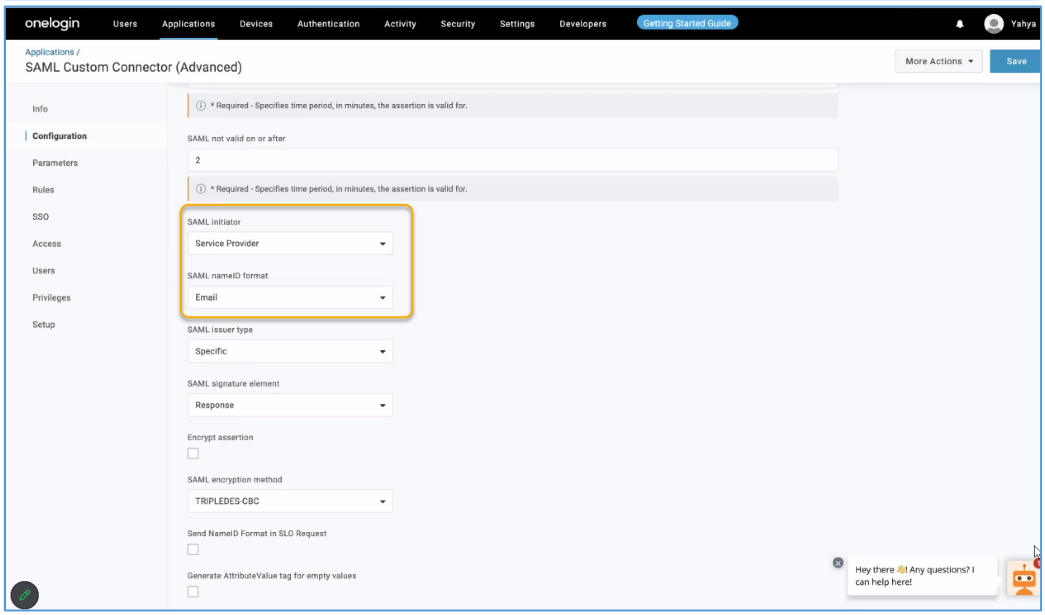
- https://api.anywhere.e911cloud.com/acme-widget-company
- https://api.primelab.e911cloud.com/mr_donut
- https://api.horizon.e911cloud.com/orion

2.3 Organization: Create Application Integration

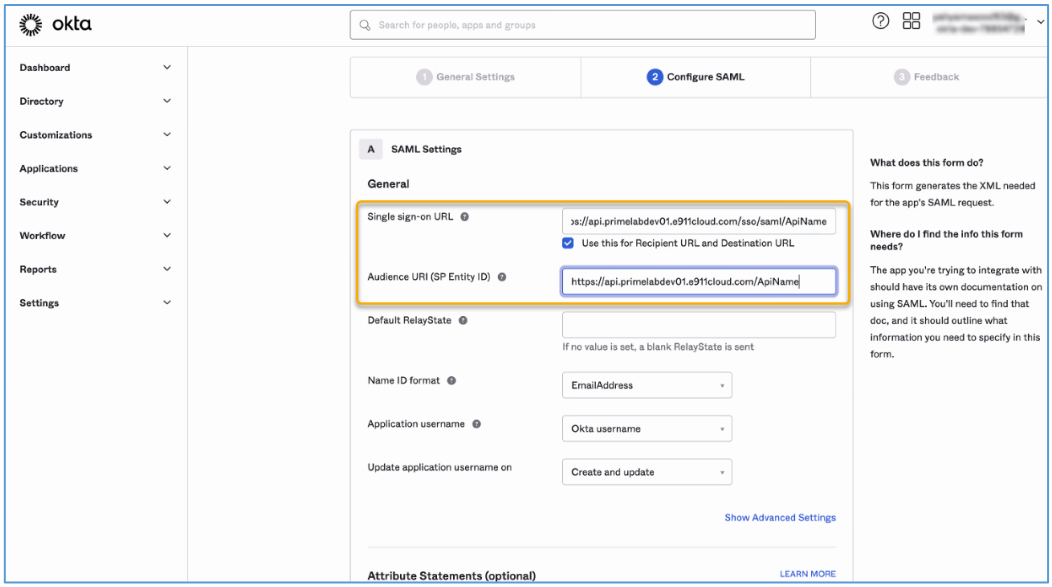
The organization will need to create the SSO application integration on the IdP admin console, using the information RedSky sent them. The following requirements need to be met:

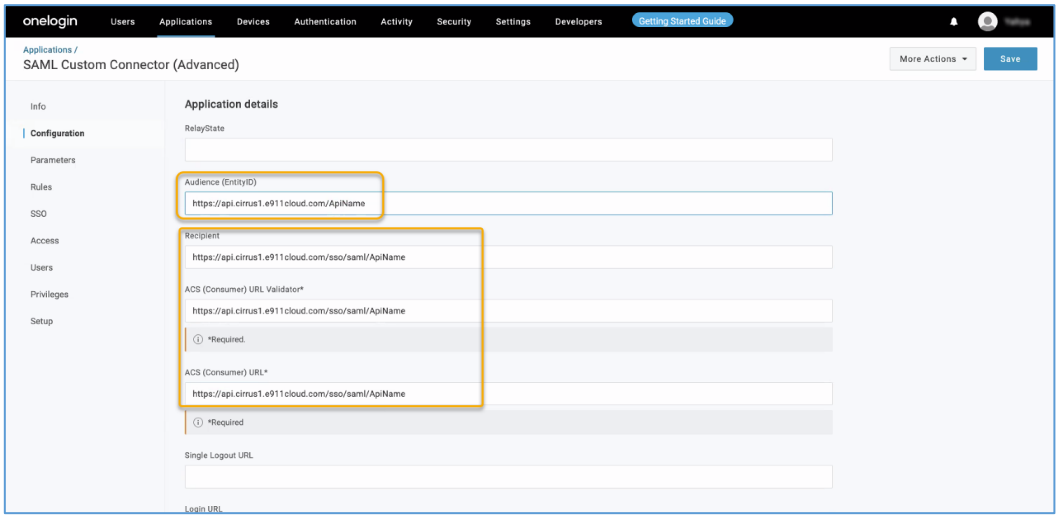
- SAML Initiator is configured as Service Provider and Email address is configured as the SAML name identifier. Below are a couple examples of where this is configured for reference:





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





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:

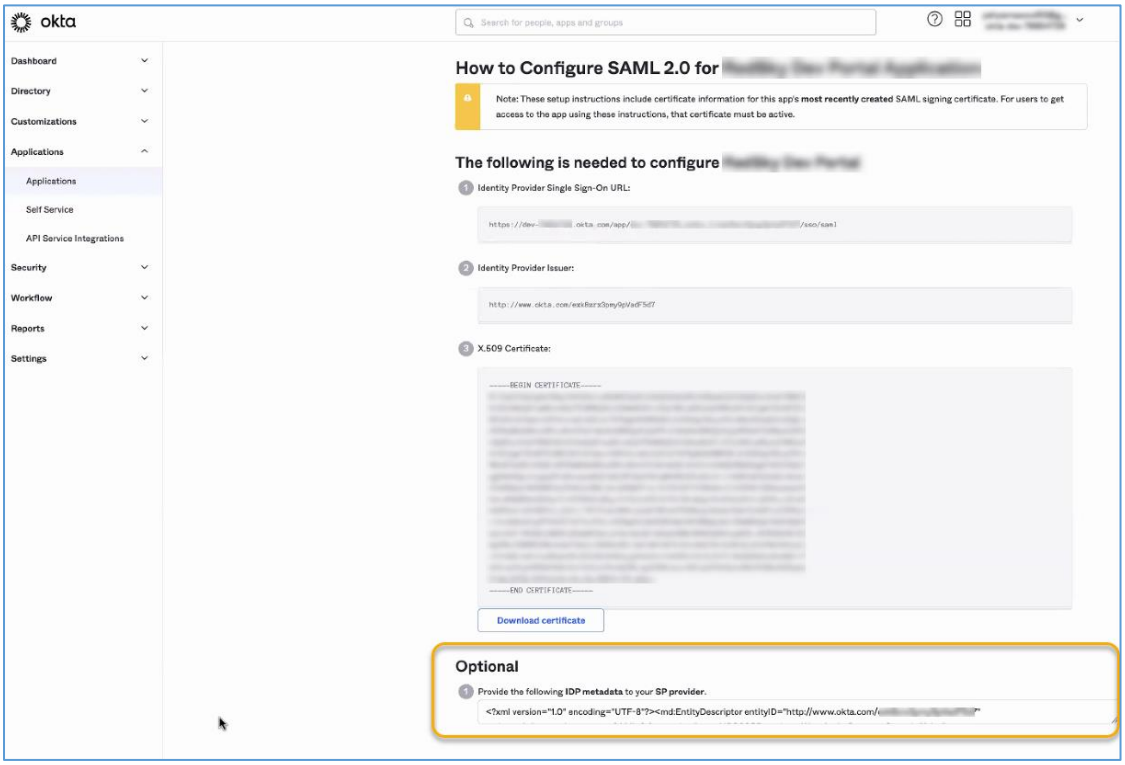
1. IdP Meta Data
2. Security Hash Algorithm
3. SAML Identity Location

