Lumen® Adaptive Network Security

Mobility user guide | February 2022

Table of contents

Adaptive Network Security: Mobility overview 3

Key features 3

Prepare for Mobility service activation 4

What to expect during Mobility service activation 4

Adaptive Network Security: Mobility service guidance 5

General guidance 5

IPSec tunnel guidance 5

SSL tunnel guidance 6

Clientless web access guidance 6

FortiClient endpoint guidance 6

FortiClient installation instructions 7

FortiClient download 7

Windows - IPSec VPN mobility 7

Windows – SSL VPN mobility 11

iOS - IPSec VPN setup 13

iOS - SSL VPN setup 16

Android - IPSec VPN setup 18

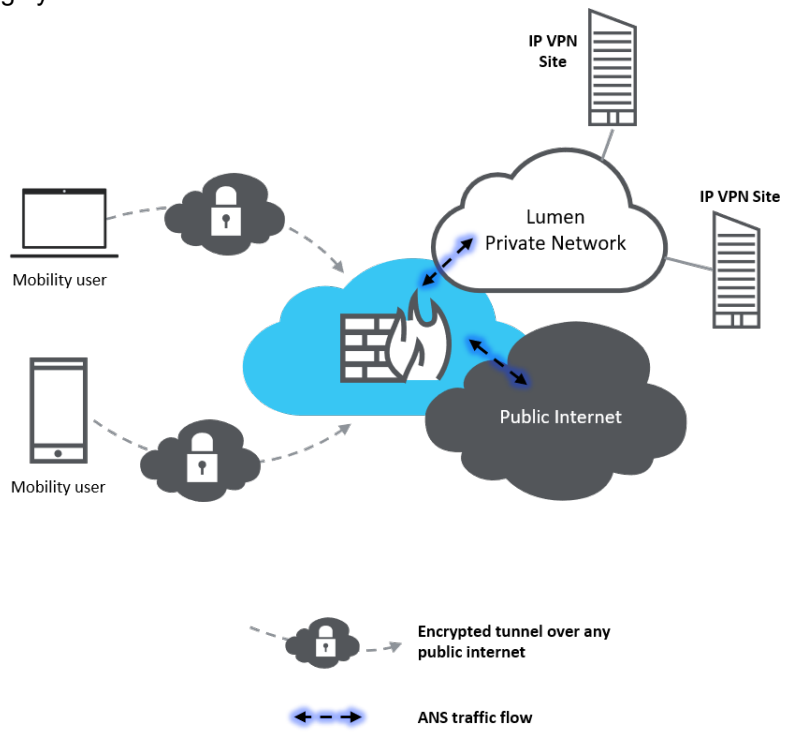
MSI package implementation guidance for administrators 23

Adaptive Network Security: Mobility overview

Adaptive Network Security – Mobility allows you to remotely connect to your Lumen MPLS/IPVPN network securely over the internet using a mobile device.

Key features

- Remote ANS Mobility users connect via SSL/IPsec VPN encrypted tunnels over any internet.
- Requires FortiClient to be installed on each endpoint, or SSL clientless web access to user applications.
    - OS support for Windows, Linux, Mac OSX, iOS, Android, Chromebook.
    - Clientless web access standard support is up to four landing pages (e.g. portals) with three AD groups and eight bookmarks (e.g. internal links). Expanded scale can be reviewed as a specials request.
    - Bookmarks can support these protocols: Citrix, FTP, HTTP/HTTPS, port forwarding, RDP, SMB/CIFS, SSH, Telnet, VNC.
- You are responsible for your own DNS resolution and zone updates for either client tunnel access or clientless web access.
- Authentication and group policies via your Active Directory (AD)/LDAP.
- ANS Mobility user 2FA authentication via customer-provided 3rd Party MFA Radius server.
- Full Tunnel Mode (all internet traffic is sent to ANS gateway) recommended configuration to help ensure remote traffic is protected.
- Users can split tunnel their internet as an optional configuration; however, end-point security protection is highly recommended.



Prepare for Mobility service activation

The Lumen sales engineer and security solutions architecture team contact will review the following points with you before the Adaptive Network Security (ANS) – Mobility activation. Ensuring these questions are completed prior to the activation call with the Lumen service activation team will help you start using the Adaptive Network Security – Mobility service more quickly.

1. What ANS gateway firewall will be used for the Mobility Service and how many total users and concurrent users are expected per ANS gateway firewall?
2. Are you able to use your own Active Directory (AD) server for direct authentication and group policy?
3. Please provide IP address.
4. Build user account for Mobility proxy use (with no PW expiration, and only user account, no admin rights).
5. Your administrator must ensure they have downloaded the Fortinet® FortiClient and have tested the installation and confirmed remote access meets their needs, including group access and policy usage.
6. For assistance on FortiClient downloads and instructions, please see the installation instructions in the *FortiClient Endpoint Guidance* section.
7. Please ensure you have a Lumen Control Center account with access to the **Monitoring** tab.

What to expect during Mobility service activation

Here is a summary of the Adaptive Network Security – Mobility implementation process:

1. Customer acknowledges and sign quote for new Adaptive Network Security – Mobility service.
2. Lumen customer care manager (CCM) reviews the Adaptive Network Security – Mobility order with you and provides updates as it progresses through design and activation.
3. If you haven't been previously set up in Lumen Control Center, you will receive an email with instructions for setting up 2FA authorization for access to security reports.
4. Lumen technical design engineering team reviews technical details for the new Adaptive Network Security – Mobility service with you.
5. You install user endpoint FortiClient and user authentication method. *See FortiClient Endpoint Guidance section.*
6. CCM confirms scheduled activation date of Adaptive Network Security – Mobility Service.
7. Lumen activations team activates Adaptive Network Security – Mobility service and notifies you that service is ready for acceptance.
8. You accept and confirm Adaptive Network Security – Mobility activation is complete.
9. Billing starts and you can now view Adaptive Network Security reports on Lumen Control Center.

