



VPN CONNECTION GUIDE FOR CLOUDSAMS CLOUD SERVICE

Version: 5

November, 2024

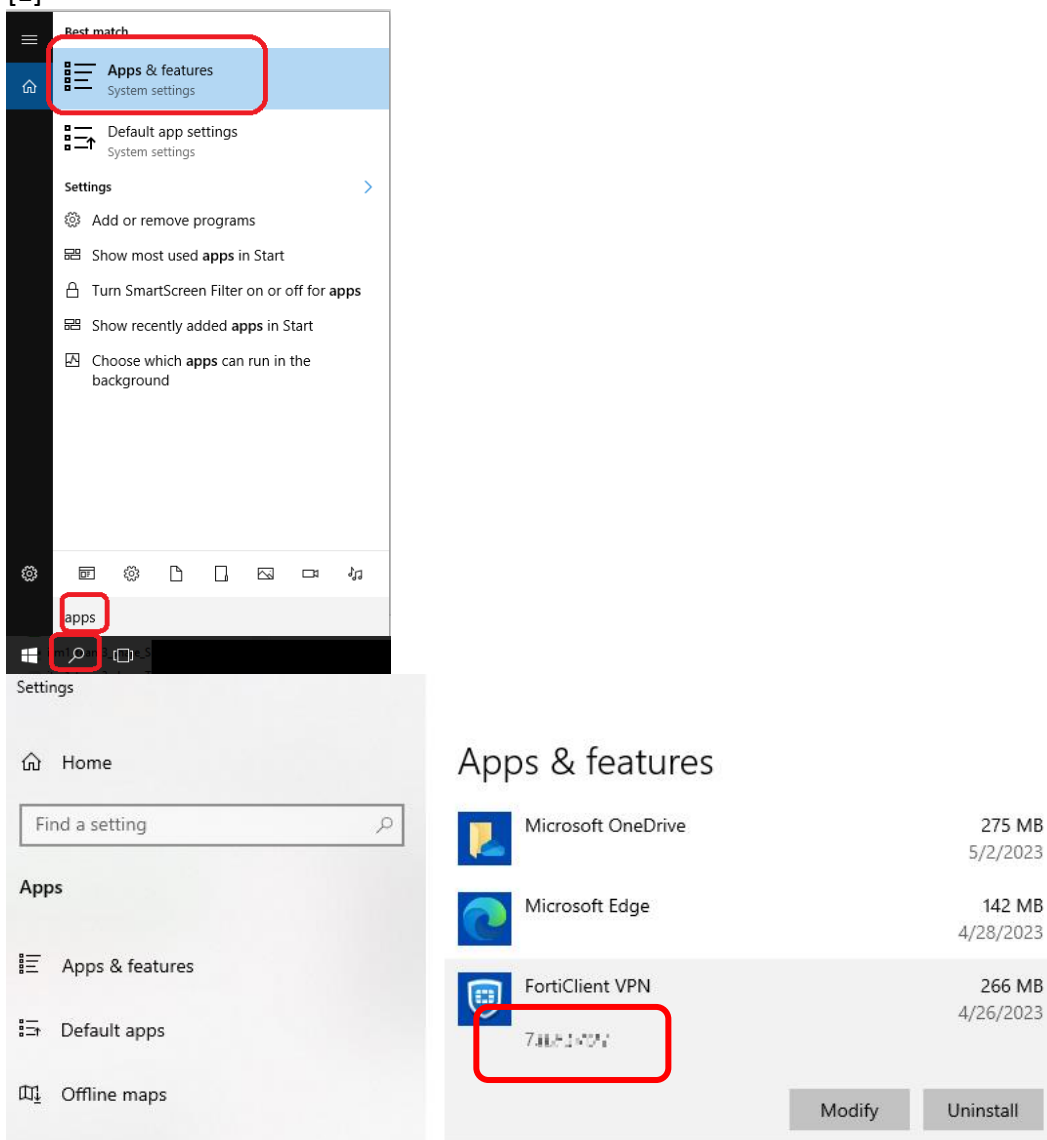
Table of Contents

1.	PREREQUISITE	2
2.	DOWNLOAD THE VPN CLIENT	4
3.	INSTALL THE VPN CLIENT FOR THE 1ST TIME	5
4.	UPGRADE THE INSTALLED VPN CLIENT TO NEWER VERSION	7
5.	SET UP VPN CONFIGURATION	9
6.	GET THE VPN TOKEN	11
6.1	SOFTWARE TOKEN.....	11
6.1.1	<i>For Android Devices</i>	13
6.1.2	<i>For Apple iOS Devices</i>	15
6.1.3	<i>For Windows Devices</i>	17
7.	CONNECT VPN TO THE CLOUD	19
7.1	NORMAL CONNECTION PROCEDURE.....	19
7.2	TROUBLESHOOTING FOR CONNECTIVITY ISSUE	22
7.2.1	<i>PERMISSION DENIED. (-455) OCCUR AFTER ENTERED PASSWORD</i>	22
7.2.2	<i>ERROR MESSAGE "PERMISSION DENIED. (-455)" OCCUR AFTER ENTERED TOKEN CODE</i>	25
7.2.3	<i>"THE CLOUDSAMS SERVICE IS TEMPORARILY UNAVAILABLE." OCCURS WHEN YOU OPEN the CLOUDSAMS URL AFTER CONNECTING TO VPN</i>	26
7.2.4	<i>CONNECTION PROGRESS STUCK AT 9X%, CANNOT REACH 100%, WHEN YOU ARE TRYING TO CONNECT VPN</i>	28
7.2.5	<i>Other problems</i>	28
8.	CHANGE VPN PASSWORD (WHEN YOU STILL HAS THE ORIGINAL PASSWORD)	30
9.	RESET VPN PASSWORD (WHEN YOU LOST THE ORIGINAL PASSWORD)	33
10.	TRANSFER OF SOFTWARE TOKEN FROM OLD TO NEW DEVICE (AVAILABLE FOR ANDROID AND APPLE IOS DEVICE ONLY)	35
10.1	FOR ANDROID DEVICES	35
10.2	FOR APPLE IOS DEVICES.....	38

1. PREREQUISITE

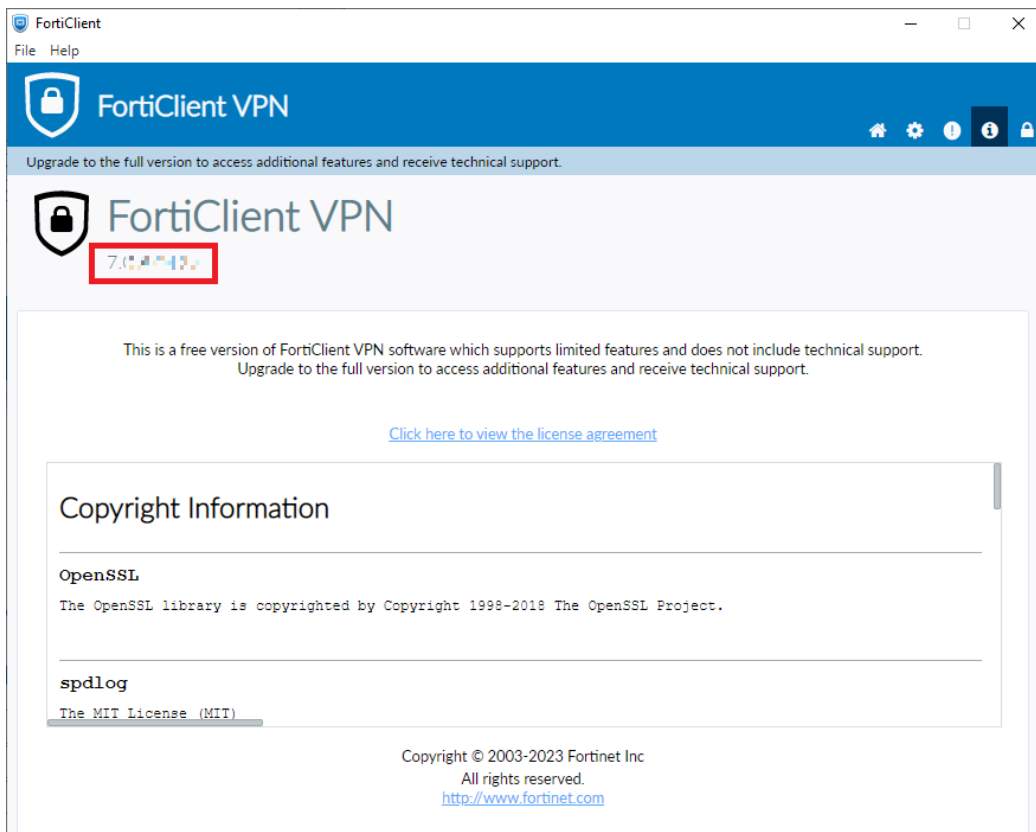
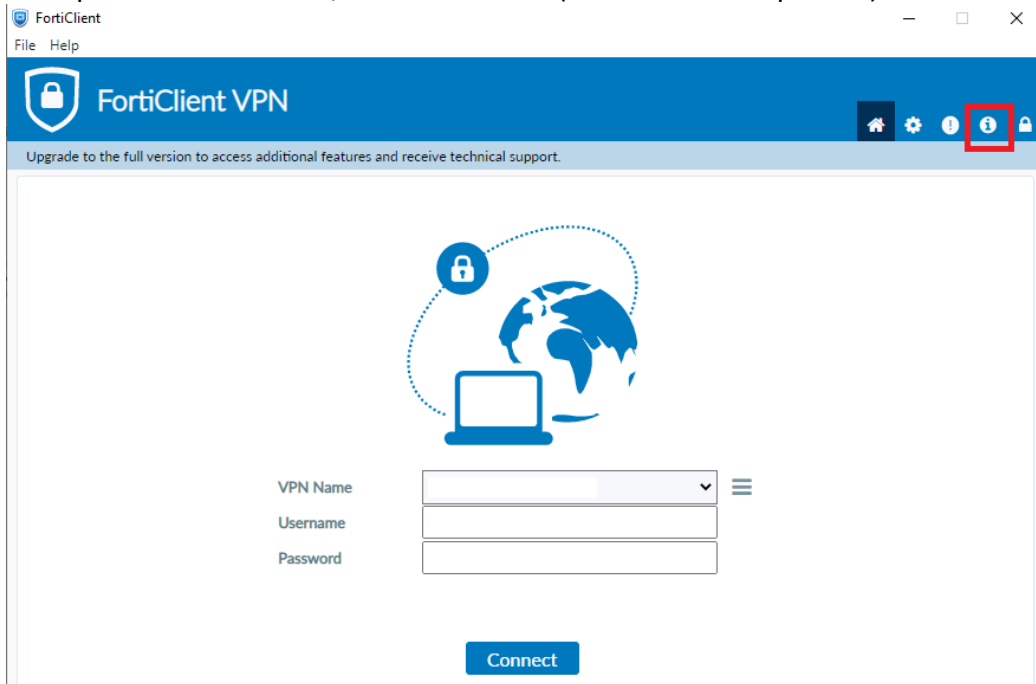
- Please install the latest version of VPN client software – FortiClient. If you have installed it before, and are still using FortiClient 6.X or older version, please reinstall 7.X or above.
- Please always update the VPN client software – FortiClient to the latest version once available for the best security protection.
- FortiClient 7.X supports PC Operating Systems with Microsoft Windows 10 or above only.
- You can check the version of your installed FortiClient under Apps and Features on your Windows PC [1].
- Alternatively, you can open FortiClient software to check the installed version [2].
- The PC Operating Systems **must have Internet access during the installation.**

[1]



[2]

- Open FortiClient VPN, click the button (as shown in the picture).



Note: If school has difficulty in finding the software version, school can seek help from Cloud Service Helpdesk.

<https://cdrcloudsams.edb.gov.hk/聯絡我們/>

2. DOWNLOAD THE VPN CLIENT

1. On the Windows PC if you wish to connect VPN, download the VPN Client installation program at <https://www.fortinet.com/support/product-downloads#vpn>

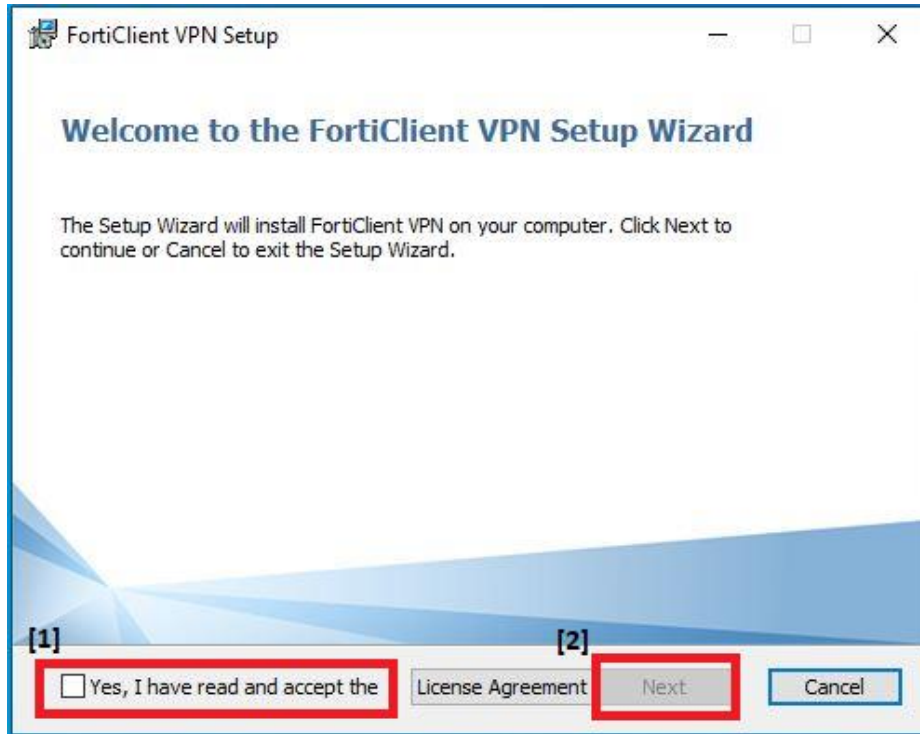
Choose the correct one (The highlighted one below).

