

# Remote Access

## *End User Reference Guide*

---

**VERSION 7**

**08/25/21**

# Contents

INTRODUCTION .....	3
Purpose of This Document .....	3
Intended Audience .....	3
Process Overview .....	3
To Get Started You Will Need: .....	3
REQUIREMENTS .....	4
RSA SecurID Software Mobile Device .....	4
Supported Devices for Remote Access .....	4
Supported Browsers for Remote Access.....	4
Supported Operating Systems for Remote Access .....	4
REMOTE ACCESS PROCESS .....	5
Remote Access Request .....	5
RSA SecurID Authentication.....	5
Launch a Remote Session.....	9
Installing or Updating Citrix Receiver .....	10
Logging Off .....	10
Things to Note Once Connected .....	11
Tips & Hints .....	11

## INTRODUCTION

### Purpose of This Document

This document provides detailed steps on setting up and accessing your Santa Clara County resources remotely.

**Please read this document in its entirety before calling the TSS Service Desk for assistance.**

### Intended Audience

All **County** employees and designated and approved third-party vendors who are authorized for remote access to **County** applications.

### Process Overview

1. Request Remote access (**new remote access users**), existing remote access users will submit a Service Desk request via Cherwell  
<https://connect.sccgov.org/teams/forms/isd/csd/SitePages/ServiceDesk.aspx> for a confirmation URL
2. Download the RSA SecurID Software Token App to your mobile device
3. Import the token using the confirmation URL on your mobile device that you will receive from the Service Desk
4. Access the remote access site at <https://scvhhsremote.sccgov.org/vpn/index.html>
5. Update Citrix Workspace (if needed)
6. Enter your Tokencode that is being generated from your smartphone. If less than 20 seconds, wait for the next rotation of random numbers.

### To Get Started You Will Need:

1. A current active network account (also known as your Active Directory account).
2. You must have completed the necessary remote access permission forms supplied by IS.
3. A mobile device for your authentication code.
4. A supported device to remotely access your HHS resources.
5. A supported internet browser.

## REQUIREMENTS

### RSA SecurID Software Mobile Device

- iPhone iOS 9 and above
- Android
- iPad

### Supported Devices for Remote Access

- Windows supported Workstations
- Windows supported Laptops
- Windows supported Laptops
- Apple Workstations
- Apple Laptops

### Supported Browsers for Remote Access

#### Windows:

- Internet Explorer V11 or higher
- Firefox v10 or higher
- Google Chrome
- Microsoft Edge

#### Apple/OS X:

- Apple Safari v9 or higher
- Firefox v10 or higher
- Google Chrome

### Supported Operating Systems for Remote Access

- ~~Windows 7~~
- Windows 8
- Windows 10
- Maverick – Sierra (10.9 – 10.12)

### Configurations *not* Supported for Remote Access

- iPad devices (limited support)
- Android Devices or pads
- Smart phones of any type
- Virtualized local desktops, like VBOX or FUSION running on Windows or OS X
- **NOTE:** On non-County owned devices, the Information Services department will make a best effort to provide troubleshooting assistance should you require it. On County owned devices we provide full service.