Adaptive Network Security: Mobility service guidance

General guidance

1. A distinct IP pool/subnet will be configured to accommodate all remote users per ANS gateway network firewall instance. This IP space cannot span across multiple ANS gateways.
2. When building your LDAP structure for mobility authentication, please ensure you add an ANS LDAP username and password in the root.
    a. You must ensure they have tracking in place for service account password expiration, and notification must be made to Lumen at time of change. If this password expires, the remote users will lose authentication.
    b. You must ensure LDAP structure is reachable on the Lumen MPLS/IP VPN network.
3. Your domain controller naming convention will be used for your ANS Mobility username.
    a. This is your Active Directory name, e.g. security account manager (SAM).
    b. We recommend the use of a new “remote access” AD group(s) to allow only authorized users permission to use this remote access method. Simply create a group (maximum of 9), and we will allow only members of that new AD group to have remote access connectivity to the MPLS/IP VPN.
    c. Multiple groups are only supported using AD/LDAP authentication.
4. Lumen supports full tunnel mode as the recommended standard configuration for IPSec or SSL tunnel connectivity to your MPLS/IP VPN network to ensure remote traffic is securely protected. Split tunnel mode or full tunnel mode with local LAN access are optional configurations but have a higher risk of security exposure when used without security protection on user endpoints. Lumen is not responsible for vulnerabilities due to unprotected endpoints.
    a. Full Tunnel means ALL traffic from remote user flows through the tunnel to the ANS gateway to have common Unified Threat Management (UTM) filters applied to ALL traffic (MPLS/IP PVN + internet). This is the most secure and is recommended. You will not be able perform tasks from your remote or home office such as local printing, home sharing, etc.
    b. Full Tunnel Mode with Local LAN Access means ALL traffic flows up the tunnel EXCEPT local LAN traffic. This allows remote users to have access to their local LAN devices such as printers or shared storage. This is configured on the client side within the XML configuration in the client.
    c. Split Tunnel Mode means only traffic destined to the corporate network goes through the tunnel, defined by IP ranges, to common corporate resources. Everything else uses the local LAN egress to the internet.

IPSec tunnel guidance

1. IPSec Mobility uses the FortiClient application to enable a network connection that allows users to access all functions and applications on their MPLS/IP VPN network.
2. Distinct pre-share key will be provided for each ANS gateway. Pre-shared keys cannot be shared across multiple ANS gateways.

SSL tunnel guidance

1. SSL Mobility uses the FortiClient application to enable a network connection that allow users to access all functions and applications on their MPLS/IPVPN network.
2. Lumen supports using a public certificate with our Mobility Service for ANS gateway firewall server authentication.
3. Lumen will generate a certificate signing request (CSR) for customer to obtain SSL certificates from their certificate authority (CA). The input is captured in the Adaptive Network Security – Mobility provisioning workbook with the technical design engineer during the data gathering review. Fields needed for Lumen to create the CSR are:
    a. Common name (URL customer will setup to access mobility service on ANS gateway firewall).
    b. Organization (customer's company name).
    c. Locality (the organization's city).
    d. State (the organization's state).
    e. Country (the organization's country).
4. You can also choose to have us use the Fortinet factory certificate but be aware that you will see certificate errors unless you select to ignore them when configuring the FortiClient.
5. The technical design engineer will request the CSR generation and post the file with your account documents within Control Center or provide using our secure email platform.
    a. You are responsible for downloading the CSR, purchasing SSL certificate(s), and uploading them to the account documents section of Control Center or returning the certificate back to the technical design engineer through the secure email platform. You should enter your technical design engineer's email address as the target user within the account documents upload form if portal access is already setup and this route is chosen for certificate handling.
    b. Elliptical-Curve Cryptography (ECC) is not supported at this time.

Clientless web access guidance

Clientless web access standard support is up to four landing pages (e.g., portals) with three AD groups and eight bookmarks (e.g. internal links). Expanded scale can be reviewed via a specials request.

1. Clientless portals are presented as bookmarks within the web portal. This bookmark allows HTTPS proxy access to access it.
2. Bookmarks can support only these protocols: Citrix, FTP, HTTP/HTTPS, port forwarding, RDP, SMB/CIFS, SSH, Telnet, VNC.
3. Portal authentication groups are based on LDAP groups.

FortiClient endpoint guidance

1. The Lumen SFTP server provides client software for Windows. If you need client software for another platform, discuss your requirement with the technical design engineer during the technical data gathering review.
2. Lumen does not provide a default packaged installation file, but it can be generated upon request. Suggested MSI configuration guidance for your administrator is provided in the next section.

FortiClient installation instructions

FortiClient download

Below are the directions to download the FortiClient from the Lumen sftp server.

- **SFTP server:** 67.128.43.98
- **Username**: forticlient
- **Password:** ctlvpn-609

The file name is: FortiClientSetup_6.0.9.0277_x64.zip

You can use any of the available SFTP clients like WinSCP, FileZilla, PSFTP and the Firefox add-on 'FireFTP'.

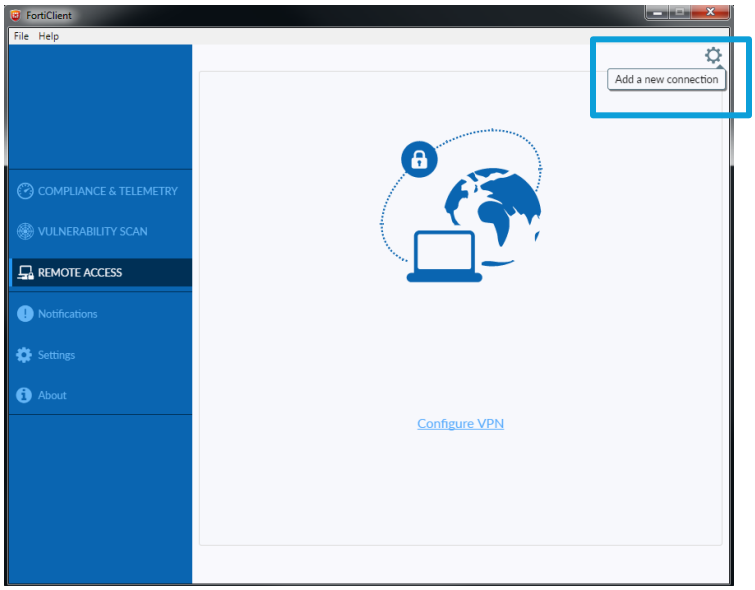
Industry-available installers can be deployed to thousands of Windows computers through Active Directory MSI deployment.

- Suggested MSI package configuration guidance for customer administrators with optional use of FortiClient Configurator to create an xml is explained in the next section. This can be requested with your technical design engineer during the technical data gathering review.

Launch client after install.

Windows - IPSec VPN mobility

1. From the FortiClient console, click on the settings cogwheel and select **Add a new connection**.



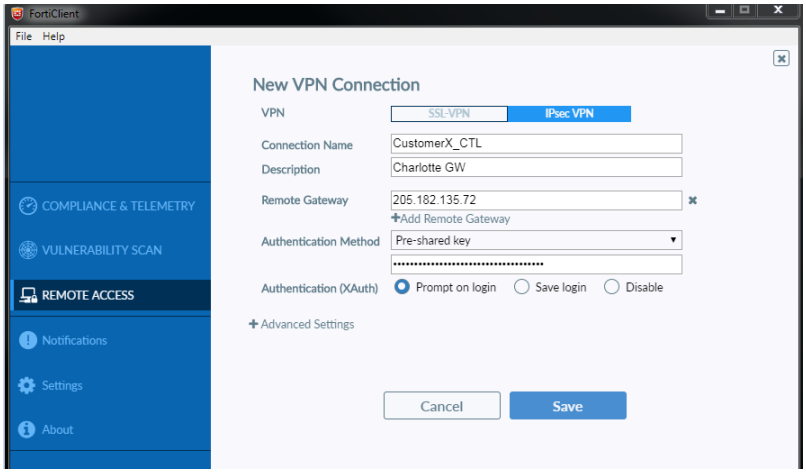
2. Once connected, you will need to edit your VPN connection.

   a. Select IPsec VPN.

   b. **Remote Gateway**—Lumen will provide you the remote GW IP by email.

   c. **Authentication Method**—Lumen will provide the pre-shared key using Control Center. Instructions are included in your customer notification.

