# FEITIAN FIDO Security Key

# For

# RSA

## Table of Contents

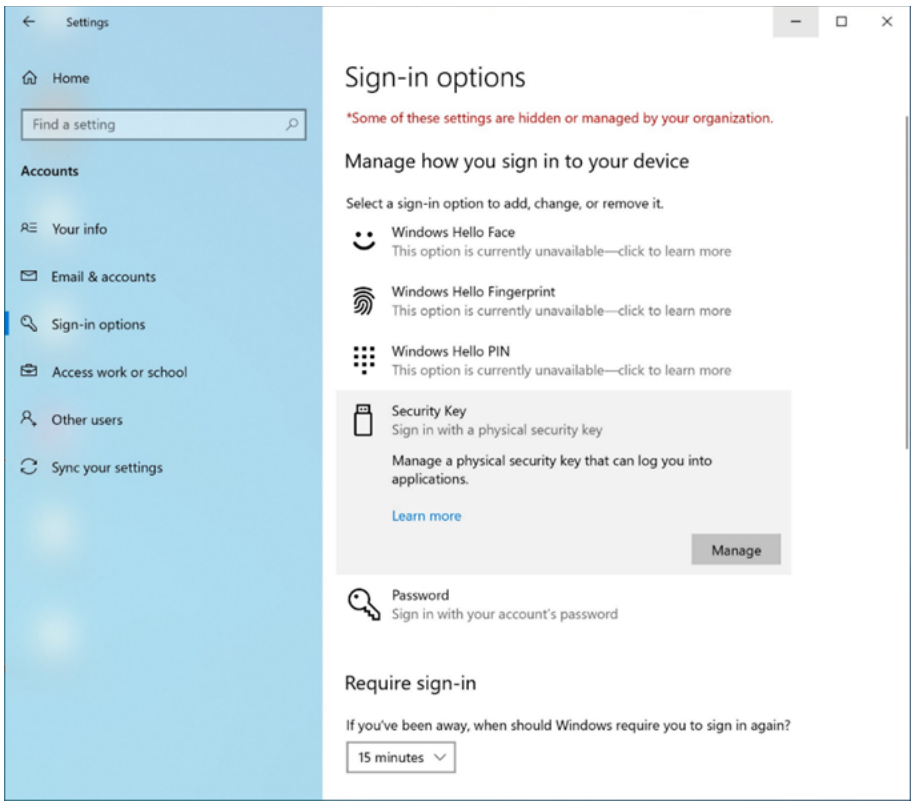
## 1. Overview

This document introduces how to integrate FEITIAN FIDO security key or authenticator with RSA service. Chapter 2 is a guidance to lead a user to manage a security key, add/change a PIN or fingerprint, for example. Chapter 3 especially describes how to register FEITIAN FIDO security key for RSA.

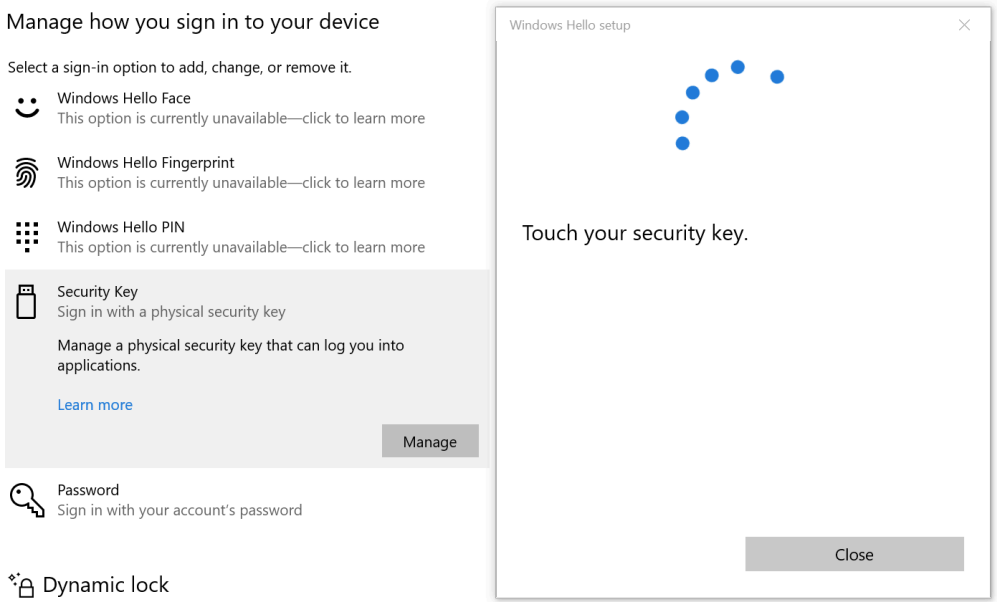
## 2. FEITIAN FIDO security key/authenticator management

