



Setting up FortiToken on Android devices

Overview

Before you can use remote access on an Android device, you need to request access to *Remote Access Token Mobile FortiToken*.

FortiToken is an extra layer of security to keep you and our information secure when working remotely.

The application is required to use remote access.

This article is designed to help you set up FortiToken on an Android device.

Examples of an Android device include Samsung, Sony Nokia or HTC smartphones or tablets.

Use these links to navigate the document:

- [Download the FortiToken Mobile app](#)
- [Configure the FortiToken Mobile app](#)
- [Manage multiple mobile remote access tokens](#)
- [How to uninstall the FortiToken Mobile app](#)
- [Support](#)

Important note:

These instructions have been prepared using an Samsung Note 8, Version 7.1 (Nougat).

You may have a different experience on your device if using a different device or a different Android version.

Separate instructions are available for staff using an *Apple iOS device* or those who need to request a physical FortiToken device.

Download the FortiToken Mobile app

Step 1

From the *Google Play Store*, search for and download/install *FortiToken Mobile*.

Tap **Install**.



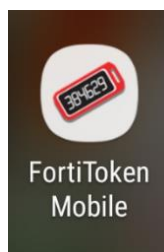
Configure the FortiToken Mobile app

Note: These steps take around 10 minutes to complete.

Important note: *FortiToken Mobile* uses your device's PIN or registered thumb/fingerprint. If you use a swipe pattern for security, you will be asked to create a PIN during the configuration process.

Step 1

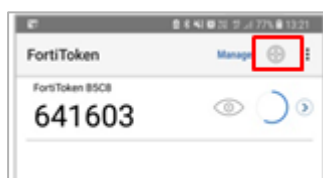
Tap the **FortiToken Mobile** app icon to open the application.



Step 2

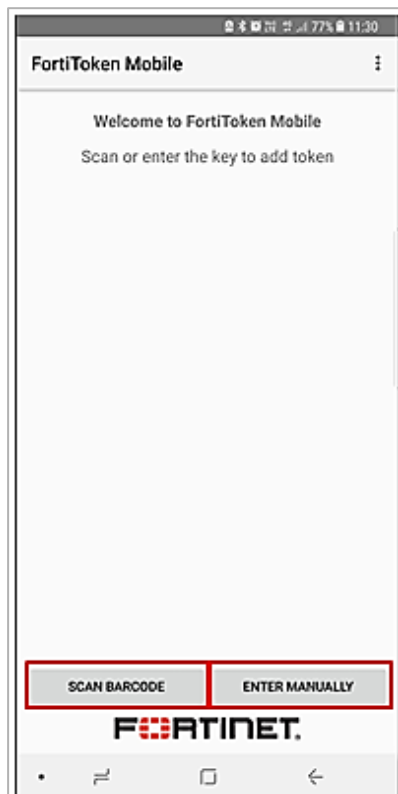
Note: If you are a first time user of the *FortiToken Mobile* app please follow on from Step 3.

If you already use the FortiToken app for Health PROTECTED Environment access, on the top right hand corner tap the + button to add a new FortiToken.



Step 3

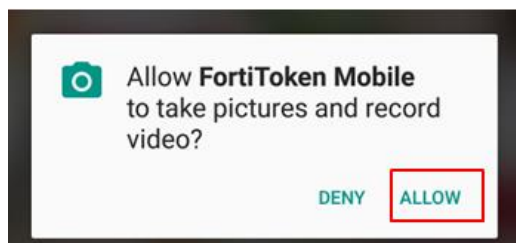
Tap **SCAN BARCODE** to scan the Quick Response (QR) code sent to you by email from tokenauthentication@health.gov.au, or tap **ENTER MANUALLY** to enter the activation code.



Scan barcode

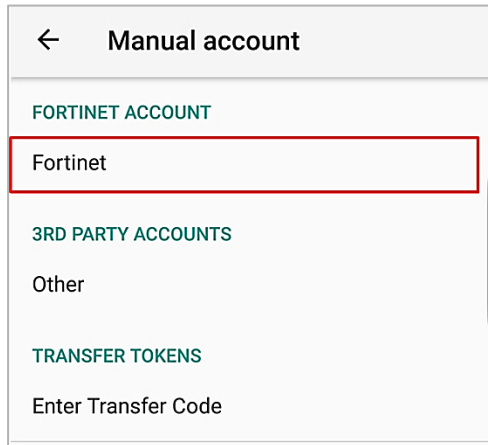
To scan QR code, review the request asking to allow *FortiToken Mobile* to take pictures and record video and tap **ALLOW**.

Note: If you choose **DENY** you will not be able to use a QR code to set up the *FortiToken Mobile* app.