# REMOTE ACCESS PROCESS

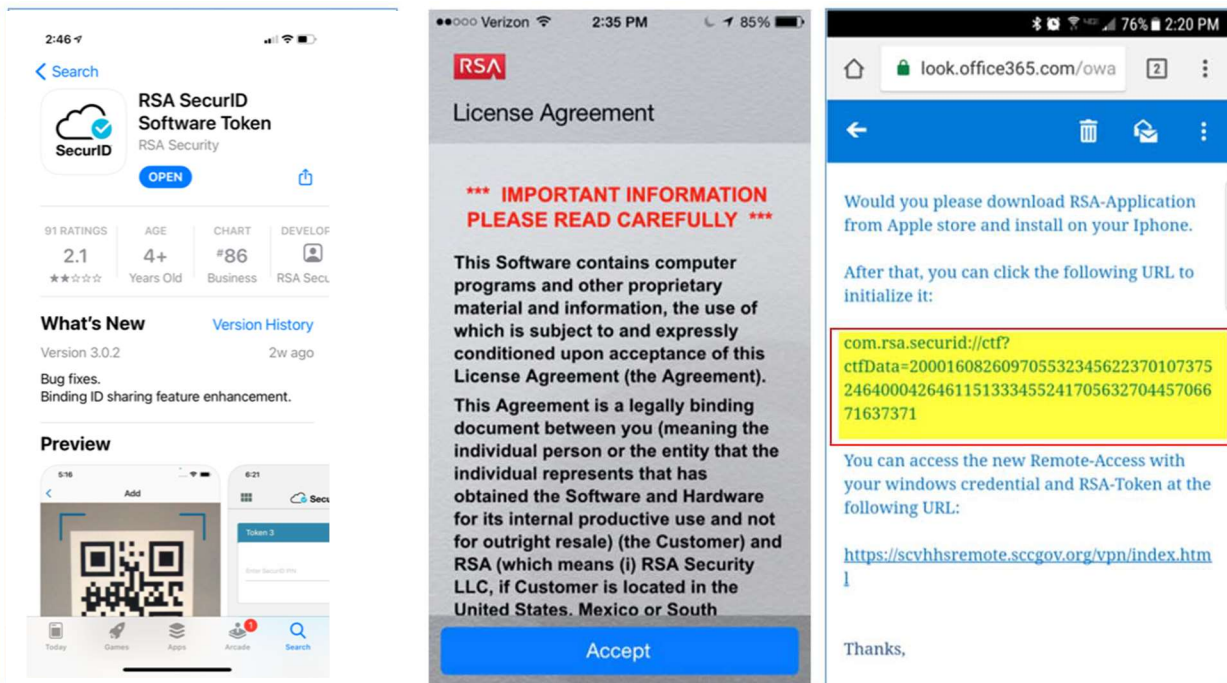
## RSA SecurID Authentication

The RSA SecurID Software Token app generates one-time passwords for additional security when remotely accessing County internal resources. The app needs to be downloaded to an iPhone or Android mobile device. To connect a remote session you will enter both your Username and password (Active Directory username and password) along with the generated token from the RSA SecurID app on your mobile device.

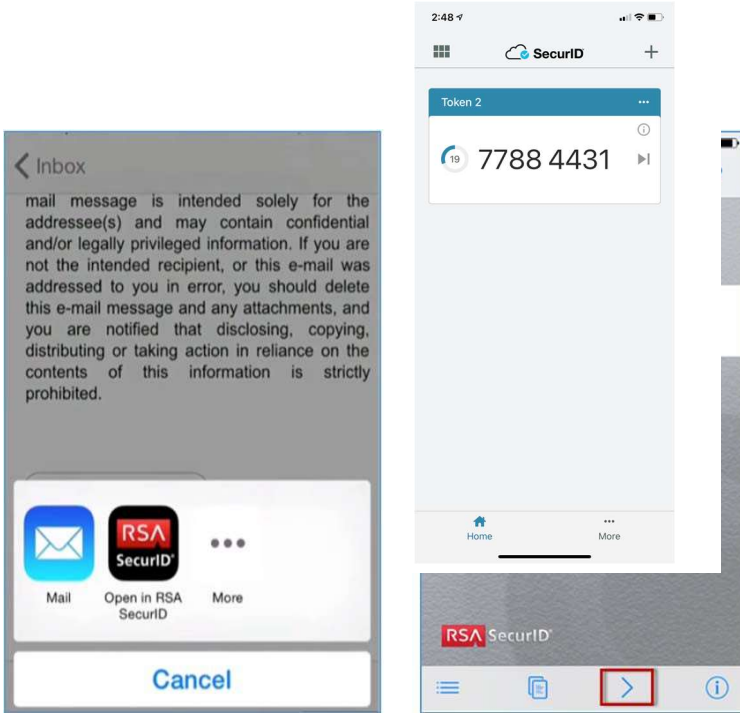
### Download RSA SecurID on an iPhone device:

In this step you will download the app and then use the URL you receive via email from the Service Desk to initiate the App once you've installed it.

1. Open App Store and search for RSA SecurID in the search field.
2. Select **RSA SecurID Software Token** app
3. Tap on the **download** (Cloud with checkmark) button to begin installation process
4. Once installed, **open** your SecurID app
5. **Accept** the license agreement and you will be taken to the import window
6. Go to the email sent by the Service Desk and copy/paste the link and *Submit*. The app will immediately begin working.
  - a. If you do not have access to your SCC email account on your mobile device; you can forward the email to your personal email account



- 7. Note that the token will update every 60 seconds, you must enter the token in the Remote Access logon window within the time noted
  - a. You can tap Next >to get a new token