- Manage a FIDO security key through Windows

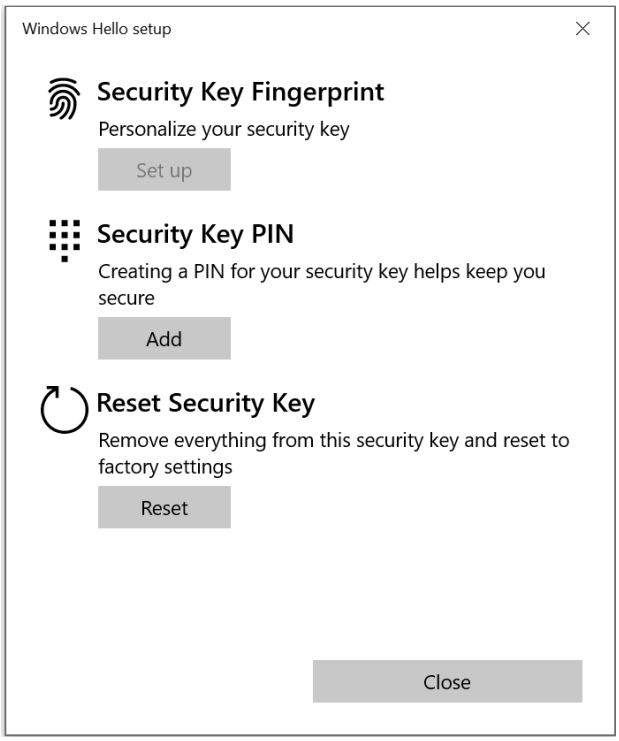
Users can manage fingerprints, PIN and reset a security key straight from settings of Windows 1903 and above via the selection of *Sign-in options/Security Key* tab.




Hit '*Manage*' button, and below window pops up to indicate you to touch your FEITIAN authenticator.




Once user touch their authenticator, the pop-up window will provide interface to manage authenticator, including add or change PIN, reset authenticator and manage fingerprint if supported.