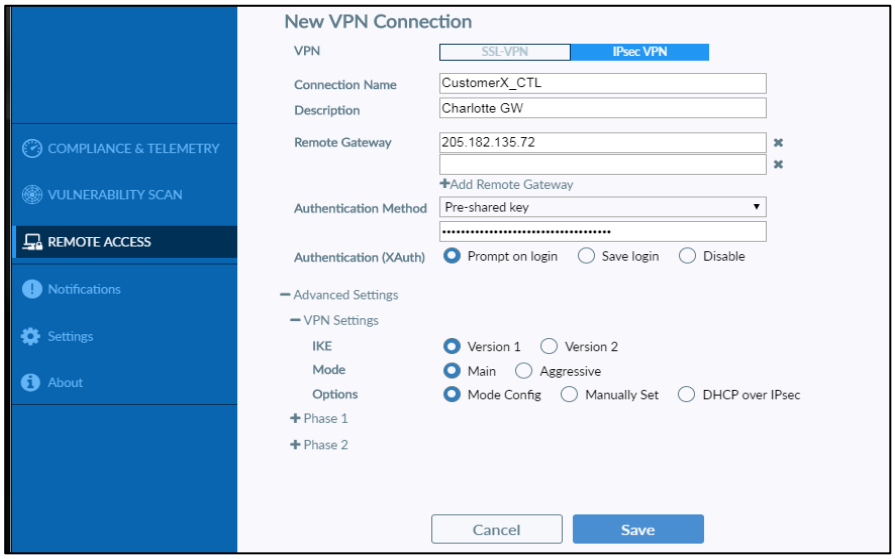
   d. Authentication (XAuth) —**Select Prompt on login**.



3. Additional changes are needed in **Advanced Settings**.

4. VPN Settings:

   a. Mode = **Main -** Options = **Mode Config** IKE – Version 1.



5. Staying on the **Advanced Settings** section, click the down arrow for **Phase 1** to access the drop-down options.

   a. IKE Proposal.

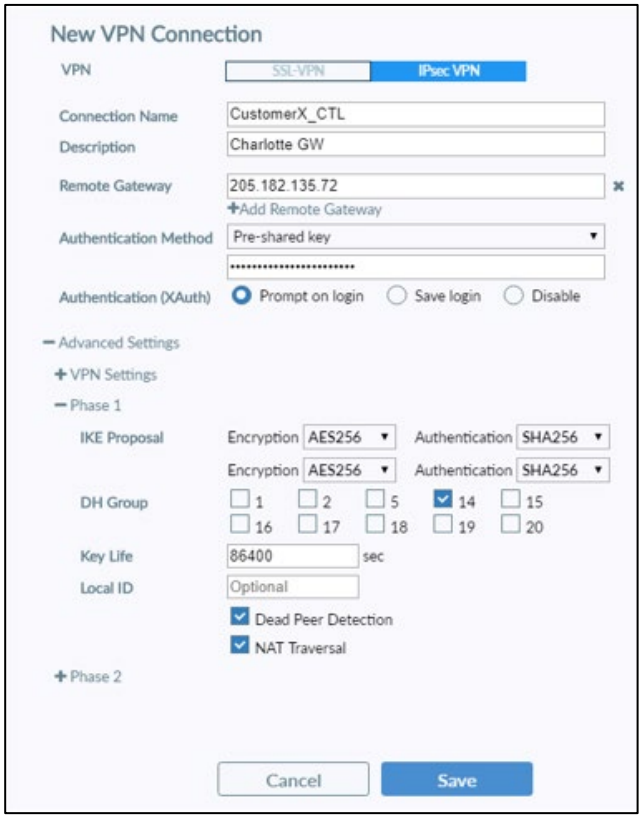
   b. **Encryption (BOTH)** = AES256.

   c. **Authentication =** SHA256.

   d. **DH Group** = 14 is checked.

   e. Validate **Key LIFE** = 86400.

   f. Validate **Dead Peer Detection** is check marked.



   g. Validate **NAT Traversal** is check marked.

6. Staying on the Advanced Settings section, click the down arrow for Phase 2 to access the drop-down options.

   a. IKE Proposal.

      i. **Encryption (BOTH)** = AES256.

      ii. **Authentication** = SHA256.

b. Key Life.

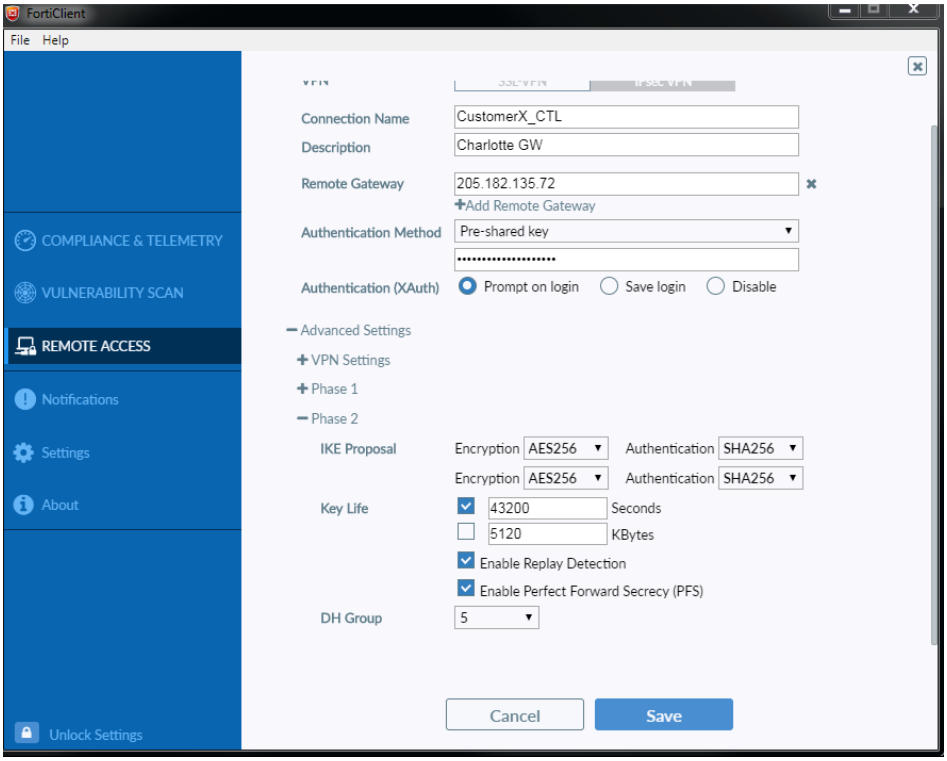
i. Validate **Seconds** is checked and has a value of 43200.

ii. Validate **Kbytes** is unchecked and has a value of 5120.

iii. Validate **Enable Replay Detection** is checked.

