THE JUDICIARY

DIRECTORATE OF ICT

GUIDELINESS ON THE INSTALLATION AND CONFIGURATION OF VPN CLIENT ACCESS - FORTICLIENT

DATE: 8th April 2022

Contents

1. INTRODUCTION

The Judiciary in the FY-20/21 acquired enterprise Network and Security solutions in order to host and manage core Judiciary systems. In order to mitigate cyber-attacks and to ensure that access to Judiciary systems is secure, the Directorate of ICT acquired FortiClient enterprise VPN for secure access to the Judiciary Data centers housing core Judiciary systems.

The Directorate of ICT has developed this guide with the installation set of steps on how to install and configure FortiClient to be used to access Judiciary Applications such as CTS and JFMIS in our new environment.

2. PREREQUISITE:

These are the necessary prerequisites that are needed to have a complete and successful installations.

i. Computer or a laptop

ii. You must have Administrator rights to the above computer

iii. Internet connection

Note: Your computer must be connected to the internet.

3. GUIDELINESS ON THE INSTALLATION AND CONFIGURATION OF FORTICLIENT IN PRIMARY DATA CENTER

3.1 WINDOWS COMPUTER GUIDE

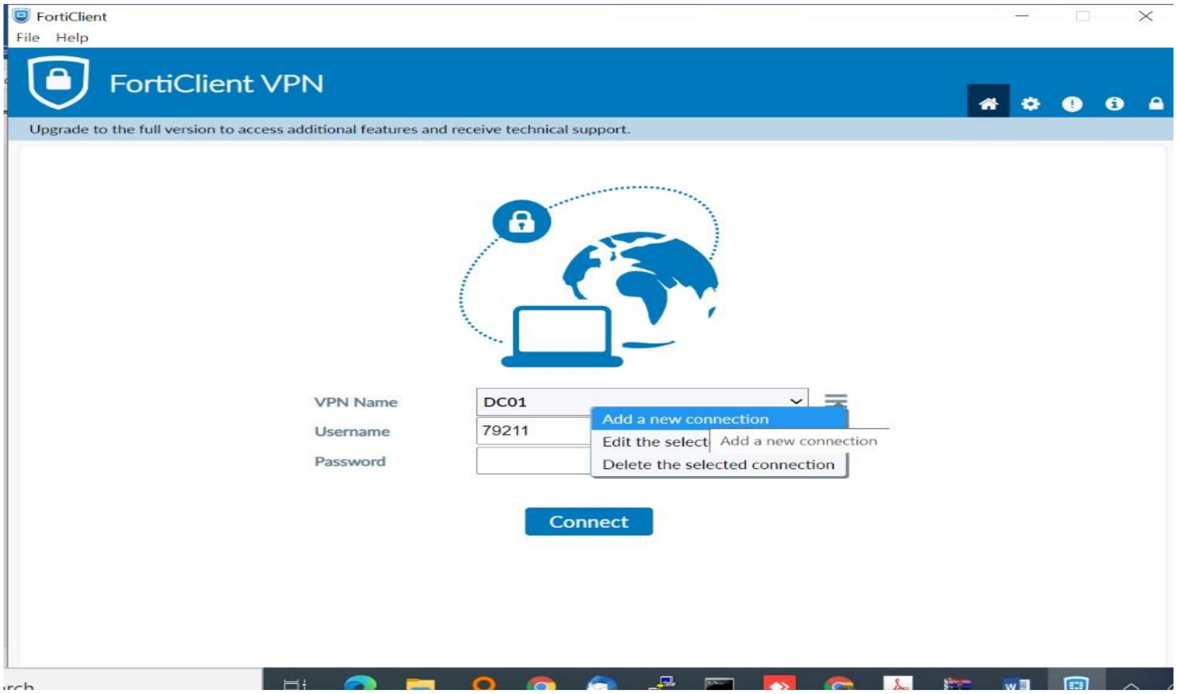
To install Fortinet-client VPN on a Windows computer, follow the following steps.

1. Step one is to navigate to the URL below, download VPN Client applications and install it. This is the Fortinet VPN Client application.

   https://drive.google.com/drive/folders/1QAU8bOuvyZQkN7okjsI1qw8-1QN80Ry0

2. Step two is to add new connection.

   Add a New Connection as shown below:



FortiClient
File Help
FortiClient VPN
Upgrade to the full version to access additional features and receive technical support.
Add a new connection
Edit the select
Add a new connection
Delete the selected connection
Connect

