

RSA SecurID Software Token Prerequisites

Description

- A software token (or soft token) is an application used in two-factor authentication systems.
- It generates a code that is used with your access credentials to login securely to an AHS network service. This provides additional security as you must have two separate pieces of authentication to login.
- Software tokens are issued via email to a device, typically a smartphone.

Prerequisites

The following are the prerequisites for requesting a software token.

1. Device must be supported

- 1.1 Apple (iOS) Devices – iPhone, iPad, or iPod Touch
- 1.2 Android Devices – this is an operating system across many manufacturers of different smartphones. Examples: Samsung, Sony, and Google.

2. Technical Specifications

- 2.1 Each type of smart device also has minimum technical requirements. Please refer to these when trying to download the RSA soft token app on your device. Check the Google Play® app store on Android devices, and the App Store® on Apple devices.
- 2.2 Whichever smart device you choose must be able to run the latest version of the RSA Soft Token application.

3. User Requirements

- 3.1 a valid email address that can be accessed from the device
- 3.2 the ability / access to install the software token application on the device
- 3.3 an internet connection on the device
- 3.4 an internet connection on another device to access the activation website
- 3.5 no organizational / departmental restrictions regarding the use of mobile devices
- 3.6 appropriate approval process is followed.

Security Requirements

- One token is provisioned per end-user – a soft token or hard token, but not both. You can switch types if your needs change.
- The device the software token is configured on must be password / PIN protected and be regularly maintained with the latest security patches.
- Only install the RSA SecurID App from a trusted source (the official application store or marketplace) and keep the software updated.
- Never share your device or token information (e.g., password, PIN, passcode) with anyone.
- Report lost or stolen devices immediately to the AHS IT Service Desk at 1-877-311-4300.