RSA SECURID® ACCESS
Implementation Guide

Google Chrome OS

Gina Salvalzo, RSA Partner Engineering
Last Modified: April 5, 2018

RSA READY

Configuration SAML Single Sign-on for Chrome OS

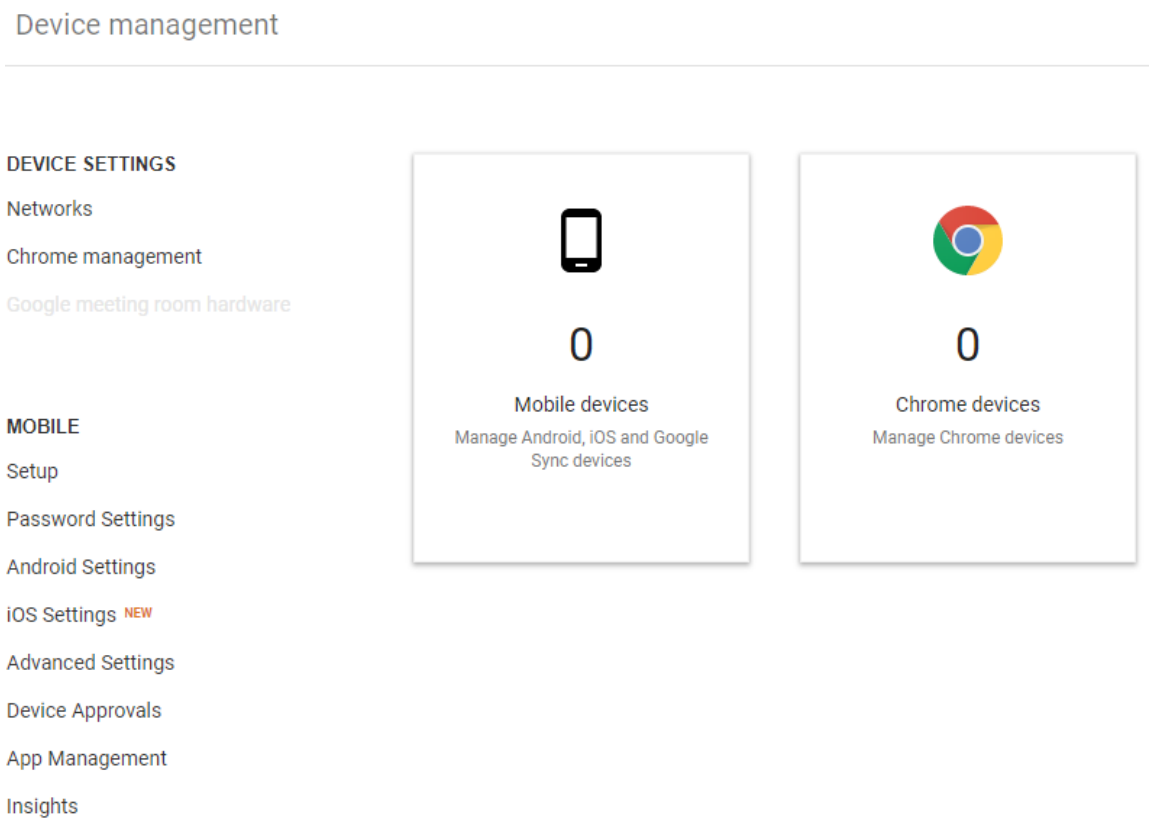
Single Sign-On (SSO) support for Chrome devices allows users to sign in to a Chrome device with the same authentication mechanisms that you use within the rest of your organization.

Before You Begin

- Acquire an administrator account to RSA SecurID Access.
- Acquire an administrator account to Google Suite.