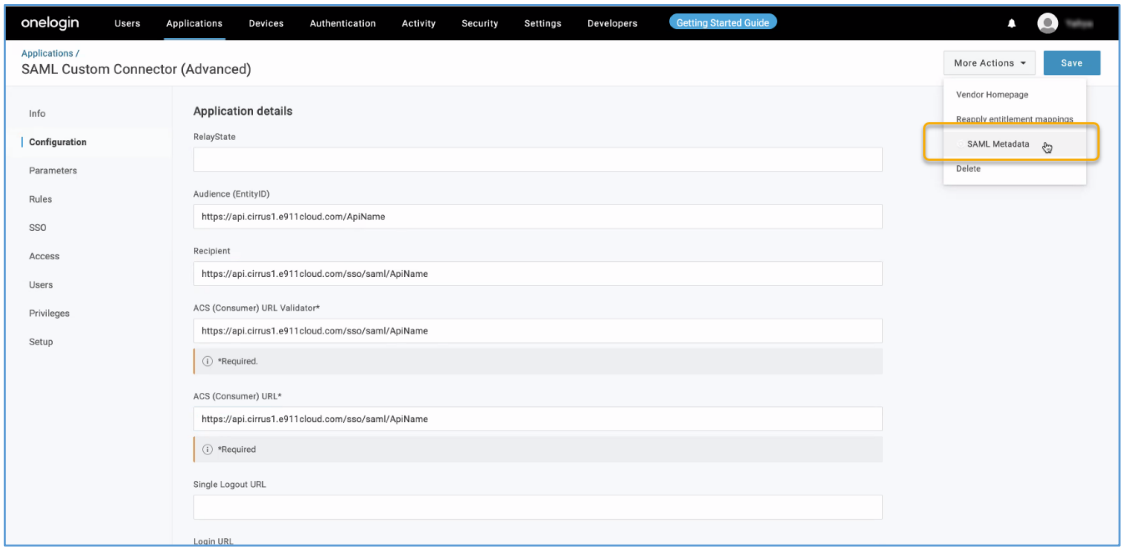
Where this information is used will be covered in Section 4.

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.