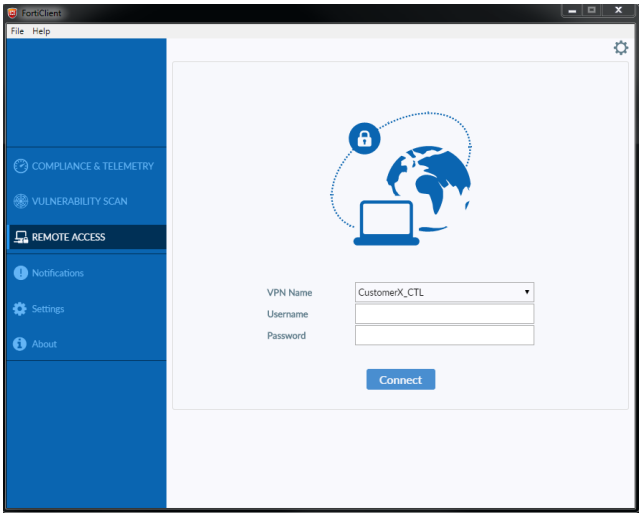
iv. Validate **Enable Perfect Forward Secrecy (PFS)** is checked.

v. Validate is **DH Group** set to 5.



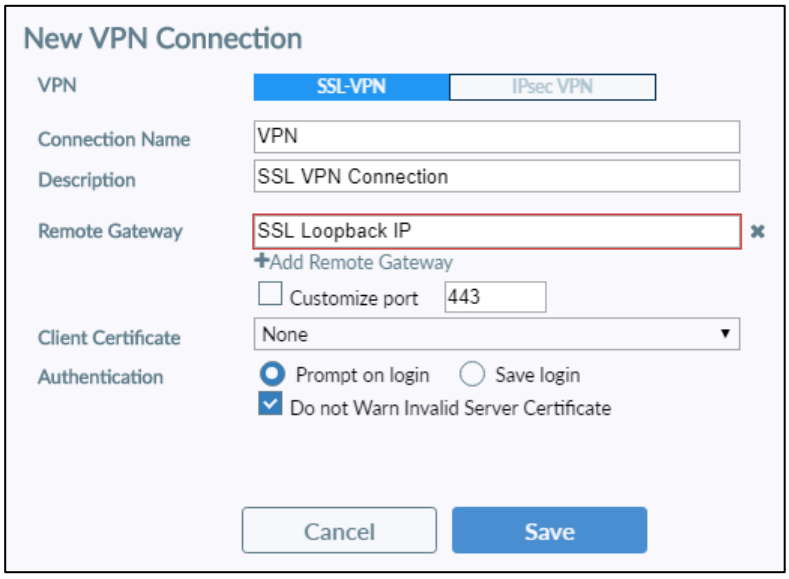
7. Select **SAVE** and then **CLOSE**. Your FortiClient is now configured. You will be returned to the log-in screen.

a. Be aware upon connection if you are on a VoIP call, your current call will terminate.