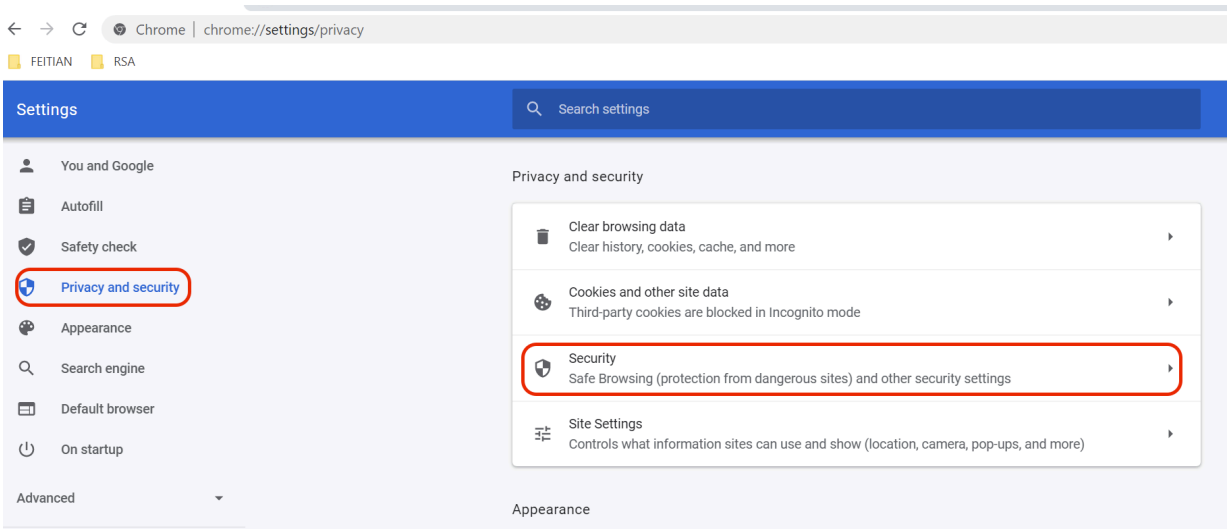

Note:

- Reset requires to be done with 10 seconds after powering up, and a touch is needed to prove user presence.
- A PIN is required before you are able to set up fingerprint.

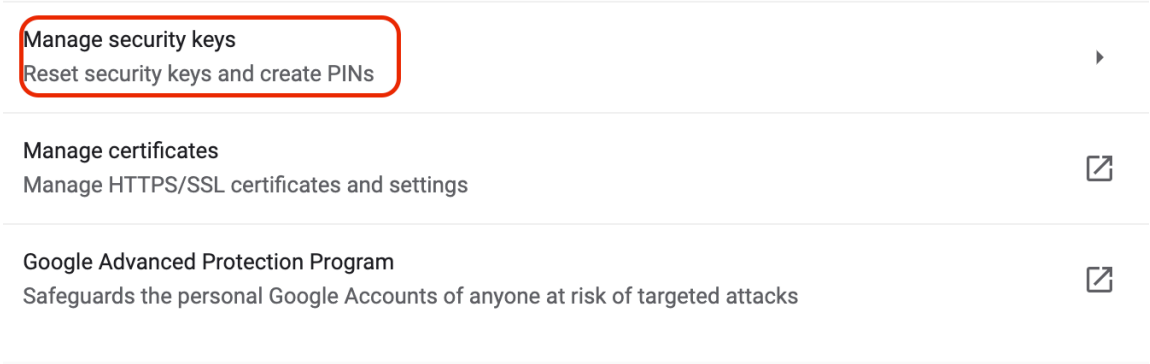
- Manage a FIDO security key through Chrome browser

On Mac OS or Linux OS, user is able to manage authenticator within Chrome.

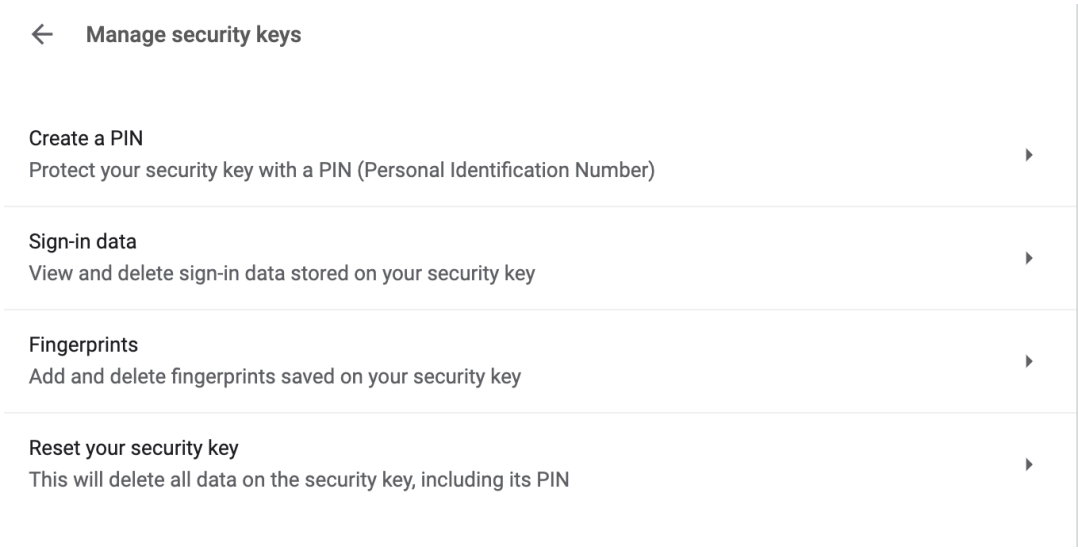
To manage FEITIAN FIDO security key with Chrome browser, user needs to go to Chrome's settings page and select *'Privacy and security'*. And choose '*Security'* on the left, as is shown below.