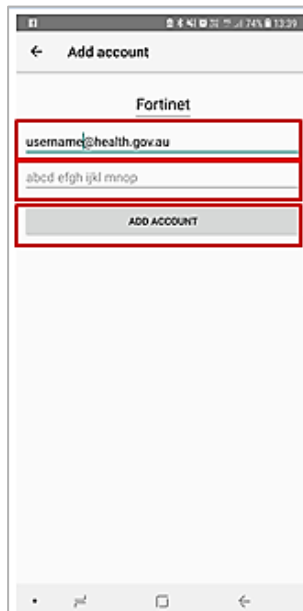


Enter manually

To enter manually, tap **Fortinet**.



Enter your Health email address and the activation code sent to you by email from tokenauthentication@health.gov.au into the fields provided and tap **ADD ACCOUNT**.

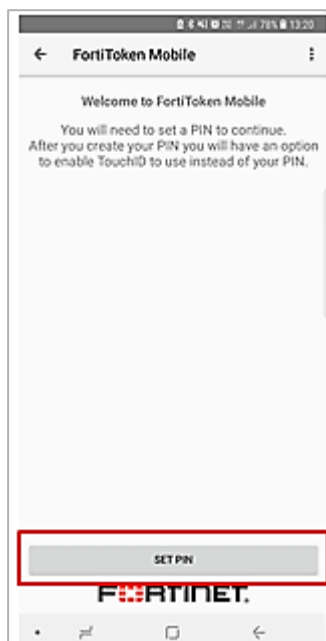


Important: Your password will expire after 7 days of receiving the email, to get a new password the user is required to contact the IT Service Desk.

Note: The token for remote access to the UNCLASSIFIED network will be added instantly for Health PROTECTED Environment users. The following steps do not apply for these users.

Step 4

You will be required to setup a PIN to activate and access your token. Tap **SET PIN**.



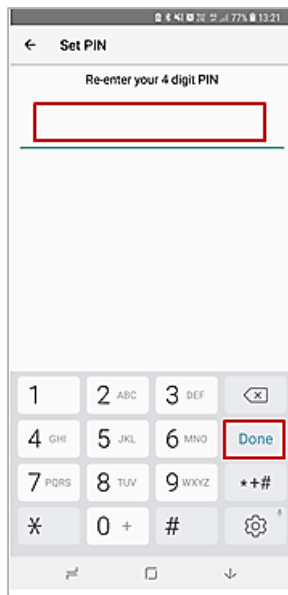
Step 5

Enter a 4 digit PIN then tap **Done**.



Step 6

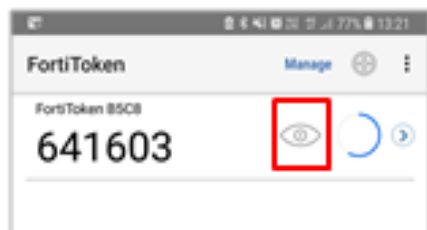
Re-enter the same 4 digit PIN then tap **Done**.



Step 7

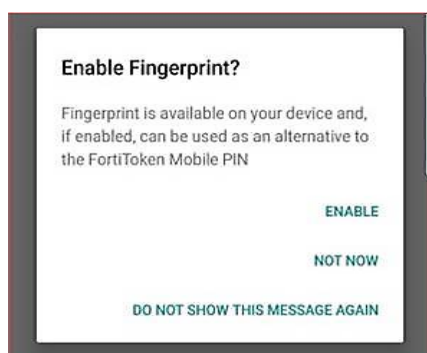
Token code will be displayed.

Note: Token codes are generated every 60 seconds and can be viewed by tapping on the **eye** symbol next to the code.



Step 8

On the next logon, you can enable fingerprint if your device supports this functionality to access your token. Tap **Enable** if you wish to do that.



Existing remote access users: Re-configure your default server (Windows)

If you are an existing remote access user you will need to re-configure the *Big-IP edge client* on your Windows laptop/PC before connecting to the Health network remotely.

Note: New users do not need to complete these steps and can now follow the instructions to get started with remote access for Android devices.

See the instructions available *Getting started with remote access for Android tablet devices* article.

Step 1

Open the **Big-IP edge client** on your local Windows computer.

Ensure you are disconnected by clicking the **Disconnect** button.



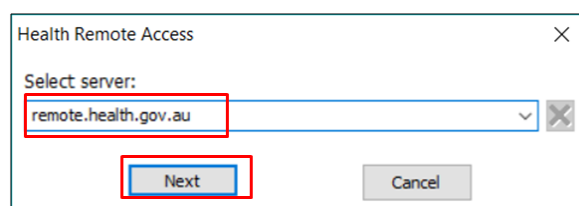
Step 2

In the Big-IP edge client, select **Change Server**.