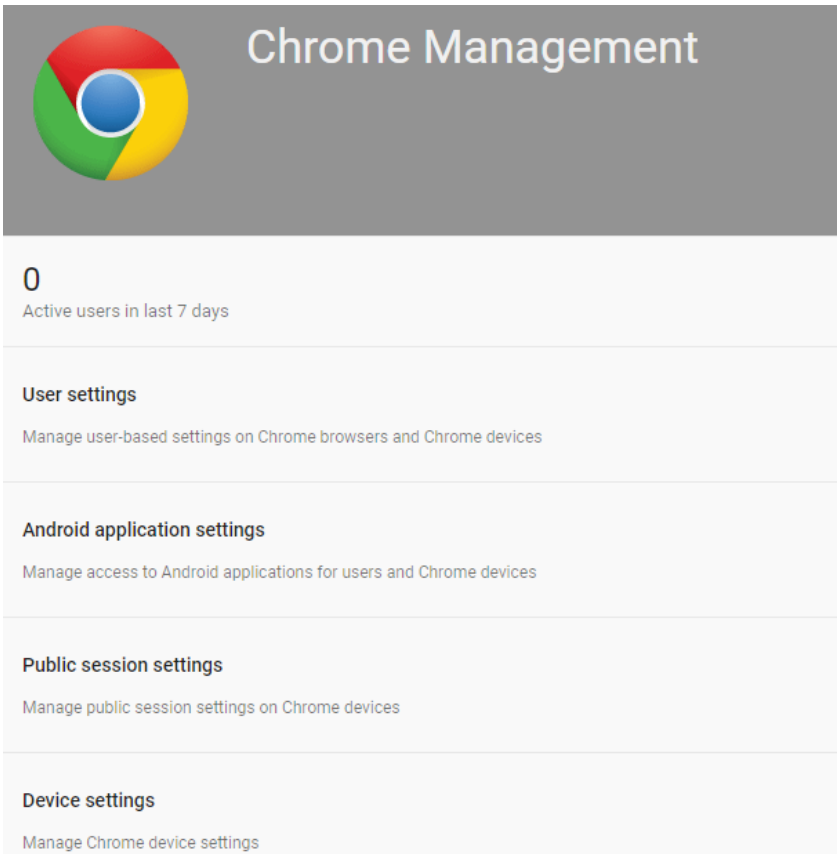
Note: Chrome device running Chrome OS version 36 or higher

1. Setup RSA SecurID Access as the IdP for your Google Suite domain by following the **Google Apps -RSA SecurID Access Implementation Guide**.
2. In the Google Admin console, navigate to **Device Management.**

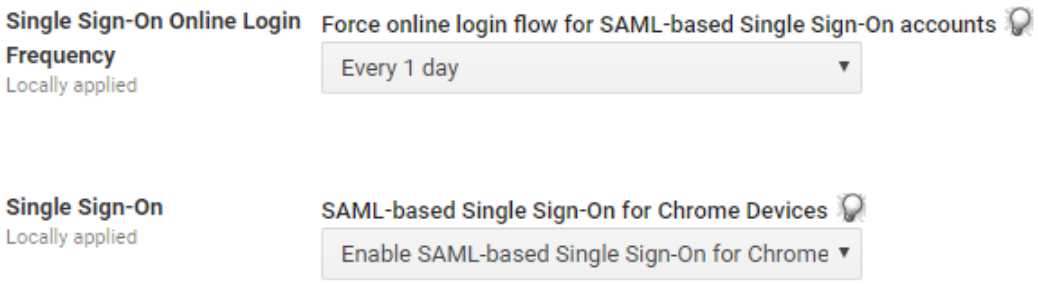


3. Select **Chrome management**.

4. Select **User settings**.



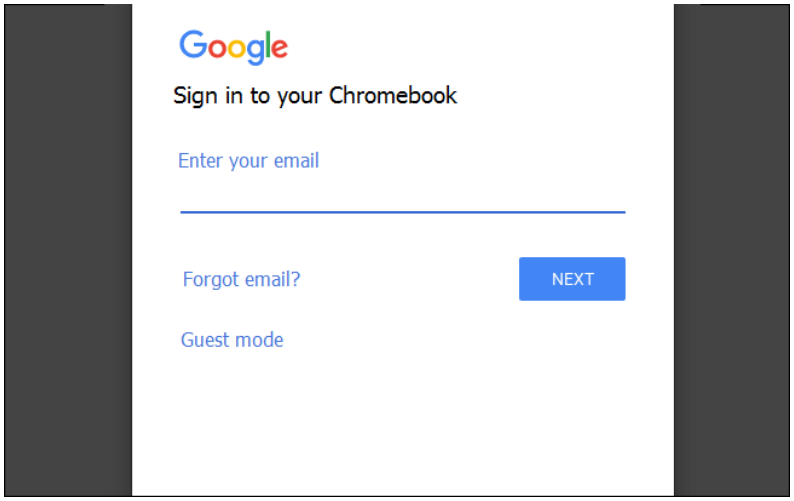
5. Scroll down to the Security section.
6. Choose **Enable SAML-based Single Sign-On for Chrome Devices** from the Single Sign-on pulldown list.