In the new page, scroll down, you will find '*Manage security keys*' option, and choose it.




In following page, there are four options for user to manage authenticator: PIN management, Sign-in data management, fingerprint set-up and reset as below picture:




Note:

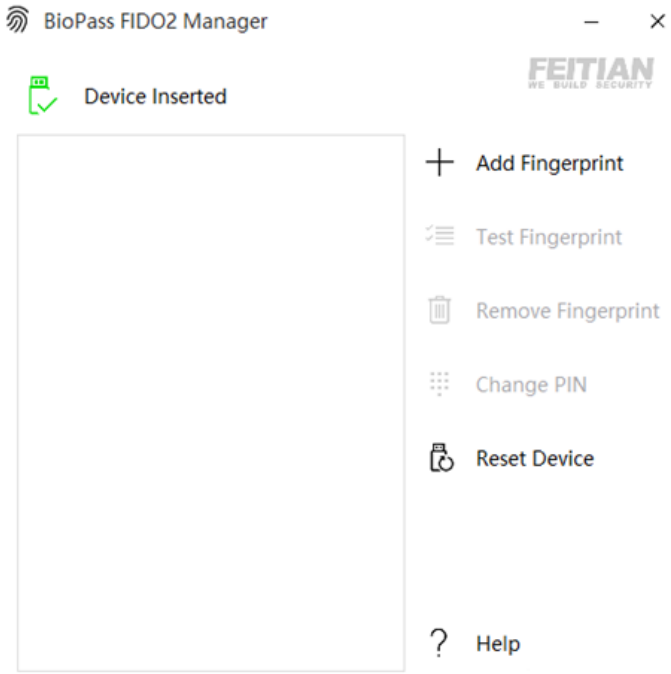
- Reset requires to be done with 10 seconds after powering up, and a touch is needed to prove user presence.
- A PIN is required before you are able to set up fingerprint.
- User is able to manage resident credential through ‘Sign-in data’.

- Manage a FIDO security key through desktop APP
  BioPass FIDO2 Manager and FIDO2_PIN_Manager.exe

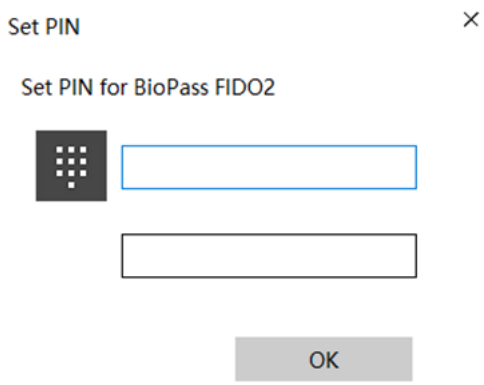
  Apart from Windows platform and Chrome browser, FEITIAN also offers desktop APP on Windows, Mac OS and Linux.
  For Windows and Mac OS, you can search 'BioPass FIDO2 Manager' in each APP store to manage the biometric security key. And for Linux, a desktop app is available at: https://download.ftsafe.com/files/FIDO/BioPassFIDO2-Manager-Linux-20200702.tar.gz.

  For non-biometric security key management tool is available at: https://download.ftsafe.com/files/FIDO/FIDO2_PIN_Manager.exe.

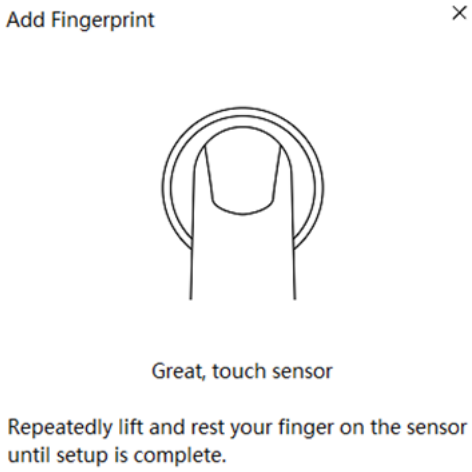
  Launch the 'BioPass FIDO2 Manager' and plug in the FEITIAN BioPass FIDO2 authenticator.



