

RSA SECURID[®] ACCESS

Implementation Guide

Google Chrome OS

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



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**.

Device management

DEVICE SETTINGS

Networks

Chrome management

Google meeting room hardware

MOBILE

Setup

Password Settings

Android Settings

iOS Settings NEW

Advanced Settings

Device Approvals

App Management

Insights

The screenshot shows the 'Device management' page in the Google Admin console. On the left is a navigation menu with 'DEVICE SETTINGS' expanded to show 'Chrome management'. Two main cards are displayed: 'Mobile devices' (with a smartphone icon) and 'Chrome devices' (with the Chrome logo icon). Both cards show a count of '0' and a description: 'Manage Android, iOS and Google Sync devices' for mobile and 'Manage Chrome devices' for Chrome devices.

3. Select **Chrome management**.



4. Select **User settings**.

The screenshot shows the Chrome Management interface. At the top, there is a header with the Chrome logo and the text 'Chrome Management'. Below the header, there is a section for '0 Active users in last 7 days'. The main content area is divided into several sections: 'User settings' (Manage user-based settings on Chrome browsers and Chrome devices), 'Android application settings' (Manage access to Android applications for users and Chrome devices), 'Public session settings' (Manage public session settings on Chrome devices), and 'Device settings' (Manage Chrome device settings). The 'User settings' section is highlighted, indicating it is the selected option.

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.

The screenshot shows the Security settings page. There are two main sections: 'Single Sign-On Online Login' and 'Single Sign-On'. The 'Single Sign-On Online Login' section has a title 'Force online login flow for SAML-based Single Sign-On accounts' and a 'Frequency' dropdown menu set to 'Every 1 day'. The 'Single Sign-On' section has a title 'SAML-based Single Sign-On for Chrome Devices' and a dropdown menu set to 'Enable SAML-based Single Sign-On for Chrome'. Both sections have a 'Locally applied' status indicator.

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.

Google
Sign in to your Chromebook

Enter your email

[Forgot email?](#) [NEXT](#)

[Guest mode](#)

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

RSA SecurID Access
Application Portal

User ID

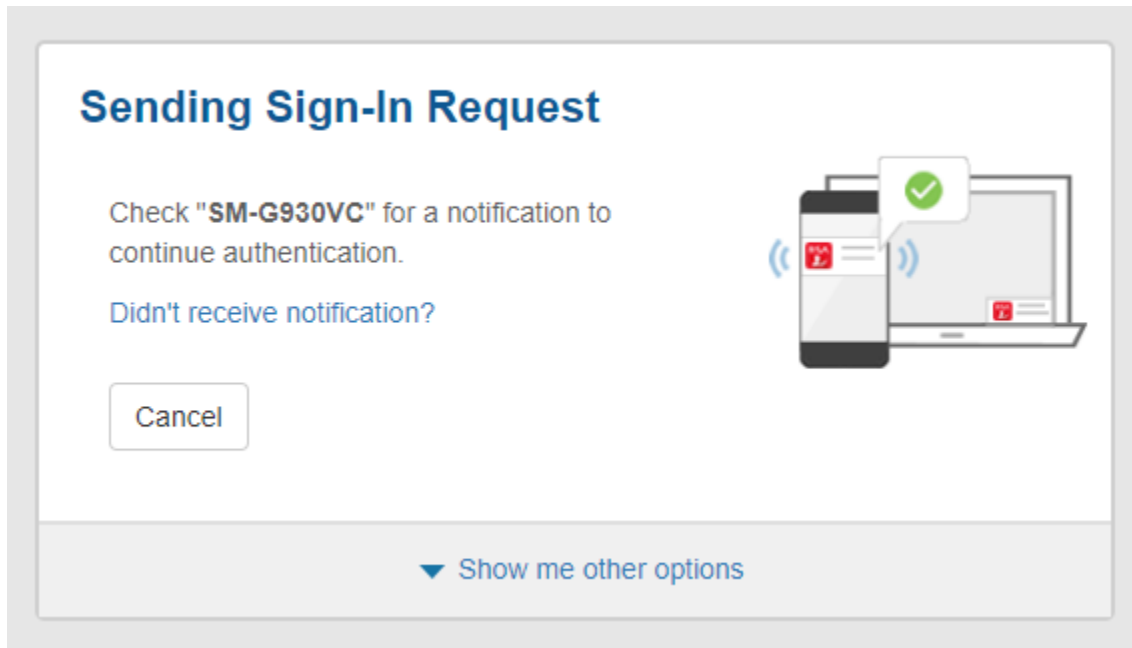
Password

[Sign In](#)

Copyright © 2015-2018 Dell Inc. or its subsidiaries. All Rights Reserved.



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.