VPN Name DC01

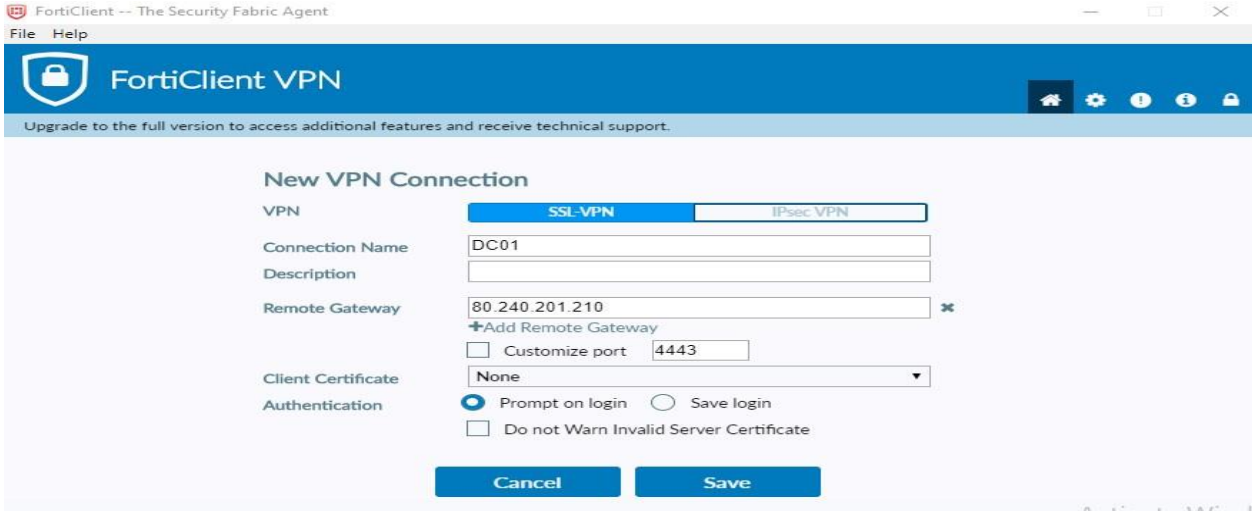
Username 79211

Password

3. The third step is to customize your Fortinet VPN Client application with the right configurations.

To connect to Primary Data Centre, configure your VPN client with the following settings;

i. **Connection name**: CTS SERVER
ii. **Remote Gateway**: 80.240.201.210
iii. **Customize port**: 4443
iv. **Client certificate**: None
v. **Authentication**: Tick “Prompt on login”
vi. **Log in Credentials**
Username: ‘Your PJ Number’
Password: To be shared


FortiClient -- The Security Fabric Agent
File Help
FortiClient VPN
Upgrade to the full version to access additional features and receive technical support.
Cancel
Save

New VPN Connection

VPN: [✓ SSL-VPN] IPsec VPN

Connection Name: DC01

Description:

Remote Gateway: 80.240.201.210

+Add Remote Gateway

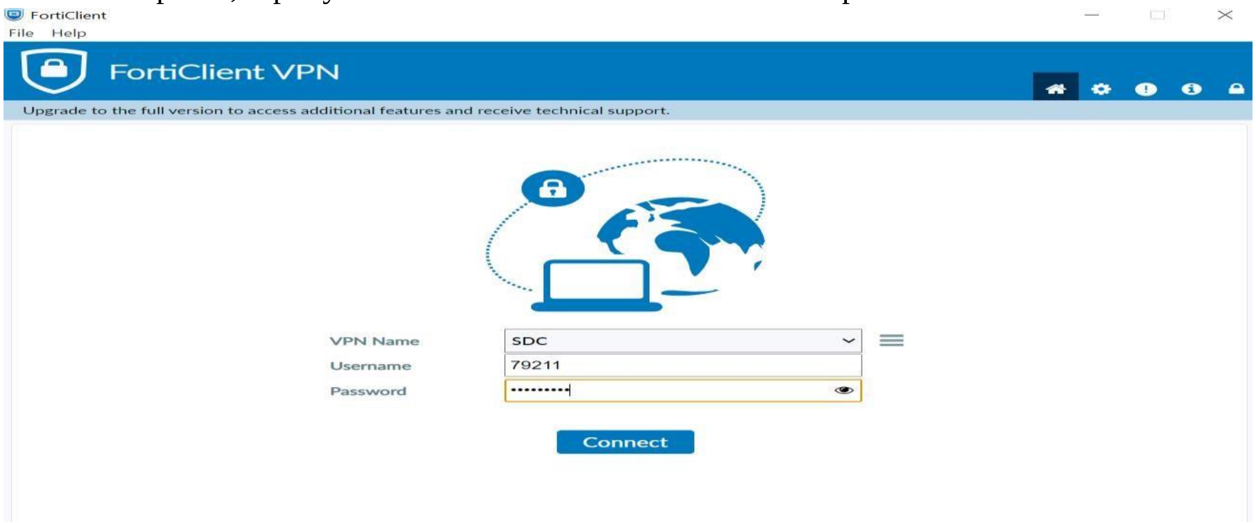
□ Customize port 4443

Client Certificate: None

Authentication: ● Prompt on login ○ Save login

□ Do not Warn Invalid Server Certificate

4. Step four; **Click** Save
5. Step five; Input your user credentials. Your username & password:


FortiClient
File Help
FortiClient VPN
Upgrade to the full version to access additional features and receive technical support.
Connect