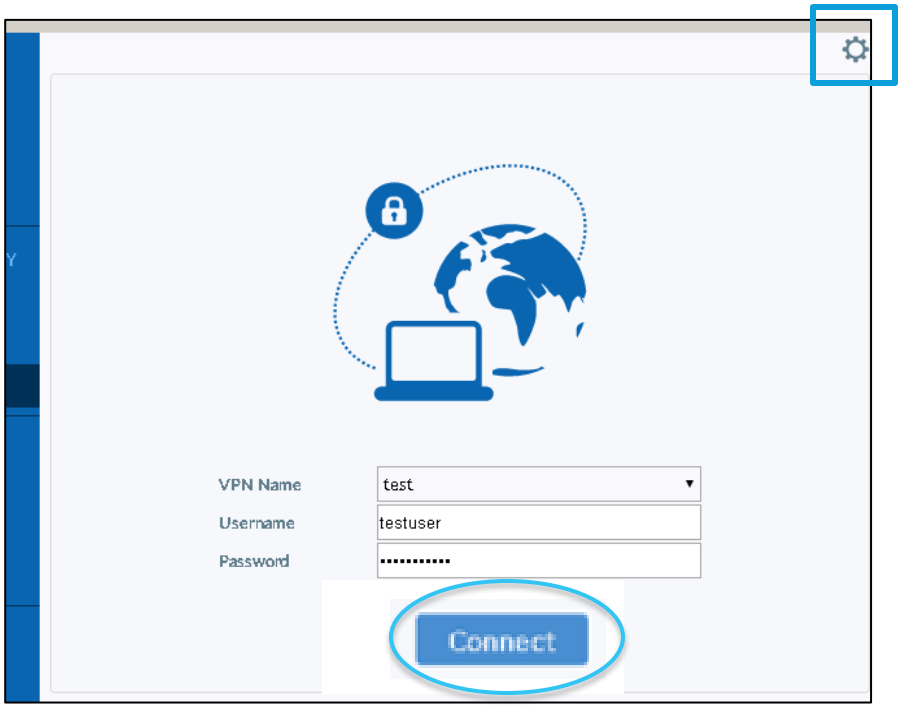
Windows – SSL VPN mobility

1. Click remote access and SSL VPN to configure new SSL VPN connection.

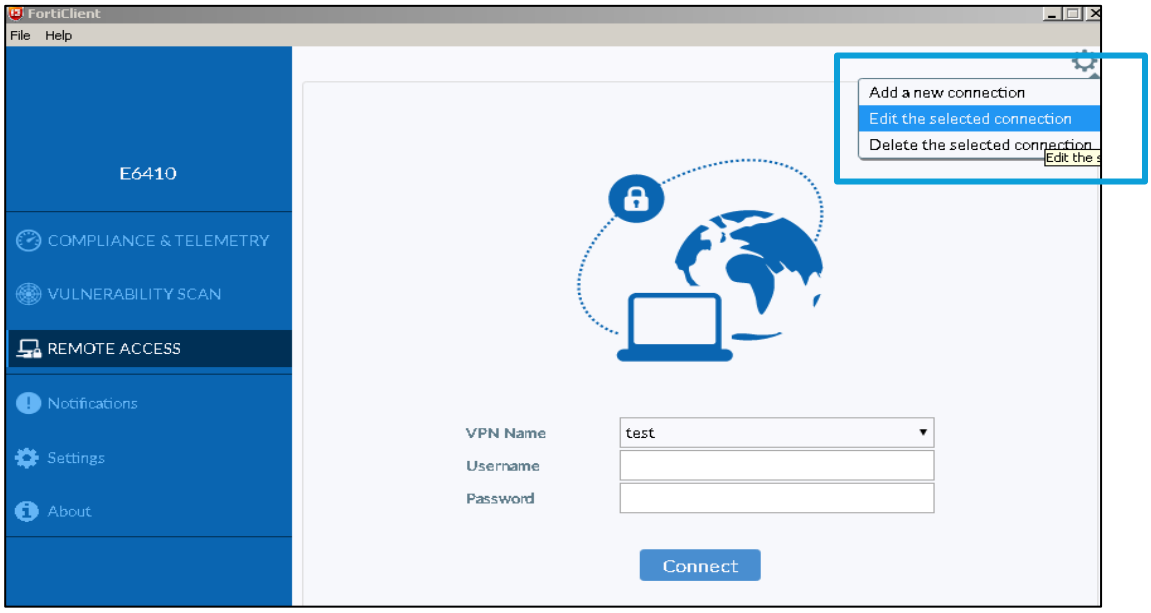


2. Click **Save**, then click **Close**.

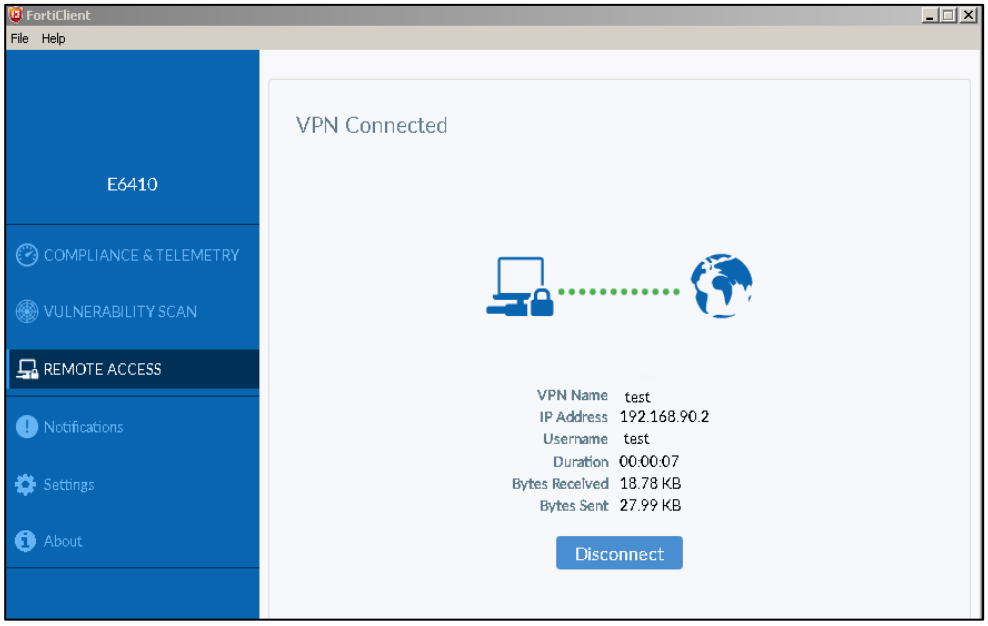
3. After your setup is complete, enter your username and password then click **Connect**.



4. If you do need to edit any settings click the gear box on the upper right-hand side to edit.



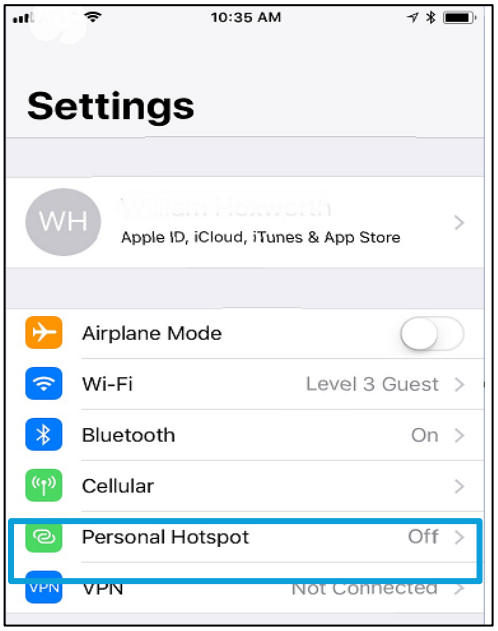
5. When authentication is successfully completed page below will be displayed.



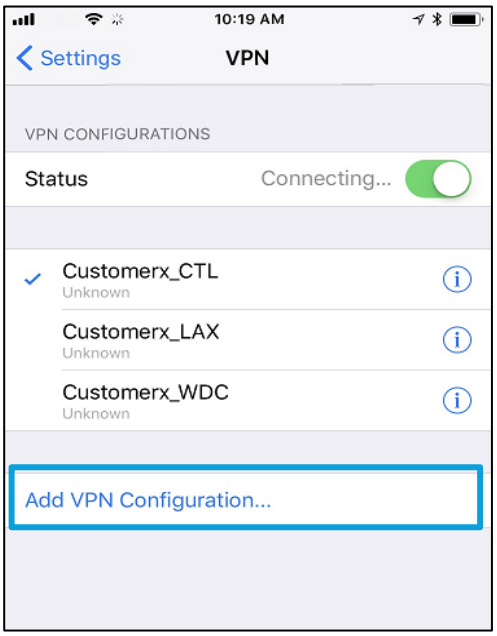
iOS - IPSec VPN setup

The following steps will take users through how to set up your ANS Mobility IPSec solution on an Apple device.

1. Under Settings tap **VPN** in the iOS settings page.



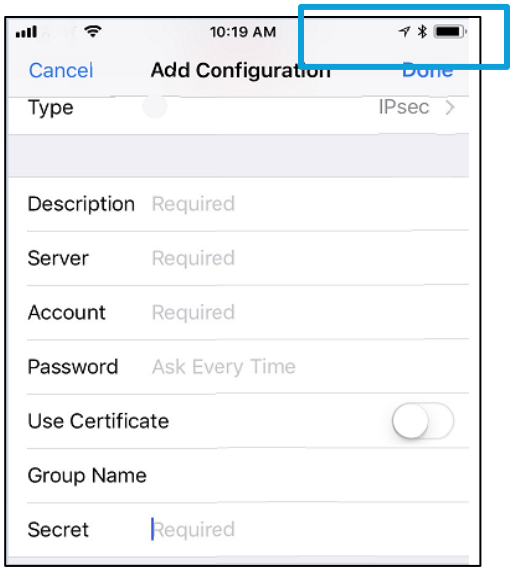
2. Tap Add **VPN Configuration**.