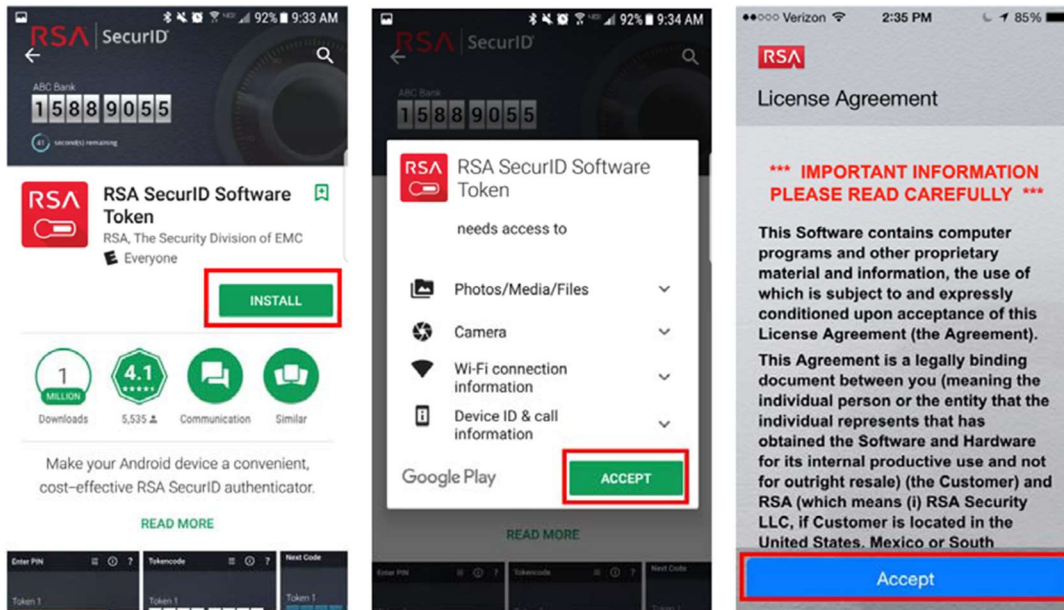


## Download RSA SecurID on an Android device:

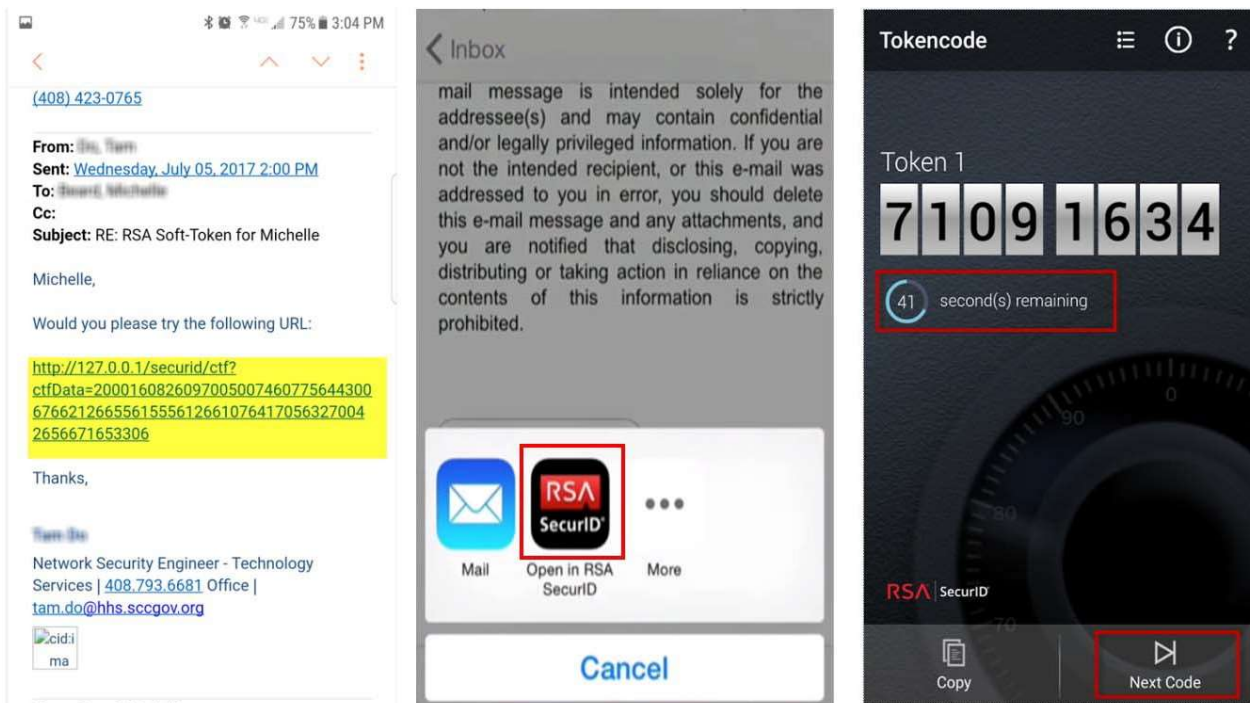
In this step you will download the app and then use the URL you receive via email from the Service Desk to initiate the App once you've installed it.