The screenshot shows the FortiClient VPN download page. A large red arrow points to the 'FortiClient VPN' header, which is also enclosed in a red box. Below the header, there is a description: 'The VPN-only version of FortiClient offers SSL VPN and IPsecVPN, but does not include any support. Download the best VPN software for multiple devices.' Underneath, the 'Remote Access' section lists two options: 'SSL VPN with MFA' and 'IPSEC VPN with MFA', both with green checkmarks. To the right, there is a grid of download buttons for various operating systems: Windows, MacOS, Linux (.rpm), iOS, Android, and Linux (.deb). The 'DOWNLOAD VPN for Windows' button is highlighted with a red box and a red arrow pointing to it.

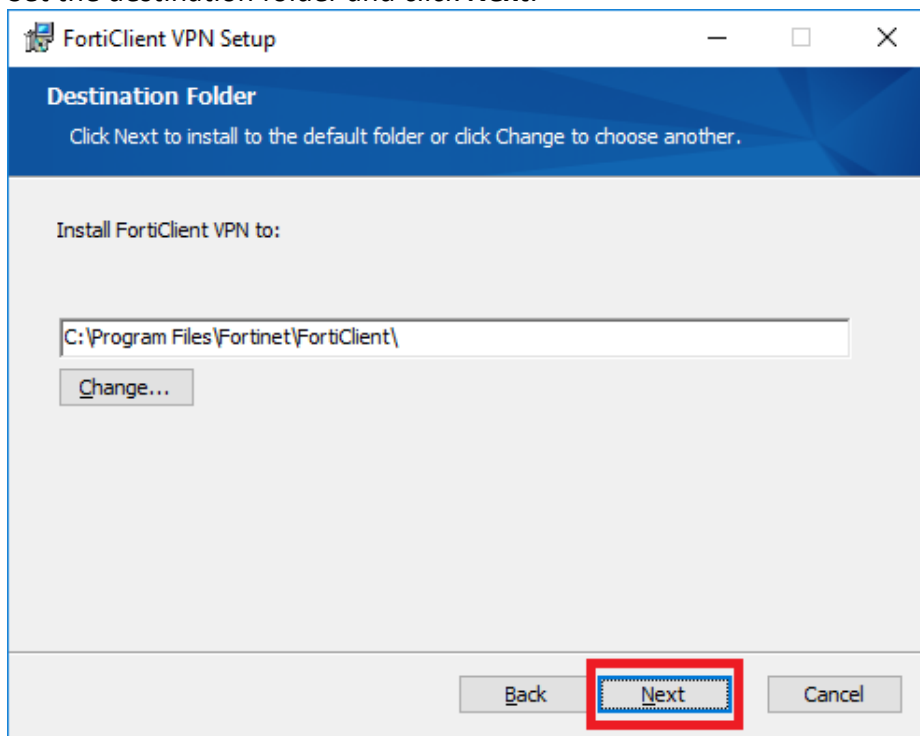
2. After download is completed, go to the next sections to continue installing or upgrading the VPN client.

3. INSTALL THE VPN CLIENT FOR THE 1ST TIME

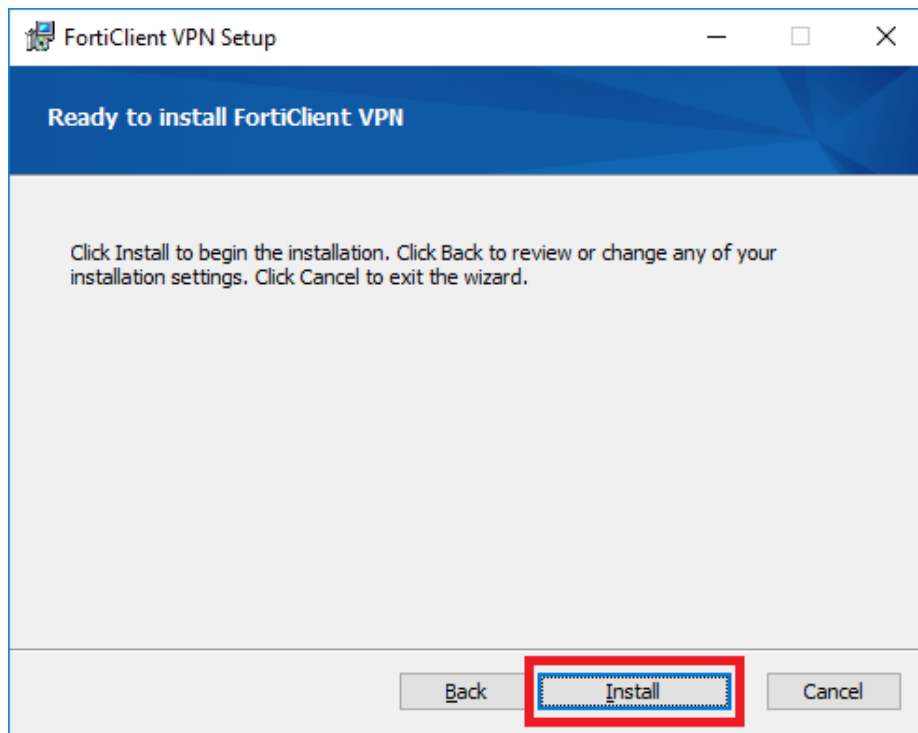
1. Double click the installation program to execute it.
2. Check the checkbox if you accept the license agreement and click **Next**.



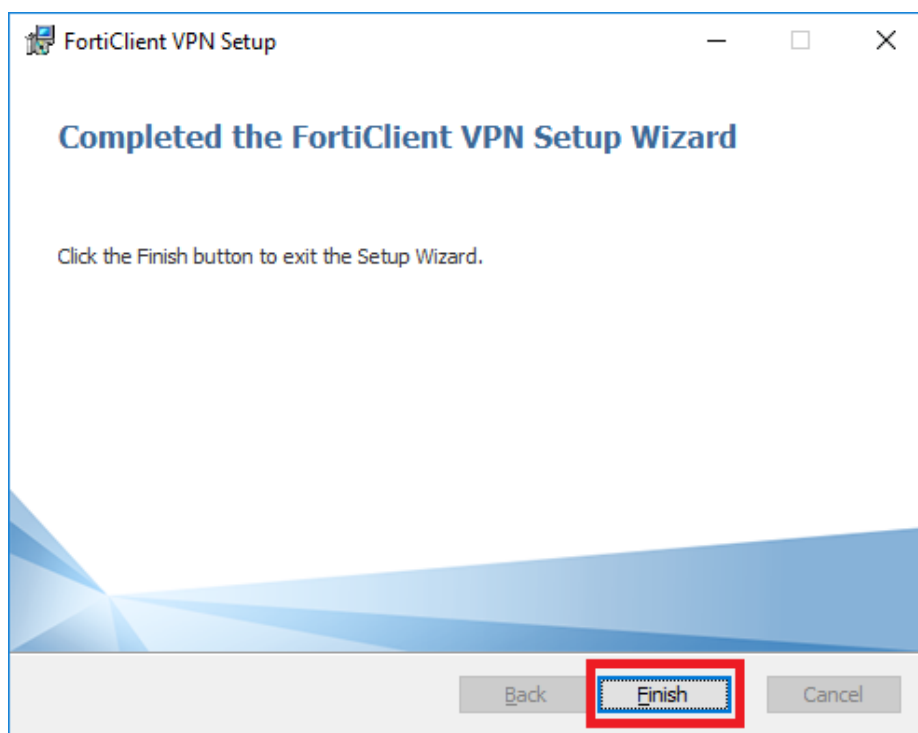
3. Set the destination folder and click **Next**.



4. Click **Install**.

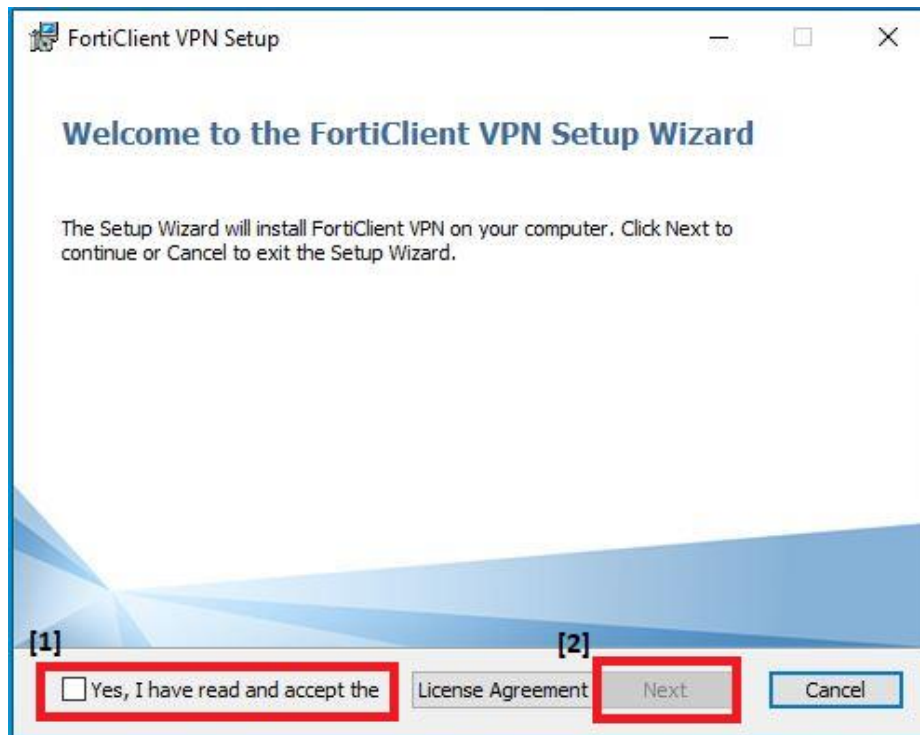


5. Click **Finish**.

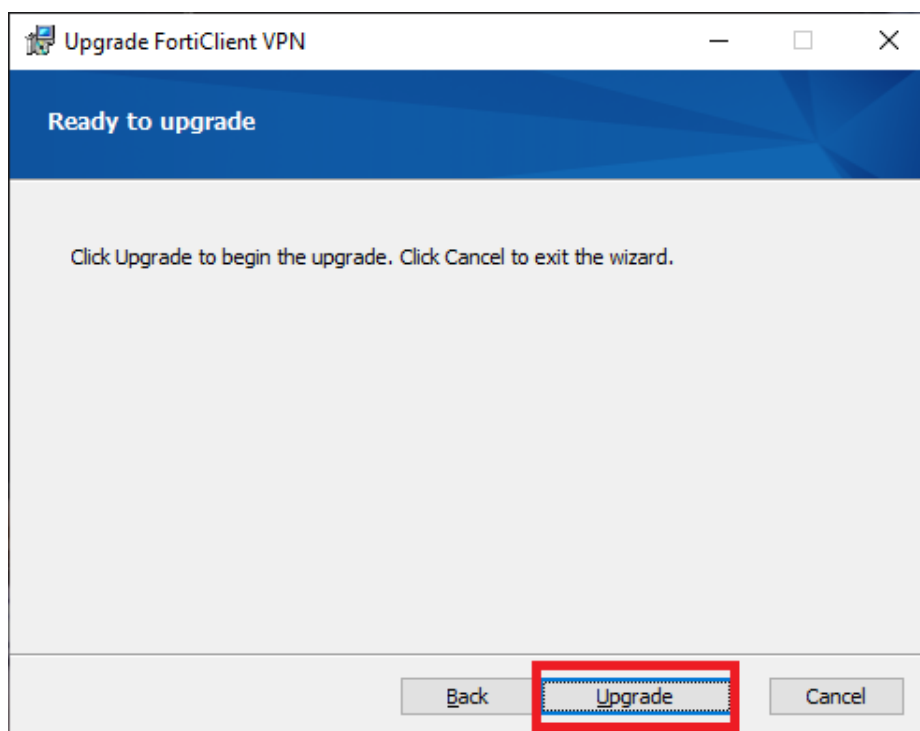


4. UPGRADE THE INSTALLED VPN CLIENT TO NEWER VERSION

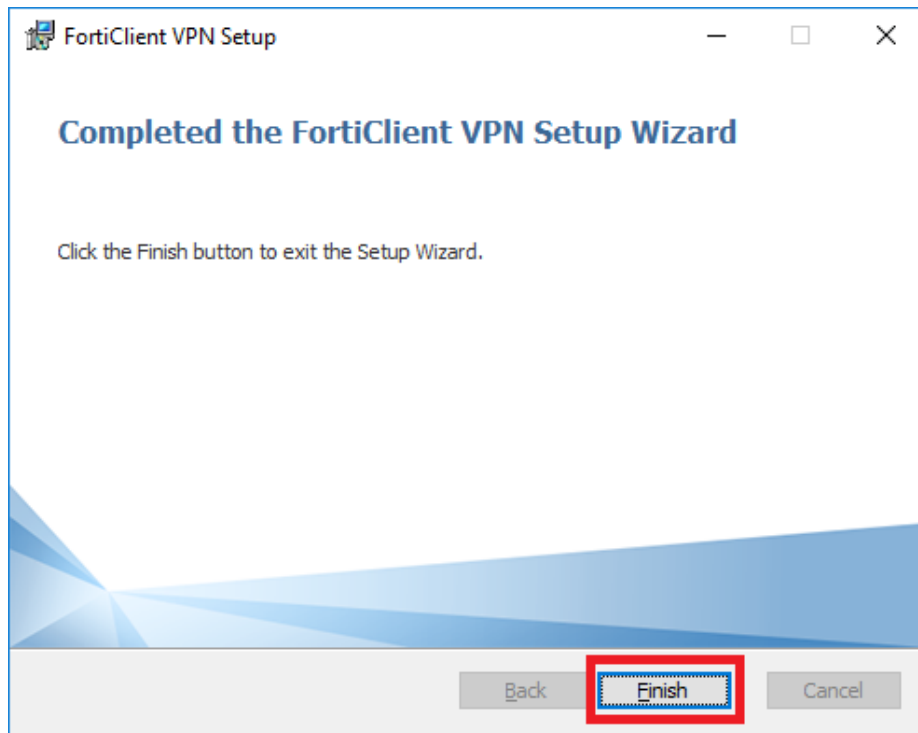
1. Double click the installation program to execute it.
2. Check the checkbox if you accept the license agreement and click **Next**.