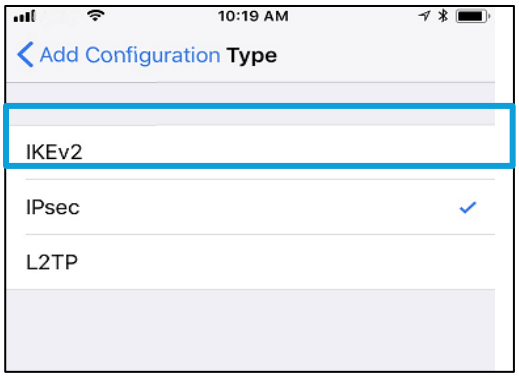


3. IKEv2 is the default configuration type.

   a. Tap the **Arrow** to change the type.

   b. Tap **IPsec** to change the configuration type.





4. Continue with Configuration.

   a. **Description** – Customer's choice. Example "CustomerX_Lumen"

   b. **Server** – Lumen will provide the gateway IP address that should be used here.

c. **Account** – your LDAP UserID.

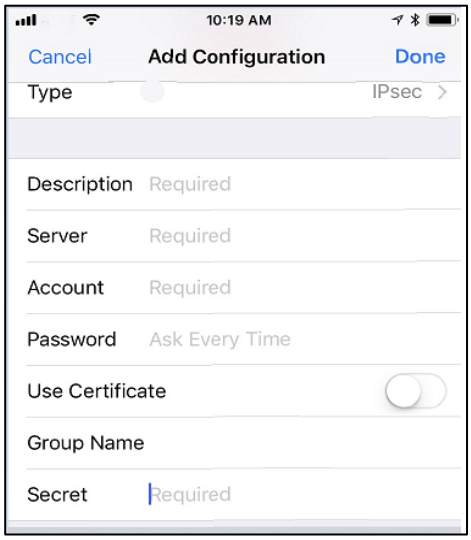
d. **Password**– your LDAP password.

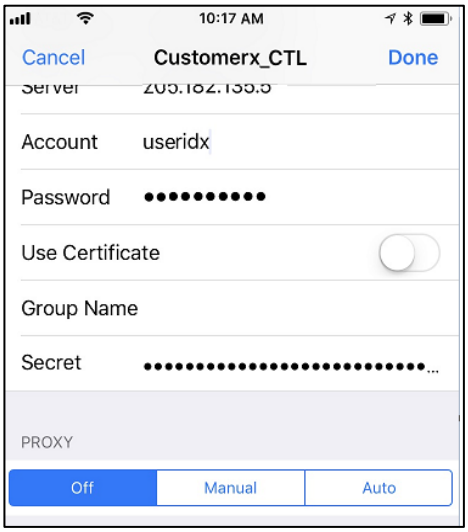
e. **Use Certificate** – Set to off.

f. **Group Name** – left blank.

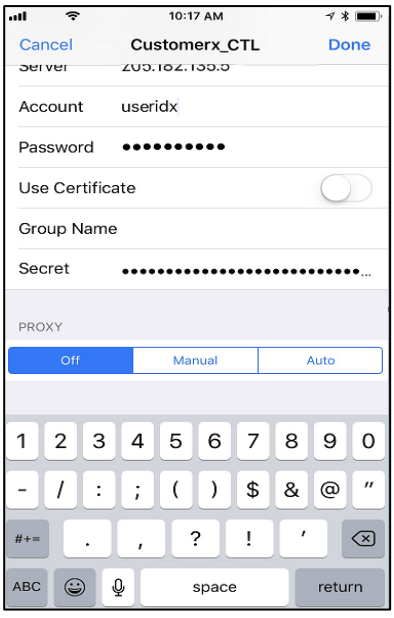
g. **Secret** – Lumen will provide to you with instructions.

h. **Proxy** – Tap **OFF**.