VPN Name: SDC

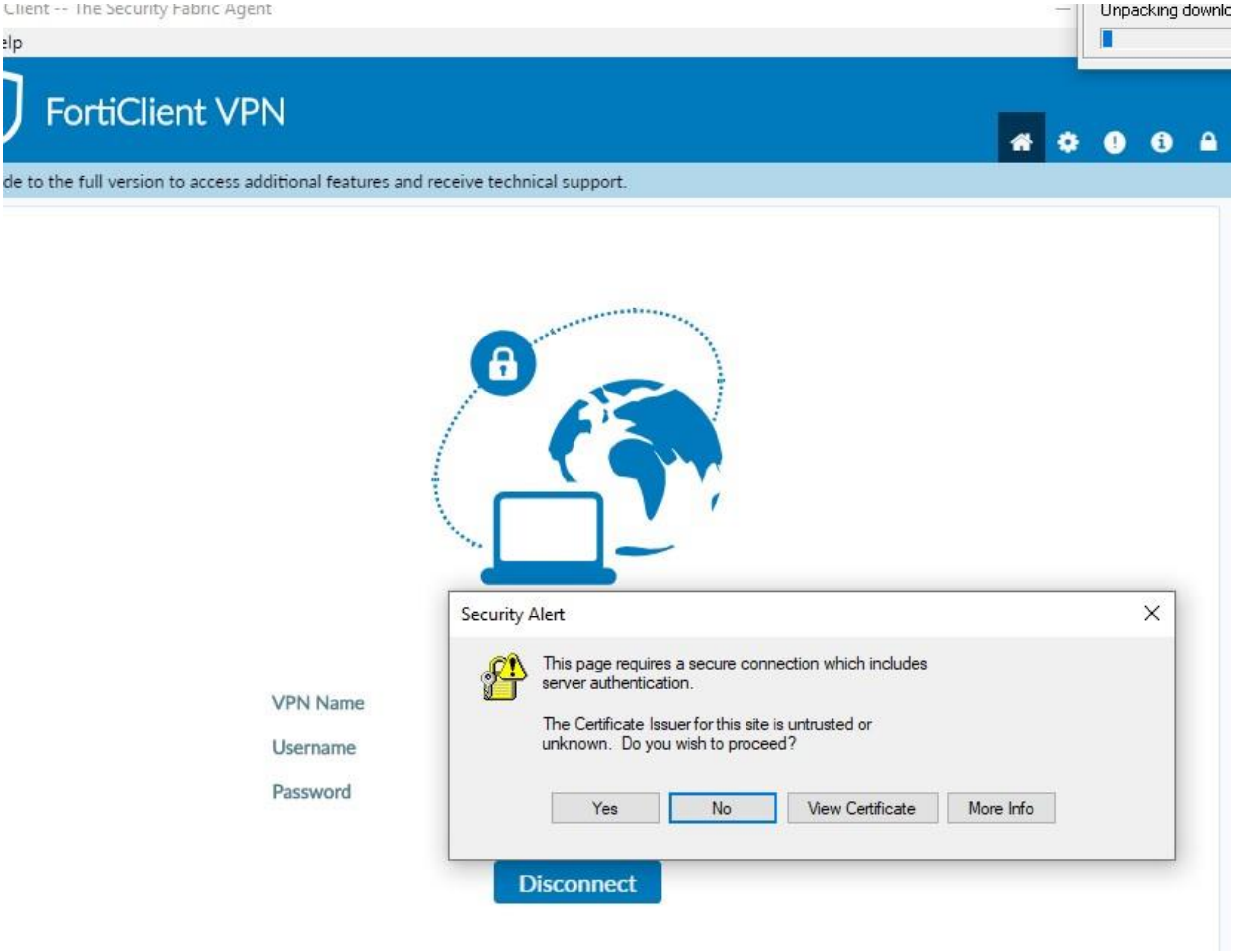
Username: 79211

Password: ••••••••••

\

6. Step six is to click Connect. **Accept certificate Security alert**

   Click **Yes** as shown in the snippet below


Client -- The Security Fabric Agent
elp
Unpacking downlo
FortiClient VPN
de to the full version to access additional features and receive technical support.
VPN Name
Username
Password
Disconnect

Security Alert

This page requires a secure connection which includes server authentication.