3. Click **Upgrade**.



4. Click **Finish**.



Note:

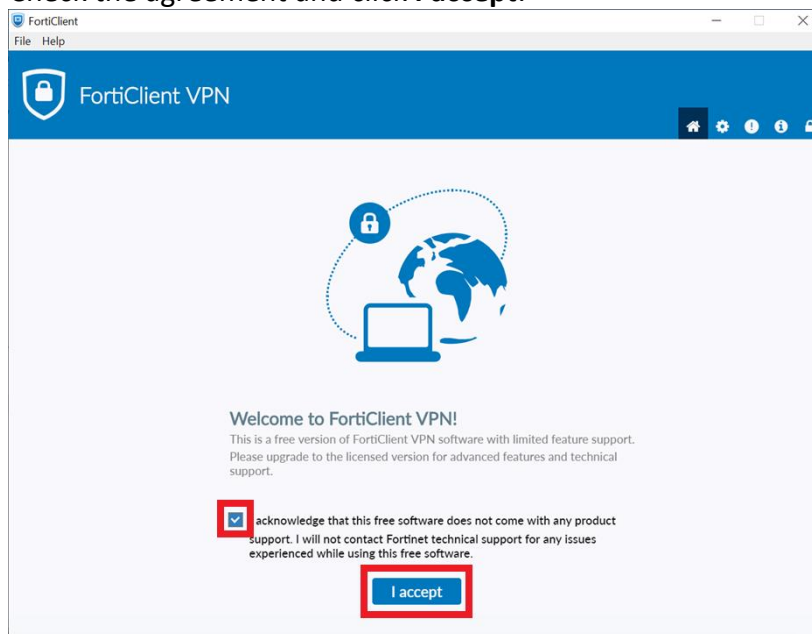
- The program for installation and upgrade is the same program.
- No need to uninstall the older version before executing the installation program.
- Restarting Windows is recommended after the upgrade.

5. SET UP VPN CONFIGURATION

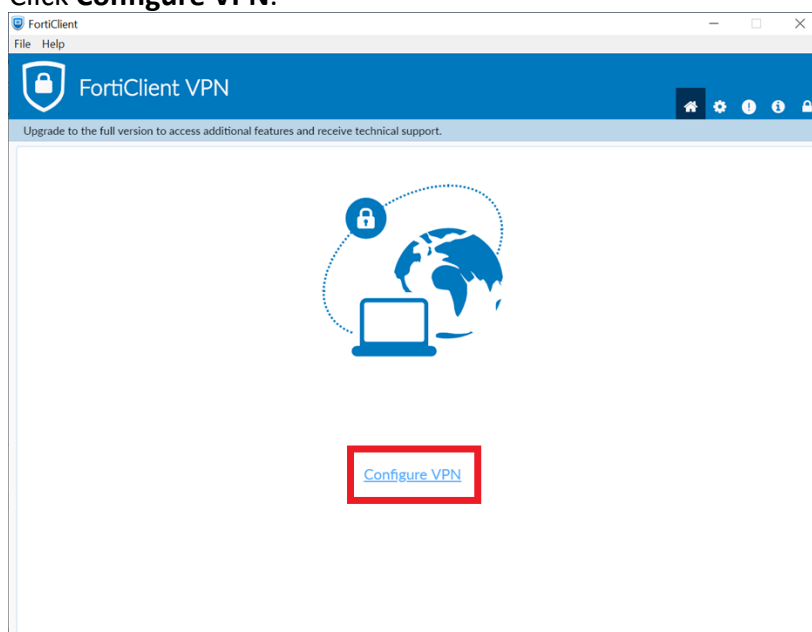
No matter if you are installing the VPN Client for the 1st time, or upgrading the version, you must configure/reconfigure the VPN connection settings.

This is a one-time only procedure after each installation or upgrade. You do not need to do this every time when connecting VPN.

1. Launch the VPN Client.
2. Check the agreement and click **I accept**.



3. Click **Configure VPN**.



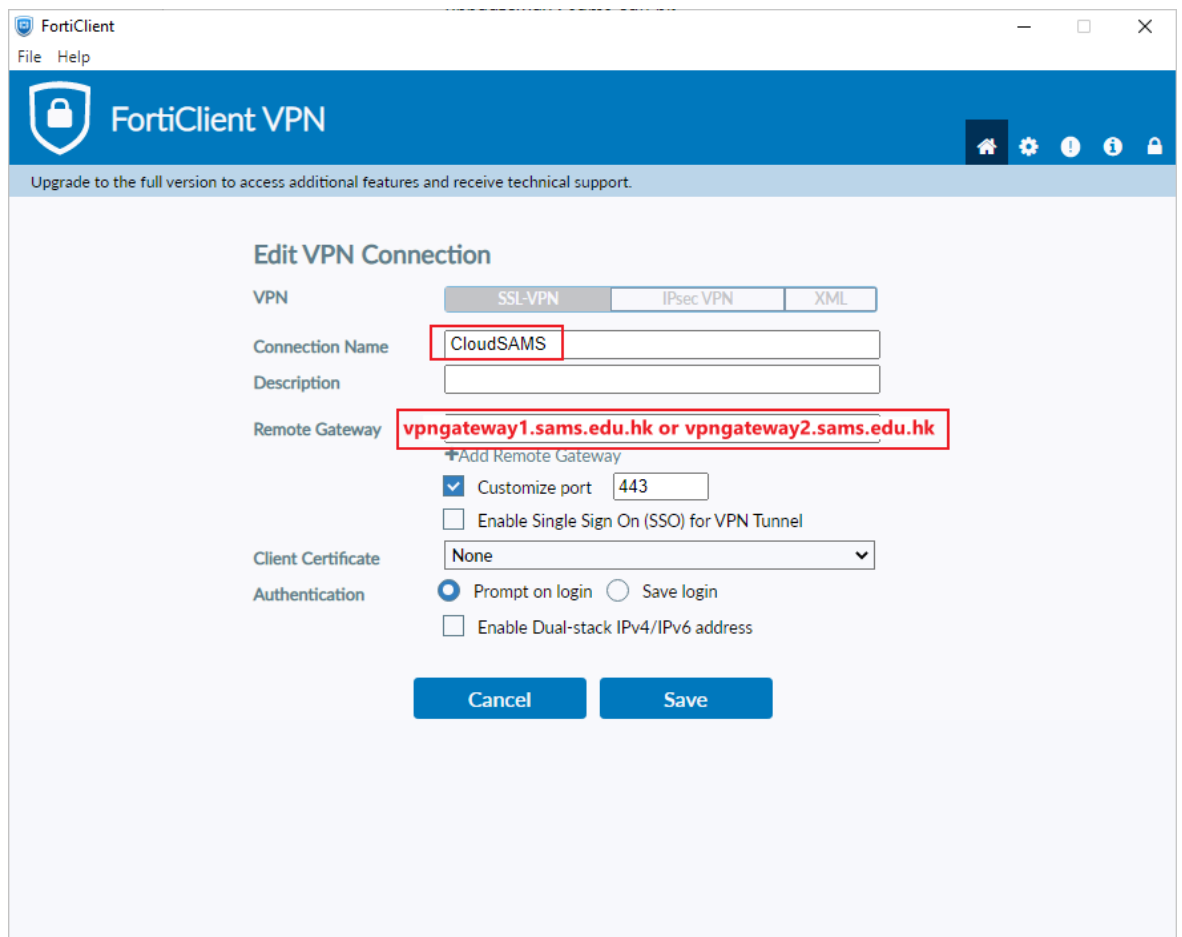
4. Choose **SSL-VPN** to set up the new VPN connection.
 - **Connection Name** can be any name you prefer.
 - **Remote Gateway:**

vpngateway1.sams.edu.hk
or
vpngateway2.sams.edu.hk

Note:

- If you are not sure which gateway you should use, you can try them one by one. Eventually, only one of them (when VPN is connected) will allow you to open your school's CloudSAMS.
- If any problem is encountered during configuration, school can seek help from Cloud Service Helpdesk.

<https://cdrcloudsams.edb.gov.hk/聯絡我們/>



5. Click **Save**.

6. GET THE VPN TOKEN

To connect to the cloud, each school is assigned with two software tokens, which are mobile applications (apps) for 2-factor-authentication during VPN login process to strengthen the security. It is necessary during login of VPN connection.

6.1 SOFTWARE TOKEN

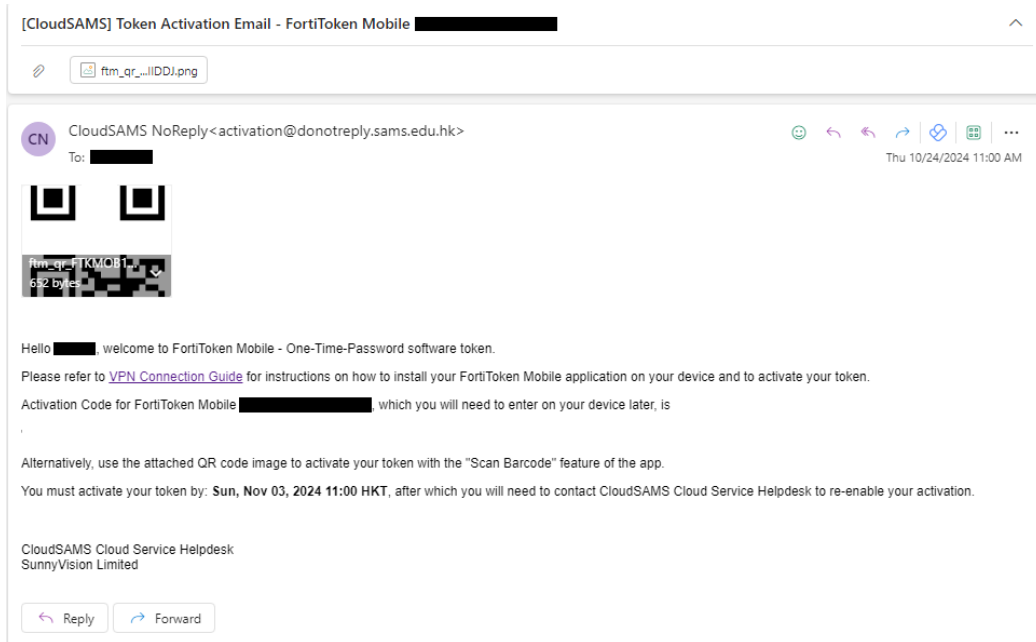
Software token requires several steps to set up. Please follow the procedures to install the mobile app (FortiToken Mobile) for registering the token on your mobile device. You can download the Apps from

- Google Play Store (for Android)
- App Store (for Apple iOS device)
- Microsoft Store (for Windows device)

An activation procedures is required after each new installation.

If you still have the old device that was activated in the past, you can use the Transfer Token feature. You may refer to the later section [**Transfer of software token from old to new device**]

Otherwise, you will need to contact the [Cloud Service Helpdesk](#) to request for resending token activation email. After request, your **school principal** should receive an activation email from **<activation@donotreply.sams.edu.hk>**, which contains a QR code for software token activation. You should follow the instructions below to activate the token within 10 days before the QR code expires. You may refer to procedures in later sections.



You may need to contact the [Cloud Service Helpdesk](#) if

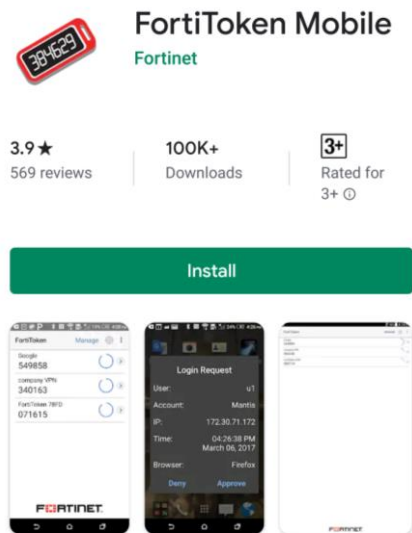
- (i) the activation code is expired; or
- (ii) your activated device is lost/ stolen; or
- (iii) transfer of token is required but you do not have access to the original activated device.

6.1.1 For Android Devices

Prerequisite

- FortiToken Mobile is compatible with devices running certain versions of Android only. Please observe the compatible versions specified in Google Play Store.
- Beware of the end of support date of the Android version your devices are using. For security reason, you should not use an Android version that has passed its end of support date.
- The devices **must have Internet access during the token activation process.**
- Each time when login VPN, **the devices' system time must be correct,** better be automatically synchronized from trustable source.