Step 3

Enter **remote.health.gov.au**. Click **Next**.



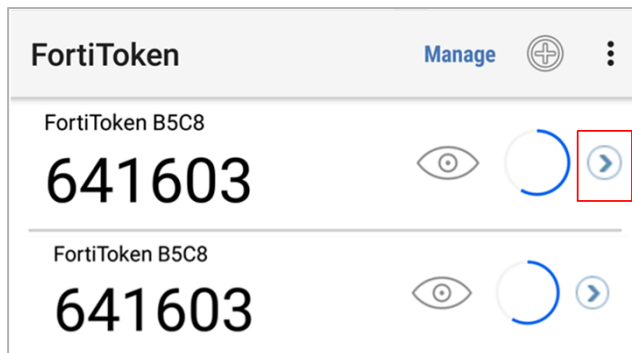
Your default server should now be updated. You can now follow the instructions to get started with remote access for Android devices. See the instructions available *Getting started with remote access for Android tablet devices* article.

Manage multiple mobile remote access tokens

If you already utilise the *FortiToken Mobile* app for another token, it may be useful to rename them to differentiate between the tokens (e.g. if you have a token assigned for Health PROTECTED Environment access).

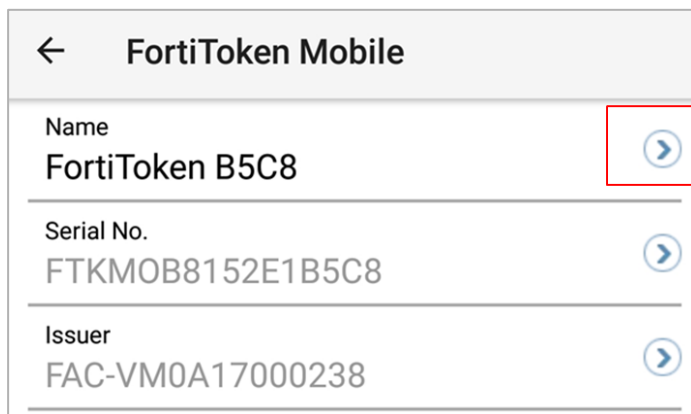
Step 1

Select the token you wish rename.



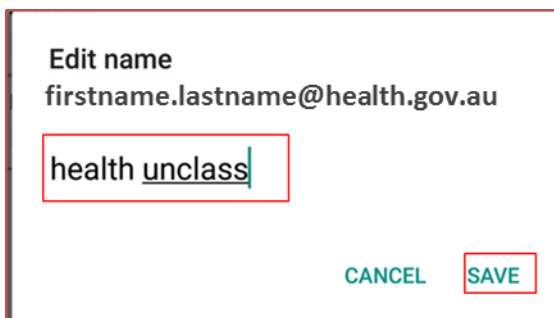
Step 2

Tap **Name**.



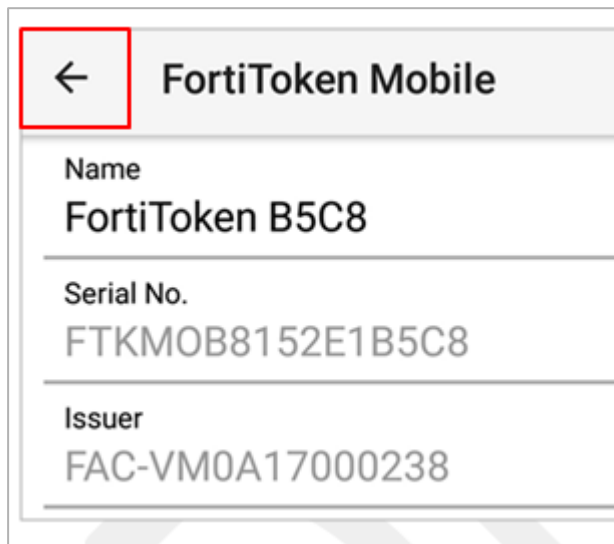
Step 3

Input a name and tap **SAVE**.



Step 4

Tap the **back arrow** to return to the *FortiToken Mobile* app's home screen and see your changes.



How to uninstall the FortiToken Mobile app

Press and hold (long press) the **FortiToken Mobile** icon on your device's home screen. A trash bin icon will appear at the top of your device's home screen. Drag and drop the app icon to the trash bin to remove the application.

Support

For assistance, contact the IT Service Desk on x8444 (Central Office) or 1800 500 380 (all other locations) or email ITServiceDesk@health.gov.au.

Content Owner: IT Operations

Business Owner: Director, ITD CA Digital Wkspce Transf SN

Current as of: 26 March 2020

Keywords: remote access, FortiToken, Android device