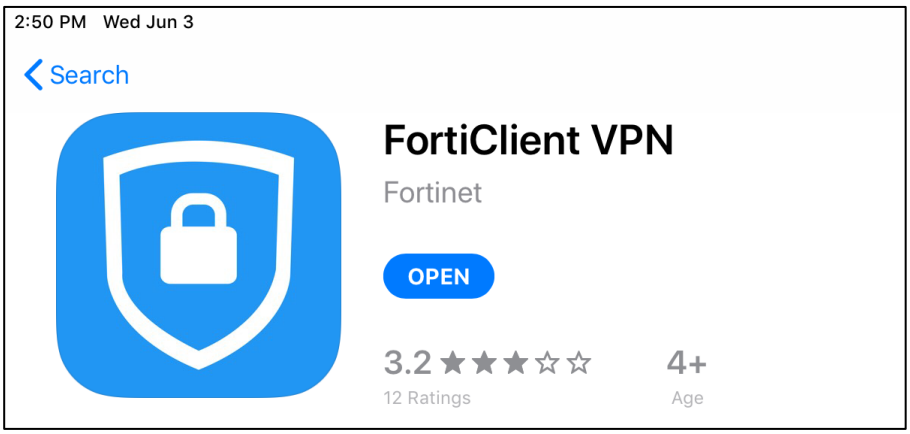


5. Tap **Done**. You are now ready to use your Apple device to connect as a remote user.



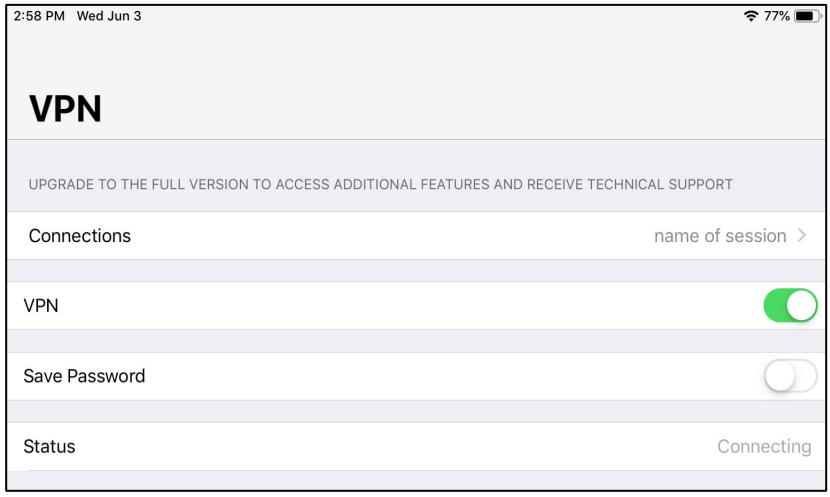
iOS - SSL VPN setup

1. Install Forticlient from App store.

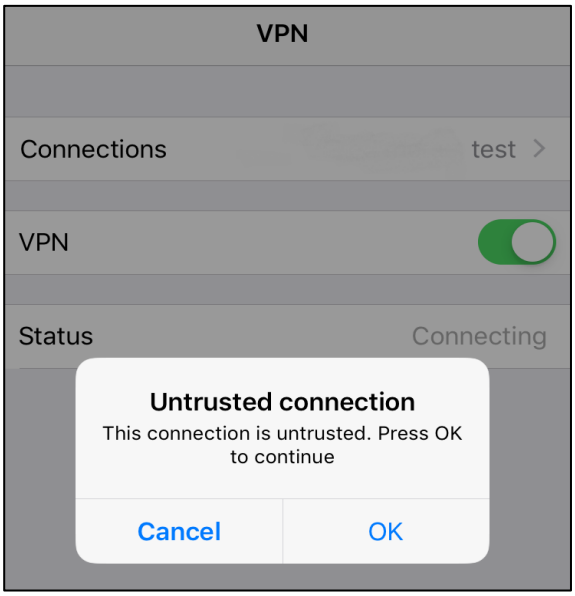


2. Once client is installed page for VPN Add/Edit will load.
3. Name session and enter SSL loopback provided by Lumen.
4. **Check** Hide invalid certificate warning.

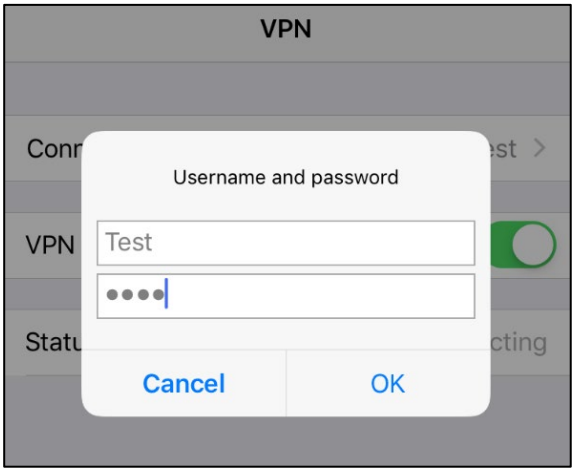
5. Click **Save** then check toggle the button next to VPN to connect session.



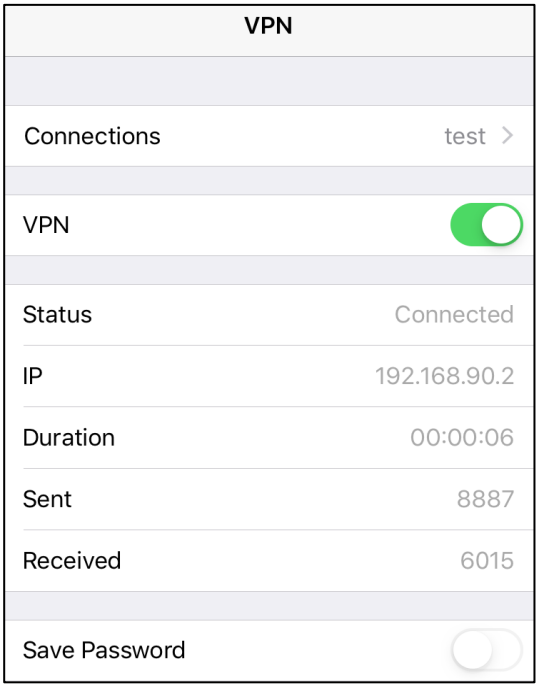
6. Click **OK**.



7. Enter mobility/remote username and password.



8. When authentication is successfully completed page below will be displayed, toggle VPN button to disconnect.



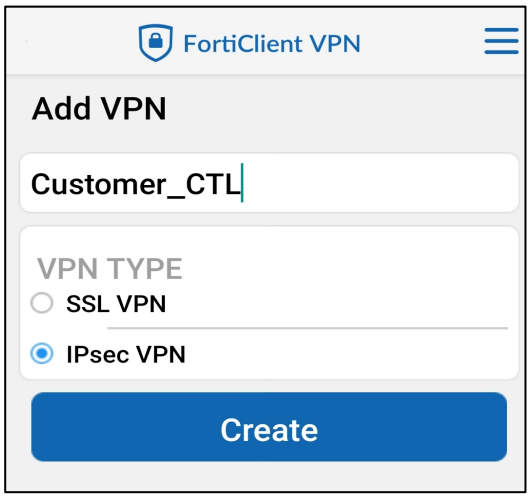
Android - IPSec VPN setup

The following steps will take users through how to set up your ANS Mobility IPSec solution on Android devices.

1. Download the FortiClient app from your Android store.
2. Once installed go to **Add VPN**.
    a. **VPN Name** – defined by you.

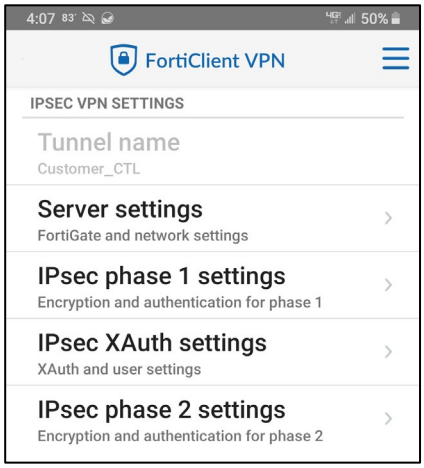
b. **VPN Type** – SSL VPN or IPSec VPN based on services purchased from Lumen.

c. Click **Create**.

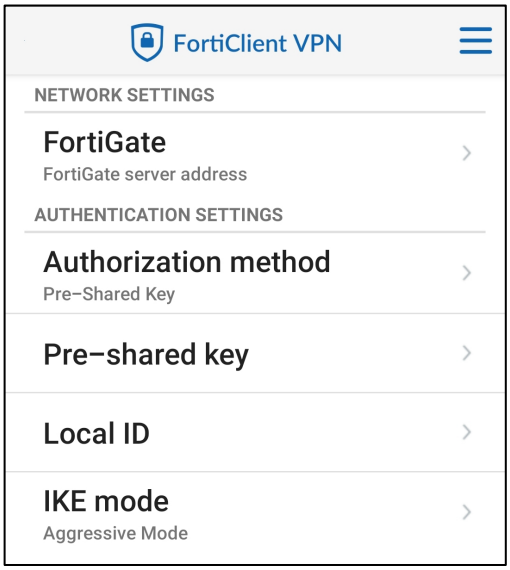


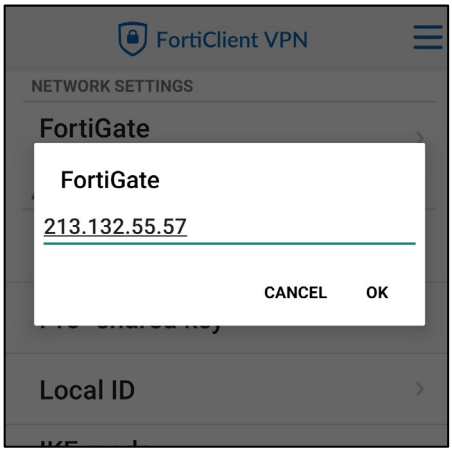
3. Access IPSEC VPN Setting.

a. Click arrow next to **Server settings** to access **Network Settings**.



b. Then click the arrow next to FortiGate to enter the FortiGate server address. Lumen will provide you the IP address.