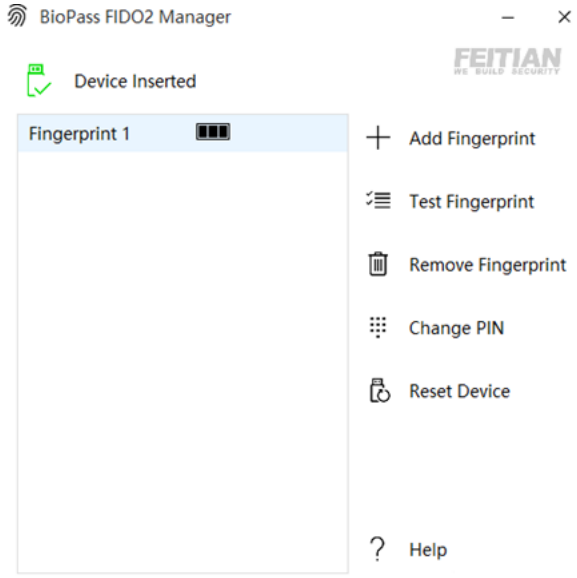

  Click "*Add Fingerprint*." you will then be prompted to set a PIN.



And then you are able to add a fingerprint by following the instructions.



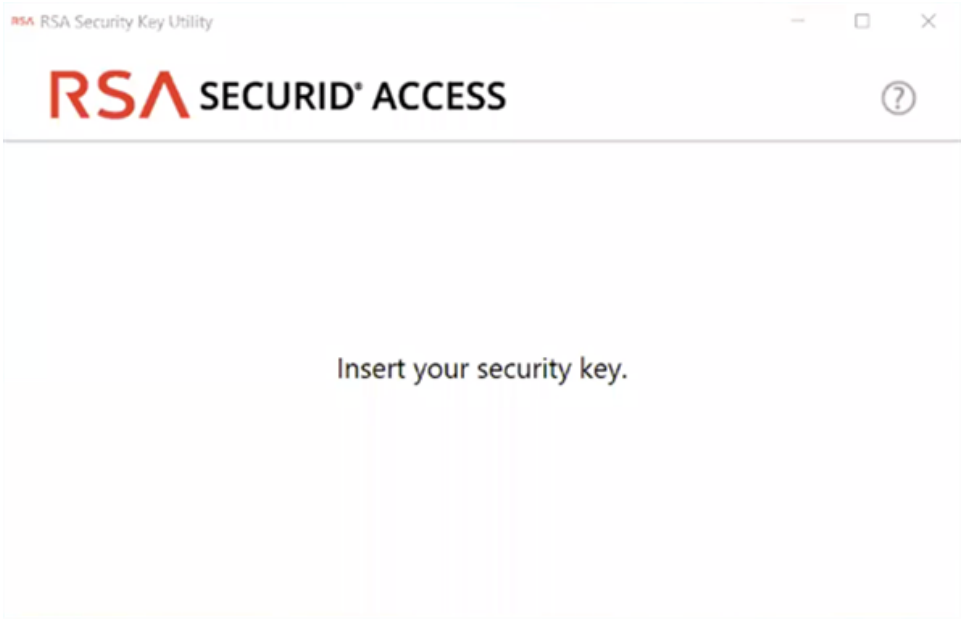

After a fingerprint is enrolled, more options are available, including add another fingerprint, test the enrolled fingerprint, removed fingerprint change PIN and reset.



- Manage a FIDO security key through desktop APP -*RSA Security Key Utility*

  It is also possible to manage your authenticator using the '*RSA Security Key Utility'*, more information is available at: https://community.rsa.com/docs/DOC-111192.

  Launch the '*RSA Security Key Utility',* you will have the below window to instruct you to insert your authenticator.




After the security key is inserted he USB port and tap the security key, you are able to add a PIN, reset the authenticator and even add a fingerprint.