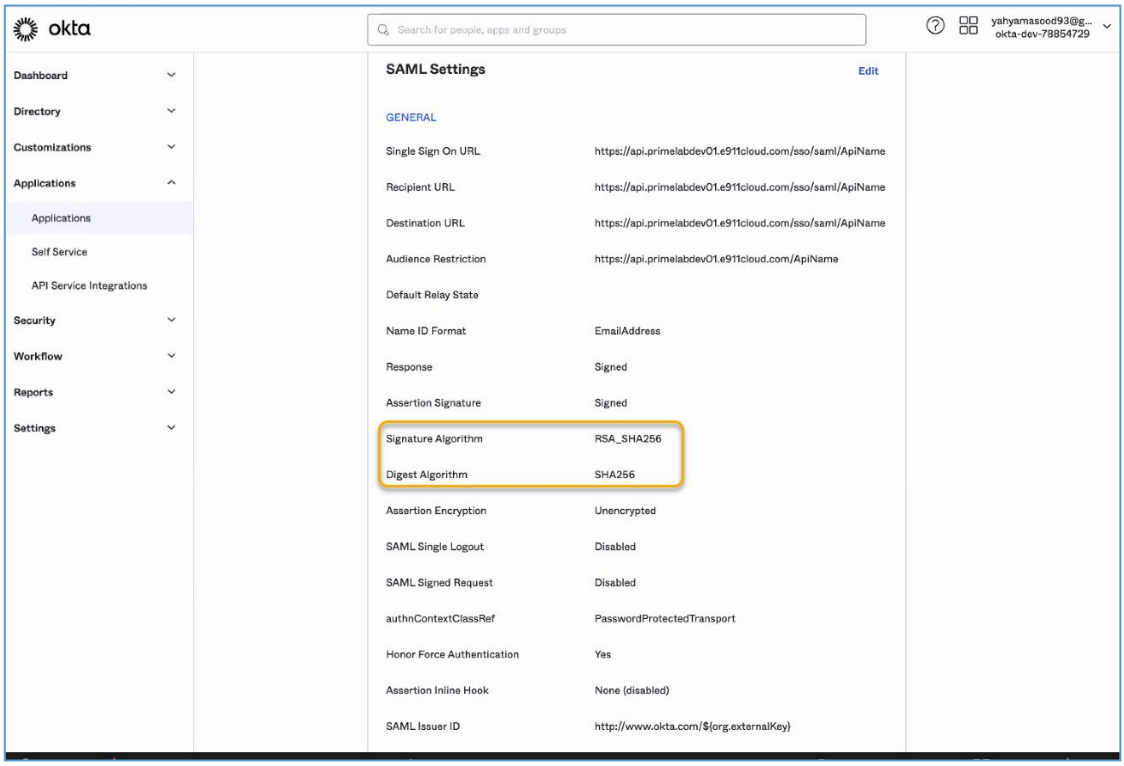
Below are screenshots of the Okta and OneLogin admin consoles to help illustrate where this information can be gathered in the case that an organization may need some assistance in finding the information.:

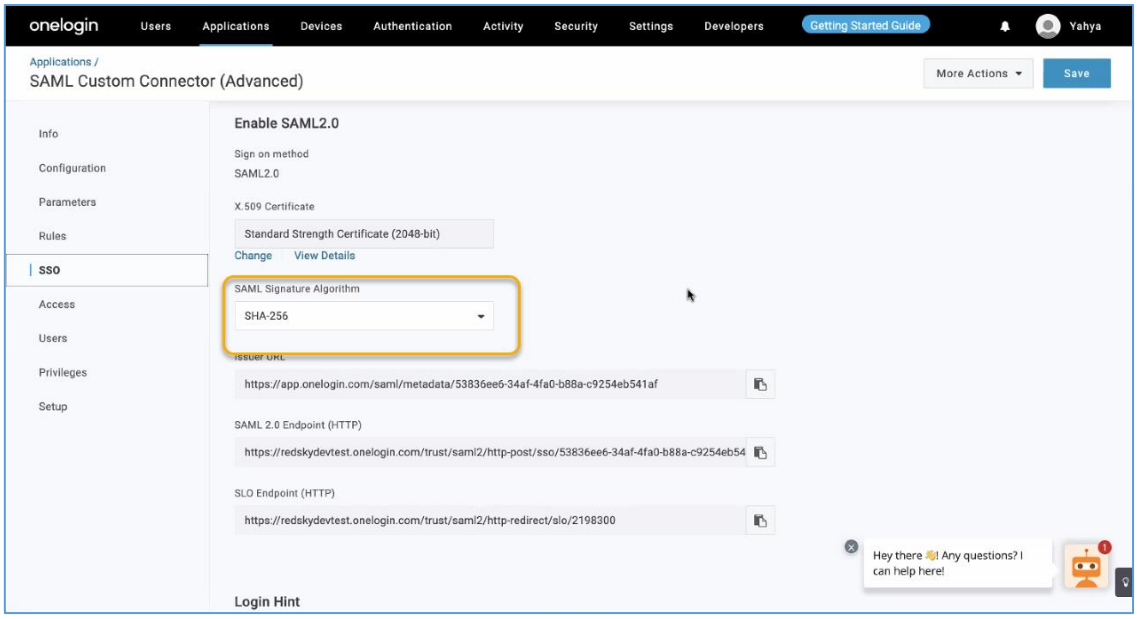




3.2 Security Hash Algorithm

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:



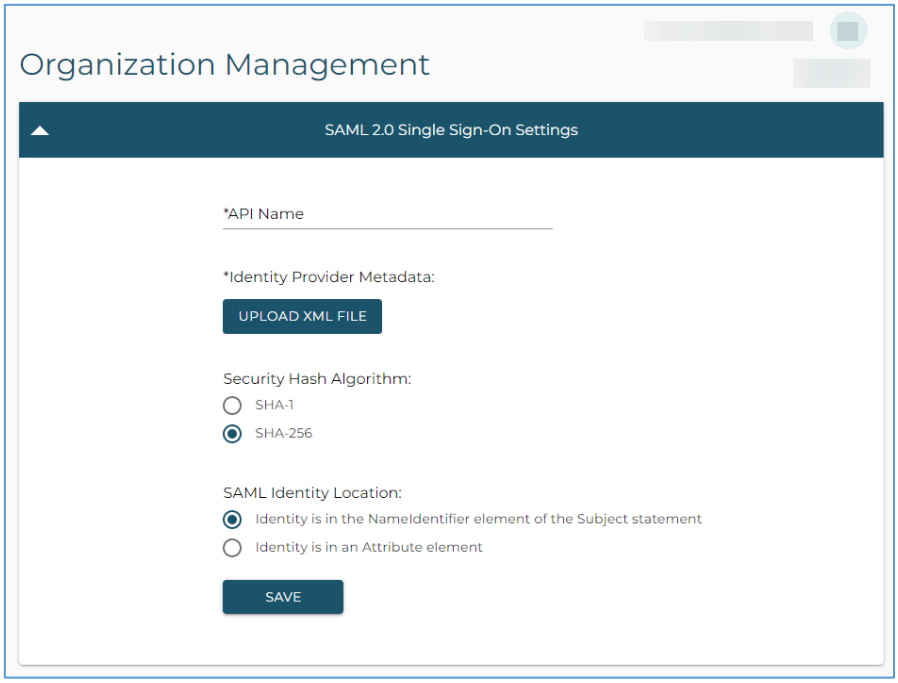

onelogin
Users
Applications
Devices
Authentication
Activity
Security
Settings
Developers
Getting Started Guide
Yahya
Applications /
SAML Custom Connector (Advanced)
More Actions
Save
Info
Configuration
Parameters
Rules
SSO
Access
Users
Privileges
Setup
Enable SAML2.0
Sign on method
SAML2.0
X.509 Certificate
Standard Strength Certificate (2048-bit)
Change
View Details
SAML Signature Algorithm
SHA-256
Issuer URL
https://app.onelogin.com/saml/metadata/53836ee6-34af-4fa0-b88a-c9254eb541af
SAML 2.0 Endpoint (HTTP)
https://redskydevtest.onelogin.com/trust/saml2/http-post/sso/53836ee6-34af-4fa0-b88a-c9254eb54
SLO Endpoint (HTTP)
https://redskydevtest.onelogin.com/trust/saml2/http-redirect/slo/2198300
Hey there 👋! Any questions? I can help here!
Login Hint