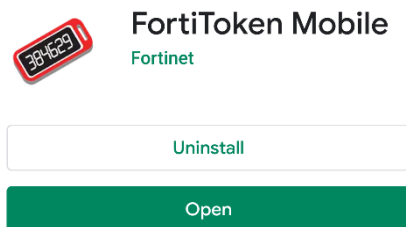
1. Go to **Google Play Store** and search for **FortiToken Mobile**. Tap



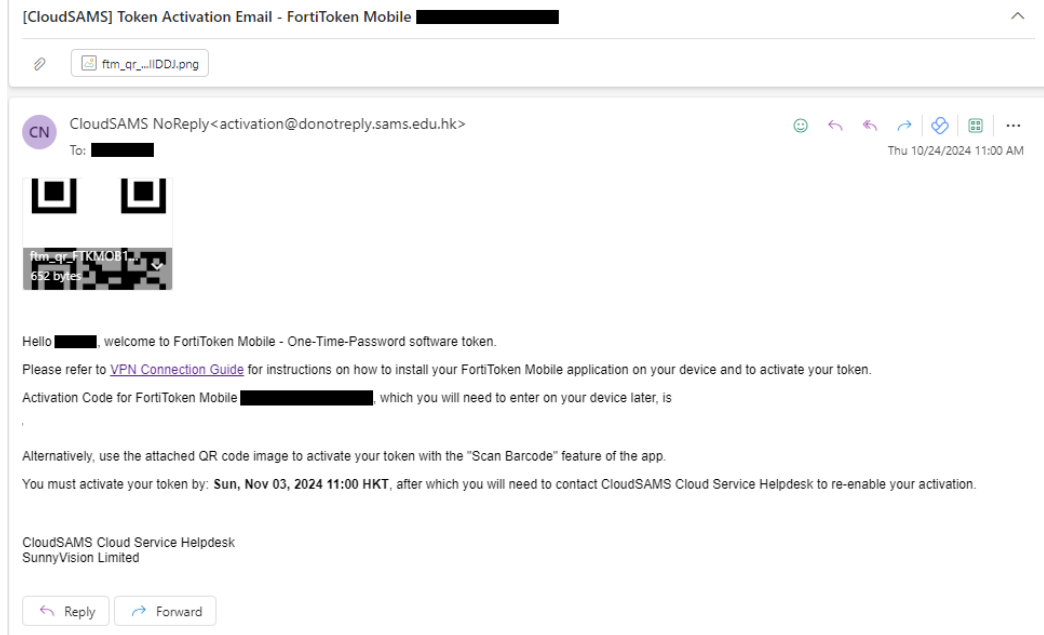
2. Tap



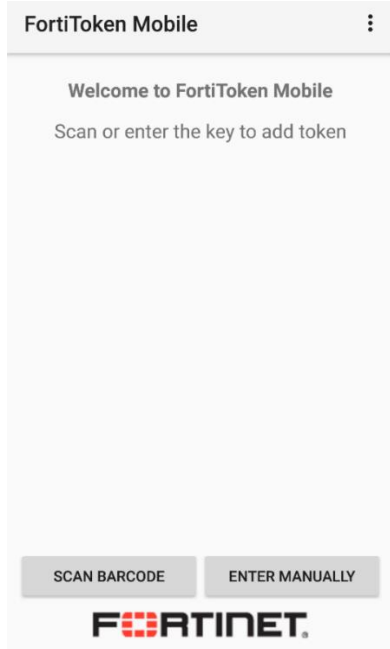
to launch the app.



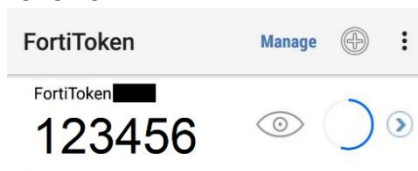
3. Open the activation email. Please note that the activation code will expire in 10 days.



4. Tap **SCAN BARCODE** to scan the QR code [1] in the activation email. You can also tap **ENTER MANUALLY** to input the activation code [2] in the same email.



5. Once the token is activated, the VPN token will be displayed on the app as follows:



6.1.2 For Apple iOS Devices

Prerequisite

- FortiToken Mobile is compatible with devices running certain versions of iOS only. Please observe the compatible versions specified in App Store.
- Beware of the end of support date of the iOS version your devices are using. For security reason, you should not use an iOS version that had passed its end of support date.
- The devices **must have Internet access during the token activation process.**
- Each time when login VPN, **the devices' system time must be correct**, better be automatically synchronized from trustable source.

1. Go to **App Store** and search for **FortiToken Mobile**. Tap **GET**.



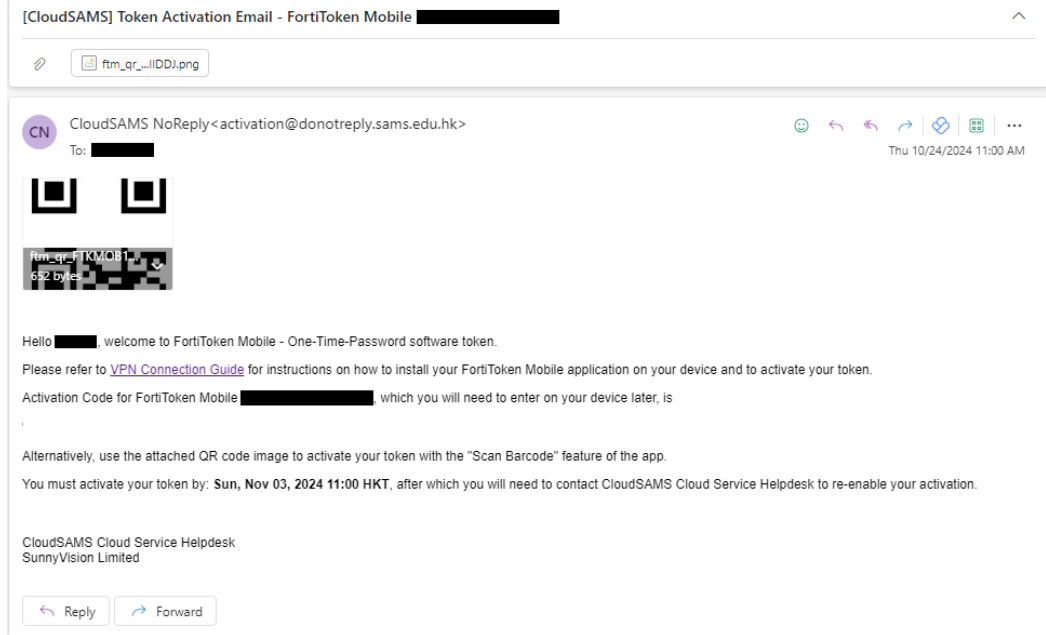
2. Tap **INSTALL** to start the installation.



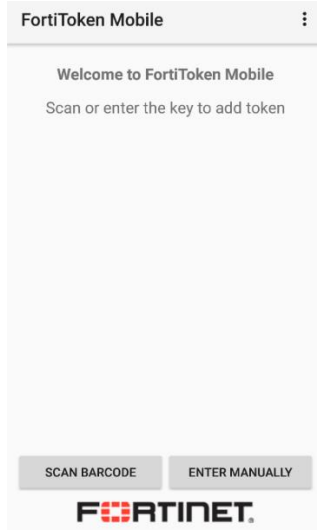
3. Tap **OPEN** to launch the app.



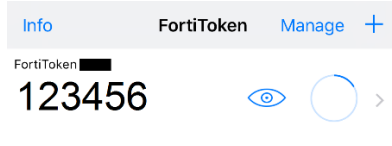
4. Open the activation email. Please note that the activation code will expire in 10 days.



5. Tap **SCAN BARCODE** to scan the QR code [1] in the activation email. You can also tap **ENTER MANUALLY** to input the activation code [2] in the same email.



6. Once the token is activated, it will be displayed on the app as follows:

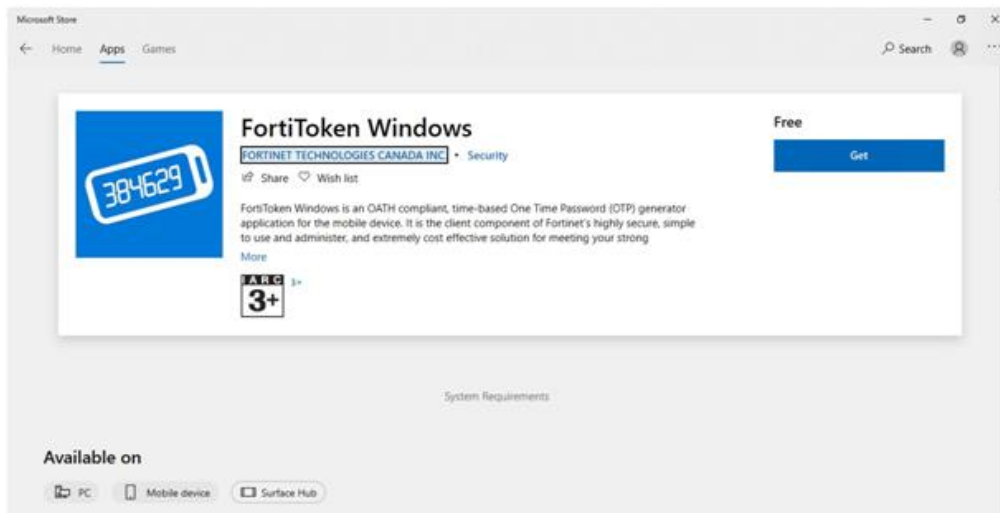


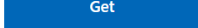
6.1.3 For Windows Devices

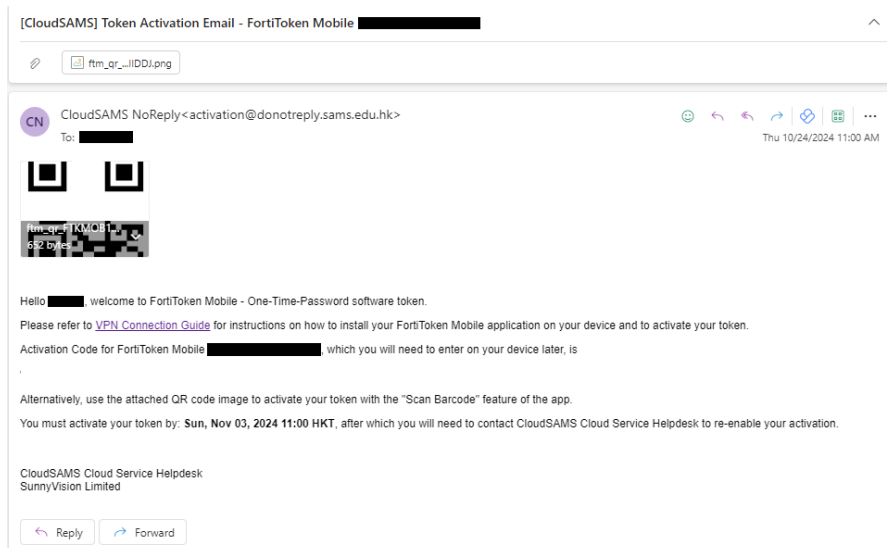
Prerequisite


- FortiToken Mobile is compatible with devices running Windows 10. For security reason, you should always install the latest Windows Updates.
- The devices **must have Internet access during the token activation process.**
- Each time when login VPN, **the devices' system time must be correct,** better be automatically synchronized from trustable source.

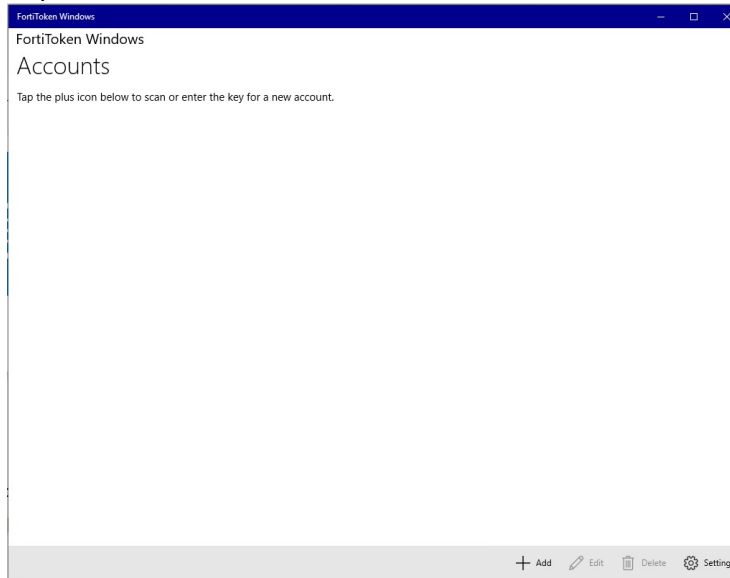
1. Go to **Microsoft Store** and search for **FortiToken Mobile**.



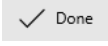
2. Tap  to start the installation.
3. Tap **FortiToken Mobile** to launch the app.
4. Open the activation email. Please note that the activation code will expire in 10 days.