The Certificate Issuer for this site is untrusted or unknown. Do you wish to proceed?

Yes
No
View Certificate
More Info

Note;

Should you encounter this error:

"VPN Server may be unreachable (-14) in Windows 10 (Forticlient SSL VPN)"

Resolve it by following these steps

- ✓ *open "IE" browser, go to "Settings > Internet Options > Advanced" and scroll down to check "TLS Version" ✓ Enable:*
- ✓ *Use SSL 3.0*

  Use TLS 1.3 (experimental)
- ✓ *Then click apply-> ok*
- ✓ *Try and launch the VPN Client Again*

3.2 LINUX COMPUTER FORTICLIENT INSTALLATION GUIDE

Users that are using open-source platform especially Linux distros will have VPN client installed as indicated below.

The installation procedures for FortiClient application on Linux as follows

1. Download the application in the site below

Ubuntu 16.04 LTS

Install gpg key by using the following command:

```
wget -O - https://repo.fortinet.com/repo/6.4/ubuntu/DEB-GPG-KEY | sudo apt-key add -
```

Add the following line in /etc/apt/sources.list

```
deb [arch=amd64] https://repo.fortinet.com/repo/6.4/ubuntu/ xenial multiverse
```

Update package lists

```
sudo apt-get update
```

Install FortiClient

```
sudo apt install forticlient
```

Ubuntu 18.04 LTS and 20.04 LTS

Install gpg key

```
wget -O - https://repo.fortinet.com/repo/6.4/ubuntu/DEB-GPG-KEY | sudo apt-key add -
```

Add the following line in /etc/apt/sources.list

```
deb [arch=amd64] https://repo.fortinet.com/repo/6.4/ubuntu/ /bionic multiverse
```

Update package lists

```
sudo apt-get update
```

Install FortiClient

```
sudo apt install forticlient
```

2. Once the application is successfully installed, proceed and do configurations as shown below
   To connect to Primary Data Centre, configure your VPN client with the following settings;

i. **Connection name**: CTS SERVER
ii. **Remote Gateway**: 80.240.201.210
iii. **Customize port**: 4443
iv. **Client certificate**: None
v. **Authentication**: Tick "Prompt on login"
vi. **Log in Credentials**
Username: 'Your PJ Number'
Password: To be shared

3. Accessing Case Tracking System (CTS)

Upon successful connection of the VPN client, Open your browser and type https://cts.court.go.ke

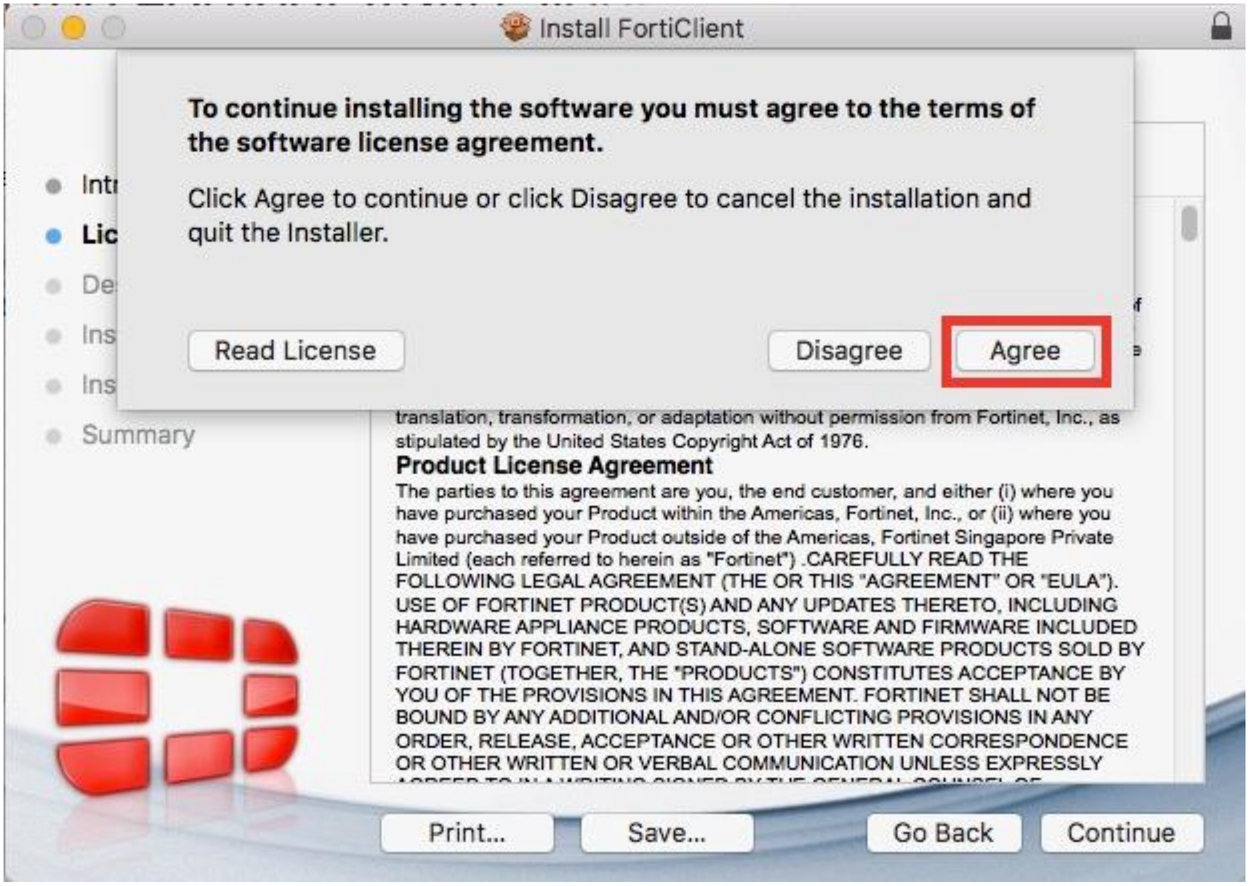
3.3 MacOS COMPUTERS FORTICLIENT INSTALLATION GUIDE