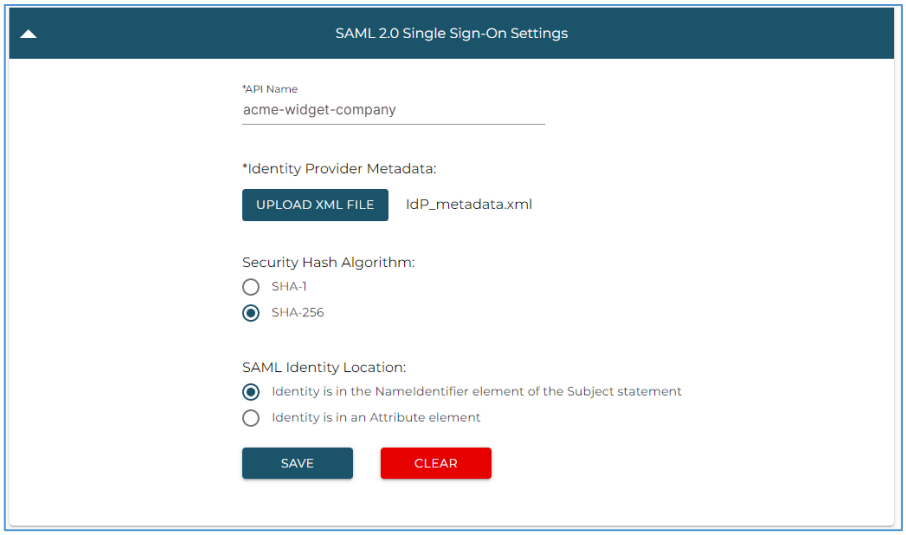
4 E911 Anywhere®/Horizon Mobility® Configuration

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:



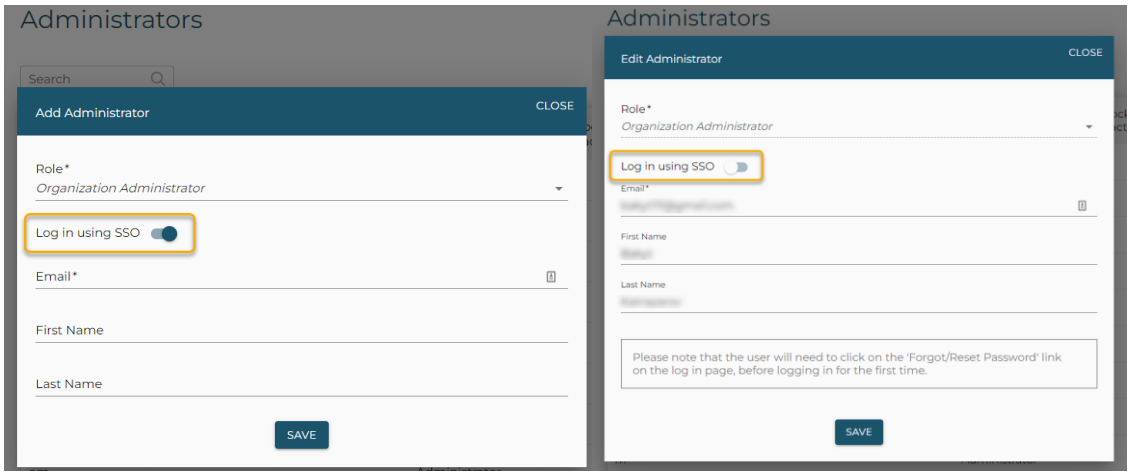


Note: As SAML 2.0 currently only supports Email as the name identifier, so the first radio button should stay selected for *SAML Identity Location*.

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.



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.

