Entrust Soft Token User Guide

Ministry of Central Services
Information Technology Division

Issued: April 2017
Reviewed: August 2020
Next Review: August 2020

This guide should be used to learn how to set-up and use an Entrust soft token on your mobile device.

About Entrust Soft Tokens

Are you working from a Government of Saskatchewan mobile device? Be sure that your device is secure by installing the Entrust IdentityGuard application.

This how-to guide will introduce you to how the IT Division (ITD) of Central Services manages soft tokens. These tokens are what enable the ITD to know the identity of the mobile device connecting to the Government of Saskatchewan network.

Installing the Soft Token on a device

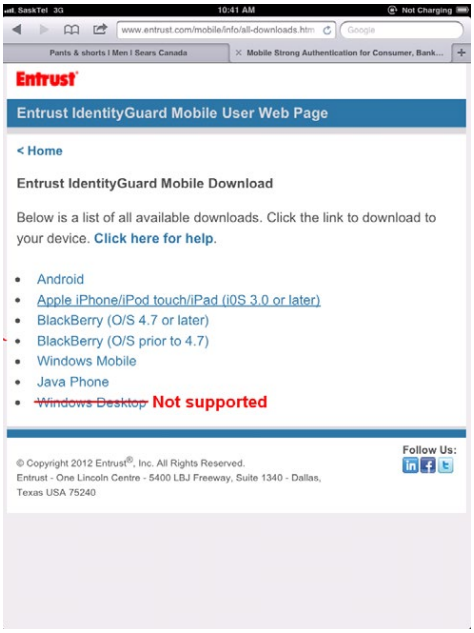
The Entrust soft token software is available for a wide variety of devices including: the Apple iPhone, Google Android, RIM BlackBerry, Microsoft Windows Mobile and Symbian. There is also a client available for the Windows operating system, but this is **not** supported by ITD at this time.

If you have issues with the download and installation of the Entrust soft token software:

- For Government of Saskatchewan employees, please call the ITD for support.
- For external users, please contact your IT provider for support.

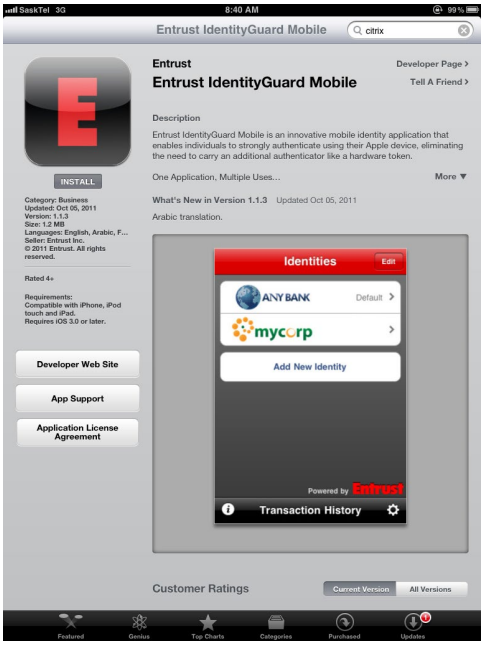
To install the soft token software on your device:

1. Using the device you want to install the soft token to, open the browser
2. In the address bar, enter the URL: **www.entrust.com/mobile/info/all-downloads.htm**
3. Choose the device that you want to download the application for. Or, alternatively, you can use this URL to auto choose the software for the device: **www.entrust.com/mobile/info/download.php**



Saskatchewan

4. A screen will be displayed that says ‘Entrust IdentityGuard Mobile.’ On this screen there should be an install button. Press it. There is no cost to install this application. It is free. You may be asked for your credentials to the App store for your device. Enter them.