Users that are using MacOS will have VPN client installed as indicated below. The installation procedures for FortiClient application on MacOS is

1. Step one is to paste below URL in your browser to download and install FortiClient

https://filestore.fortinet.com/forticlient/downloads/FortiClientVPNSetup_6.2.0_macosx.dmg

2. Step two is to accept all the certificates as per the wizard.



To continue installing the software you must agree to the terms of the software license agreement.

Click Agree to continue or click Disagree to cancel the installation and quit the Installer.

translation, transformation, or adaptation without permission from Fortinet, Inc., as stipulated by the United States Copyright Act of 1976.

Product License Agreement

The parties to this agreement are you, the end customer, and either (i) where you have purchased your Product within the Americas, Fortinet, Inc., or (ii) where you have purchased your Product outside of the Americas, Fortinet Singapore Private Limited (each referred to herein as "Fortinet") .CAREFULLY READ THE FOLLOWING LEGAL AGREEMENT (THE OR THIS "AGREEMENT" OR "EULA"). USE OF FORTINET PRODUCT(S) AND ANY UPDATES THERETO, INCLUDING HARDWARE APPLIANCE PRODUCTS, SOFTWARE AND FIRMWARE INCLUDED THEREIN BY FORTINET, AND STAND-ALONE SOFTWARE PRODUCTS SOLD BY FORTINET (TOGETHER, THE "PRODUCTS") CONSTITUTES ACCEPTANCE BY YOU OF THE PROVISIONS IN THIS AGREEMENT. FORTINET SHALL NOT BE BOUND BY ANY ADDITIONAL AND/OR CONFLICTING PROVISIONS IN ANY ORDER, RELEASE, ACCEPTANCE OR OTHER WRITTEN CORRESPONDENCE OR OTHER WRITTEN OR VERBAL COMMUNICATION UNLESS EXPRESSLY

3. Step three is to add the connections

   To connect to Primary Data Centre, configure your VPN client with the following settings;

i. **Connection name**: CTS SERVER
ii. **Remote Gateway**: 80.240.201.210
iii. **Customize port**: 4443
iv. **Client certificate**: None
v. **Authentication**: Tick “Prompt on login”
vi. **Log in Credentials**
   Username: ‘Your PJ Number’
   Password: To be shared

3. Accessing Case Tracking System (CTS)

Upon successful connection of the VPN client, Open your browser and type https://cts.court.go.ke