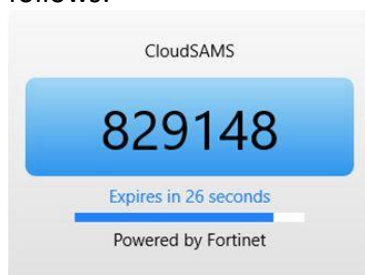


5. Tap  to add account.



6. Enter the profile to set up the token.
- **Account Name** can be any name you prefer.
 - **Key** refers to activation code sent in step 4 [1]
 - Select **Fortinet** in Category

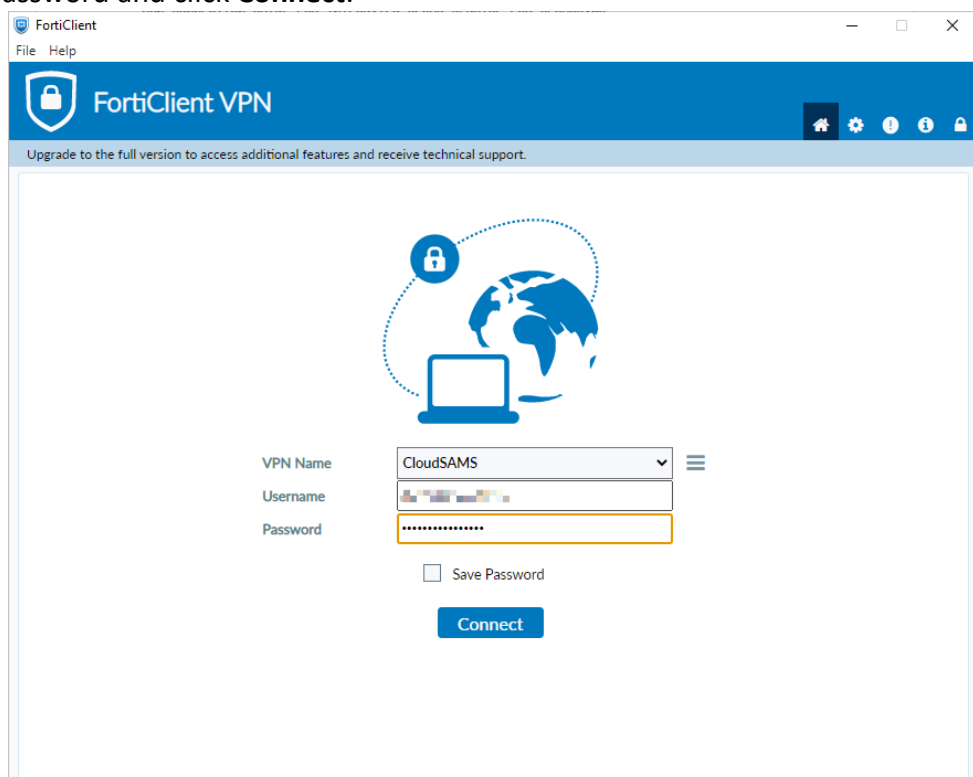
7. Click  to proceed.
8. Once the token is activated, the VPN token will be displayed on the app as follows:




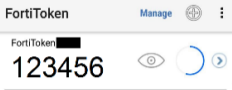
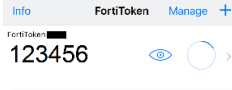

7. CONNECT VPN TO THE CLOUD

7.1 NORMAL CONNECTION PROCEDURE

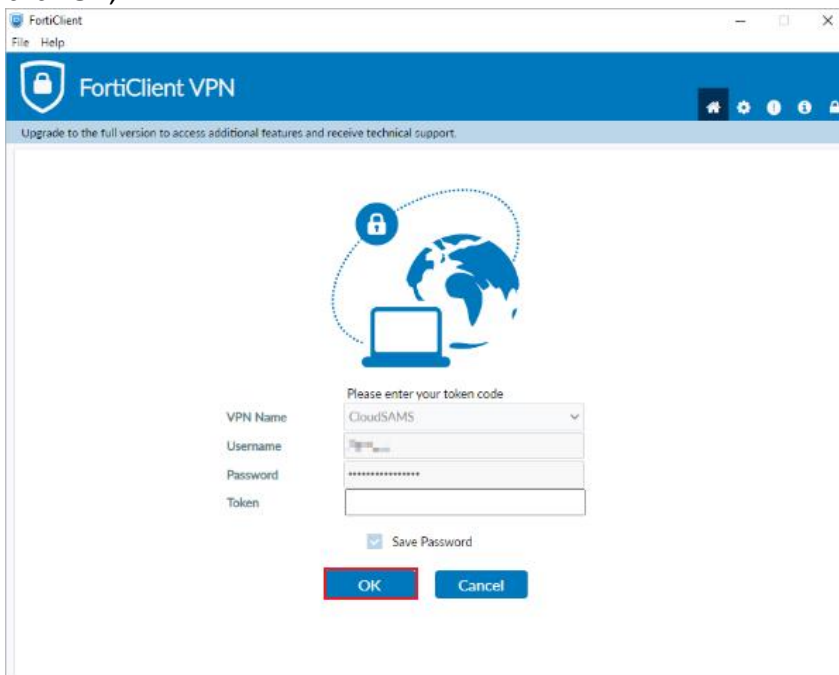
1. Launch the VPN Client.
2. Choose the configured VPN Connection Name, input the VPN Username and Password and click **Connect**.



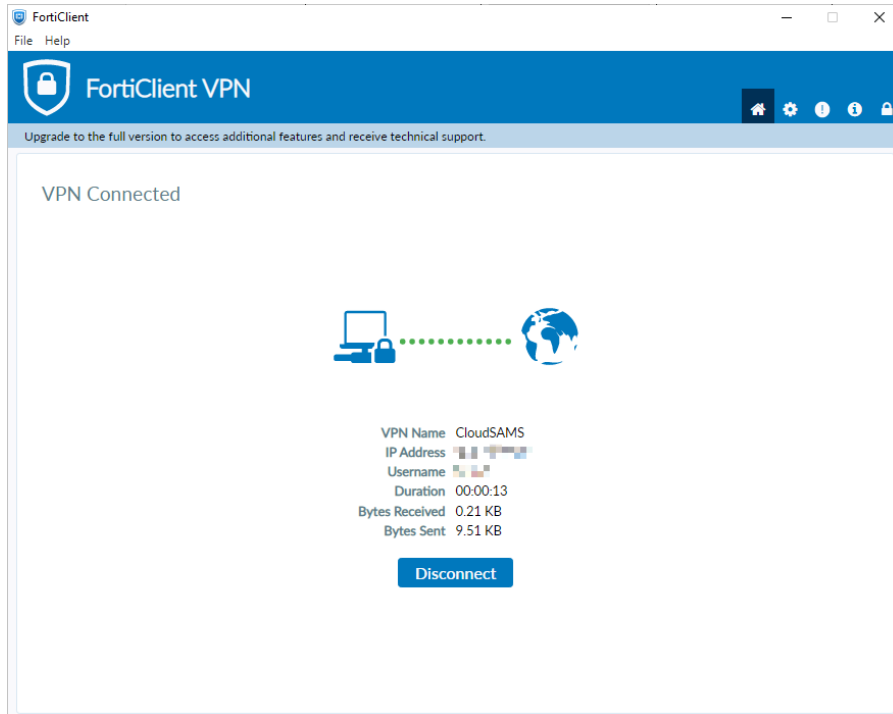
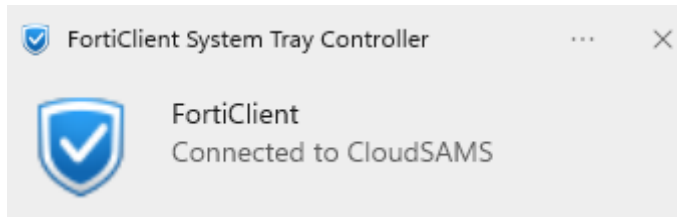
3. Enter your passcode generated by the VPN token.
 - (i) Retrieve token code from your mobile device.
Note that each token code is valid for 1 minute only.
 - (ii) Make sure your mobile device's system time must be correct, better be automatically synchronized from trustable source.

Software Token		
On Android device	On Apple iOS device	On Windows device
Open the Apps to get the token code 		
		

On your PC, enter the code generated by the VPN token from your mobile and click **OK**;



VPN should be connected to your PC successfully.



7.2 TROUBLESHOOTING FOR CONNECTIVITY ISSUE

If you fail to connect to the VPN, please check if you are encountering the following issues.

7.2.1 PERMISSION DENIED. (-455) OCCUR AFTER ENTERED PASSWORD

Error message “Permission denied. (-455)” occurs when you entered password during VPN login.



Troubleshooting steps

1. Visit [Self-Service Portal](#), and login by your VPN account.



Sign in

Username

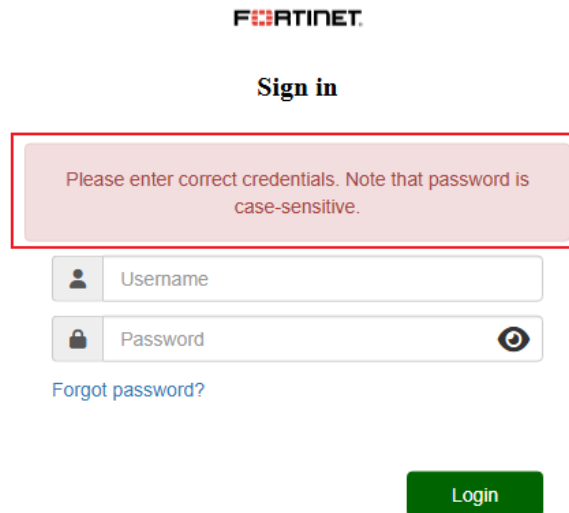
Password

[Forgot password?](#)

Login


2. If error message “**Please enter correct credentials. Note that password is case-sensitive**” occurs, that means you have entered a wrong password.

Please refer to section 9 “Reset VPN password” for instructions on how to reset password if you have lost it.



The screenshot shows the Fortinet login interface. At the top is the Fortinet logo and the text 'Sign in'. Below this is a red-bordered error message box containing the text: 'Please enter correct credentials. Note that password is case-sensitive.' Underneath the error message are two input fields: 'Username' and 'Password'. The 'Password' field has a toggle icon on the right. Below the input fields is a blue link that says 'Forgot password?'. At the bottom of the form is a green 'Login' button.

3. However, if error message “**You have been locked**” occurs, that means your VPN password has expired, or your Token Activation email has expired, and therefore your VPN account has been locked, for security consideration.



The screenshot shows the Fortinet login interface. At the top is the Fortinet logo and the text 'Sign in'. Below this is a red-bordered error message box containing the text: 'You have been locked'. Underneath the error message are two input fields: 'lionho' and 'Password'. The 'Password' field has a toggle icon on the right. Below the input fields is a blue link that says 'Forgot password?'. At the bottom of the form is a green 'Login' button.

- **VPN Password Expired**
Please visit [CloudSAMS Cloud Service Helpdesk](#) website, login by your Cloud Service Helpdesk account, create a support ticket for requesting a VPN account unlock.
- **Token Activation Email Expired.**
Please submit the [VPN連線客戶服務申請表（表D）](#) to CloudSAMS Cloud Service Helpdesk, by sending an email to

cloudsams.cloudservice@sunnyvision.com, or by creating a support ticket in the same [CloudSAMS Cloud Service Helpdesk](#) website above.

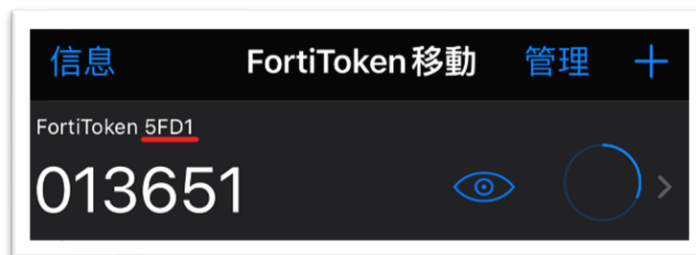
Alternatively, you can also contact the Cloud Service helpdesk by phone or email.

7.2.2 ERROR MESSAGE “PERMISSION DENIED. (-455)” OCCUR AFTER ENTERED TOKEN CODE

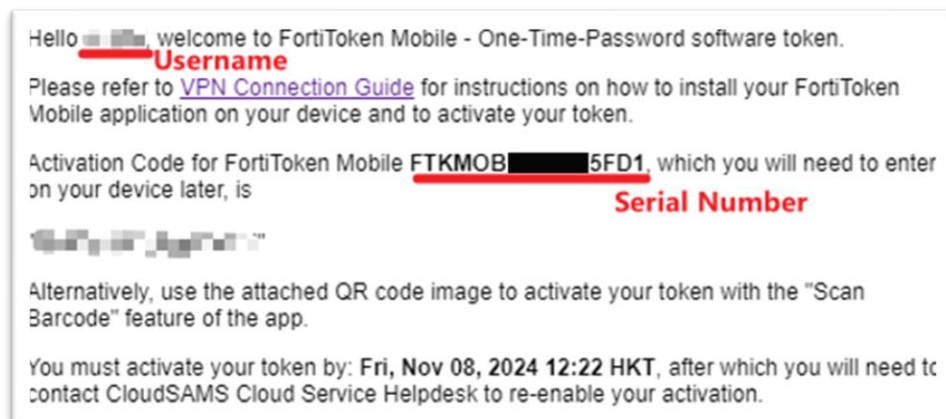
Troubleshooting steps

1. Check if the system time on your computer (the PC that needs to connect VPN) and the mobile device (that has the token) are correct, and in-sync with each other.
2. Check if the mobile device (that has the token) is connected to the Internet.
3. Check if the token serial number and the VPN account username are the same as what specified in the original token activation email.