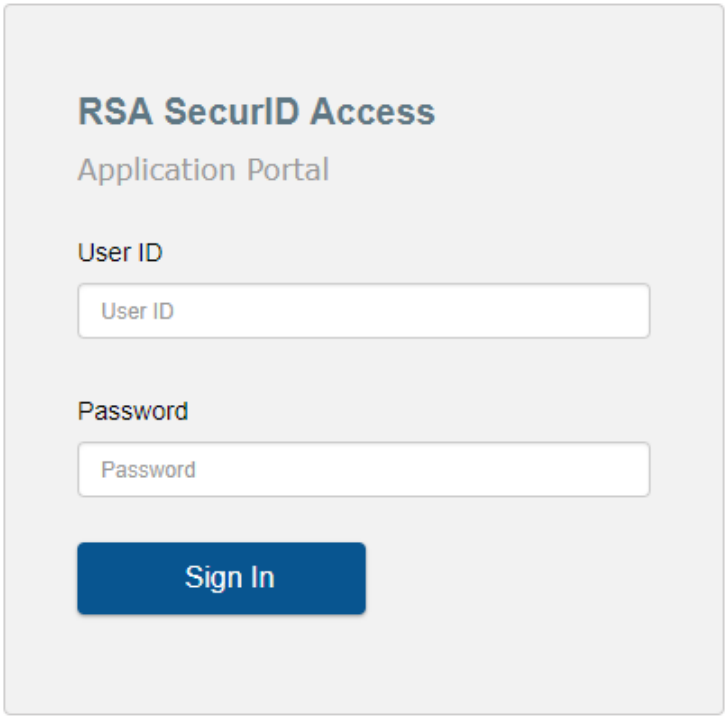
7. Click **Save Changes**.

Sign in to a Chrome device via Single Sign-on

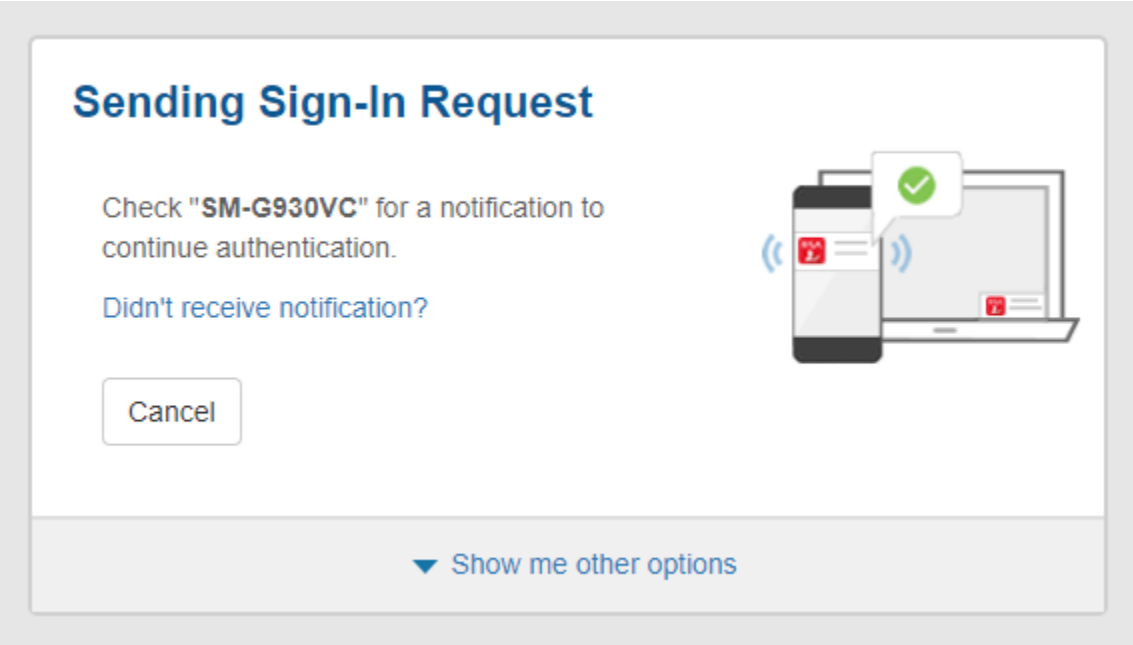
1. Enter your username in email format on the Chrome device sign in page.



2. You will be redirected to the RSA SecurID Application portal.



3. Enter your single sign-on credentials.
4. If prompted, for step up authentication complete the authentication action required.



5. Once authenticated you are granted access into your Chrome device.
6. The next time you sign in, you will only need to enter your password unless the SSO timer has been reached in which case you will be redirect to RSA SecurID Access to authenticate before gaining access to your Chrome device.