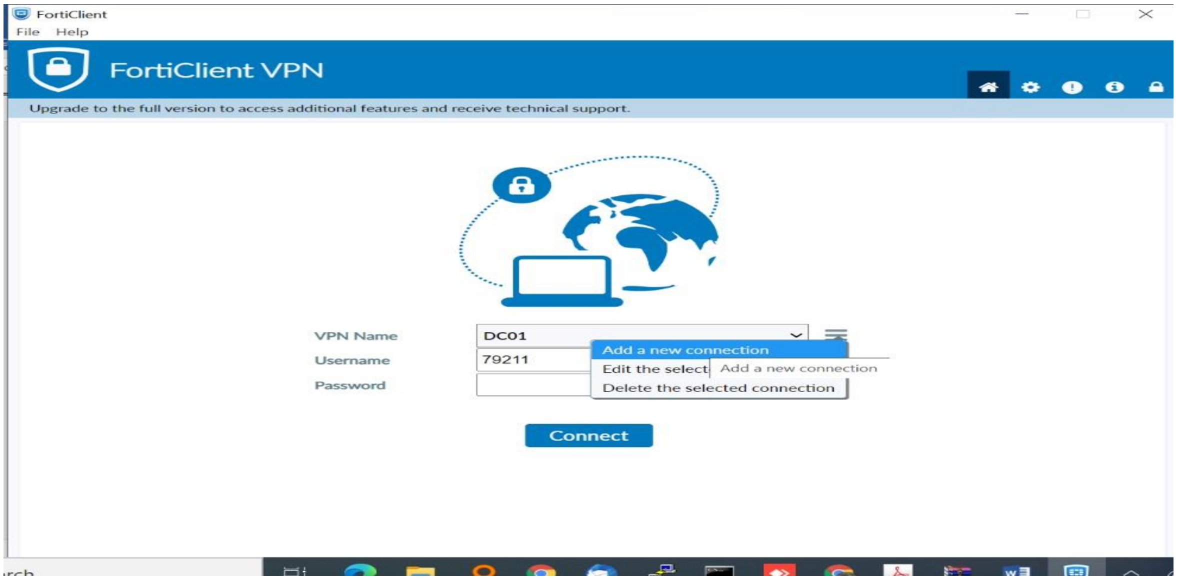
4. GUIDELINESS ON THE INSTALLATION AND CONFIGURATION OF FORTICLIENT SECONDARY DATA CENTER ON WINDOWS COMPUTER GUIDE, LINUX, MacOS

N/B: Since you have already installed FortClient on your computer as explained above successfully,

Proceed as below;

1. Step one is to add new connection:

   Click “**Add a New Connection**” as shown below:



Upgrade to the full version to access additional features and receive technical support.

VPN Name DC01

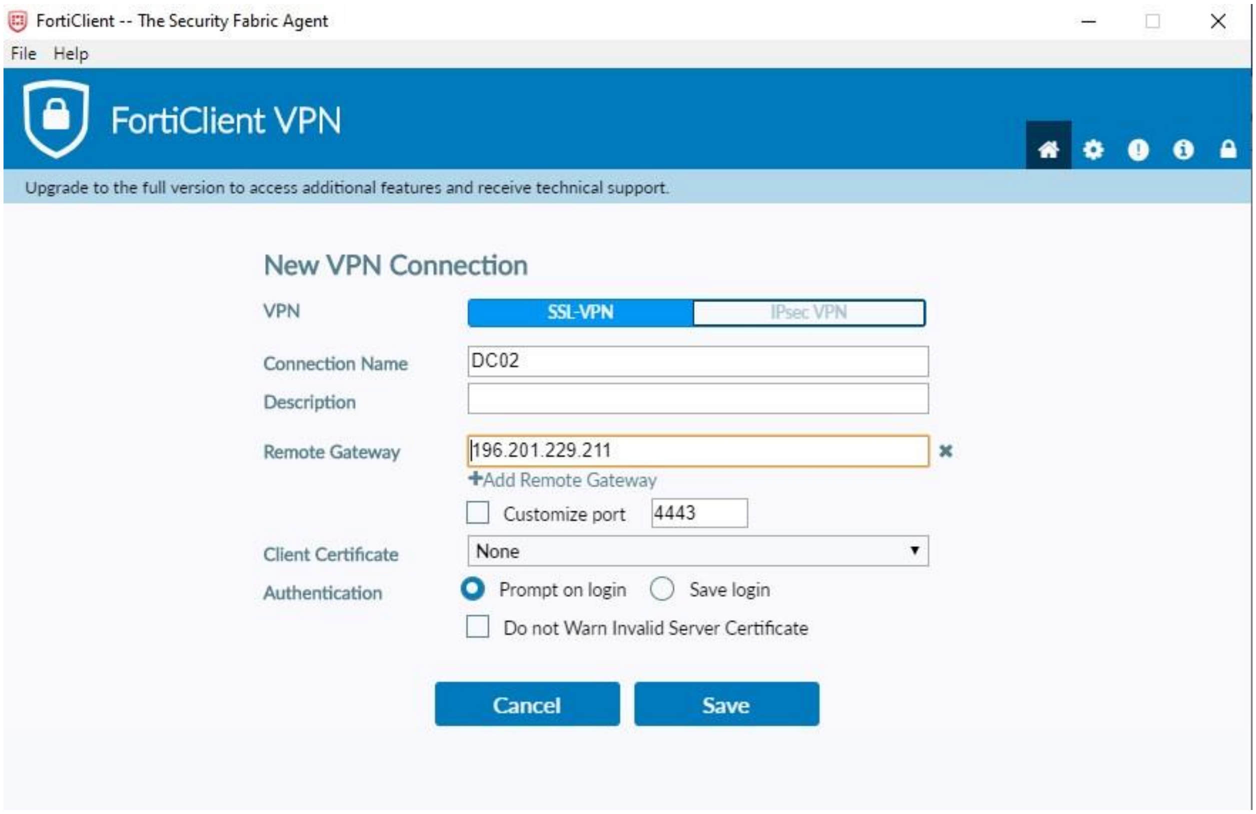
Username 79211

Password

2. The second step is to customize your Fortinet VPN Client application with the right configurations.

   For Secondary Data center, choose add a new connection & Populate as Below

i. **Connection name**: CTS SERVER
ii. **Remote Gateway**:196.201.229.211
iii. **Customize port**: 4443
iv. **Client certificate**: None
v. **Authentication**: Tick “Prompt on login”
vi. **Log in Credentials**
vii. **Username:** ‘Your PJ Number’
viii. **Password**: To be shared



Upgrade to the full version to access additional features and receive technical support.

New VPN Connection

VPN: [✓ SSL-VPN] IPsec VPN

Connection Name: DC02

Description:

Remote Gateway: 196.201.229.211

+Add Remote Gateway

□ Customize port 4443

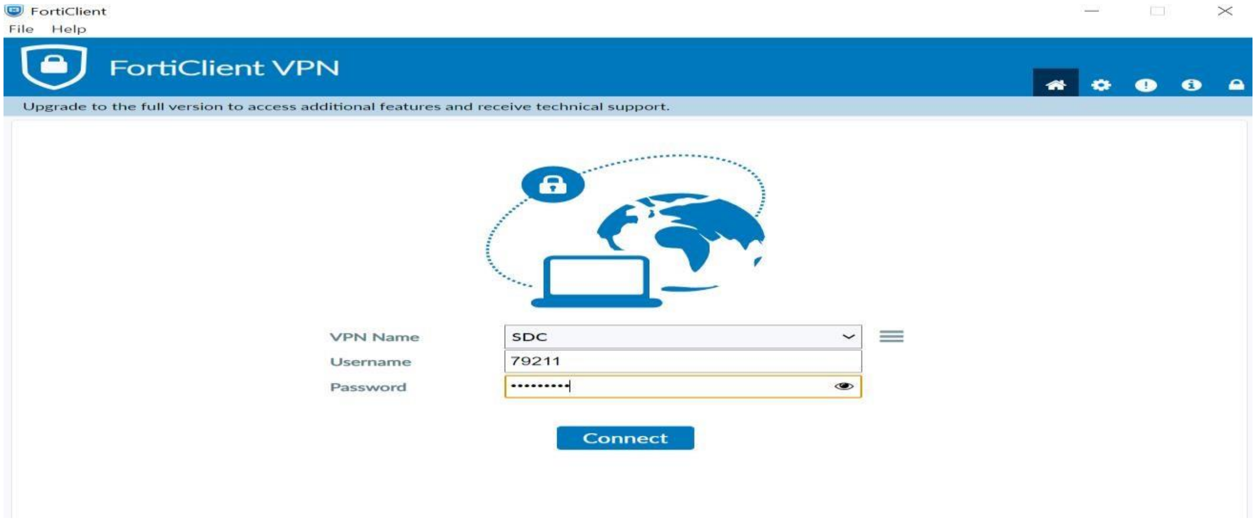
Client Certificate: None

Authentication: ● Prompt on login ○ Save login

□ Do not Warn Invalid Server Certificate

4. Step four; **Click** Save

5. Step five; Input your user credentials. Your username & password:



Upgrade to the full version to access additional features and receive technical support.

VPN Name: SDC

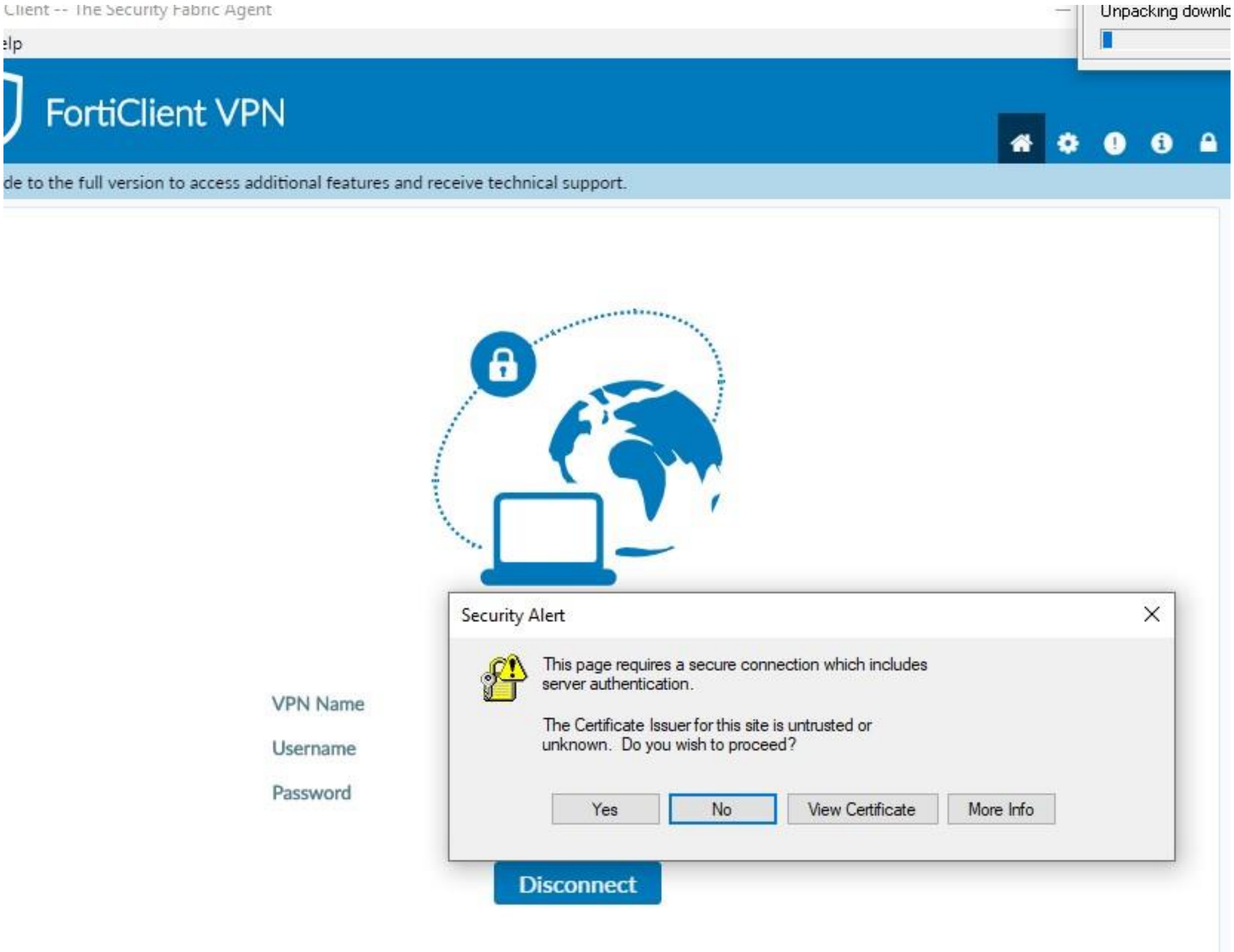
Username: 79211

Password: •••••••••

6. Step six; Click Save Click Connect.

   Accept certificate Security alert

   Click Yes



Client -- The Security Fabric Agent
elp
Unpacking downlo
FortiClient VPN
de to the full version to access additional features and receive technical support.
VPN Name
Username
Password
Disconnect
Security Alert
Yes
No
View Certificate
More Info

This page requires a secure connection which includes server authentication.

The Certificate Issuer for this site is untrusted or unknown. Do you wish to proceed?

Note;

Should you encounter this error:

"VPN Server may be unreachable (-14) in Windows 10 (Forticlient SSL VPN)"

Resolve it by following these steps

- ✓ *open "IE" browser, go to "Settings > Internet Options > Advanced" and scroll down to check "TLS Version"* ✓ *Enable:*
- ✓ *Use SSL 3.0*

  Use TLS 1.3 (experimental)
- ✓ *Then click apply-> ok*
- ✓ *Try and launch the VPN Client Again*

HOW TO:

1) How to access CTS.

Accessing Case Tracking System (CTS)

Upon successful connection of the VPN client;

i. Open your browser and type: https://cts.court.go.ke
ii. Login using your credentials

2) How to access jfmis

Upon successful connection of the VPN client;

i. Open your browser and type: https://jfmis.court.go.ke
ii. Login using your credentials

3) How to access efiling

i. Open your browser and type: https://efiling.court.go.ke
ii. Login using your credentials

5 CONCLUSION

The above guide is meant to be a guide on how to securely access the Judiciary applications by the use of secure VPN client application. It is worth noting that this access is to the test environment only and any update to the system will not reflect in the production environment.

5. DISCLAIMER

The above installation guide is a Judiciary information and shall NOT BE SHARED to the public without prior authorization of the Judiciary, the Directorate of ICT through the Chief Registrar Office.

This information is for internal use only within the Judiciary. Any person found to misuse this information is liable to breach of private information and the Judiciary code of conduct.