## 3. Provision FEITIAN FIDO security key/authenticator to RSA

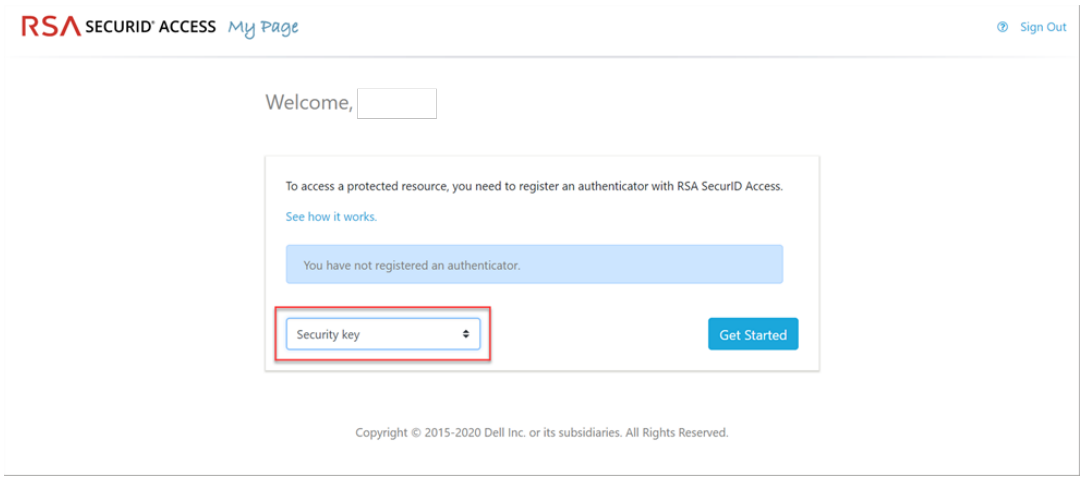
- Using a Security Key to Authenticate to a Protected Application

Before you begin:

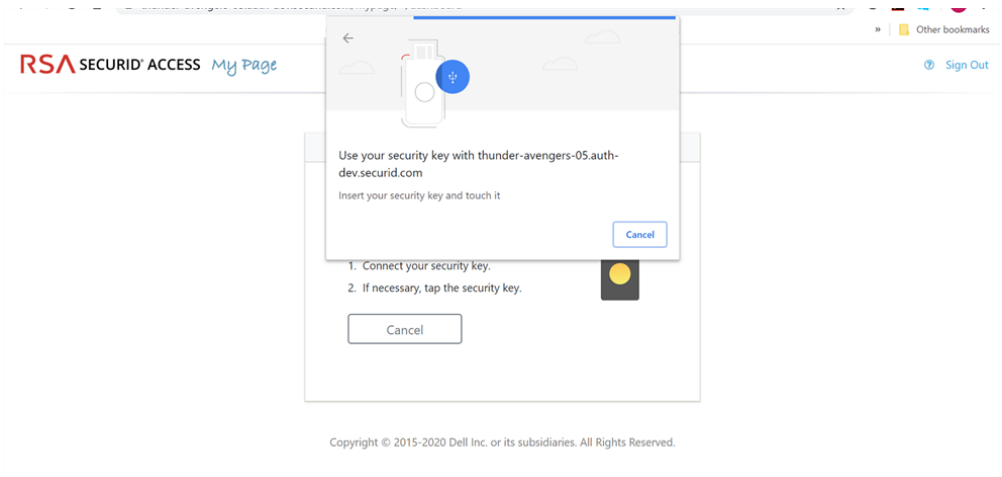
- Manage your security key (add a PIN and enroll a fingerprint) using one of the methods in chapter 2.