FortiToken Mobile



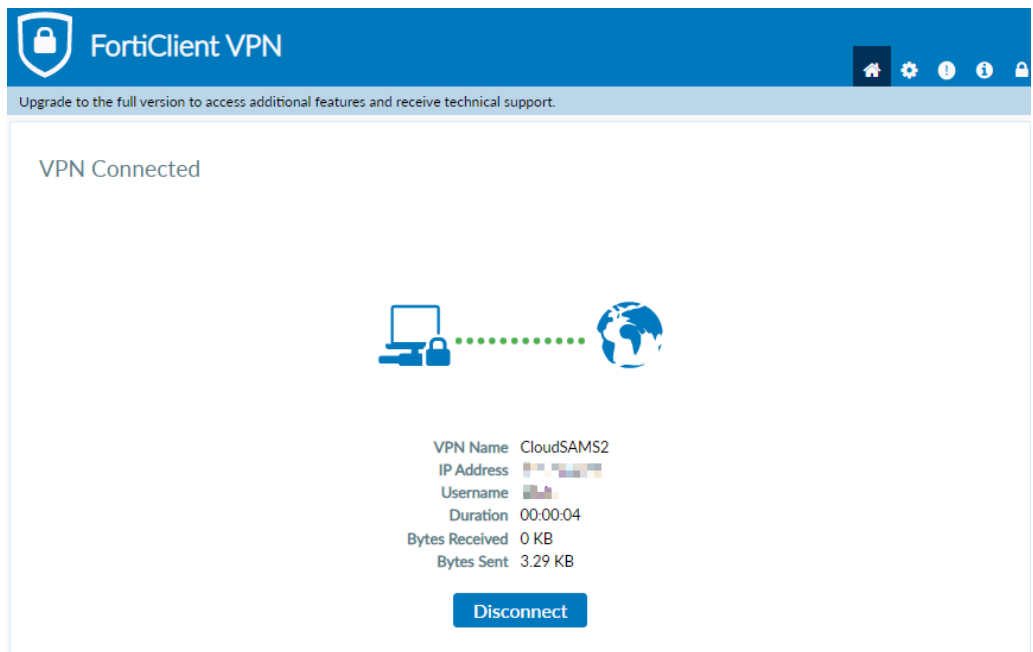
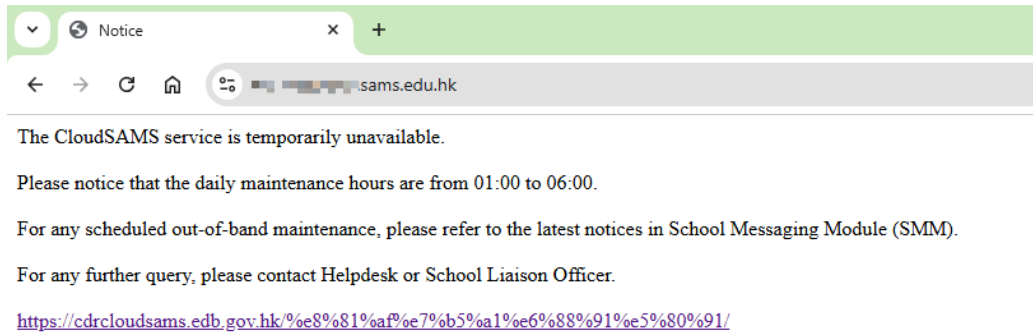
Token activation Email



4. You can contact the CloudSAMS Cloud Service Helpdesk for inquiries.

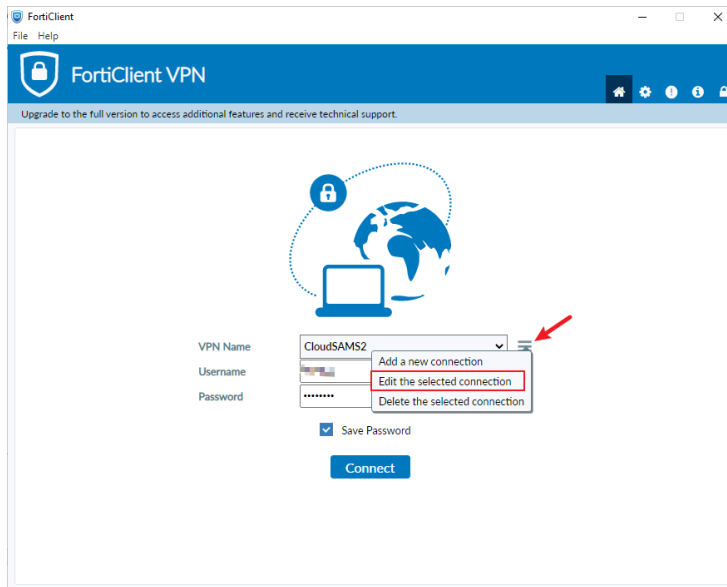
7.2.3 “THE CLOUDSAMS SERVICE IS TEMPORARILY UNAVAILABLE.” OCCORS WHEN YOU OPEN the CLOUDSAMS URL AFTER CONNECTING TO VPN

When you can visit CloudSAMS URL without VPN but error page (below) occurs when visit the same CloudSAMS URL after connecting to the VPN.



Troubleshooting steps

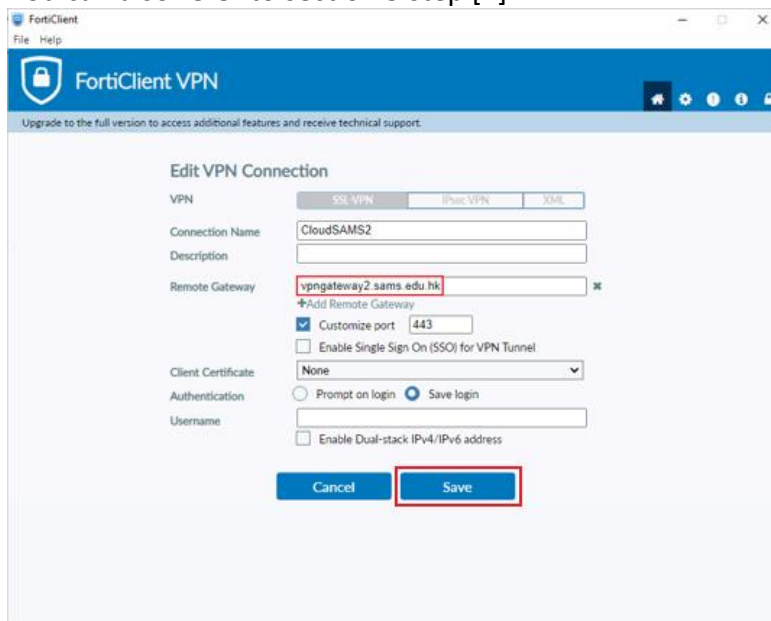
1. Disconnect the VPN and Click the  button and select “Edit the selected connection”.



2. Change the Remote Gateway to another one and try again.
vpngateway1.sams.edu.hk
vpngateway2.sams.edu.hk

For example: Change to vpngateway2.sam.edu.hk if you are connected to vpngateway1.sams.edu.hk previously.

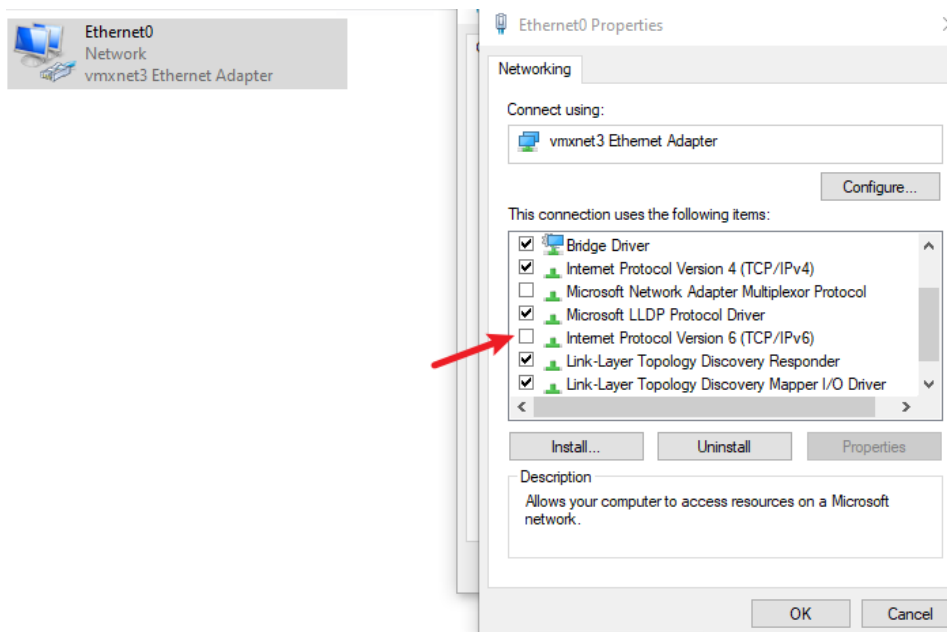
You can also refer to section 5 step [4].



7.2.4 CONNECTION PROGRESS STUCK AT 9X%, CANNOT REACH 100%, WHEN YOU ARE TRYING TO CONNECT VPN

Troubleshooting steps

Try to disable IPv6 on the network card (or Network Interface Controller (NIC)) of the PC that needs to connect VPN.



This is a rather advanced setup. If you are not sure how to disable it, please contact the Cloud Service Helpdesk for assistance.

7.2.5 Other problems

Apart from the above issues, if error occurs when connecting to the VPN even after entering the correct password, it is recommended to try following the steps to troubleshoot the issue first.

You do not need to try them all. As long as any one of them solved the VPN connection problem, you can then continue to use VPN.

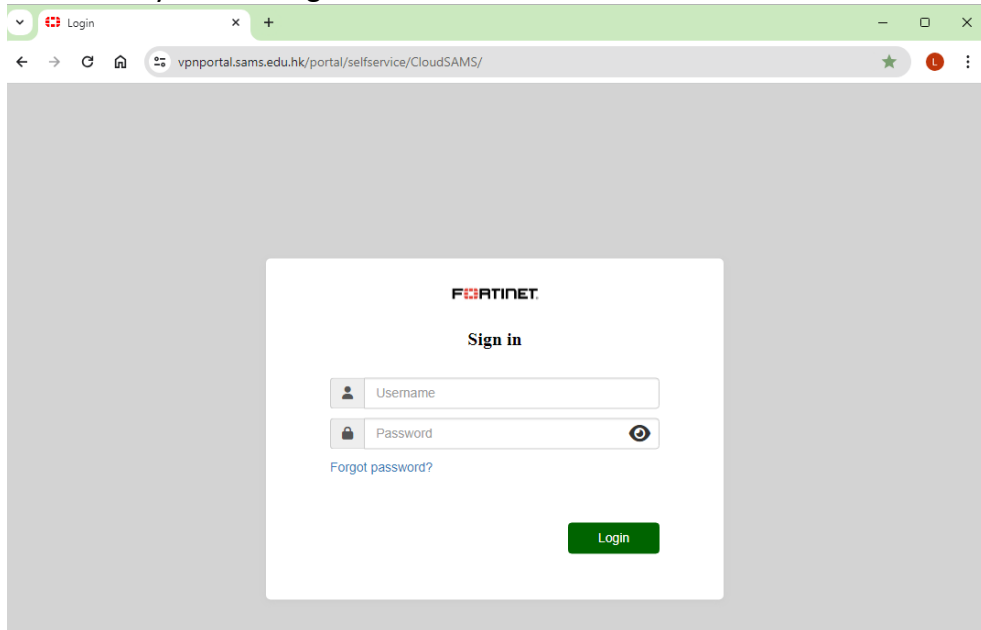
1. Verify whether the VPN configuration of FortiClient software are correct (any typo?), especially the **Remote Gateway** (Please refer to section 5 step [4]);
2. Restart Windows of the PC you are trying to connect VPN;
3. Restart the software token app on your token device.

By performing these actions and retrying the connection, you can usually resolve common connectivity issues.

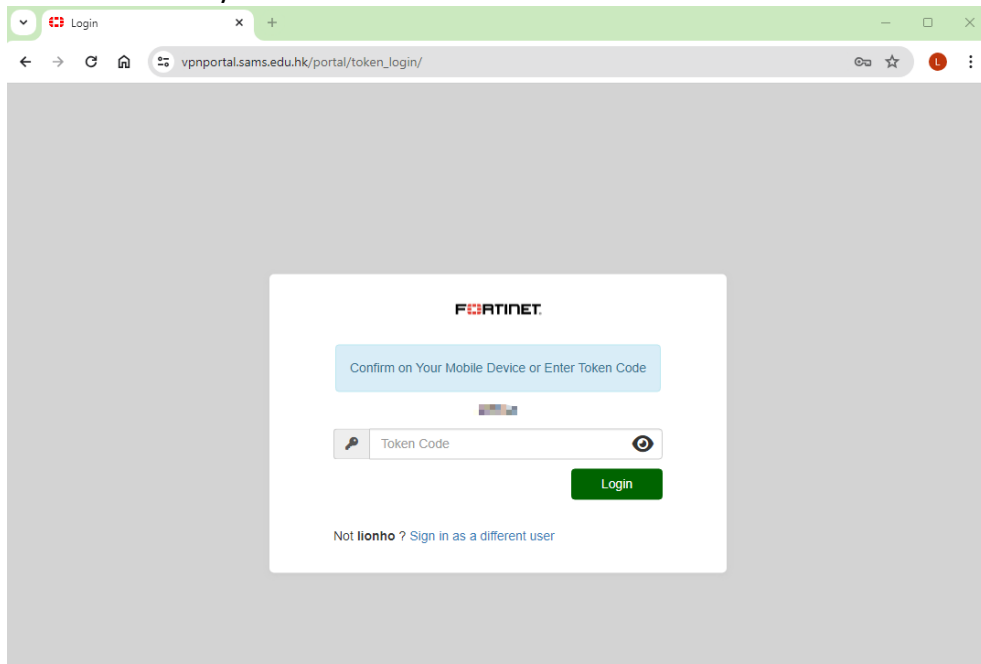
If you continue to experience problems, especially for technical matters related to VPN connection, please contact the [Cloud Service Helpdesk](#) at 2802 0218. For other questions, please contact your [School Liaison Officer of CloudSAMS Team](#).