1. Open Google Play Store and search for RSA SecurID in the search field. Select RSA SecurID Software Token app
2. Tap on the **Install** button to begin installation process
3. Click **Accept** to allow access

**Accept** the license agreement and you will be taken to the import window Once installed, **open** your SecurID app



4. Import the token using the confirmation URL emailed by the Service Desk
5. Open the email from the Service Desk containing your token URL
  - a. If you do not have access to your SCC email account on your Android you can forward the email to your personal email account
6. Tap the URL link, or Copy/Paste the entire URL into the app
7. If prompted select RSA SecurID from the list of applications to open the link
8. Tap OK to begin using your RSA SecurID to log onto the remote access
9. Note that the token will update every 60 seconds, you must enter the token in the Remote Access logon window within the time noted
  - a. You can tap Next >to get a new token

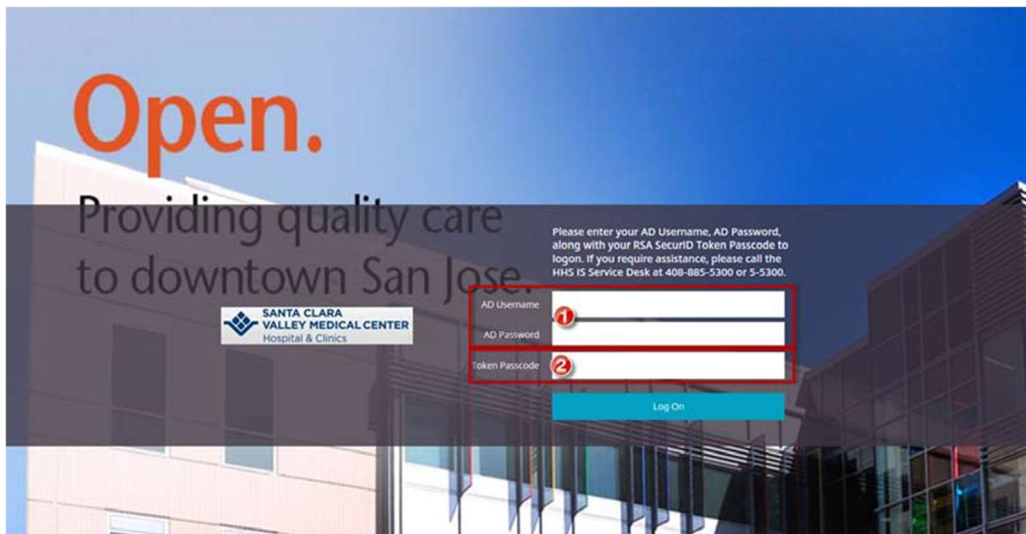




## Launch a Remote Session

NOTE: Turn off your pop-up blocker on your web browser before proceeding.

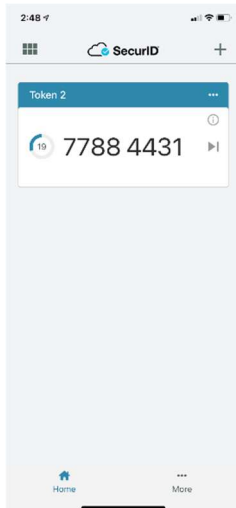
Using a supported browser on a supported device navigate to <https://scvhhsremote.sccgov.org/vpn/index.html>



1. Enter your AD Username and password. These are the same credentials you use to access your workstation at work

Open the RSA Token app on your mobile device

2. Enter the Token passcode (numbers generating on your smartphone)
  - a. Note: you must enter the passcode within the time noted; select Next if you need more time



Click **Log on**; upon which you will be connected to your remote session

- b. **If you are prompted to install or update your Citrix Workspace, follow the steps in the next section**

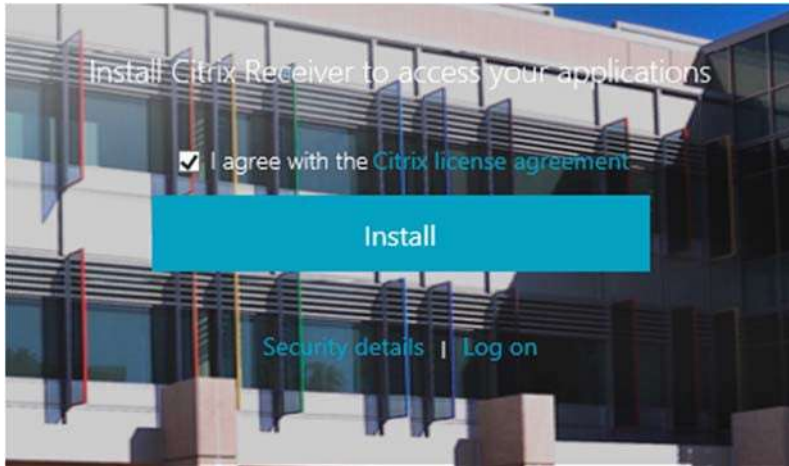
Click the Remote Access Desktop icon to be connected to your desktop resources