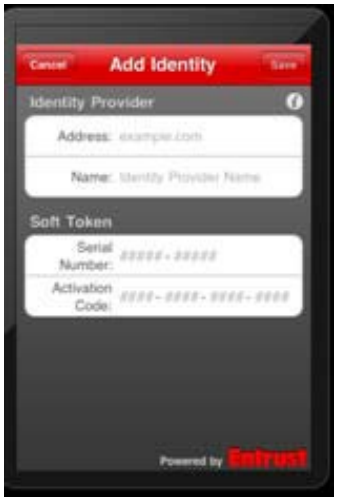


5. An icon for ‘Entrust IdentityGuard Mobile’ will appear on a page on your device. This will be a red ‘E’ on a black background and may have the word ‘Entrust’ below it.

Configuring the Soft Token

Now that the application has been installed, it needs to be configured. This requires you to work with the ITD Service Desk (1-306-787-5000). A two-way synchronization needs to be set up. You will need to enter information from IdentityGuard into the IdentityGuard Mobile application and you will need to provide information back to the administrator to enter into IdentityGuard on the server.

1. Start the ‘Entrust IdentityGuard Mobile’ application.
2. You will get a popup saying ‘Entrust would like to send you push notifications’ – the ITD would suggest choosing ‘Don’t Allow.’
3. A screen will appear to ‘Add Identity.’



4. Call the ITD Service Desk (1-306-787-5000) and tell them that you need your soft token activated. They will verify your identity and then work with you to complete the fields below and activate your soft token:

    a. Address – this field can be left blank. It isn't necessary.

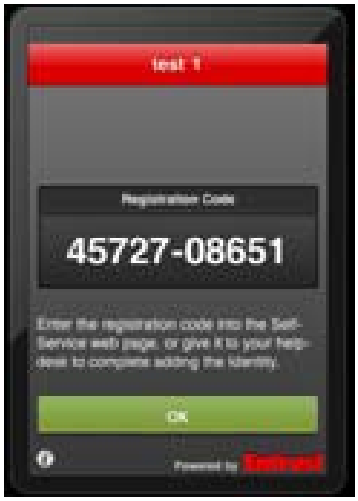
    b. Name – this is the name that will appear in the Identity list. You can have multiple identities (tokens that will be generated) – for example, you may have an ID in the dev system and a token associated with it, an ID in the test system and a different token associated with it, an ID in the production system and a different token associated with it. Each of these tokens needs to be named something that is identifiable in the list. So, choose a name that will identify this token to you. Some suggestions would be 'GoS logon', 'CJIMS dev', etc.

    c. Serial Number – The ITD will provide you with the Activation code. It will be 16 digits long.

    NOTE – it is important that the Serial Number and Activation code be typed correctly. Any discrepancy between what the Administrator sees in IdentityGuard on the server and what is typed in the soft token will cause the soft token not to work.

    d. You will be asked to supply a PIN. Choose 4 digits that you will remember for this PIN. Each time the Entrust IdentityGuard Mobile is opened, you will be asked to provide this PIN. Choose a number that is easy for you to remember. **There is no way to retrieve this number if you forget it.**

e. A Registration code will be displayed. It will be 10 digits long. Dictate this back to the ITD. It must be entered into the IdentityGuard Server application.



f. ITD will activate the token.

g. This completes the handshake synchronization.

h. Click the 'OK' button.

i. You will be asked if you have used the Registration code. If you have provided it to the ITD and they have used it to activate your soft token, click the 'Yes' button.

5. The identity that you added now appears in the Identities list. You can use this identity in conjunction with the user ID in IdentityGuard that it was associated to. It will only work with that specific user ID.

6. Clicking on that identity will display the security code that must be entered into the PIN field when Two-factor Authentication (2FA) is required in the application.

Notes

A couple things to note about using the token:

- A token (hard or soft) can get 'out of synch' with the server. This typically happens if the token is reset a number (10+) times without the number being successfully entered into a PIN field. If the token is out of synch, the user must call the ITD Service Desk (1-306-787-5000) and ask them to resynch it.
- The passcode (also called a PIN) will be displayed, and is only valid, for approximately 20 seconds. After that a new passcode will be displayed.
- For a soft token, when you are done entering the PIN and it has been accepted, close down the soft token application on your device. Otherwise it will keep generating tokens and could become out of synch with the server.