8. CHANGE VPN PASSWORD (WHEN YOU STILL HAS THE ORIGINAL PASSWORD)


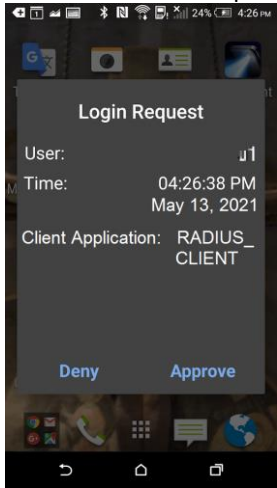

1. Open web browser, go to Self Service Portal at <https://vpnportal.sams.edu.hk/portal/selfservice/CloudSAMS> then enter your VPN login.



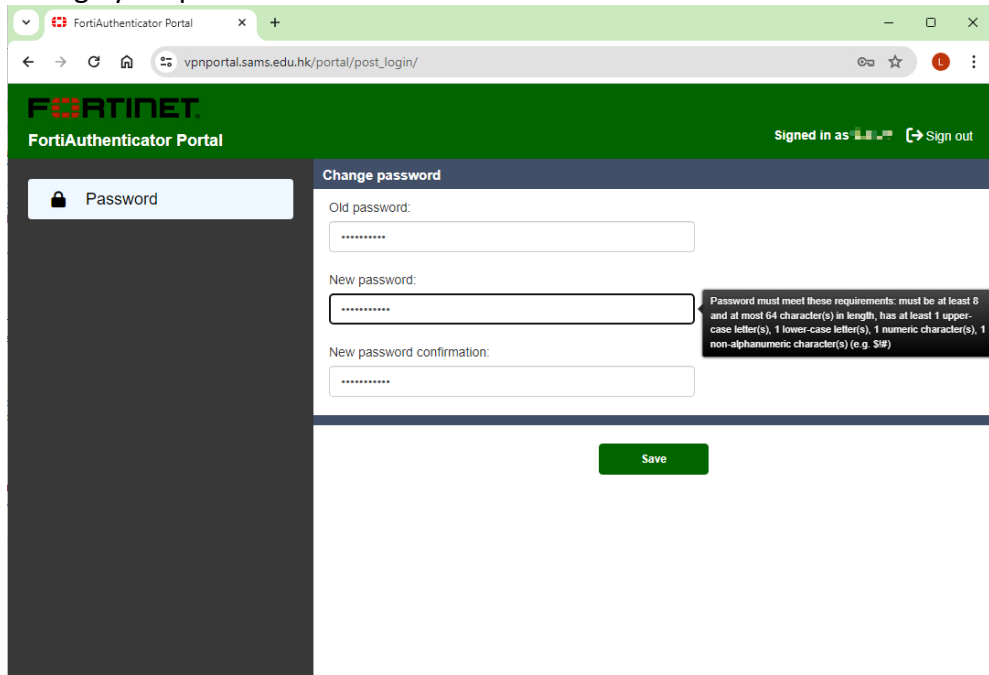
2. Enter your passcode generated by the VPN token or click **Approve** in supported devices. You may refer to remarks below:



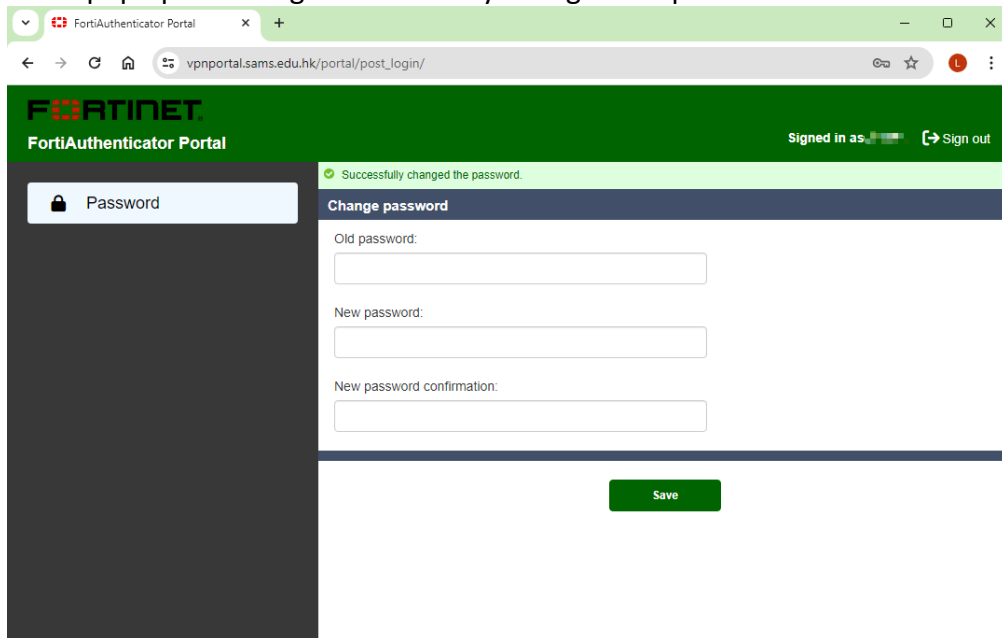
Remarks: Click Approve on your mobile device with FortiToken Mobile: (available for Apple iOS and Android only) when you receive a notification.

Software Token		
On Android device	On Apple iOS device	On Windows device
<p>Step 1: Tap the notification</p>  <p>*With notification enabled for FortiToken Mobile App</p>	<p>Step 1: Tap the notification</p>  <p>*With notification enabled for FortiToken Mobile App</p>	<p>Not available</p>
<p>Step 2: Tap approve to allow the authentication request</p> 	<p>Step 2: Tap approve to allow the authentication request</p> 	

3. Change your password as follows.



4. It will pop up a message "Successfully changed the password".



5. You may login again with your new password for testing.

6. Click "Sign out" after conducted your test in step [5].

9. RESET VPN PASSWORD (WHEN YOU LOST THE ORIGINAL PASSWORD)

Important Note: During the reset procedure, a one-time only reset email will be sent to your **school principal's** email address, and that reset email will be **valid for 5 minutes only**. Please make sure your school principal is ready to receive the email before you begin this reset procedure.

1. Open web browser, go to Self Service Portal at <https://vpnportal.sams.edu.hk/portal/selfservice/CloudSAMS> then click "Forgot password?".



Fortinet

Sign in

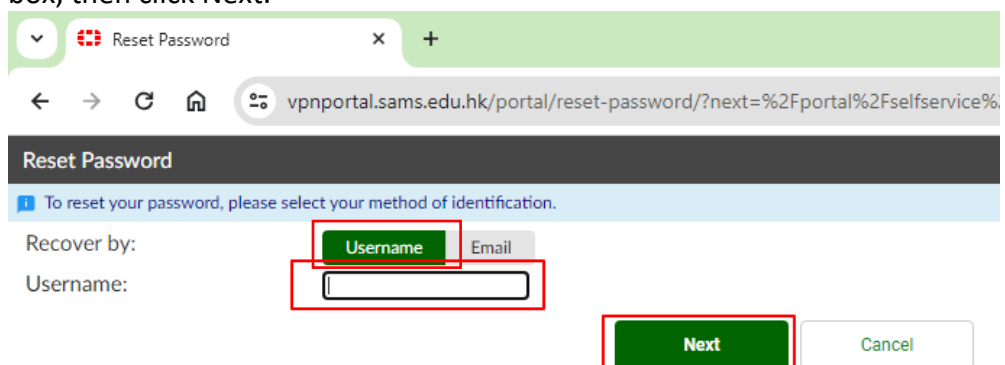
Username

Password

Forgot password?

Login

2. Enter the Username (**not Email Address**) of your VPN account into Username box, then click Next.



Reset Password

To reset your password, please select your method of identification.

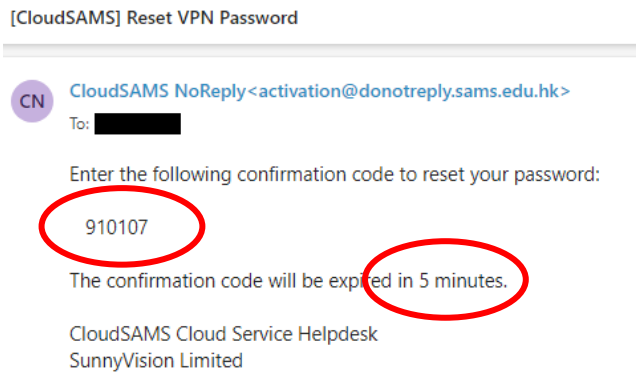
Recover by:

Username Email

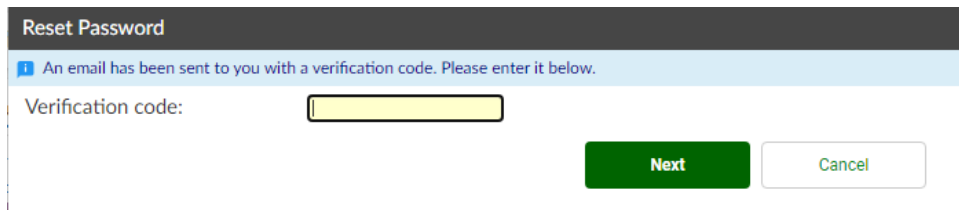
Username:

Next Cancel

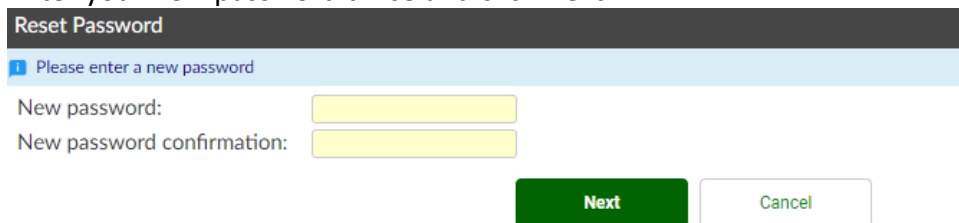
3. Your **school principal** will receive an email containing a one-time verification code similar to this one.



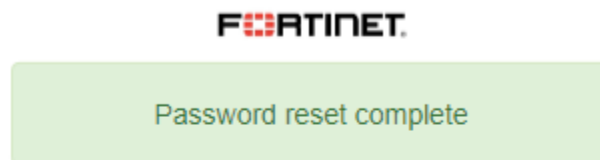
4. Get the verification code **from your school principal**, then enter the verification code into Verification code box and click Next.



5. Enter your new password twice and click Next.



6. Your VPN password had been successfully changed if you see this screen.



Your password has been set. You may go ahead and log in now

[Return to login page](#)

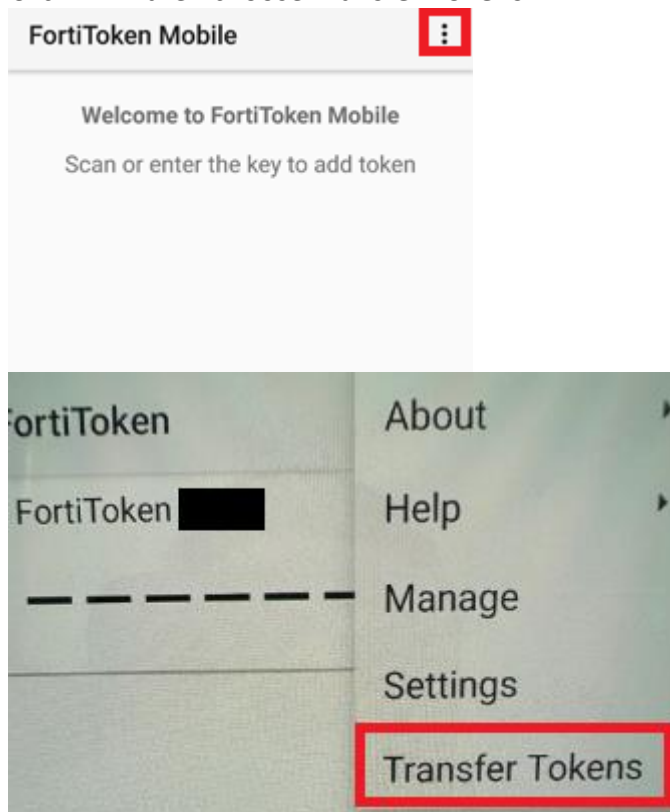
10. TRANSFER OF SOFTWARE TOKEN FROM OLD TO NEW DEVICE (AVAILABLE FOR ANDROID AND APPLE IOS DEVICE ONLY)

In case transfer of software token is required due to a change of mobile device, you can either contact [Cloud Service Helpdesk](#) to initiate the process, or initiate the process by yourself by the Transfer Token feature in the token mobile app. Either case, **help from your school principal will be required.**

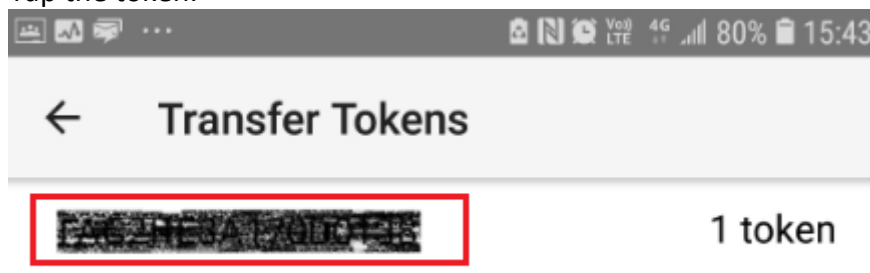
Below procedures illustrate how to **initiate Transfer Tokens** by yourself.