Register your security key in RSA SecurID Access My Page:

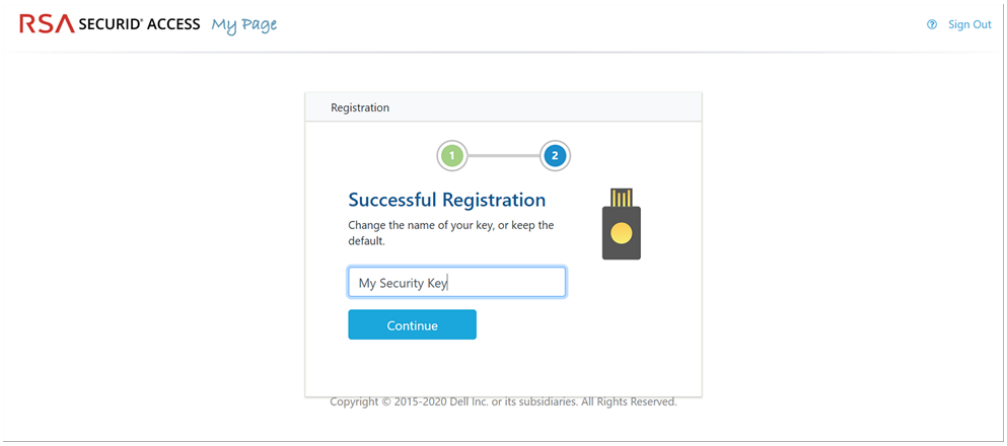
- Sign into My Page. Your IT administrator sends the My Page URL to you.
- Select '*Security key'* from the drop-down list, and click '*Get Started'*.




- Connect the security key and follow the instructions. For example, insert the security key into the USB port and tap the security key.

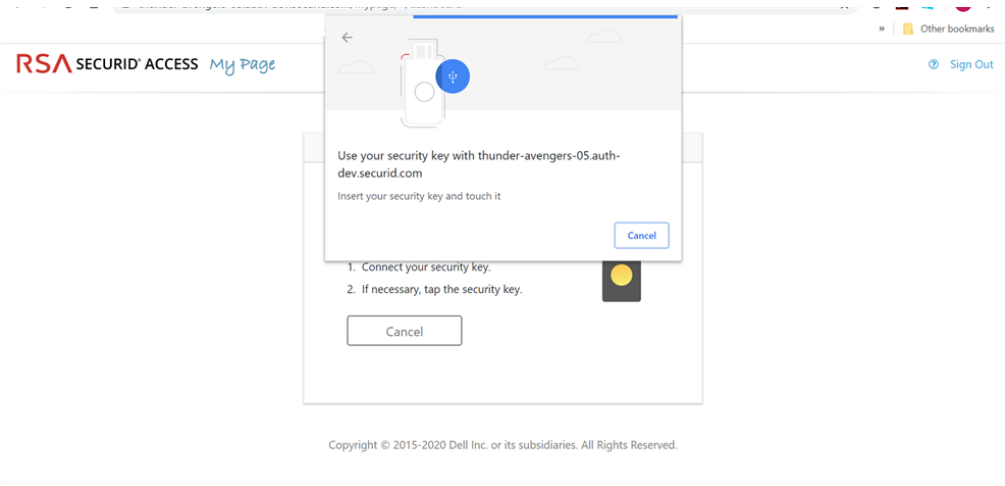



- Name your authenticator.




Authenticate to a protected application using your security key:

- Open the protected application.
- Connect the security key and follow the instructions. For example, insert the security key into the USB port and tap the security key.




- Setting Up Cloud Authentication Service for Security Keys

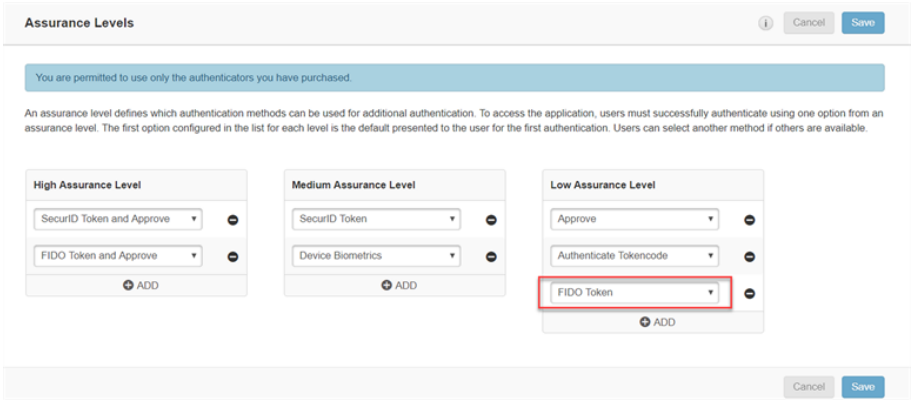
If you are an administrator, perform these steps to start using security keys with Cloud Authentication Service. These steps assume that you have an existing Cloud Authentication Service deployment.

Before you begin:

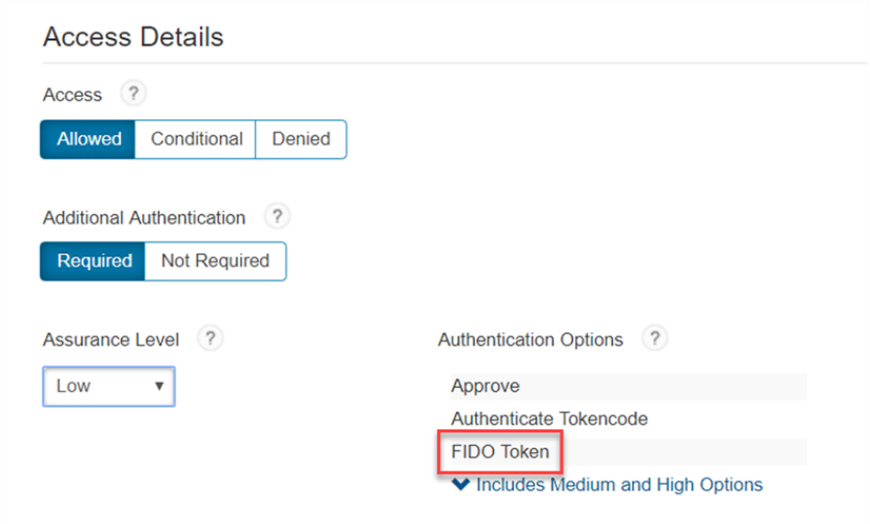
- Manage your security key (add a PIN and enroll a fingerprint) using one of the methods in chapter 2.

Set Up FIDO in Cloud Administration Console:

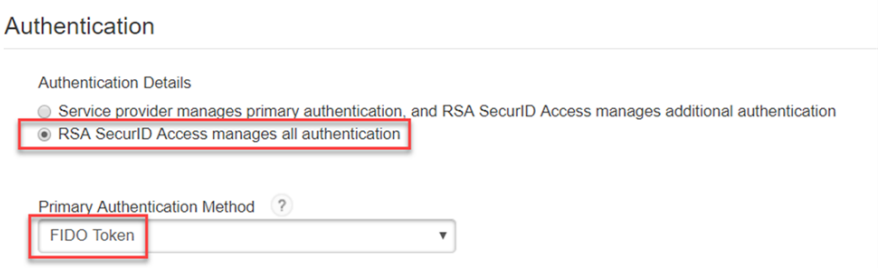
- Confirm that FIDO is in the desired assurance level:
  - In the Cloud Administration Console, click '*Access > Assurance Levels'*.
  - Add or move FIDO to the desired assurance level.



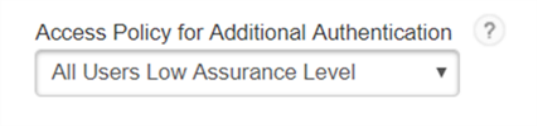

- Confirm that you have an access policy that uses that assurance level:
  - Click *Access > Policies.*
  - Click *Edit* for the policy.
  - In the Rules Sets tab, confirm that FIDO is listed in Authentication Options.




- Add a service provider:
  - Click *Authentication Clients > Relying Parties > Add a Relying Party > Add* next to Service Provider.
  - Determine if you want to use FIDO for primary authentication or additional authentication, or both.
    If you want to use FIDO for primary authentication, add a service provider and specify FIDO as the primary authentication method. In the Authentication tab, select *RSA SecurID Access manages all authentication*. In the Primary Authentication Method drop-down list, select FIDO.



- If you are using FIDO for additional authentication, in the Access Policy for Additional Authentication, select the policy that contains FIDO.




- Enable FIDO authenticator registration in My Page:
  - Click '*Platform > My Page'*.
  - Under Configuration, select *'Users can register FIDO authenticators in My Page*' and select '*Security key'*.