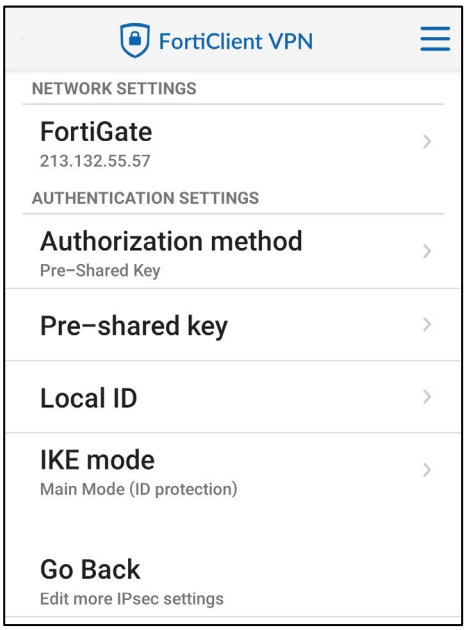
4. Staying on Access IPSEC VPN Setting, do the following:

   a. Validate **Authorization method** defaulted to pre-shared key.

   b. Click the arrow next to pre-shared key. See your system administrator for pre-share key information that was provided by Lumen.

      i. Enter pre-shared key and click OK.

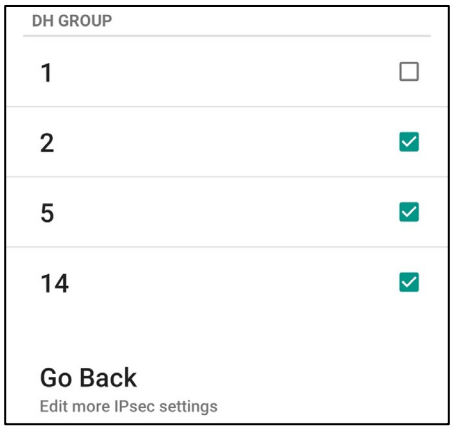
      c. Click arrow next to IKE Mode and select **Main Mode (ID Protection)** and OK.



5. Go back to the **Settings** screen, hit the arrow next to IPsec phase 1 settings.

    a. Check the 2, 5 and 14 for DH Group.

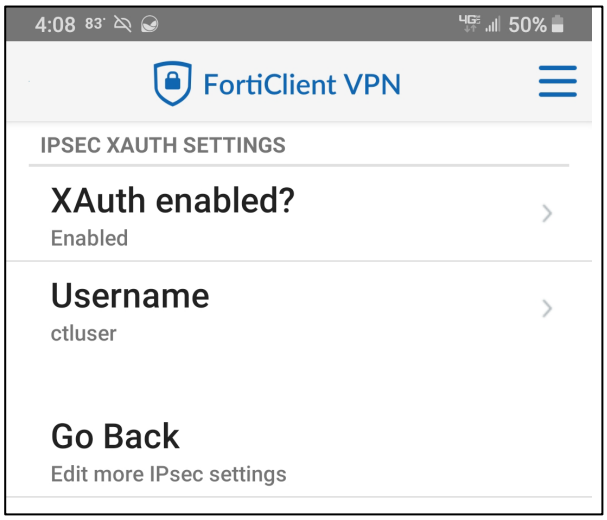
    b. Once checked, hit the **Go Back** button to return to the IPSEC VPN Settings screen.



6. From the IPSEC VPN Settings screen, hit the arrow next to IPsec XAuth settings.

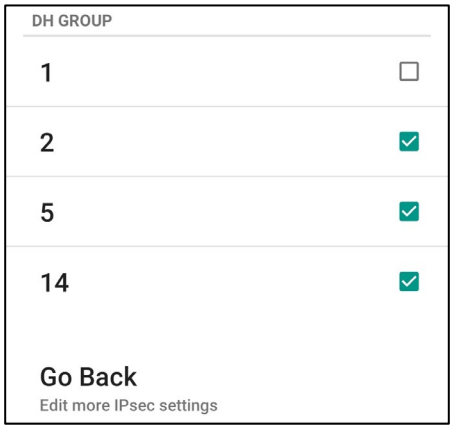
    a. Validate XAUTH enabled is set to **Enabled**.

    b. Click arrow next to Username, enter **Username** and click **OK**.



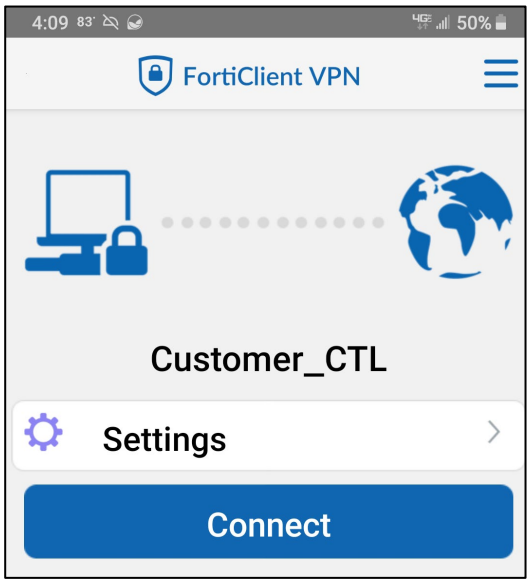
7. From the IPSEC VPN settings screen, hit the arrow next to IPsec phase 2 settings.

    a. Check the 2, 5 and 14 for **DH Group** just like you did for phase 1 settings.



8. You have now completed your configuration. Click on the arrow in the upper-left corner of your screen next to the FortiClient icon to return to the main menu. To test your connectivity, click on **Connect**. You will be prompted to enter your password.

    a. Enter your password and click on LOGIN.



9. You are now connected and ready to use your Android Adaptive Network Security – Mobility service.

MSI package implementation guidance for administrators

The following provides suggested guidance for your administrators to create an MSI package to be distributed via your Active Directory (AD) profile guided optimization (PGO). This is an optional request that should be made to your technical design engineer during the service data gathering stage.

Step 1: The Security team will generate the MSI file and .exe file, and send it to you via the SFTP server. A username and password will be provided also via email, along with the filename.

Step 2: Once the MSI file is provided you can distribute it via a group policy (GPO).