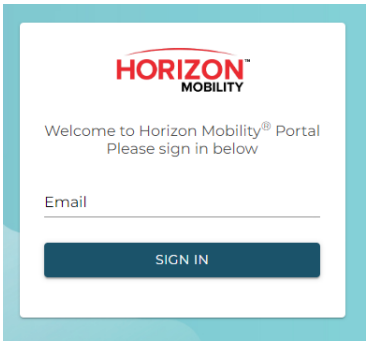
5 Testing

5.1 RedSky/Organization Administrator SSO User Login

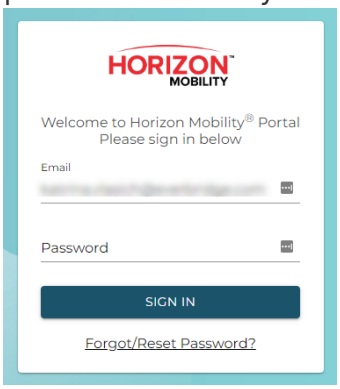
To test if the SAML 2.0 SSO integration is working, an SSO user should be created at system level or the organization in question, and they should attempt to log in to the environment in question.

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

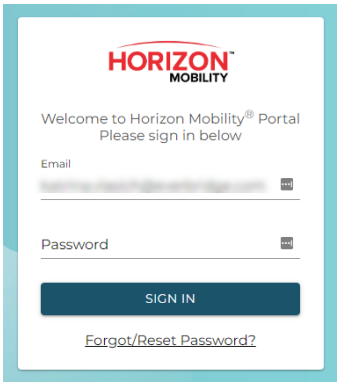
1. When a RedSky/Organization Administrator logs in, they will only be prompted for their email address at first.



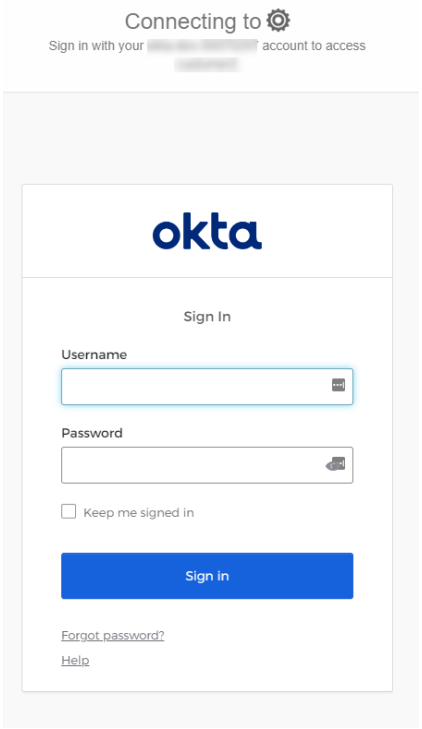
2. Once the SIGN IN button is selected, the system will check if SSO integration is enabled at the system/organization level and what SSO provider is being used.
    a. If SSO integration is not configured at the system/organization level, the RedSky/Organization Administrator will be prompted to provide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



    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.

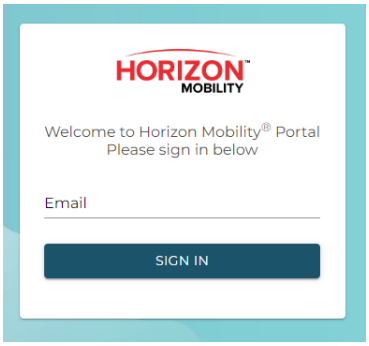


5.2 RedSky/Organization Administrator Local-User Login

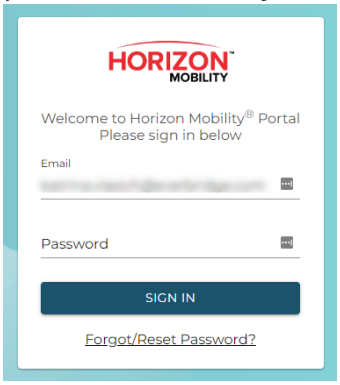
To test if a local-login user can still login using the credentials set on the E911 Anywhere®/Horizon mobility platform.

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.



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.



    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.