## Installing or Updating Citrix Workspace

**Note:** this step will be skipped if you have the current version of Citrix

1. If you do not have Citrix Workspace, or the most current version installed already, you will be prompted to install it
2. Click to check the box to accept the Citrix agreement, then click Install

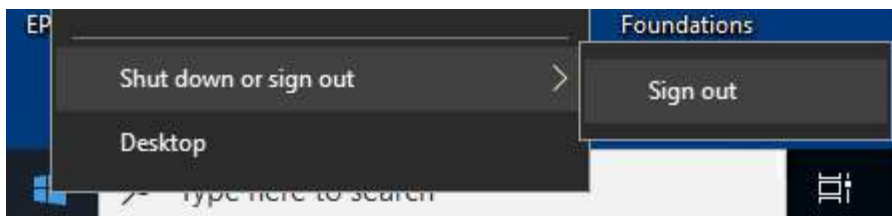


3. Click Start to begin the installation process.
4. **NOTE:** If you are prompted to “add account” or enter an address, **just bypass or cancel** this dialog.
5. Once you complete the installation, you will be returned to the remote logon screen
6. Enter your AD username, password and RSA Token as described in the previous section

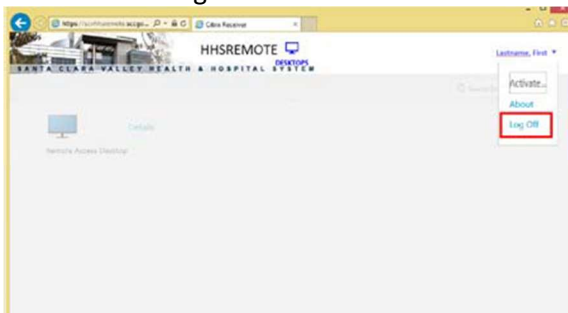
## Logging Off

When you are done with your remote session you will need to **sign out** of your remote desktop, just as you do with your desktop or laptop. Do not just disconnect/close the window. Sign out helps ensure you will be able to log onto future sessions without any issues.

1. Right-click the Windows icon, select *Shutdown or sign out > Sign out*



2. You can then Log Off of the remote session or simply close the browser window



## Things to Note Once Remotely Connected

- You may not cut and paste from your local computer into the remote session, or vice versa. This is a security precaution to protect PHI sensitive information.
- Printing to your local/home computer is disabled as a security precaution.
- Your remote session will not have access to your local/home disk drives, such as your laptop C: drive as a security precaution.
- You will see a standard set of icons on the remote session desktop, including ALL personal desktop icons from your County work computer. As such, you may see more icons than the picture shown above.
- Only our standard County enterprise-wide applications are available on the remote session desktop. For example: HealthLink. Departmental and personal workstation installed applications will not be available on the remote desktop session.
- It is important to realize you are not remotely connected to your actual work computer. Rather, what you see on the remote access session desktop is a close approximation of your work computer.

## Tips & Hints

- My session keeps disconnecting.
  - If you are wireless, try to get a better signal.
  - Make sure you don't have other applications running on your computer while you are connected to Remote Access.
  - If you have a Mac, make sure you have the latest Citrix Workspace-app receiver for MAC 12.5

If you "disconnect" for any reason you may reconnect within 5 minutes without losing any of your data or changes.

- If you have the Windows or Mac firewall turned on, please make sure you allow all traffic to/from <https://scvhhsremote.sccgov.org>. If that still won't work, then temporarily shut off your firewall.
- We recommend that you not enable "private browsing" setting in your browser. This will prevent necessary cookies from being installed as part of the first time login process.

## Support

Information Systems maintains a 24x7 Service Desk. If you are experiencing problems that you cannot resolve, please contact our TSS Service Desk at: **1-408-970-2222**

For non-urgent issues, please open your own ticket

<https://connect.sccgov.org/teams/forms/isd/csd/SitePages/ServiceDesk.aspx>

If you have suggestions / recommendations, please email us at:

[support@tss.sccgov.org](mailto:support@tss.sccgov.org)