10.1 FOR ANDROID DEVICES

1. Click  then choose **Transfer Tokens**.



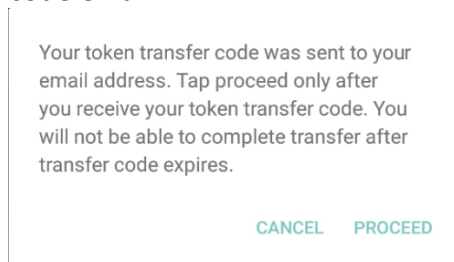
2. Tap the token.



3. Tap **YES** , then an email with a token transfer code will be sent to the email address of your **school principal**.



4. Tap **PROCEED** **ONLY AFTER** your **school principal** receive the token transfer code email.



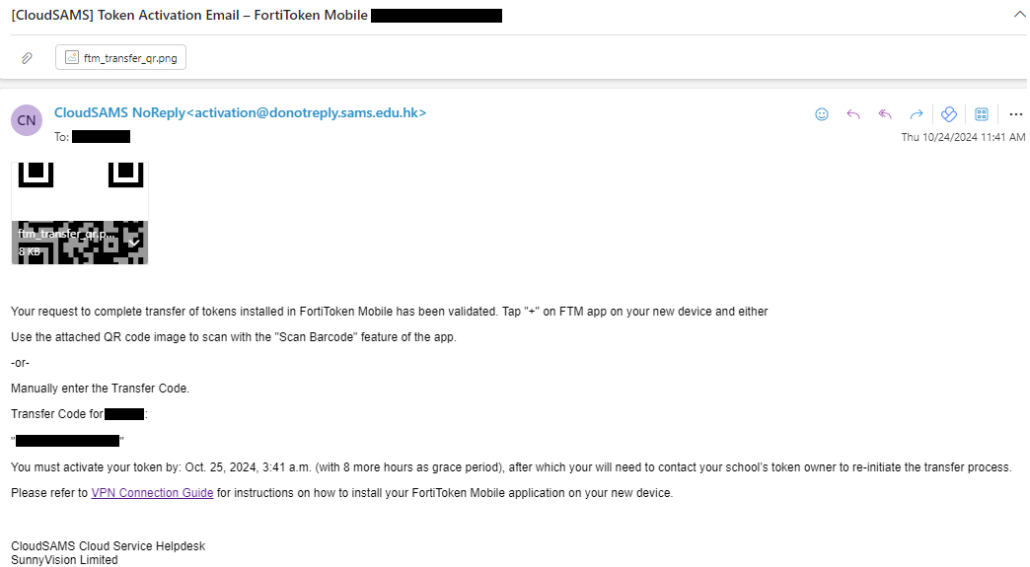
5. Tap **OK** .

Tokens successfully uploaded to the server and removed from this device. Please check your email for activation code to complete transfer of the tokens on new device.

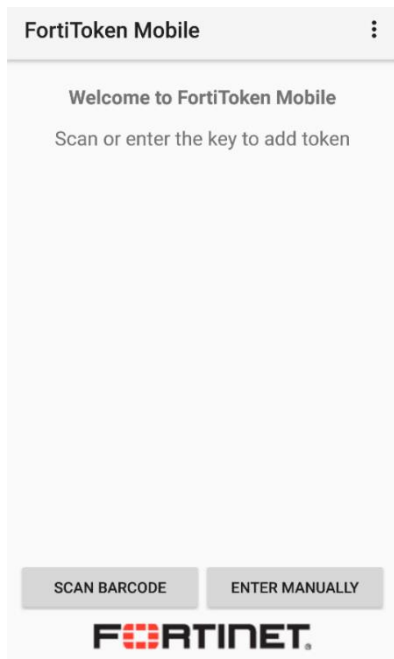
OK

6. The token is removed from FortiToken Mobile App of your old device.

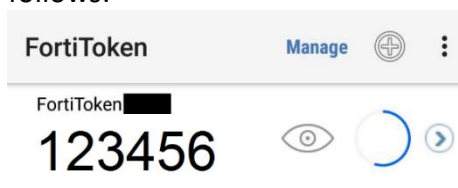
- Open the token activation email. Please note that the activation code will expire in 24+8 = 32 hours.



- Tap **SCAN BARCODE** to scan the QR code [1] in the activation email. You can also tap **ENTER MANUALLY** to input the activation code [2] in preceding sample mail.

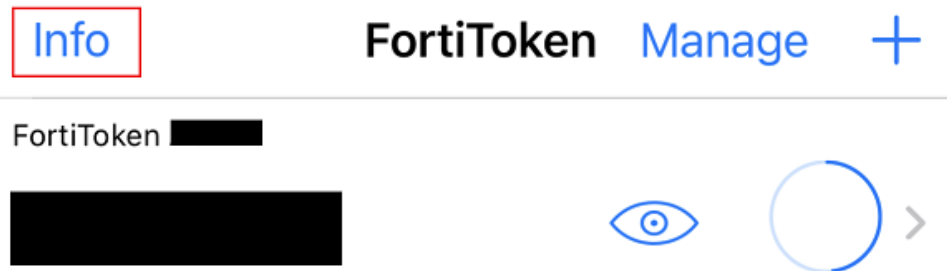


- Once the token is activated, the VPN token will be displayed on the app as follows:

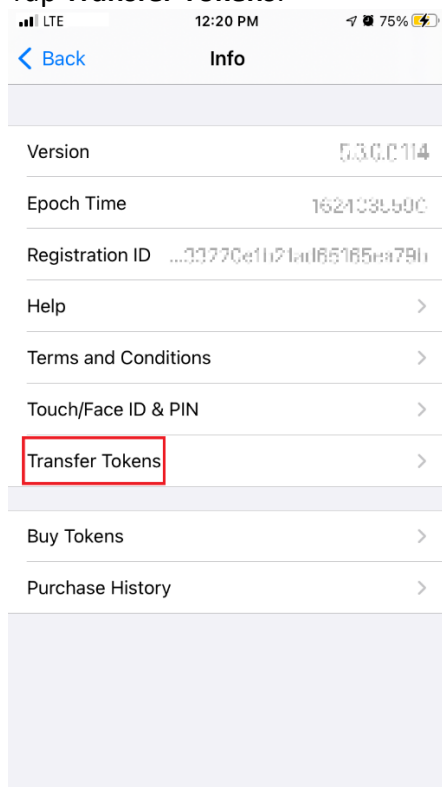


10.2 FOR APPLE IOS DEVICES

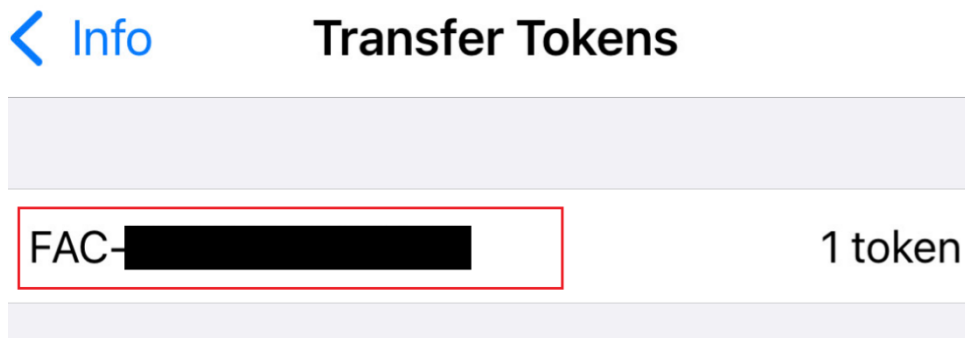
1. Tap Info



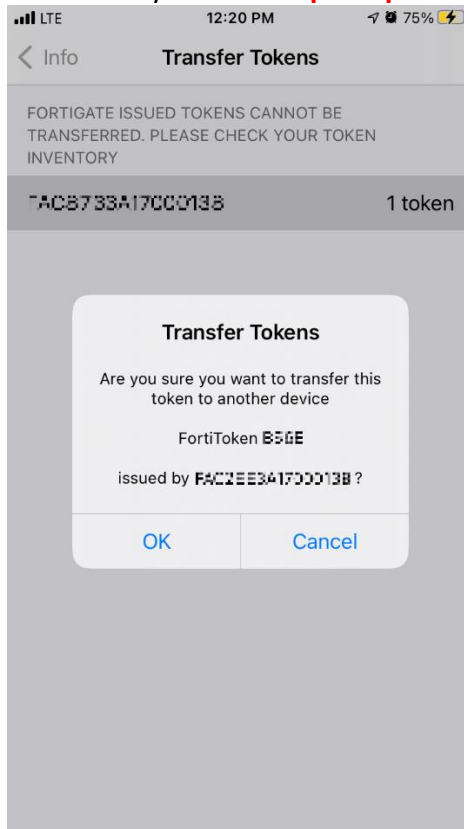
2. Tap Transfer Tokens.



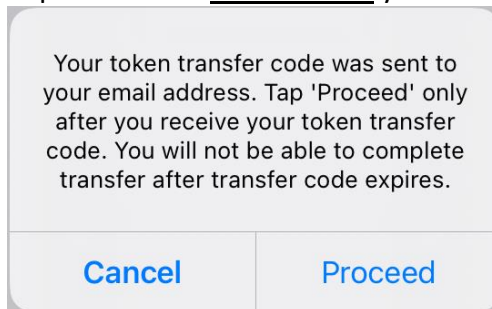
3. Tap the token.



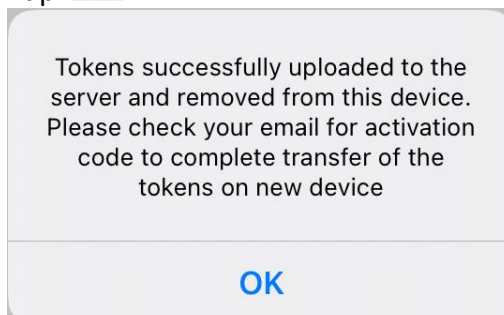
4. Tap **OK**, then an email with a token transfer code will be sent to the email address of your **school principal**.



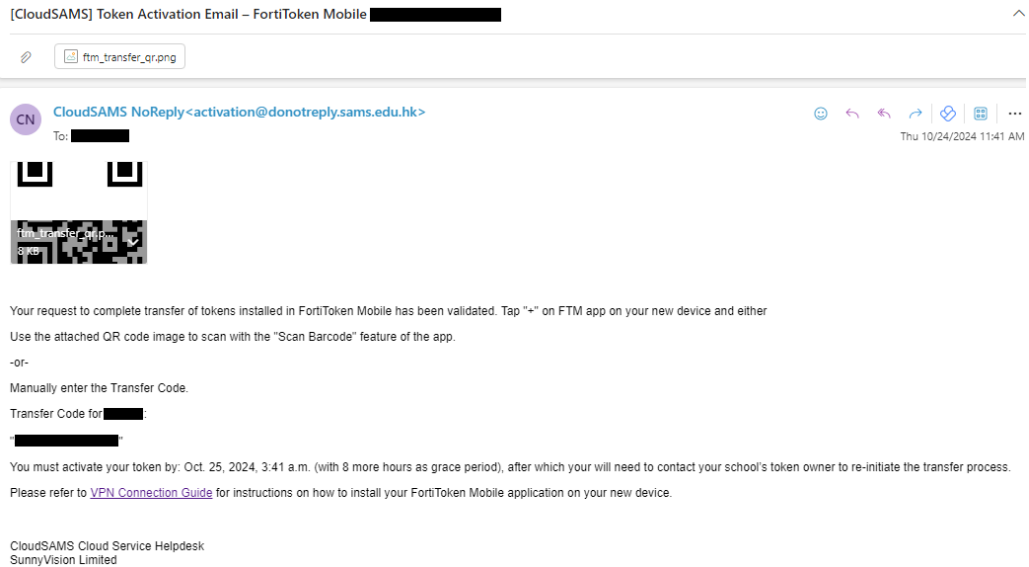
5. Tap **Proceed** **ONLY AFTER** you receive the token transfer code email.



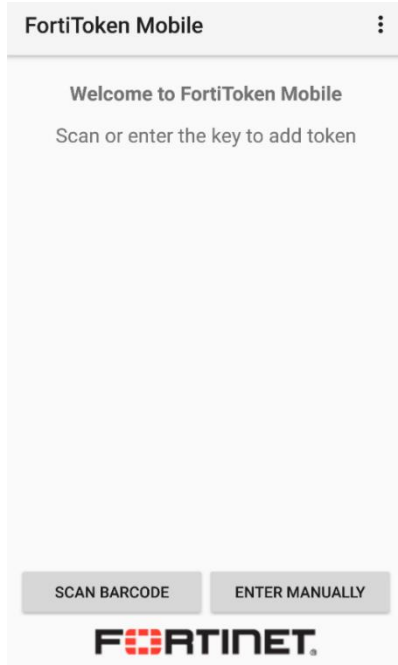
6. Tap **OK**.



- The token is removed from FortiToken Mobile App of your old device.
- Open the activation email. Please note that the activation code will expire in 24+8=32 hours.



- Tap **SCAN BARCODE** to scan the QR code [1] in the activation email. You can also tap **ENTER MANUALLY** to input the activation code [2] in preceding sample mail.



- Once the token is activated, it will be displayed on the app as follows:

