IKEv1 AGGRESSIVE Pre-shared key

You can use the NCP Secure Enterprise Management Server as a RADIUS server to authenticate users.

IKEv1 AGGRESSIVE Mode and Pre-shared key

This configuration example uses the NCP Secure Enterprise Management Server as a RADIUS server to authenticate users

CLI Quick Configuration

```
set security policies default-policy permit-all
set interfaces st0 unit 0 family inet address 172.16.10.200/24
set security zones security-zone internet interfaces st0.0 host-inbound-traffic system-services all
set security zones security-zone internet interfaces st0.0 host-inbound-traffic protocols all
set security ike proposal IKE_PROP authentication-method pre-shared-keys
set security ike proposal IKE_PROP dh-group group19
set security ike proposal IKE_PROP authentication-algorithm sha-256
set security ike proposal IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal IKE_PROP lifetime-seconds 10000
set security ike policy IKE_POL mode aggressive
set security ike policy IKE_POL proposals IKE_PROP
set security ike policy IKE_POL pre-shared-key ascii-text "12345678"
set security ike gateway RAVPN_GW ike-policy IKE_POL
set security ike gateway RAVPN_GW dynamic hostname ncp.juniper.net
set security ike gateway RAVPN_GW dynamic user-at-hostname test@ncp.juniper.net
set security ike gateway RAVPN_GW dynamic connections-limit 100
set security ike gateway RAVPN_GW dynamic ike-user-type shared-ike-id
set security ike gateway RAVPN_GW external-interface ge-0/0/0
set security ike gateway RAVPN_GW aaa access-profile radius
set security ike gateway RAVPN_GW version v1-only
set security ipsec proposal IPSEC_PROP protocol esp
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-gcm
```

```
set security ipsec proposal IPSEC_PROP lifetime-seconds 3600
set security ipsec policy IPSEC_POL perfect-forward-secrecy keys group19
set security ipsec policy IPSEC_POL proposals IPSEC_PROP
set security ipsec vpn RAVPN_VPN bind-interface st0.0
set security ipsec vpn RAVPN_VPN ike gateway RAVPN_GW
set security ipsec vpn RAVPN_VPN ike ipsec-policy IPSEC_POL
set security ipsec vpn RAVPN_VPN traffic-selector TS1 local-ip 0.0.0.0/0
set security ipsec vpn RAVPN_VPN traffic-selector TS1 remote-ip 0.0.0.0/0
set access profile radius authentication-order radius
set access profile radius radius-server 10.20.46.235 port 1812
set access profile radius address-assignment pool NCP_POOL
set access profile radius radius-server 10.20.46.235 secret "12345678"
set access address-assignment pool NCP_POOL family inet network 172.16.10.0/24
set access address-assignment pool NCP_POOL family inet xauth-attributes primary-dns 172.16.10.10/32
set access address-assignment pool NCP_POOL family inet xauth-attributes primary-wins 172.16.10.20/32
set security ike gateway RAVPN_GW tcp-encap-profile NCP
set security tcp-encap profile NCP
commit
```

Step-by-step Procedure

1) Define tunnel interface and policies

```
set security policies default-policy permit-all
set interfaces st0 unit 0 family inet address 172.16.10.200/24
set security zones security-zone internet interfaces st0.0 host-inbound-traffic system-services all
set security zones security-zone internet interfaces st0.0 host-inbound-traffic protocols all
```

2) Create IKE proposals (policies)

```
set security ike proposal IKE_PROP authentication-method pre-shared-keys
set security ike proposal IKE_PROP dh-group group19
set security ike proposal IKE_PROP authentication-algorithm sha-256
set security ike proposal IKE_PROP encryption-algorithm aes-256-cbc
set security ike proposal IKE_PROP lifetime-seconds 10000
```

set security ike policy IKE_POL mode aggressive
set security ike policy IKE_POL proposals IKE_PROP
set security ike policy IKE_POL pre-shared-key ascii-text “12345678"

3) Create IKE gateway

set security ike gateway RAVPN_GW ike-policy IKE_POL
set security ike gateway RAVPN_GW dynamic hostname ncp.juniper.net
set security ike gateway RAVPN_GW dynamic connections-limit 100
set security ike gateway RAVPN_GW dynamic ike-user-type shared-ike-id
set security ike gateway RAVPN_GW dynamic user-at-hostname test@ncp.juniper.net
set security ike gateway RAVPN_GW external-interface ge-0/0/0
set security ike gateway RAVPN_GW aaa access-profile radius
set security ike gateway RAVPN_GW version v1-only

4) Create IPsec proposals (policies)

set security ipsec proposal IPSEC_PROP protocol esp
set security ipsec proposal IPSEC_PROP encryption-algorithm aes-256-gcm
set security ipsec proposal IPSEC_PROP lifetime-seconds 3600
set security ipsec policy IPSEC_POL perfect-forward-secrecy keys group19
set security ipsec policy IPSEC_POL proposals IPSEC_PROP

5) Define VPN interface and routing information

set security ipsec vpn RAVPN_VPN bind-interface st0.0
set security ipsec vpn RAVPN_VPN ike gateway RAVPN_GW
set security ipsec vpn RAVPN_VPN ike ipsec-policy IPSEC_POL
set security ipsec vpn RAVPN_VPN traffic-selector TS1 local-ip 0.0.0.0/0
set security ipsec vpn RAVPN_VPN traffic-selector TS1 remote-ip 0.0.0.0/0

6) Create access profile for RADIUS server

set access profile radius authentication-order radius
set access profile radius radius-server 10.20.46.234 port 1812
set access profile radius address-assignment pool NCP_POOL
set access profile radius radius-server 10.20.46.234 secret "12345678"

7) Create IP address pool for Remote Access Users

set access address-assignment pool NCP_POOL family inet network 172.16.10.0/24
set access address-assignment pool NCP_POOL family inet xauth-attributes primary-dns 172.16.10.10/32
set access address-assignment pool NCP_POOL family inet xauth-attributes primary-wins 172.16.10.20/32

8) Enable NCP Path Finder Technology (TCP encapsulation)

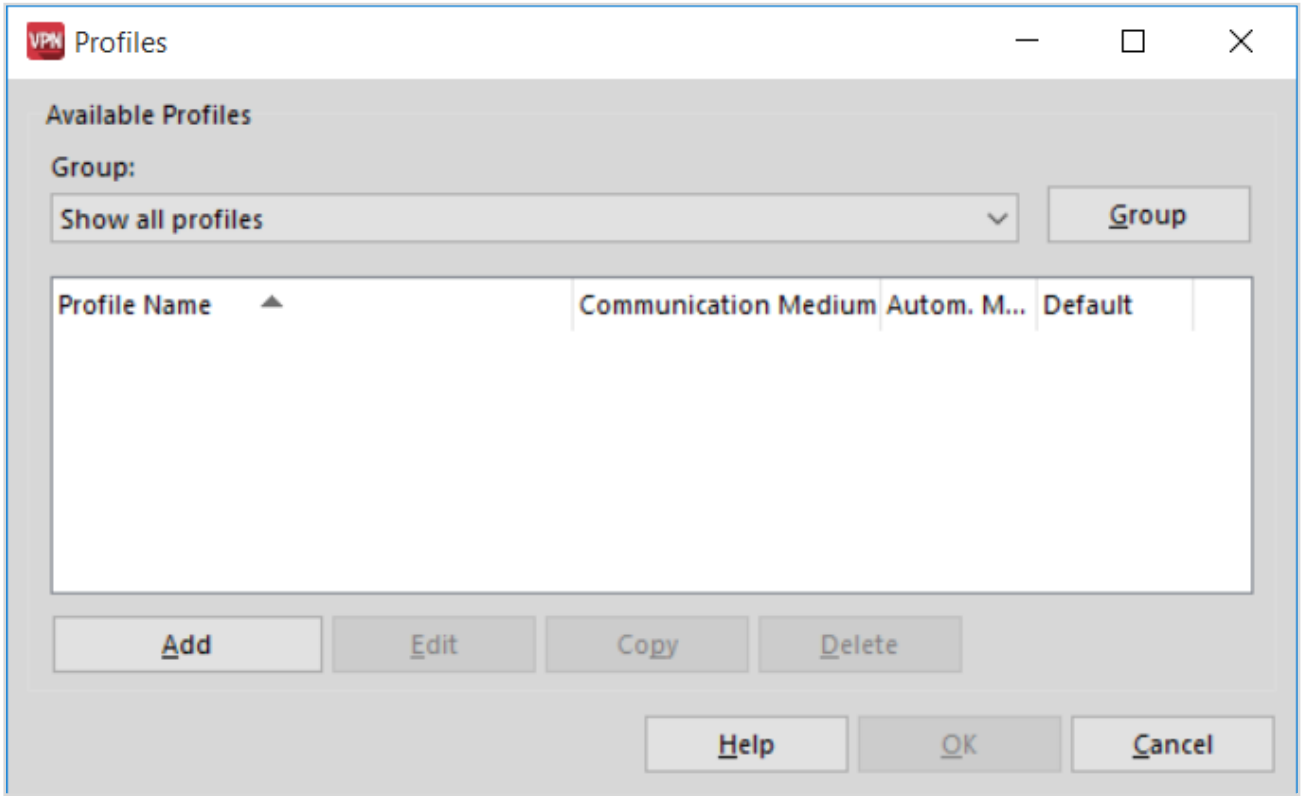
set security ike gateway RAVPN_GW tcp-encap-profile NCP
set security tcp-encap profile NCP

8) Commit changes

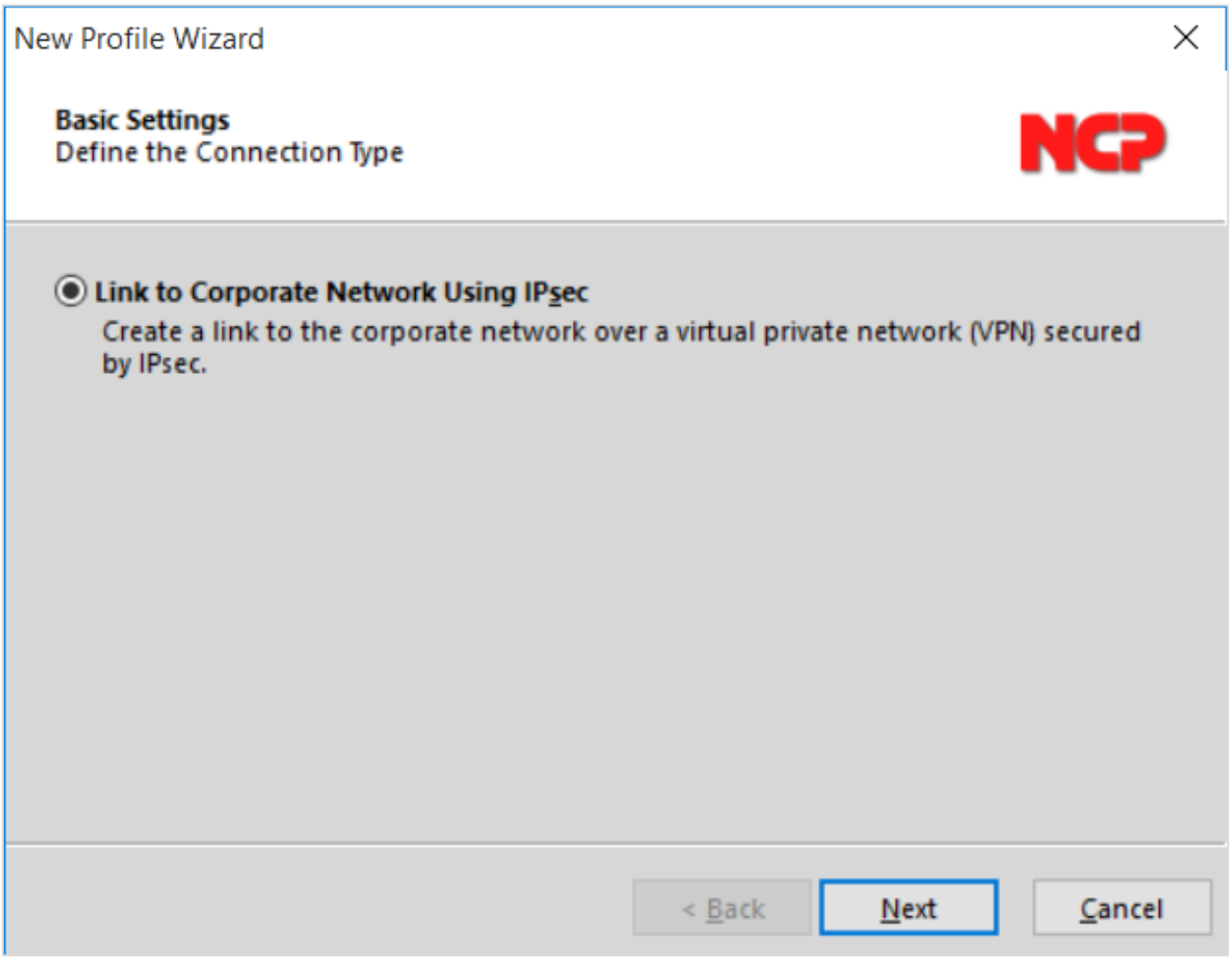
commit

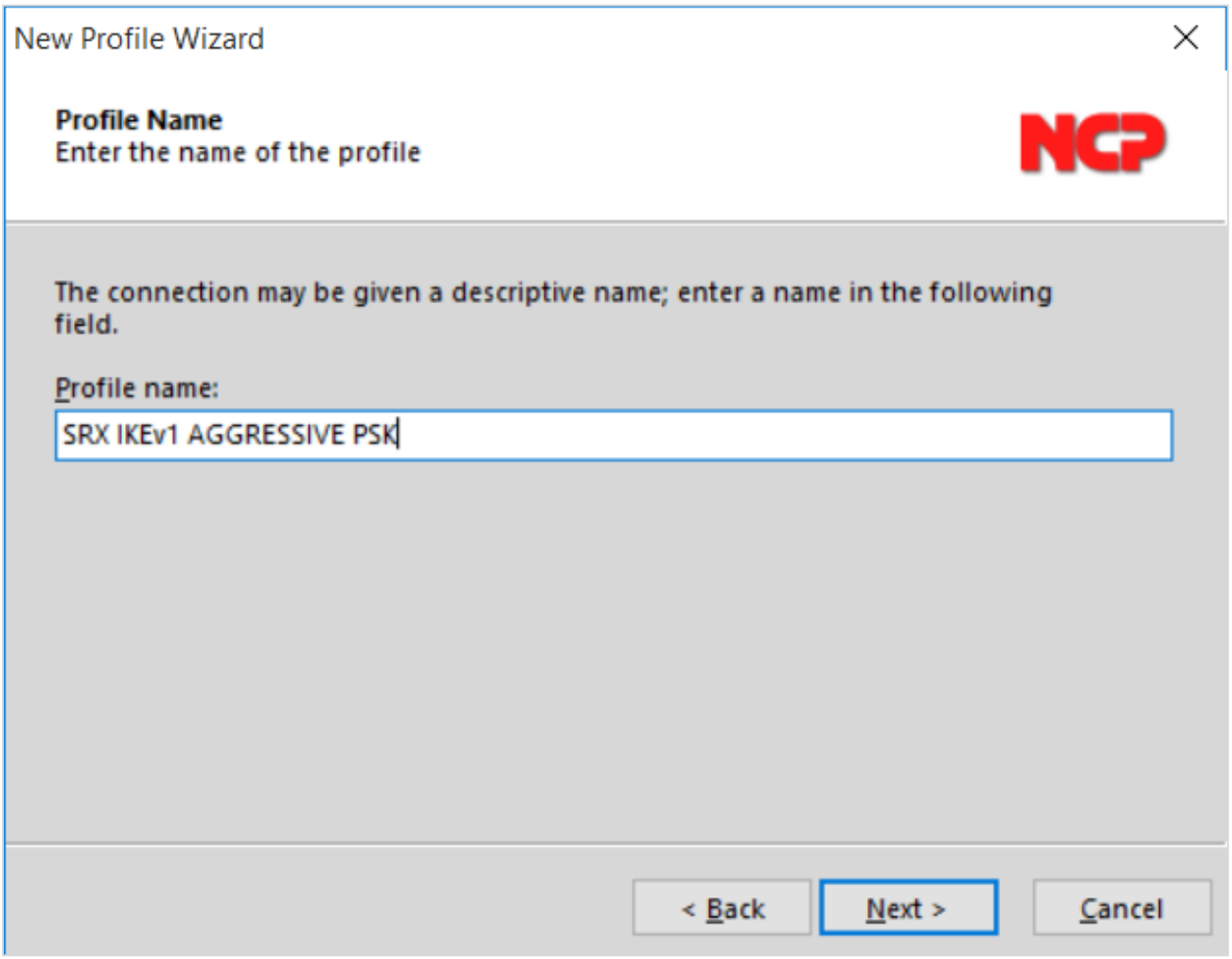
Configure NCP Exclusive Remote Access Client for Windows

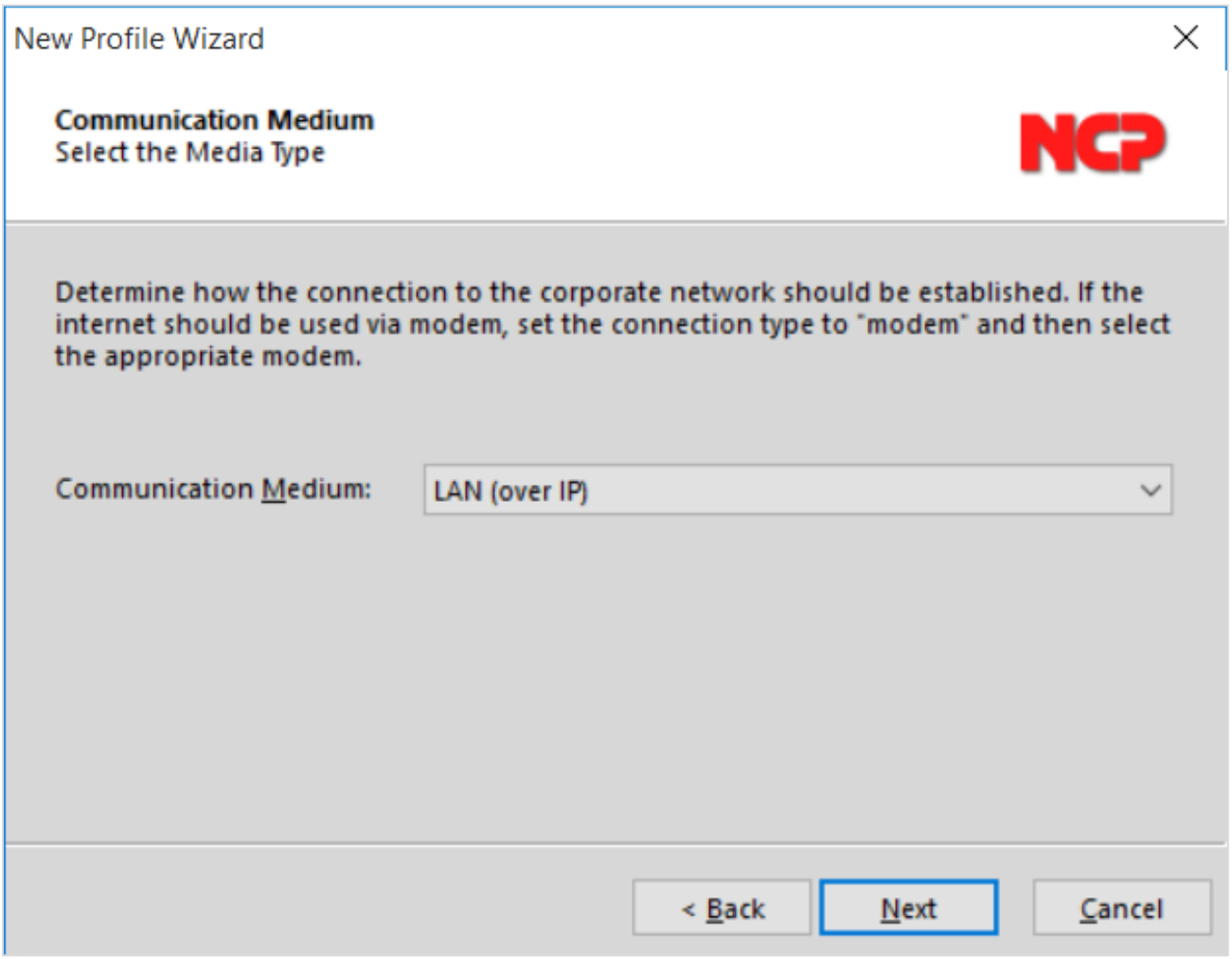
Create new Connection Profile (Configuration – Profiles)

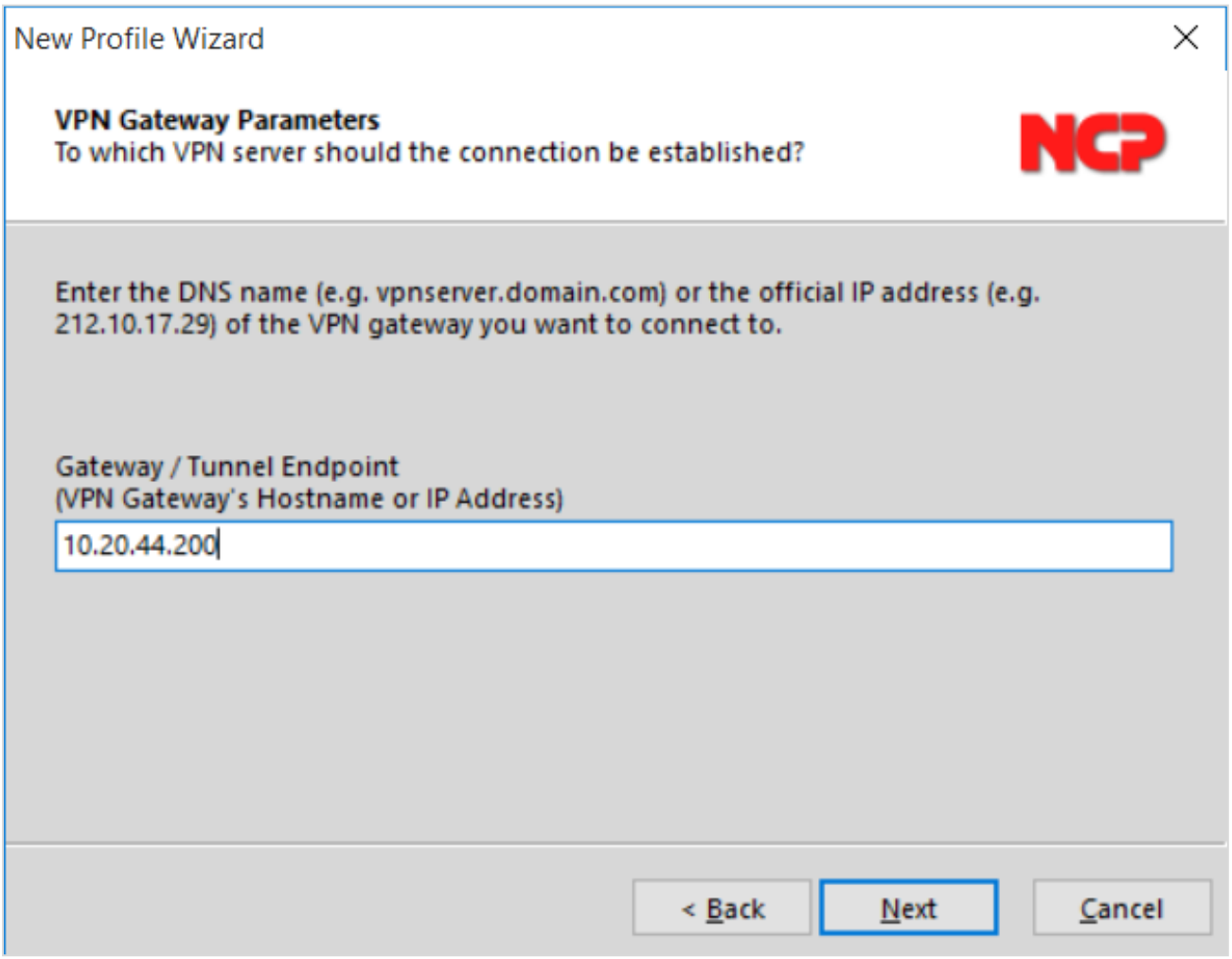


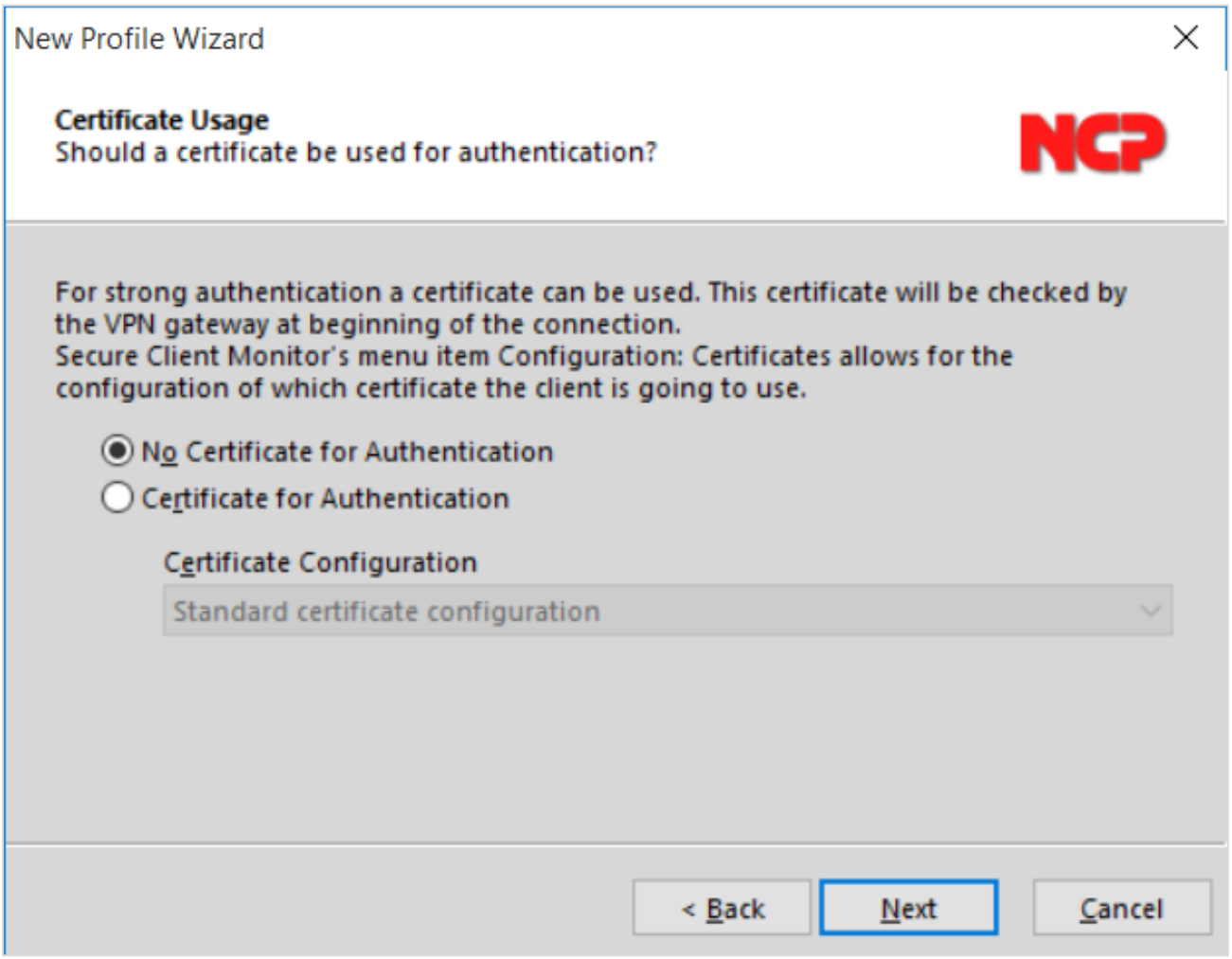
Click on “Add” to create a new Connection Profile

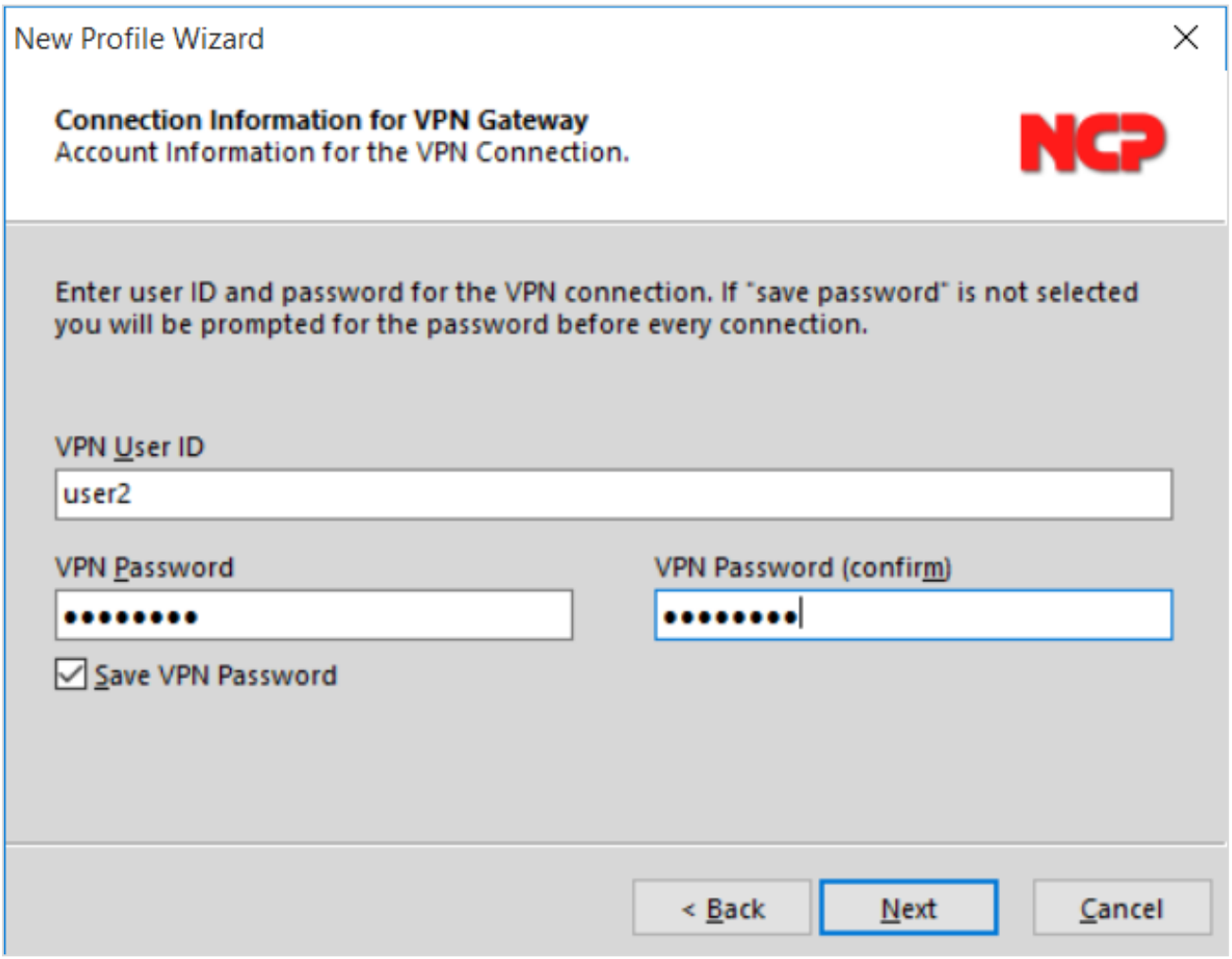

New Profile Wizard
Basic Settings
Define the Connection Type
Link to Corporate Network Using IPsec
Create a link to the corporate network over a virtual private network (VPN) secured by IPsec.
< Back
Next
Cancel

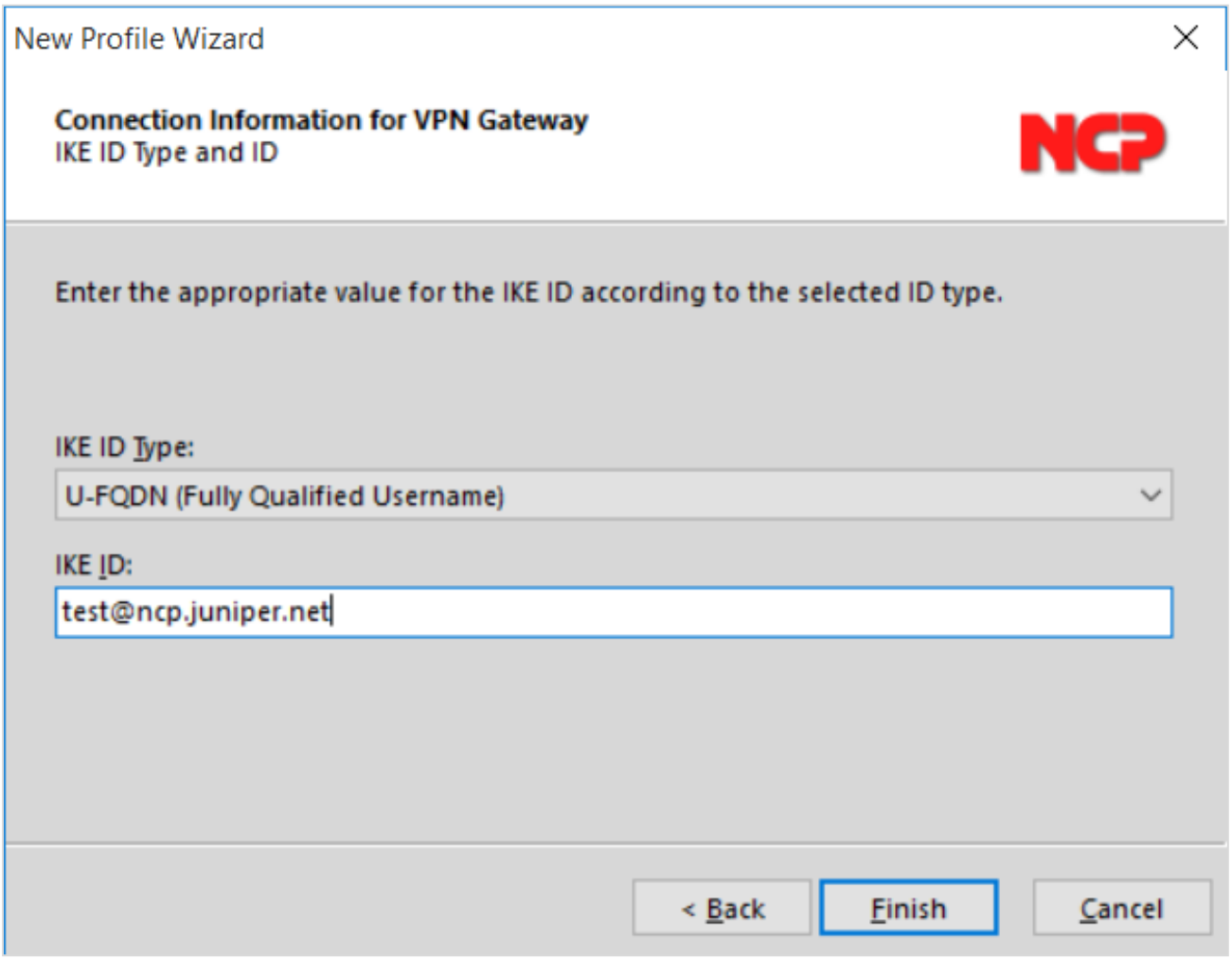

New Profile Wizard
Profile Name
Enter the name of the profile
The connection may be given a descriptive name; enter a name in the following field.
Profile name:
SRX IKEv1 AGGRESSIVE PSK
< Back
Next >
Cancel


New Profile Wizard
Communication Medium
Select the Media Type
Determine how the connection to the corporate network should be established. If the internet should be used via modem, set the connection type to "modem" and then select the appropriate modem.
Communication Medium:
LAN (over IP)
< Back
Next
Cancel

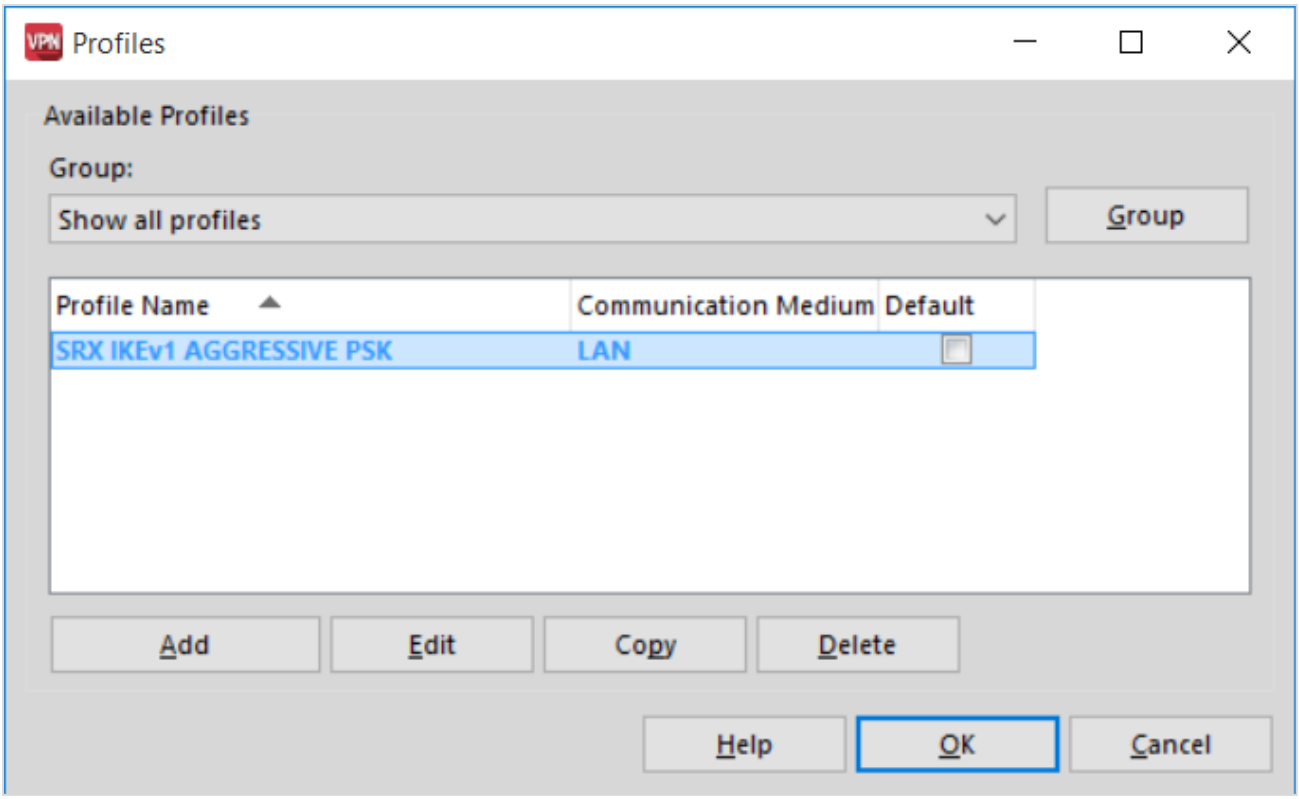

New Profile Wizard
VPN Gateway Parameters
To which VPN server should the connection be established?
Enter the DNS name (e.g. vpnserver.domain.com) or the official IP address (e.g. 212.10.17.29) of the VPN gateway you want to connect to.
Gateway / Tunnel Endpoint
(VPN Gateway's Hostname or IP Address)
10.20.44.200
< Back
Next
Cancel


New Profile Wizard
Certificate Usage
Should a certificate be used for authentication?
For strong authentication a certificate can be used. This certificate will be checked by the VPN gateway at beginning of the connection.
Secure Client Monitor's menu item Configuration: Certificates allows for the configuration of which certificate the client is going to use.
No Certificate for Authentication
Certificate for Authentication
Certificate Configuration
Standard certificate configuration
< Back
Next
Cancel

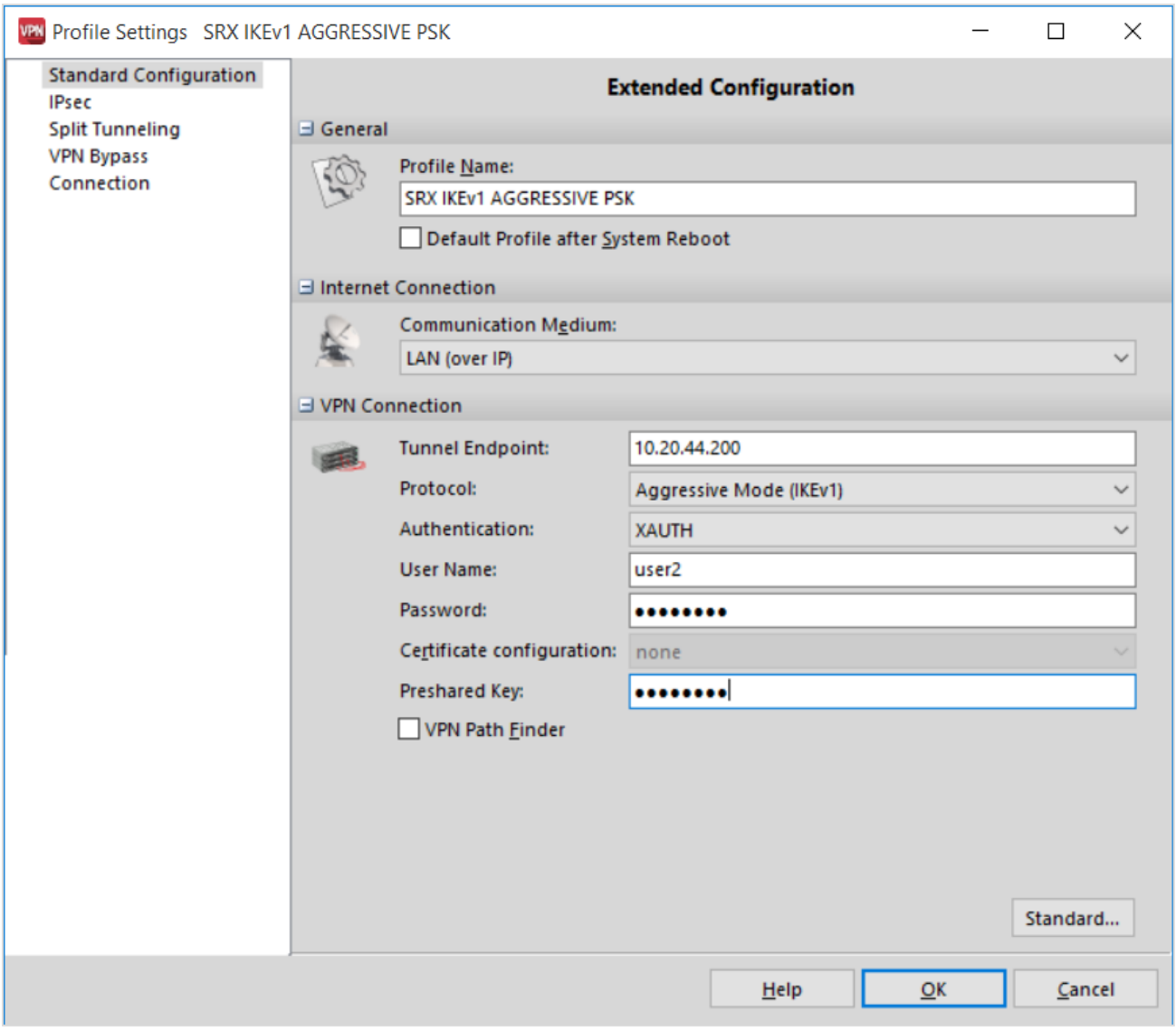

New Profile Wizard
Connection Information for VPN Gateway
Account Information for the VPN Connection.
Enter user ID and password for the VPN connection. If "save password" is not selected you will be prompted for the password before every connection.
VPN User ID
user2
VPN Password
VPN Password (confirm)
Save VPN Password
< Back
Next
Cancel


New Profile Wizard
Connection Information for VPN Gateway
IKE ID Type and ID
Enter the appropriate value for the IKE ID according to the selected ID type.
IKE ID Type:
U-FQDN (Fully Qualified Username)
IKE ID:
test@ncp.juniper.net
< Back
Finish
Cancel

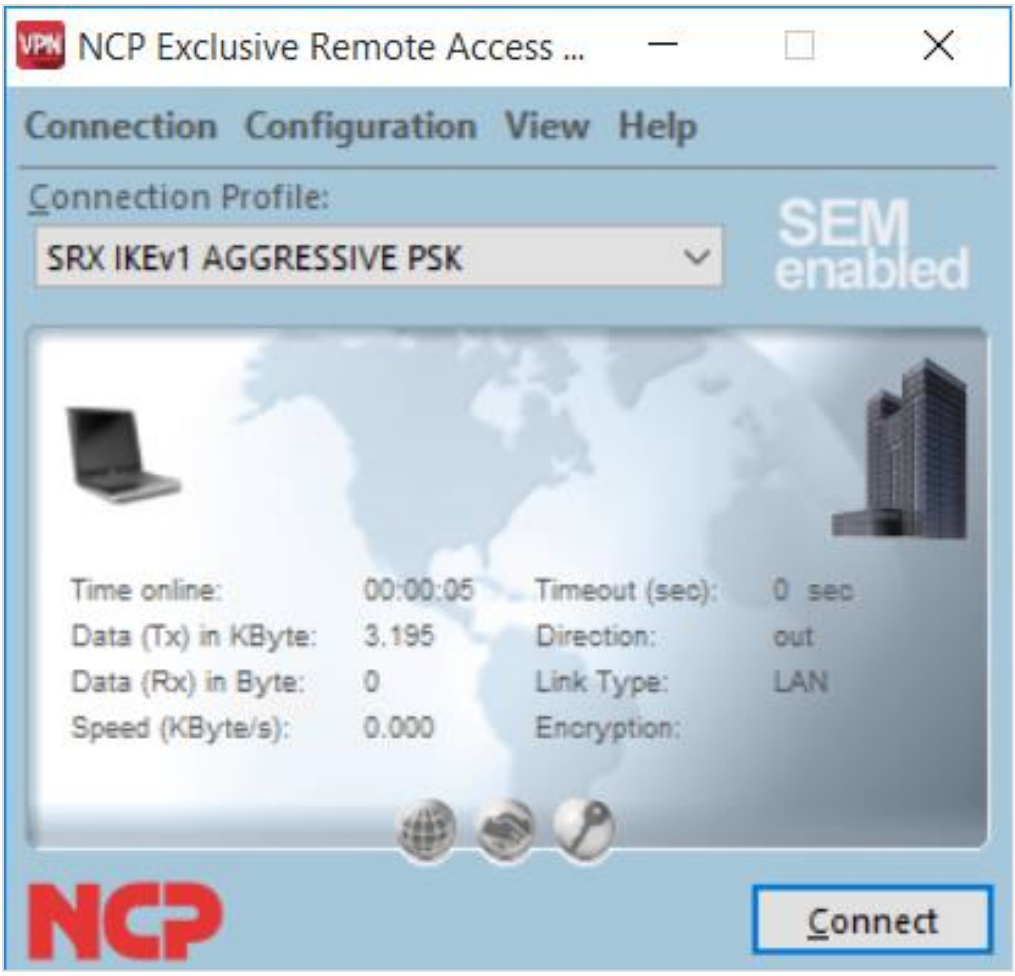
Edit the Profile

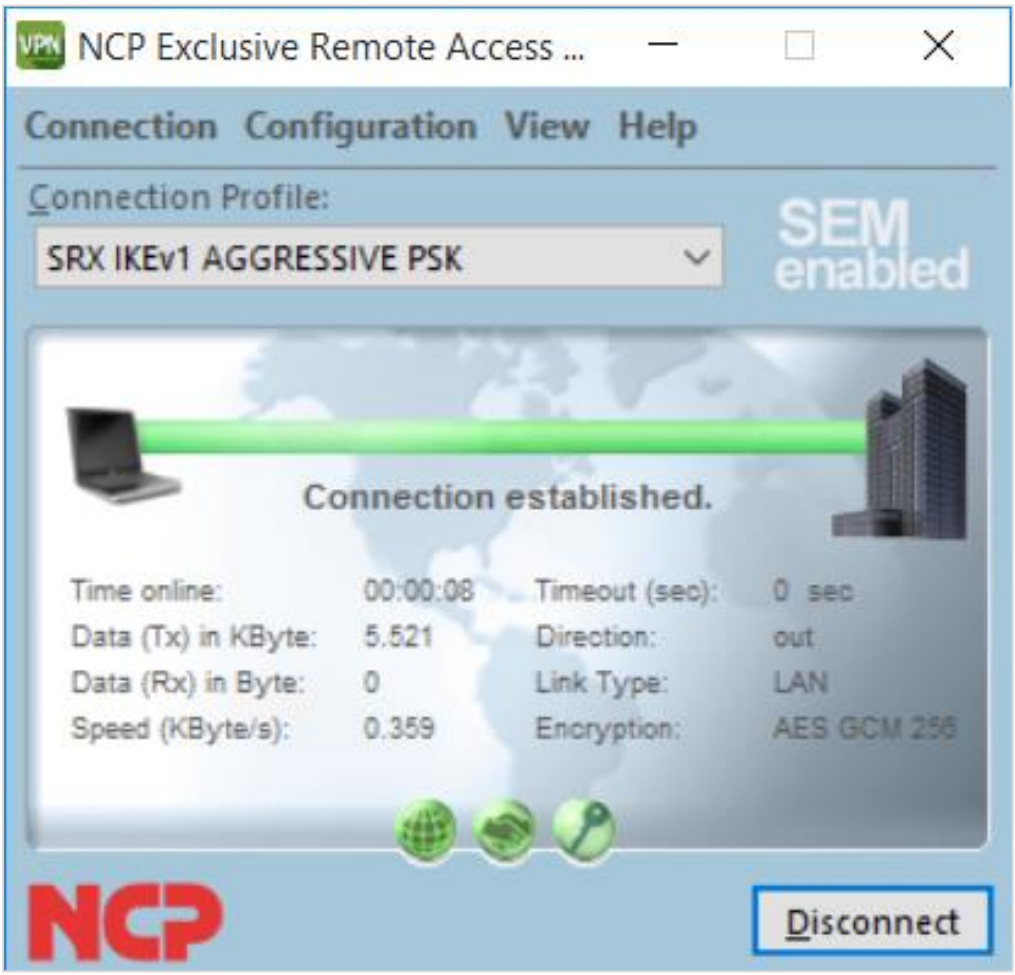


Change the protocol and enter the pre-shared key



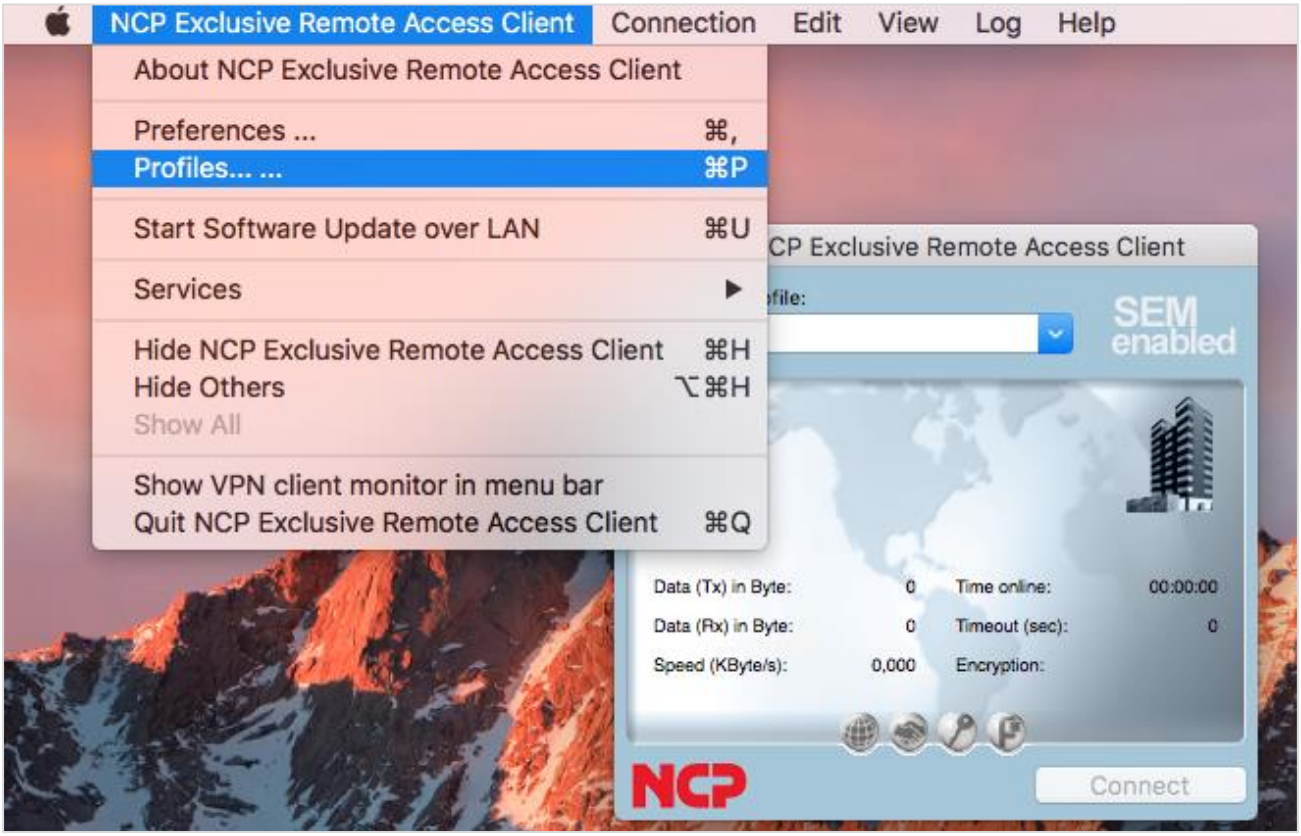
Establish the VPN connection

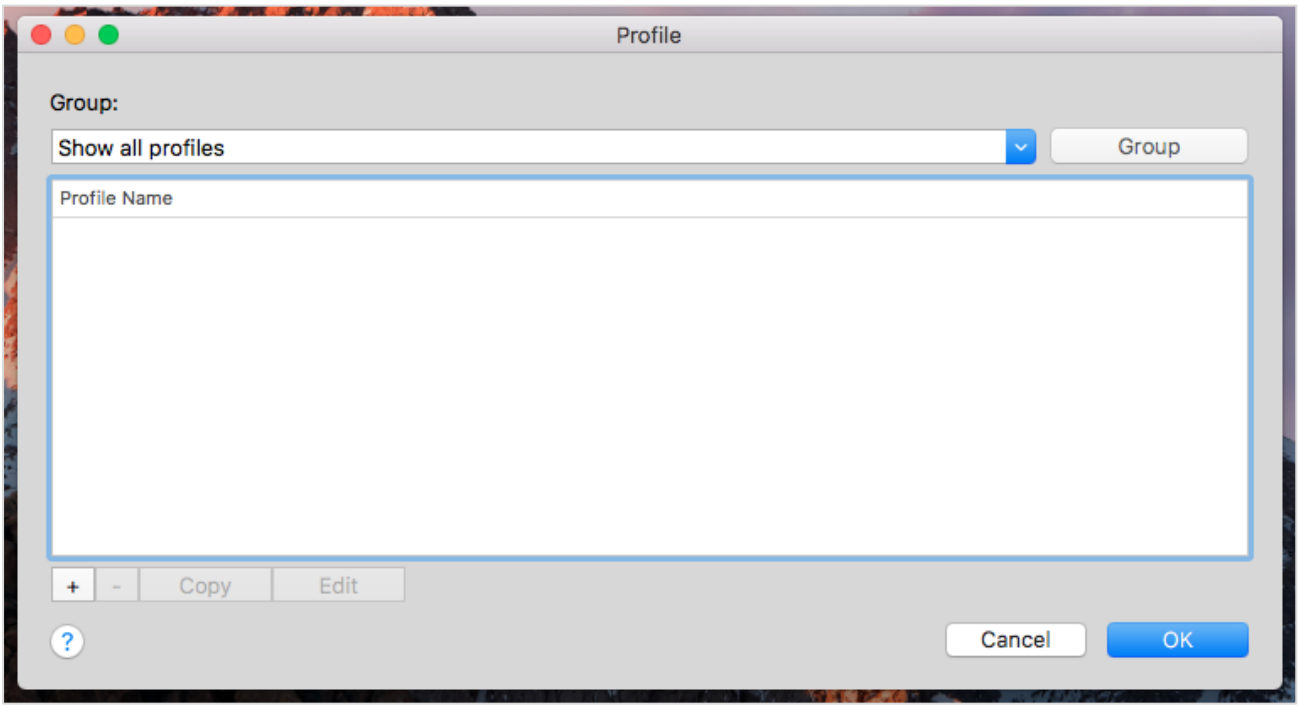



NCP Exclusive Remote Access ...
Connection Configuration View Help
Connection Profile:
SRX IKEv1 AGGRESSIVE PSK
SEM enabled
Connection established.
Time online: 00:00:08
Timeout (sec): 0 sec
Data (Tx) in KByte: 5.521
Direction: out
Data (Rx) in Byte: 0
Link Type: LAN
Speed (KByte/s): 0.359
Encryption: AES GCM 256
NCP
Disconnect

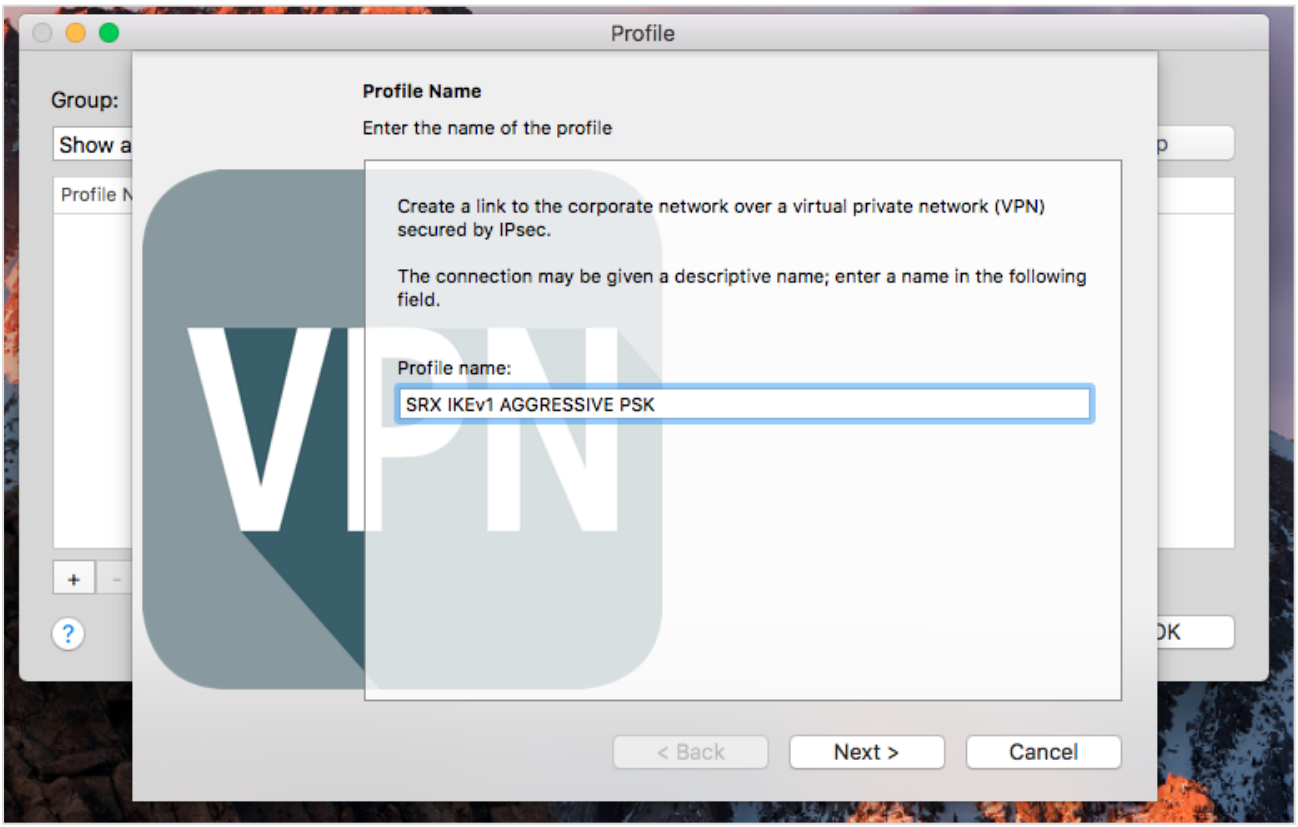
Configure NCP Exclusive Remote Access Client for macOS

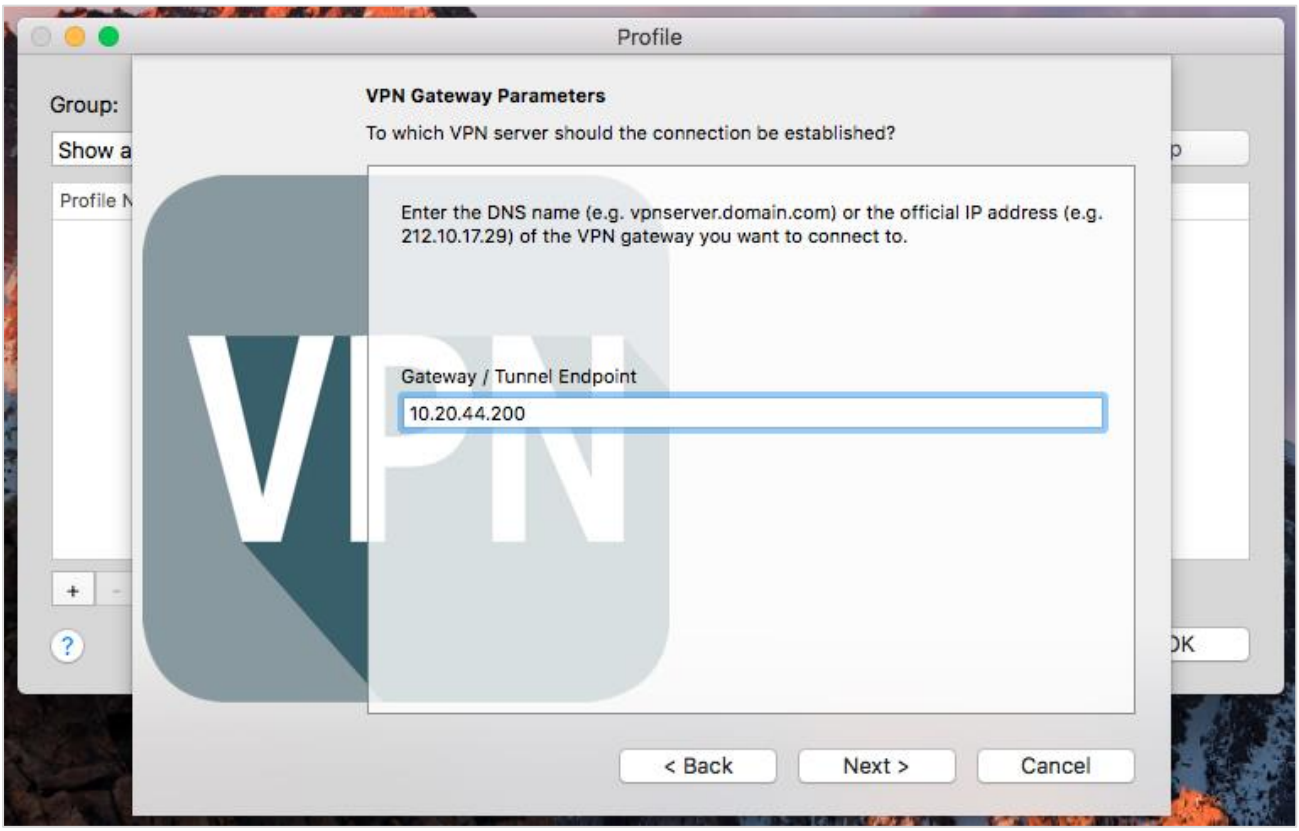
Create new Connection Profile (NCP Exclusive Remote Access Client – Profiles…)

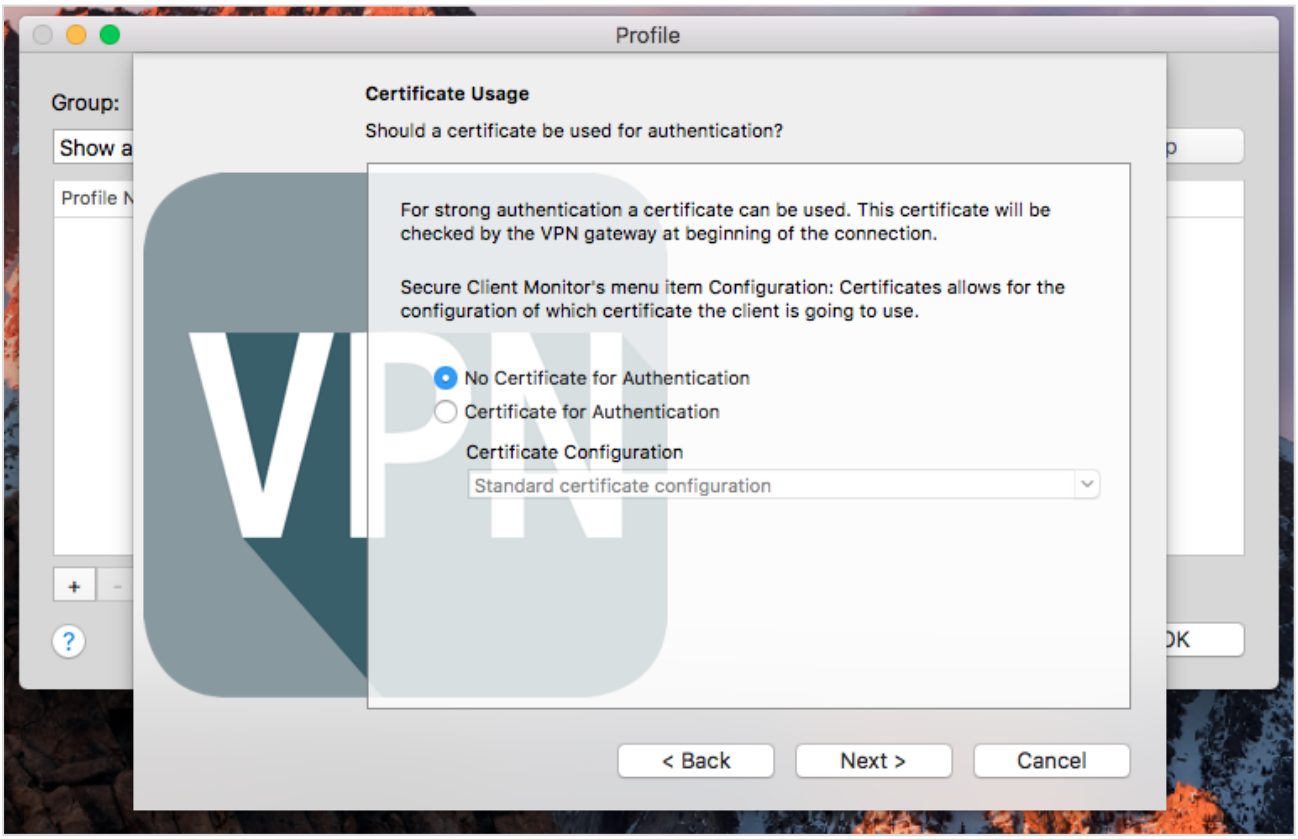




Click on “+” to create a new Connection Profile

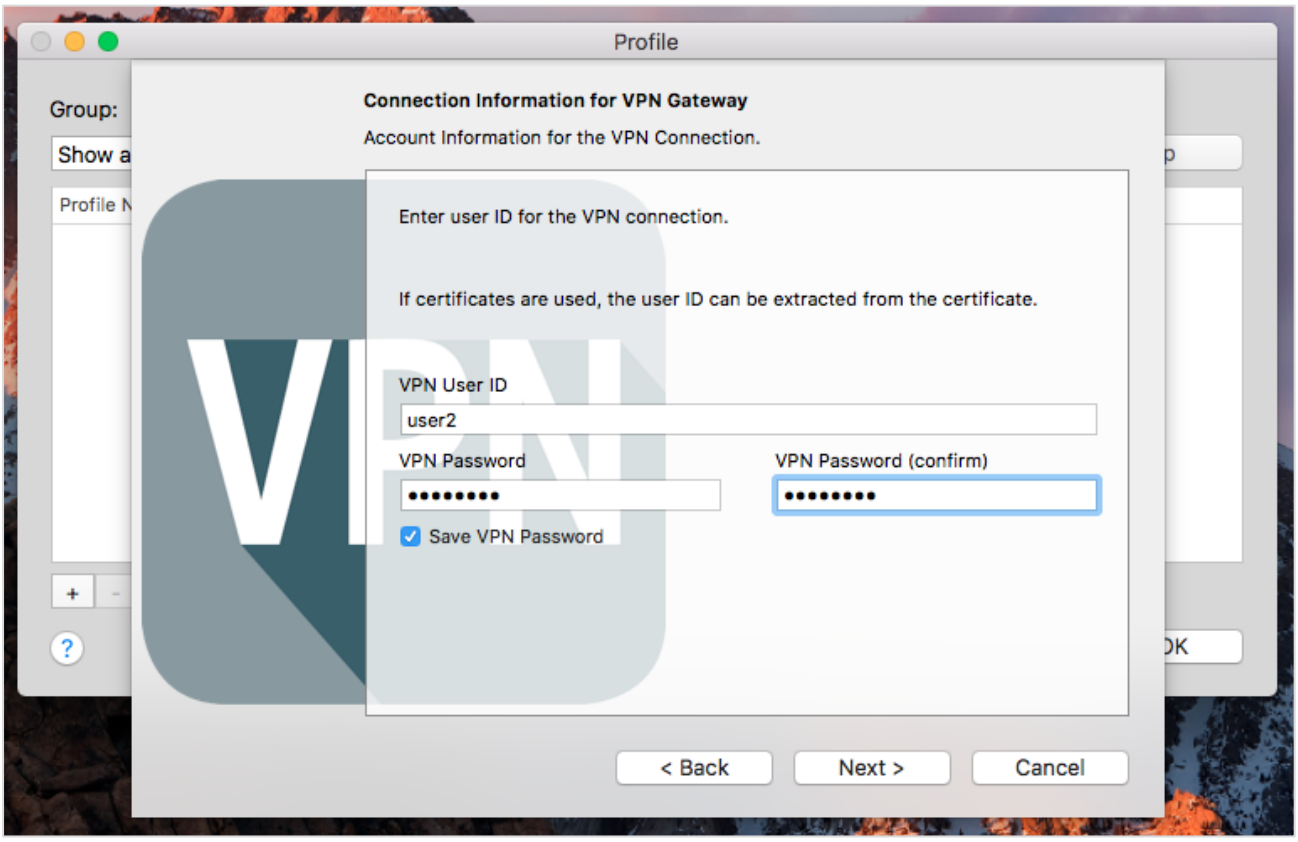

Profile
Group:
Show a
Profile N
Profile Name
Enter the name of the profile
Create a link to the corporate network over a virtual private network (VPN) secured by IPsec.
The connection may be given a descriptive name; enter a name in the following field.
Profile name:
SRX IKEv1 AGGRESSIVE PSK
VPN
< Back
Next >
Cancel
OK

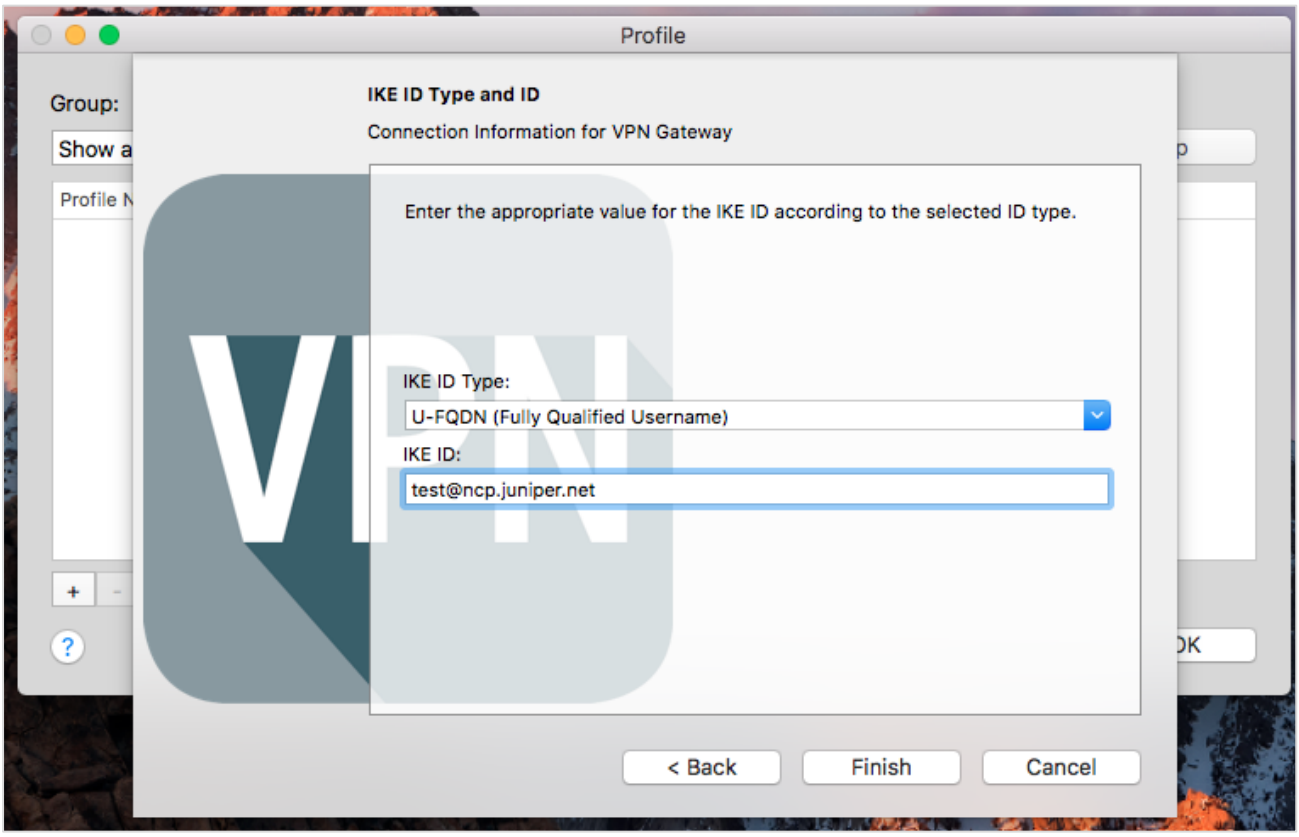

Profile
Group:
Show a
Profile N
VPN Gateway Parameters
To which VPN server should the connection be established?
Enter the DNS name (e.g. vpnserver.domain.com) or the official IP address (e.g. 212.10.17.29) of the VPN gateway you want to connect to.
Gateway / Tunnel Endpoint
10.20.44.200
< Back
Next >
Cancel
OK


Profile
Group:
Show a
Profile N
Certificate Usage
Should a certificate be used for authentication?
For strong authentication a certificate can be used. This certificate will be checked by the VPN gateway at beginning of the connection.
Secure Client Monitor's menu item Configuration: Certificates allows for the configuration of which certificate the client is going to use.
No Certificate for Authentication
Certificate for Authentication
Certificate Configuration
Standard certificate configuration
< Back
Next >
Cancel
VPN

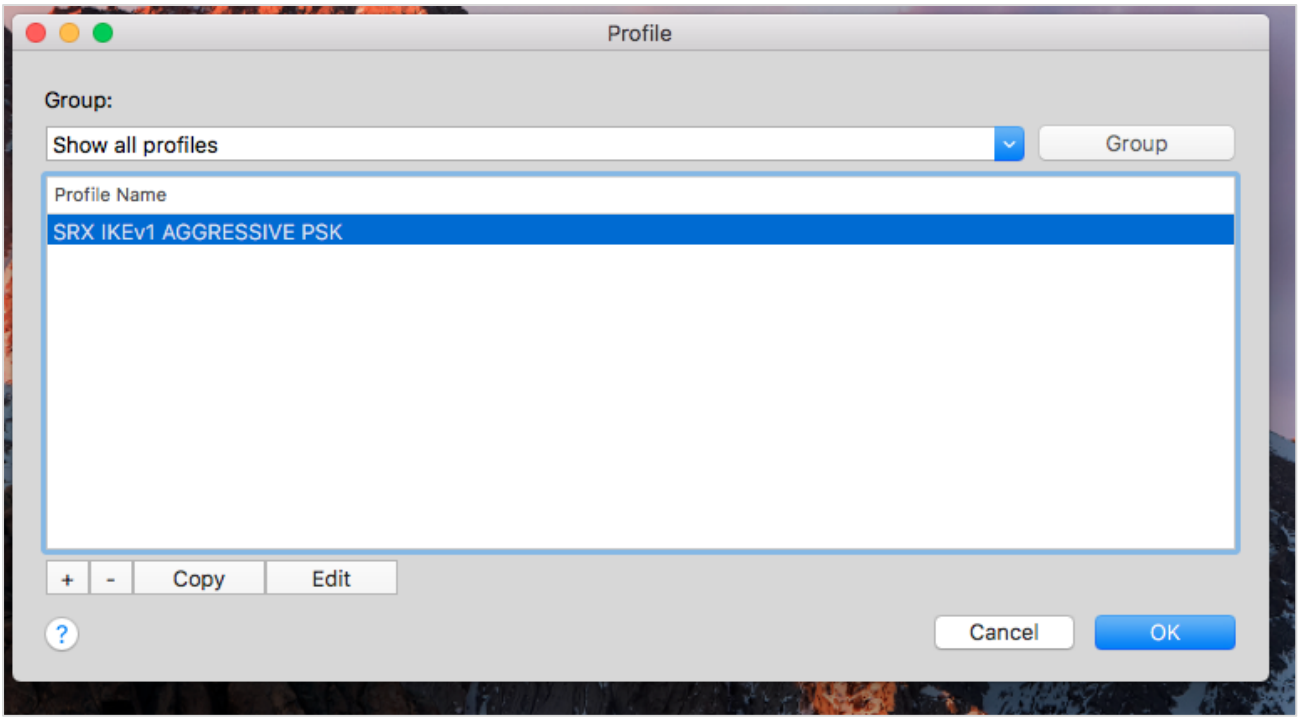
Configuration Guide

NCP Remote Access VPN Client for Juniper SRX

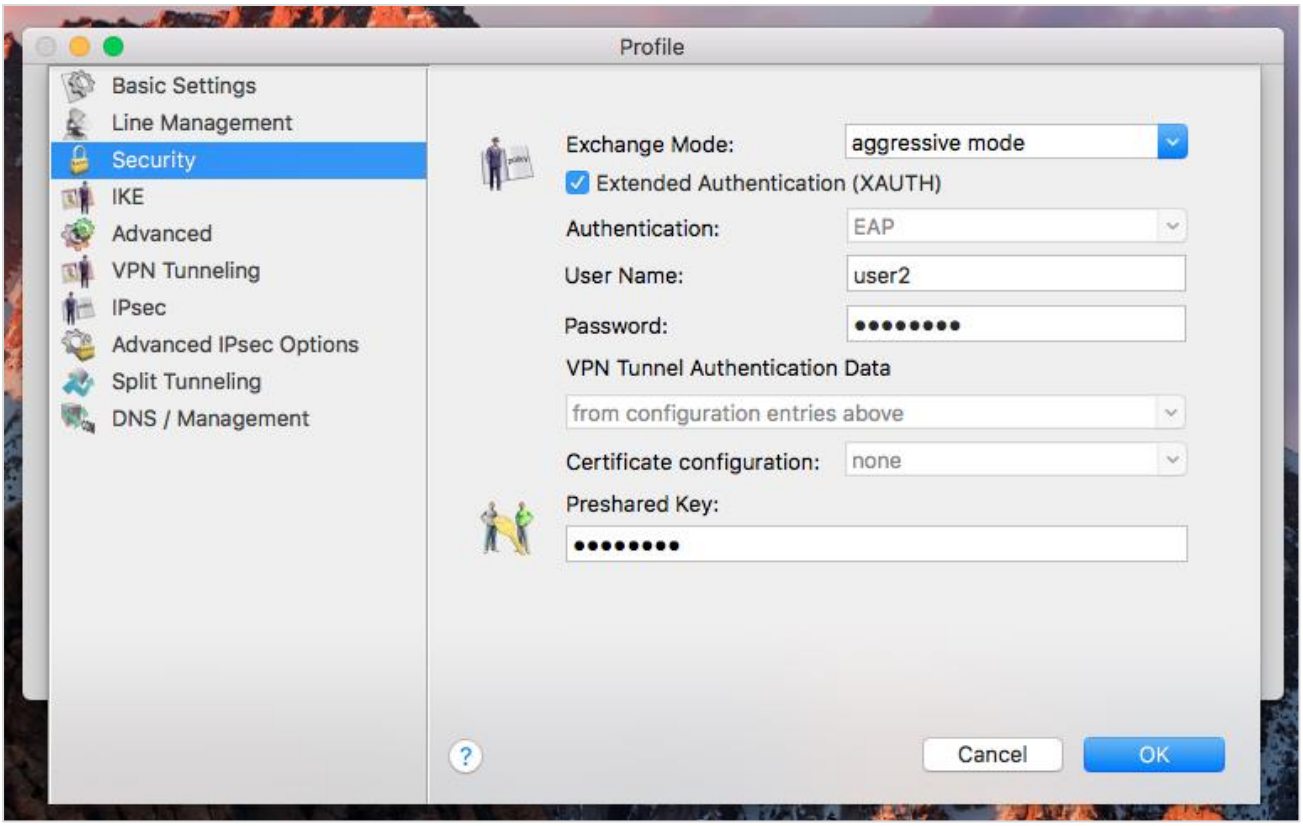



Profile
Group:
Show a
Profile N
IKE ID Type and ID
Connection Information for VPN Gateway
Enter the appropriate value for the IKE ID according to the selected ID type.
IKE ID Type:
U-FQDN (Fully Qualified Username)
IKE ID:
test@ncp.juniper.net
< Back
Finish
Cancel
OK

Edit the Profile



Change the protocol and enter the pre-shared key

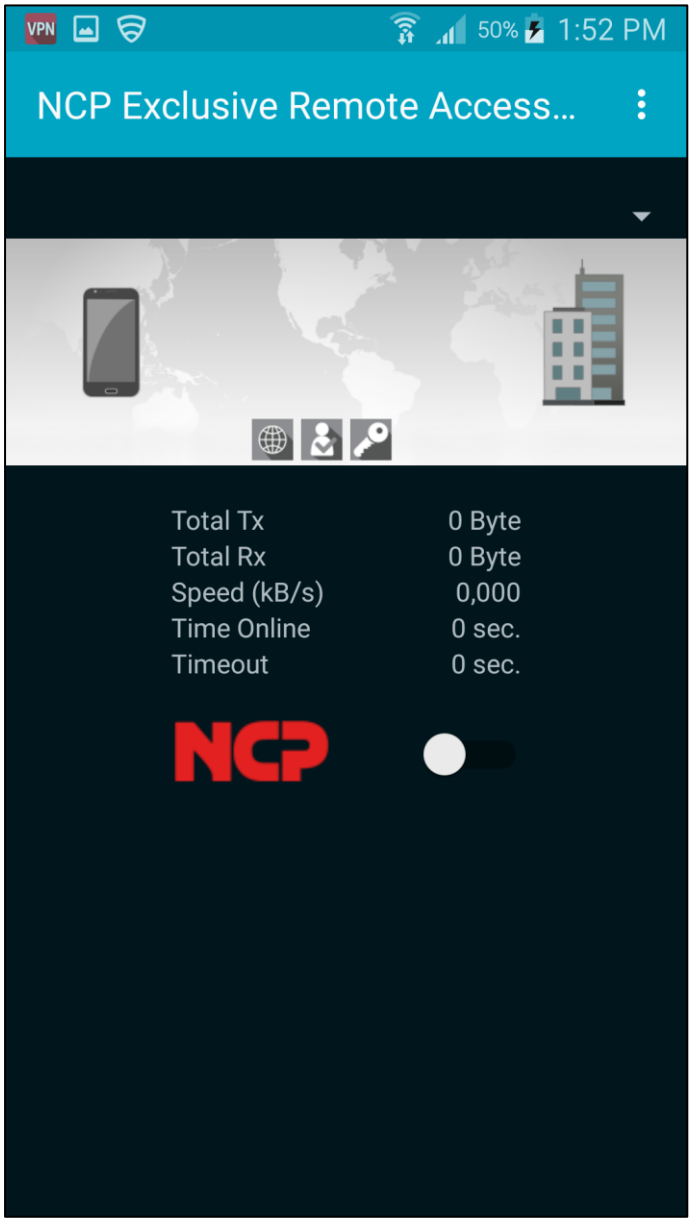


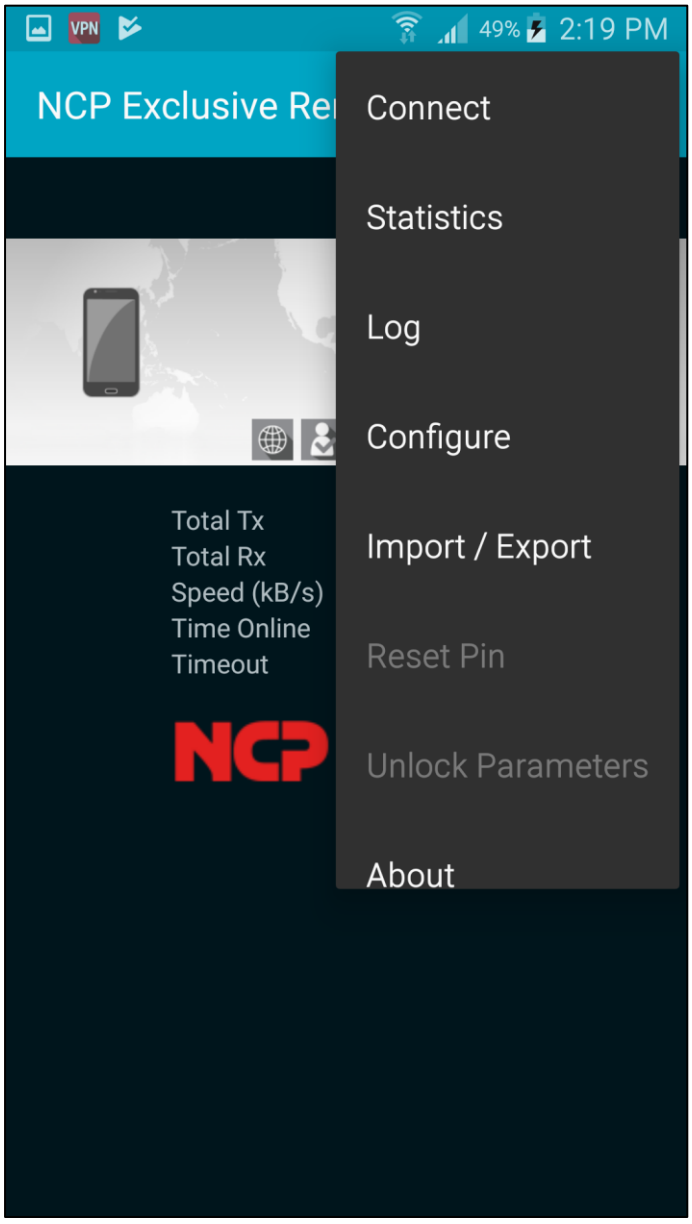
Establish the VPN connection

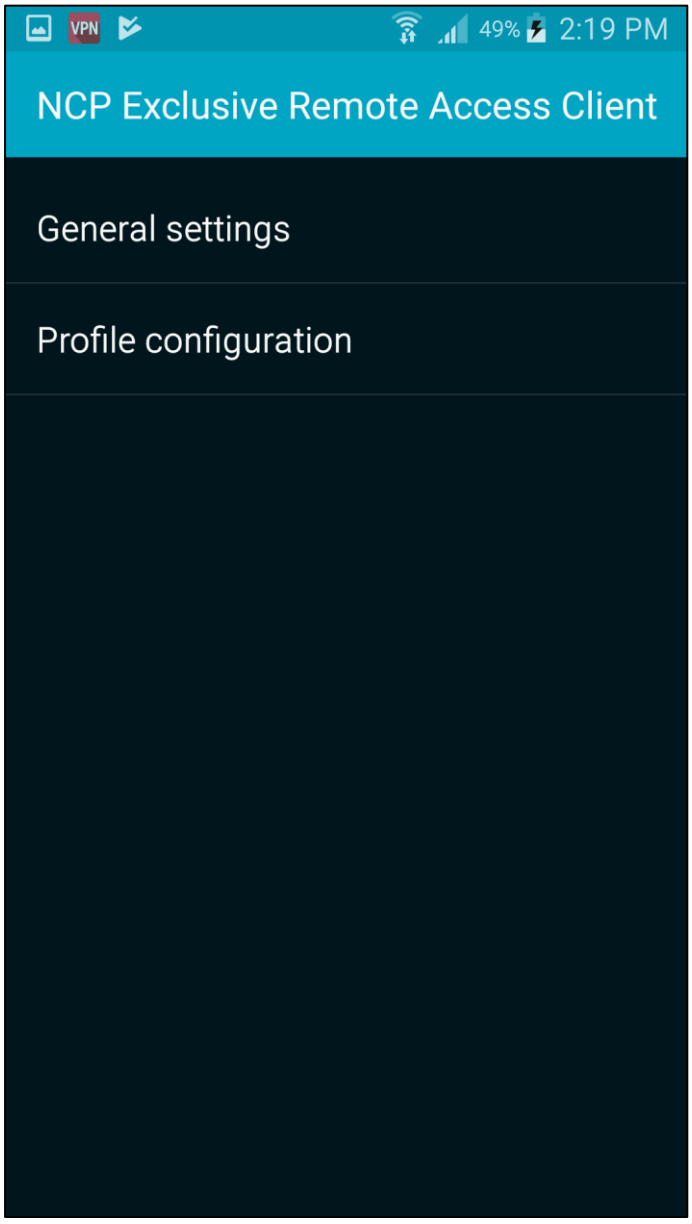
NCP Exclusive Remote Access Client
Connection Profile:
SRX IKEv1 AGGRESSIVE PSK
SEM enabled
Data (Tx) in Byte: 0
Time online: 00:00:08
Data (Rx) in Byte: 0
Timeout (sec): 0
Speed (KByte/s): 0,000
Encryption:
NCP
Disconnect

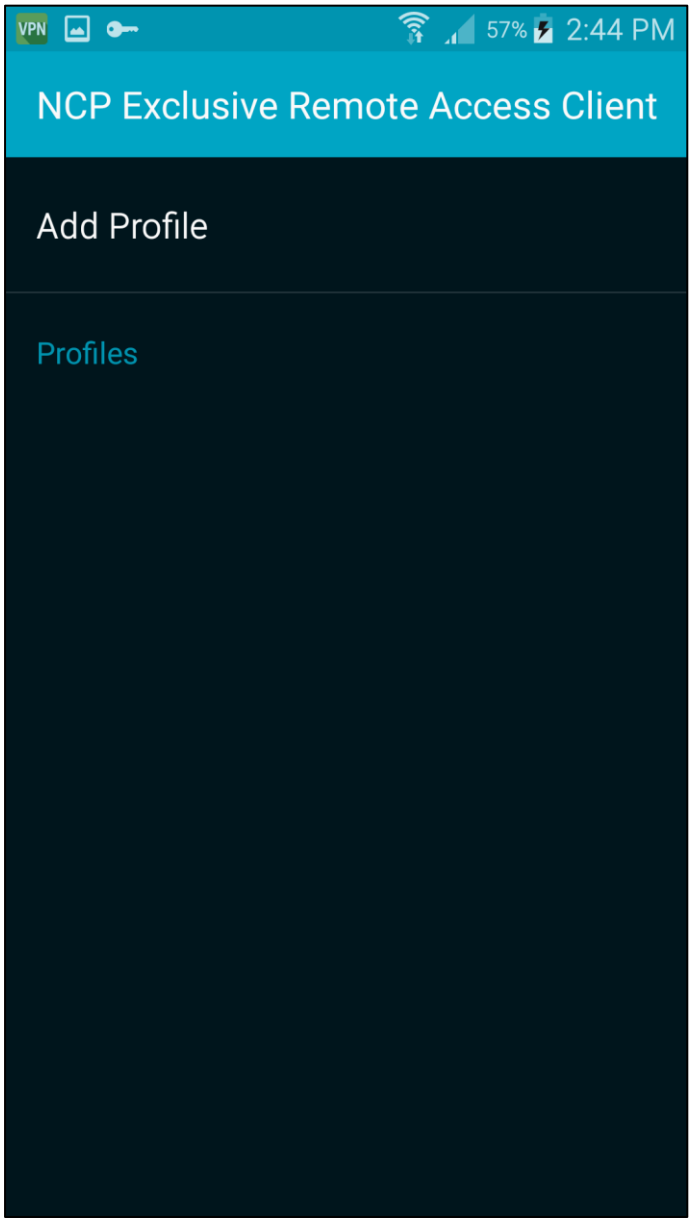
Configure NCP Exclusive Remote Access Client for Android

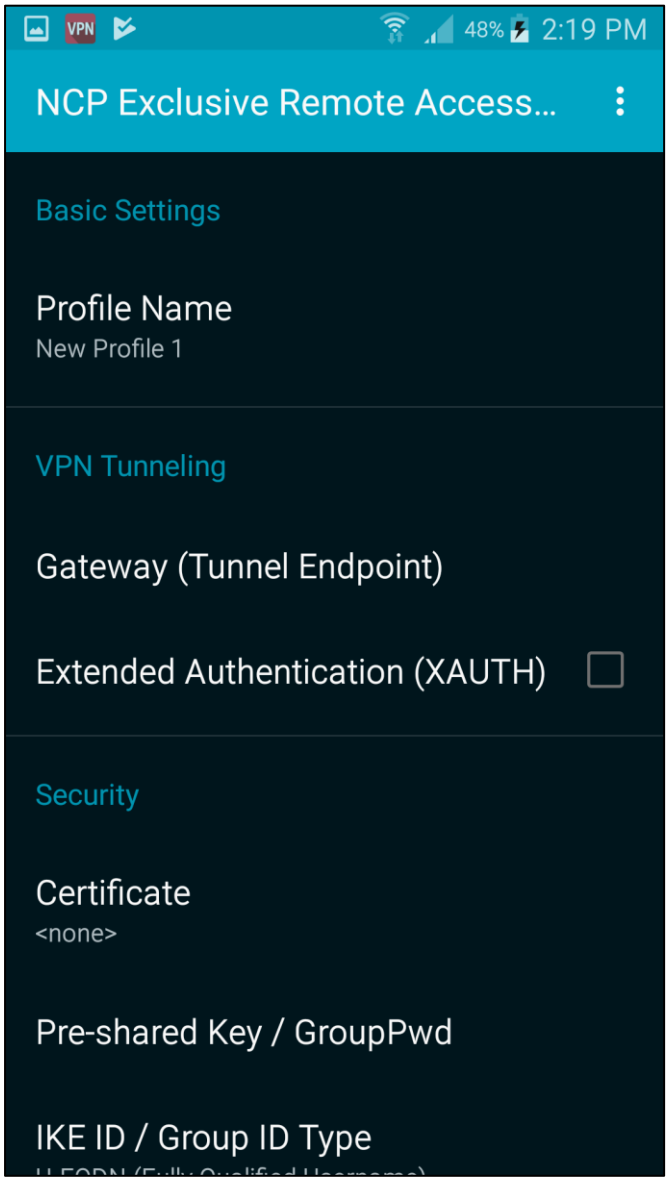
Create new Connection Profile (Menue – Configure – Profile configuration – Add Profile)



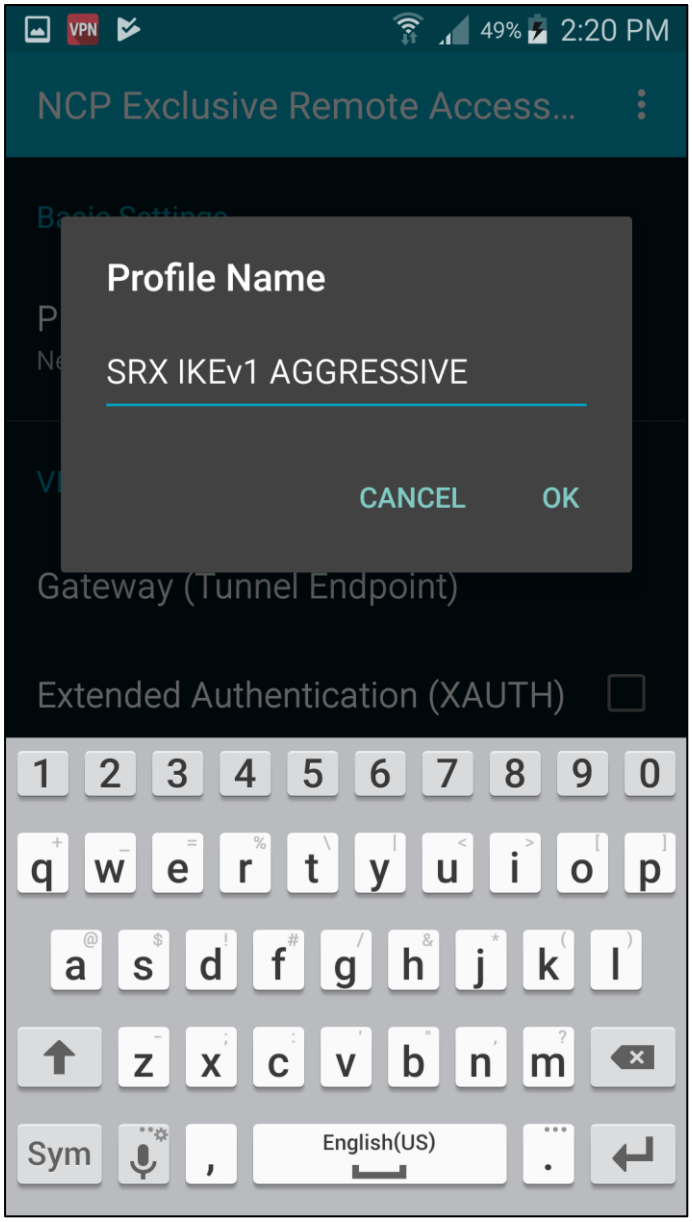

VPN
49%
2:19 PM
NCP Exclusive Re
Connect
Statistics
Log
Configure
Import / Export
Reset Pin
Unlock Parameters
About
Total Tx
Total Rx
Speed (kB/s)
Time Online
Timeout
NCP


VPN
49%
2:19 PM
NCP Exclusive Remote Access Client
General settings
Profile configuration

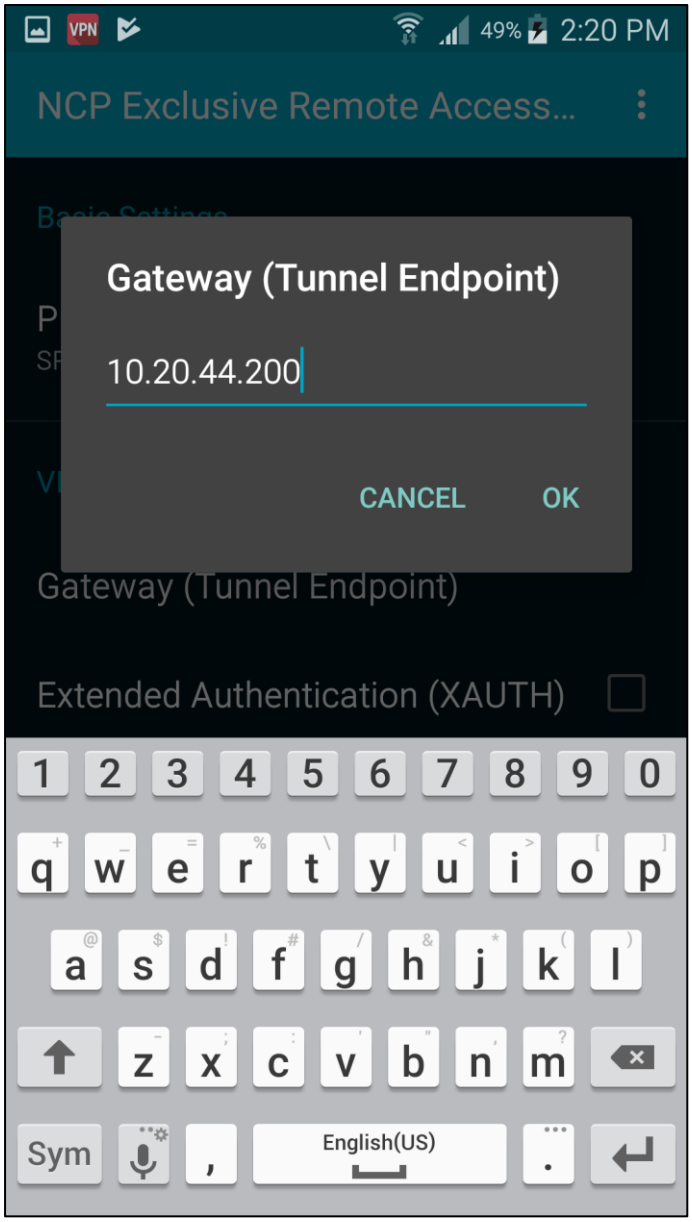

VPN
57%
2:44 PM
NCP Exclusive Remote Access Client
Add Profile
Profiles


VPN
48%
2:19 PM
NCP Exclusive Remote Access...
Basic Settings
Profile Name
New Profile 1
VPN Tunneling
Gateway (Tunnel Endpoint)
Extended Authentication (XAUTH)
Security
Certificate
<none>
Pre-shared Key / GroupPwd
IKE ID / Group ID Type

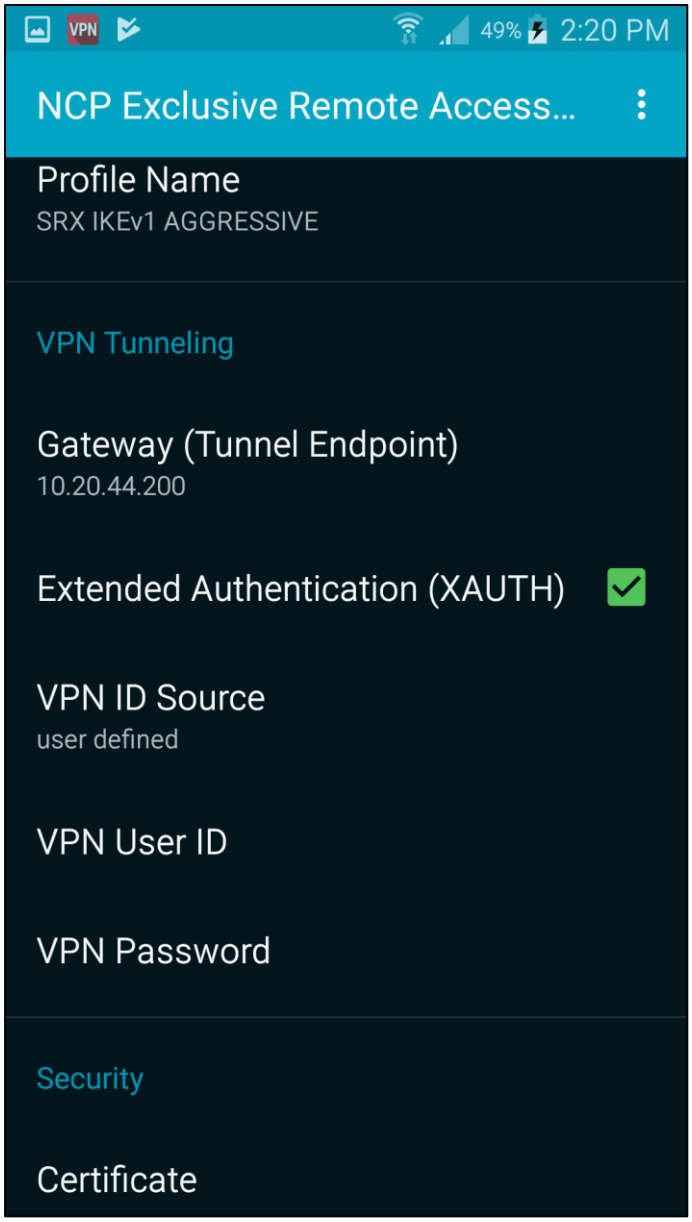
Enter name for connection profile

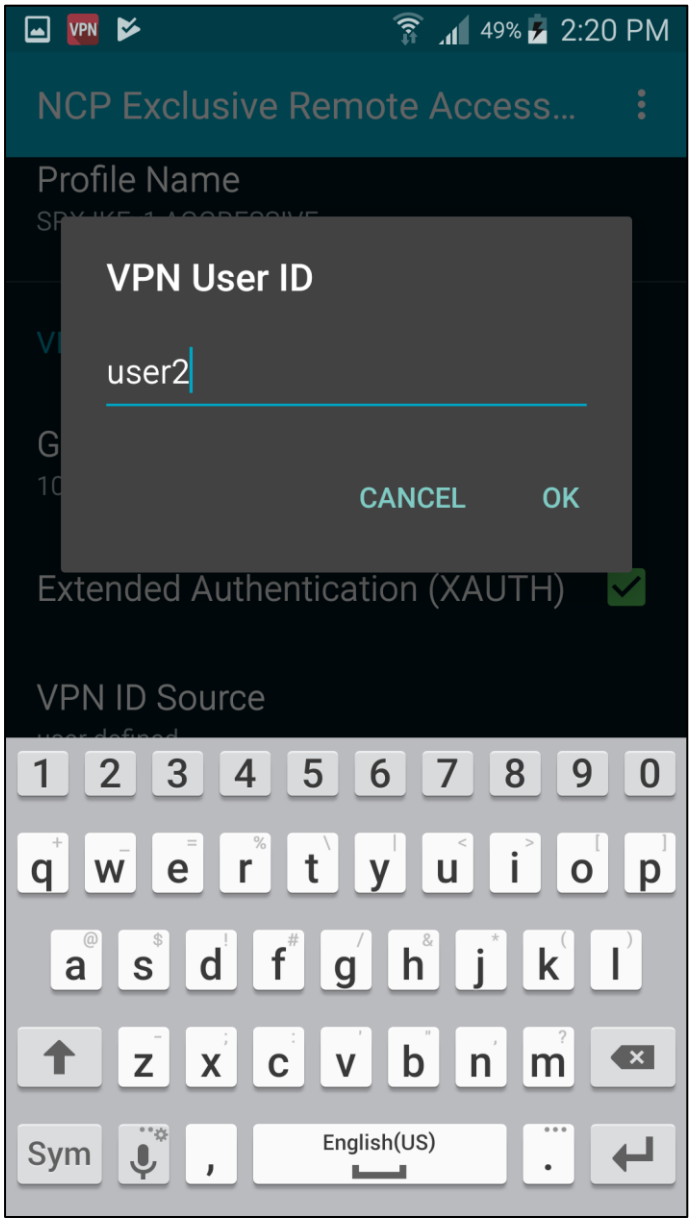


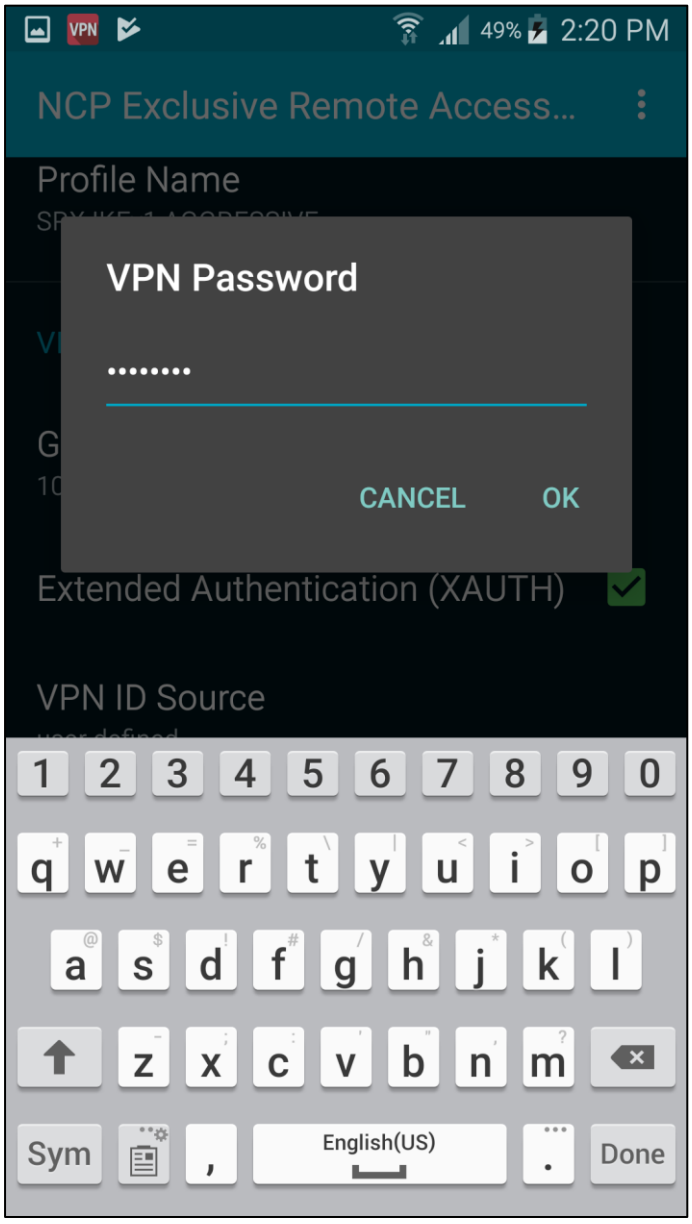
Enter name or IP address of Juniper SRX



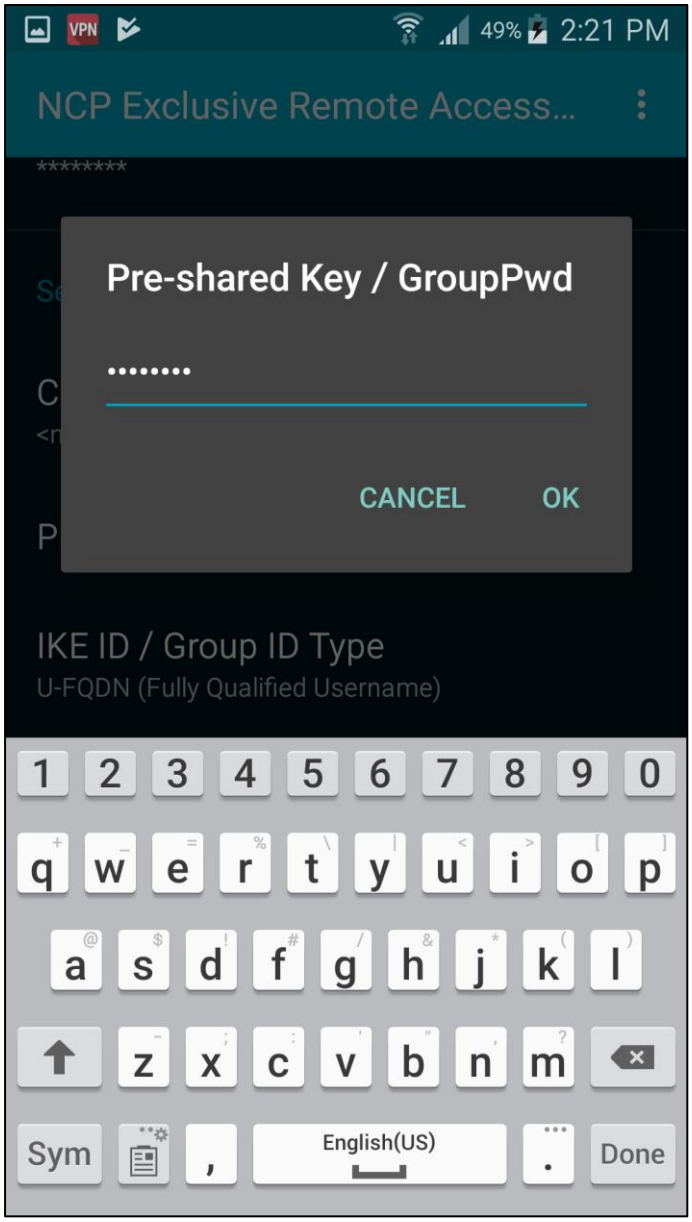
Enable Extended Authenctication (XAUTH) and enter username and password



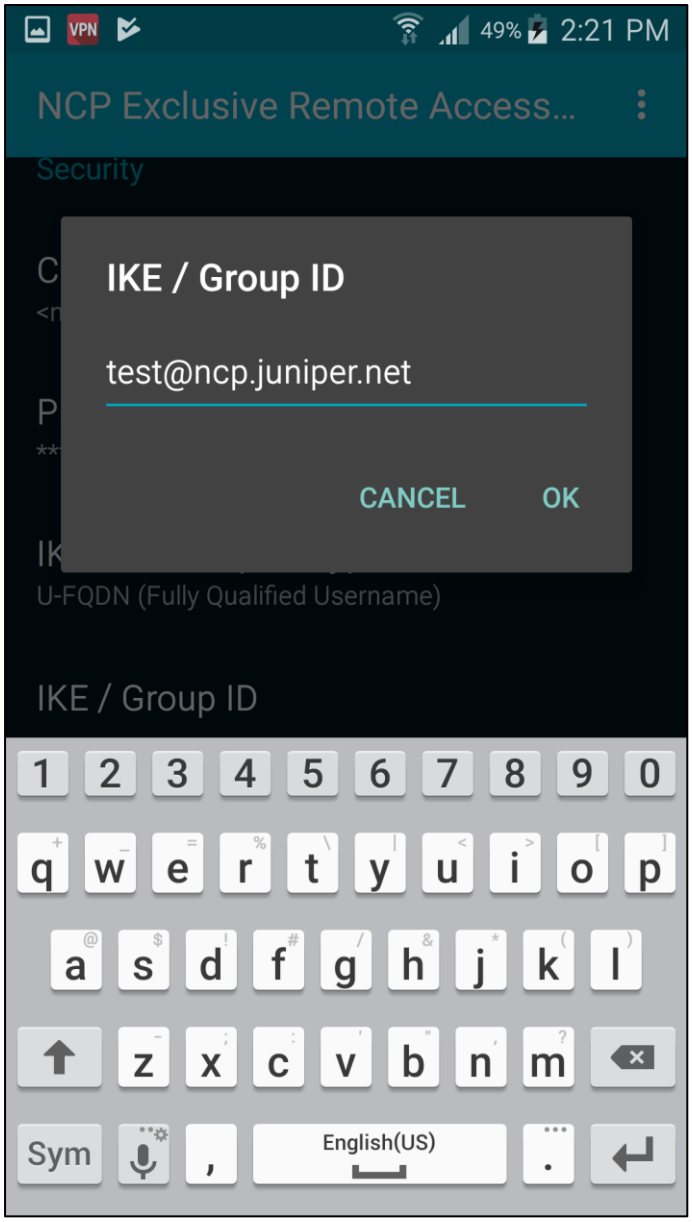

49% 2:20 PM
NCP Exclusive Remote Access...
Profile Name
VPN User ID
user2
CANCEL
OK
Extended Authentication (XAUTH)
VPN ID Source
1 2 3 4 5 6 7 8 9 0
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
Sym
English(US)


49% 2:20 PM
NCP Exclusive Remote Access...
Profile Name
VPN Password
CANCEL
OK
Extended Authentication (XAUTH)
VPN ID Source
Sym
English(US)
Done

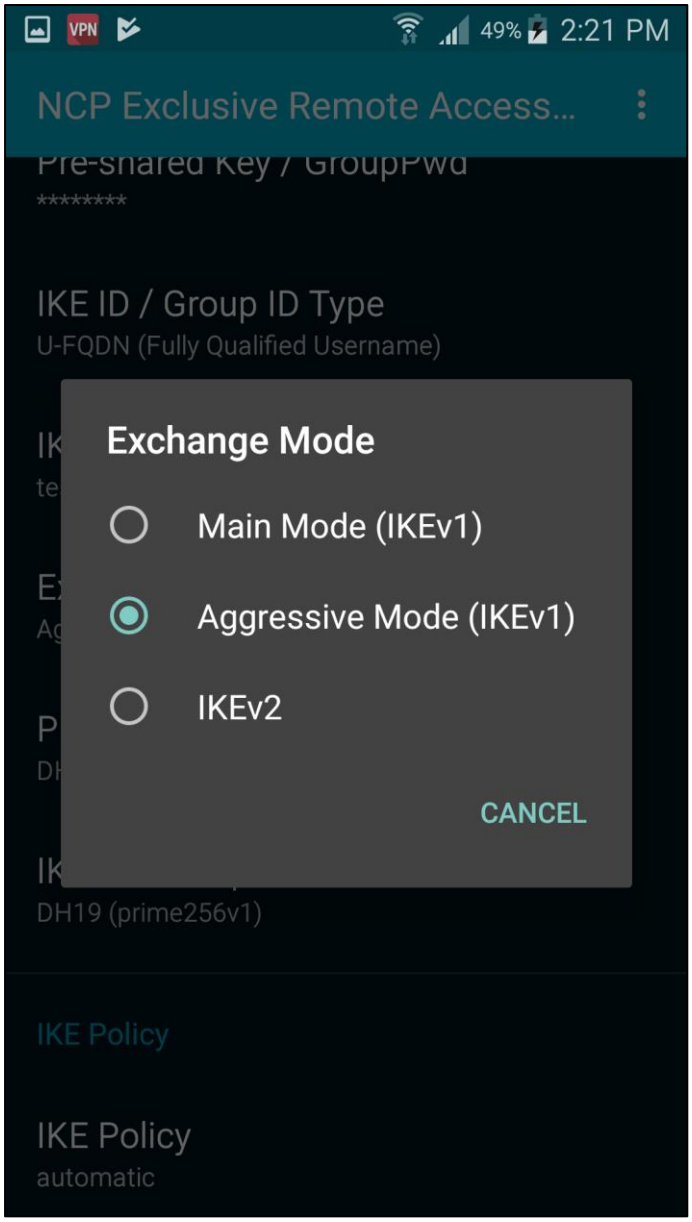
Enter the pre-shared key



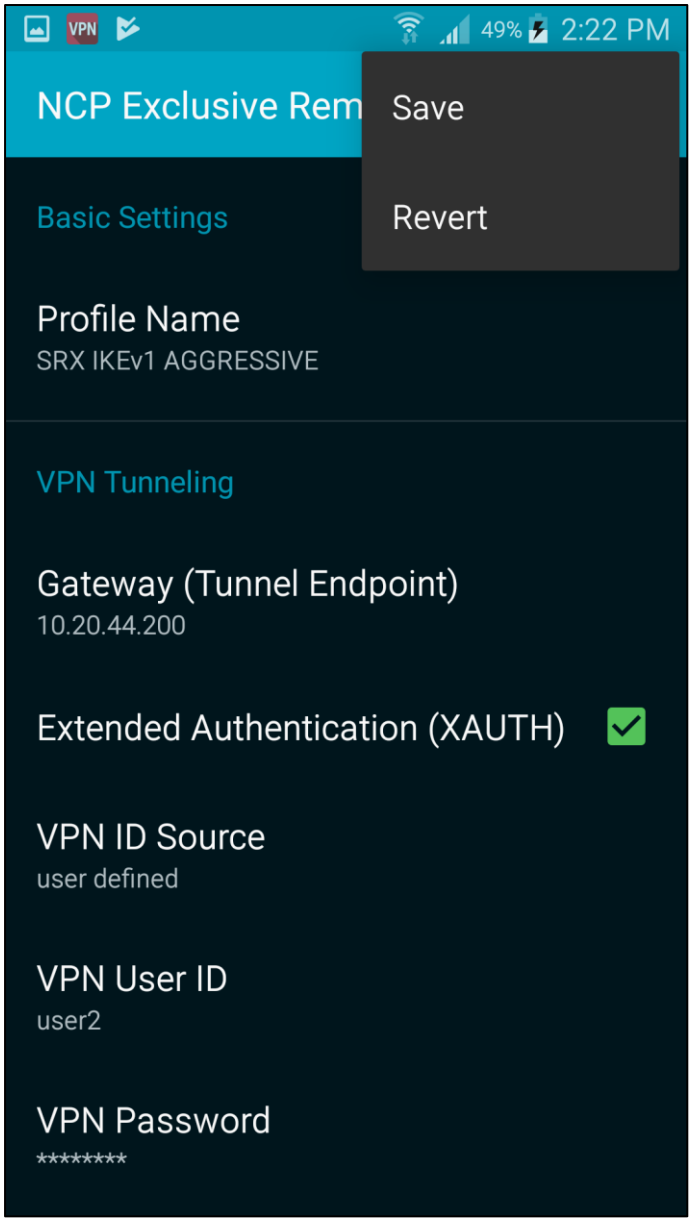
Enter IKE-ID


49% 2:21 PM
NCP Exclusive Remote Access...
Security
IKE / Group ID
test@ncp.juniper.net
CANCEL
OK
U-FQDN (Fully Qualified Username)
IKE / Group ID
1 2 3 4 5 6 7 8 9 0
q w e r t y u i o p
a s d f g h j k l
z x c v b n m
Sym
English(US)

Choose the Exchange mode (Aggressive Mode (IKEv1))



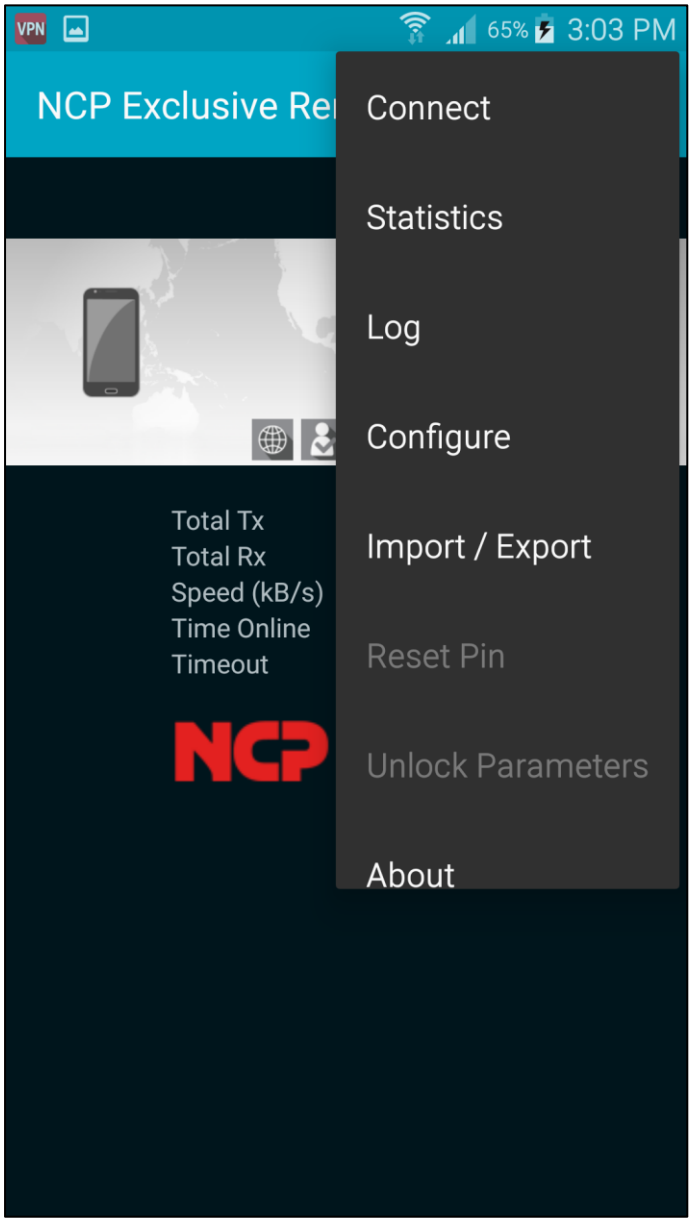
Save the profile by clicking on “Save” or the back button on the device



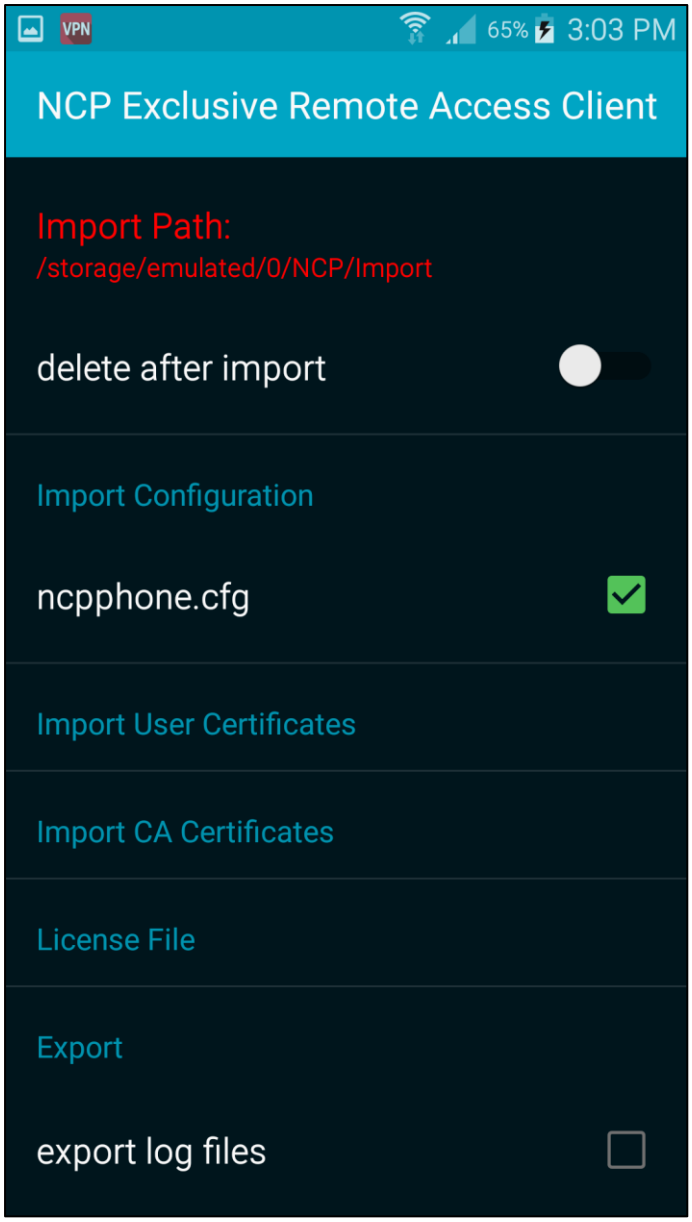
The configuration can also be imported via the app

Copy the configuration ncpphone.cfg or ncpphone.cnf into the folder Device storage/NCP/Import

Open the menu and choose “Import/Export”

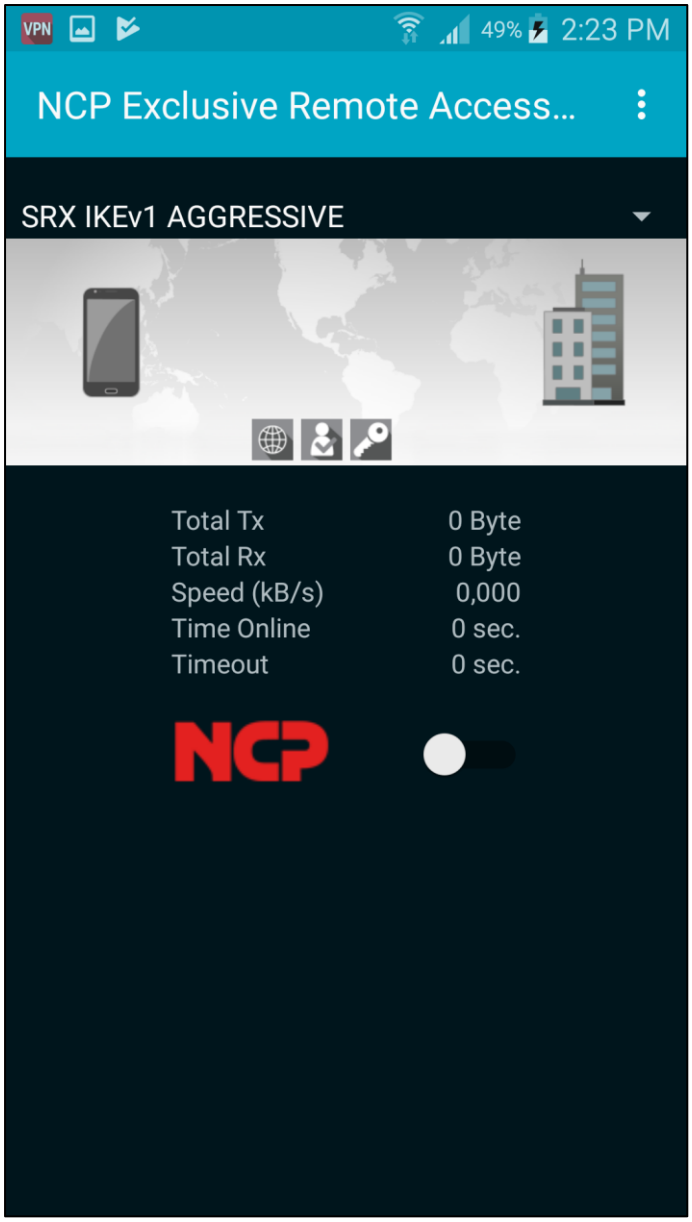


Enable ncpphone.cfg and press the back/return button on your device

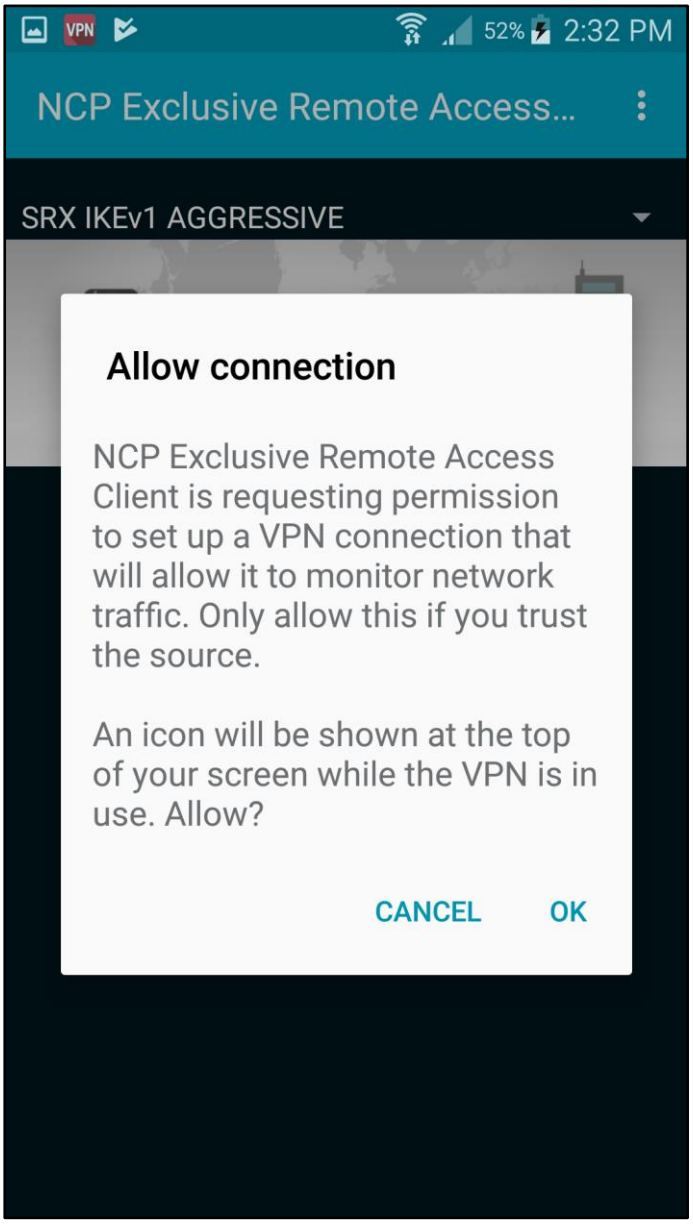


The configuration will be imported

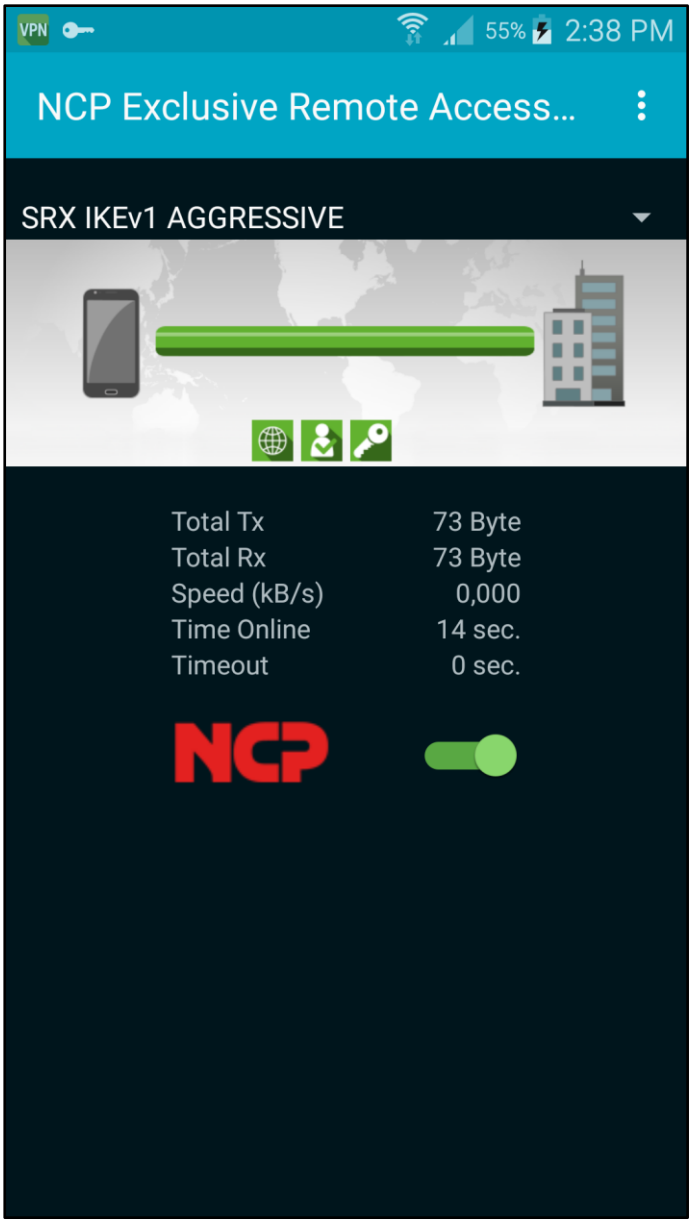
Click on the slide button to establish a connection



If the establish the connection the first time, Android will ask you to allow the VPN client to establish a connection. Click on “OK”



VPN connection is established



Configure NCP Exclusive Remote Access Client for iOS

The configuration of the iOS client is done on the NCP Secure Enterprise Management Server.
After you create a configuration on the NCP Secure Enterprise Management Server, you are able to export the configuration file ncpphone.ncpconfigsem. The file ending needs to be .ncpconfigsem

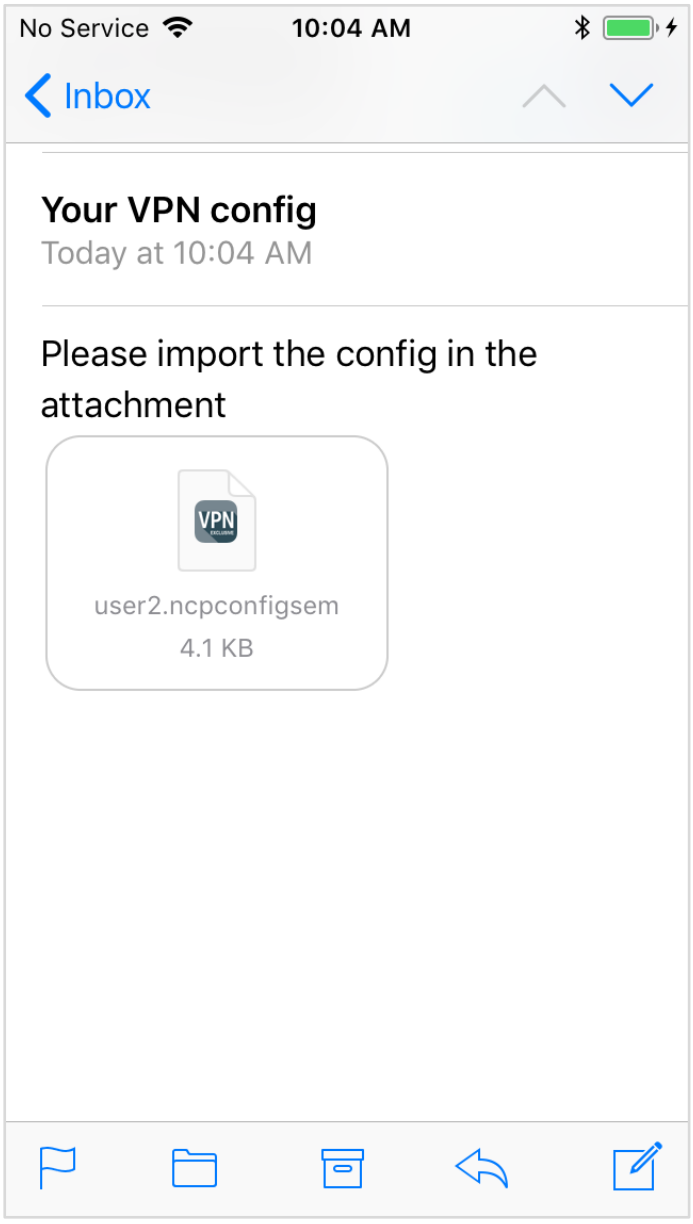
There are 2 ways to import the profile

1) Import by sending it over email or downloading it from a webserver

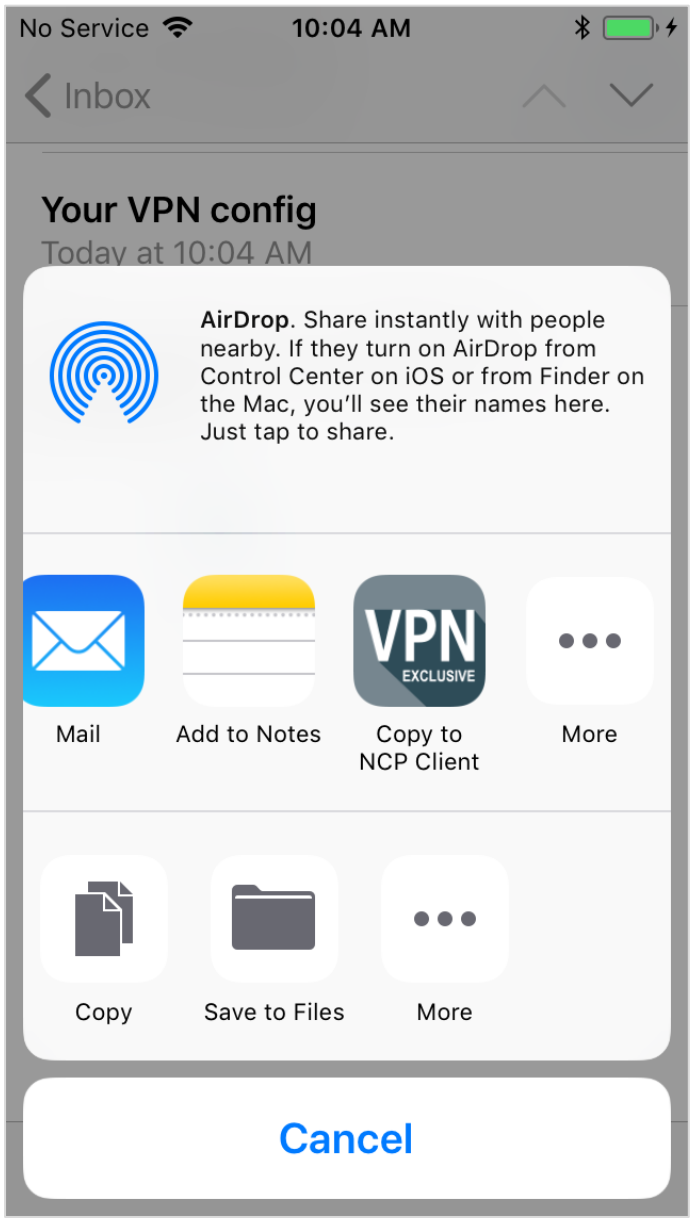
This sample will show the import if the file is sent via email

Send the .ncpconfigsem file via email to your iOS device

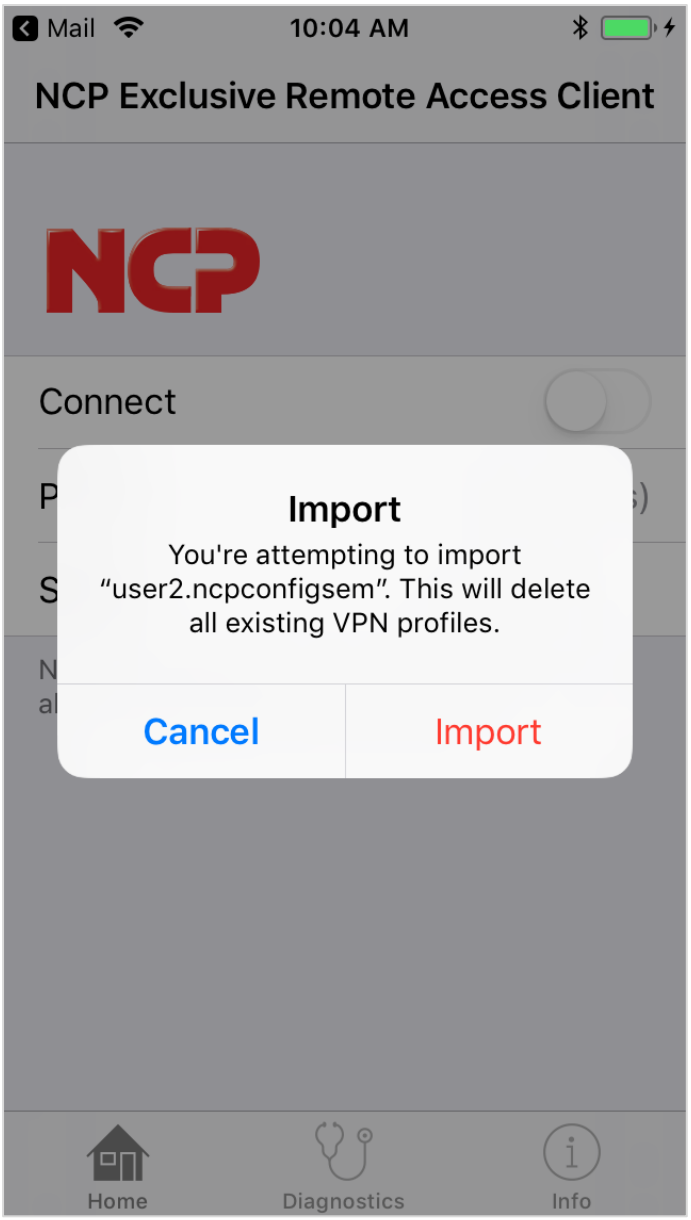
Open the email with the attachment



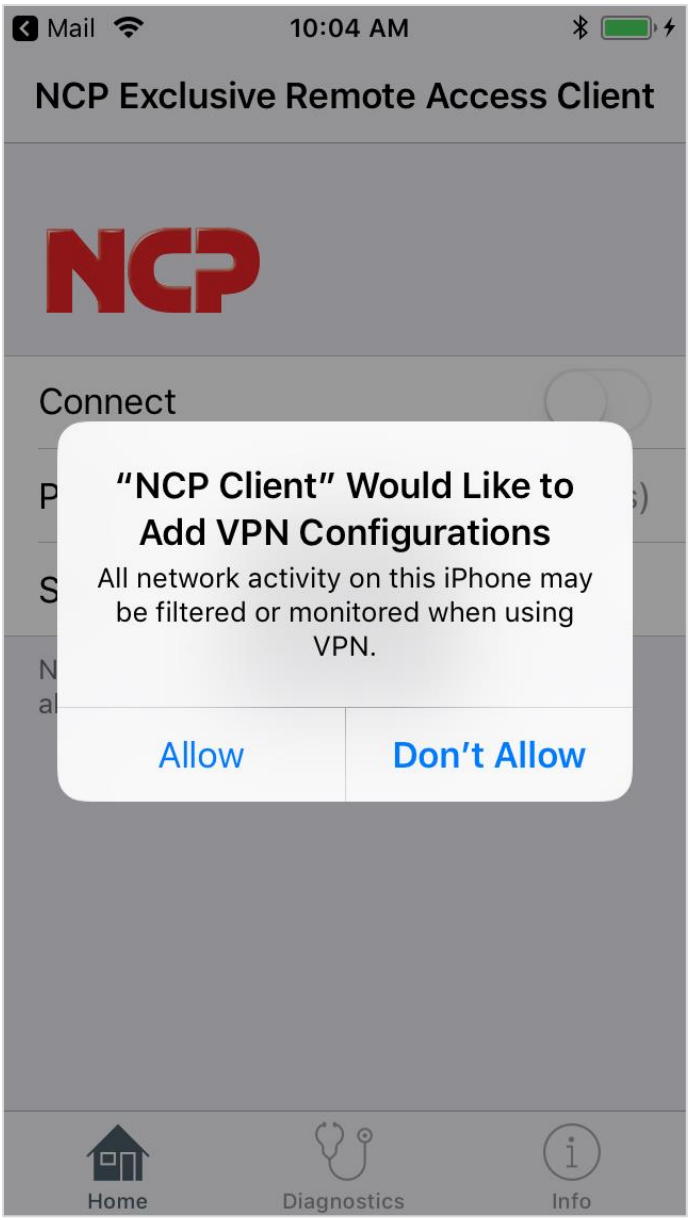
Click on the .ncpconfigsem file and choose “Copy to NCP Client”


No Service
10:04 AM
Inbox
Your VPN config
Today at 10:04 AM
AirDrop. Share instantly with people nearby. If they turn on AirDrop from Control Center on iOS or from Finder on the Mac, you'll see their names here. Just tap to share.
Mail
Add to Notes
VPN EXCLUSIVE
Copy to NCP Client
More
Copy
Save to Files
More
Cancel

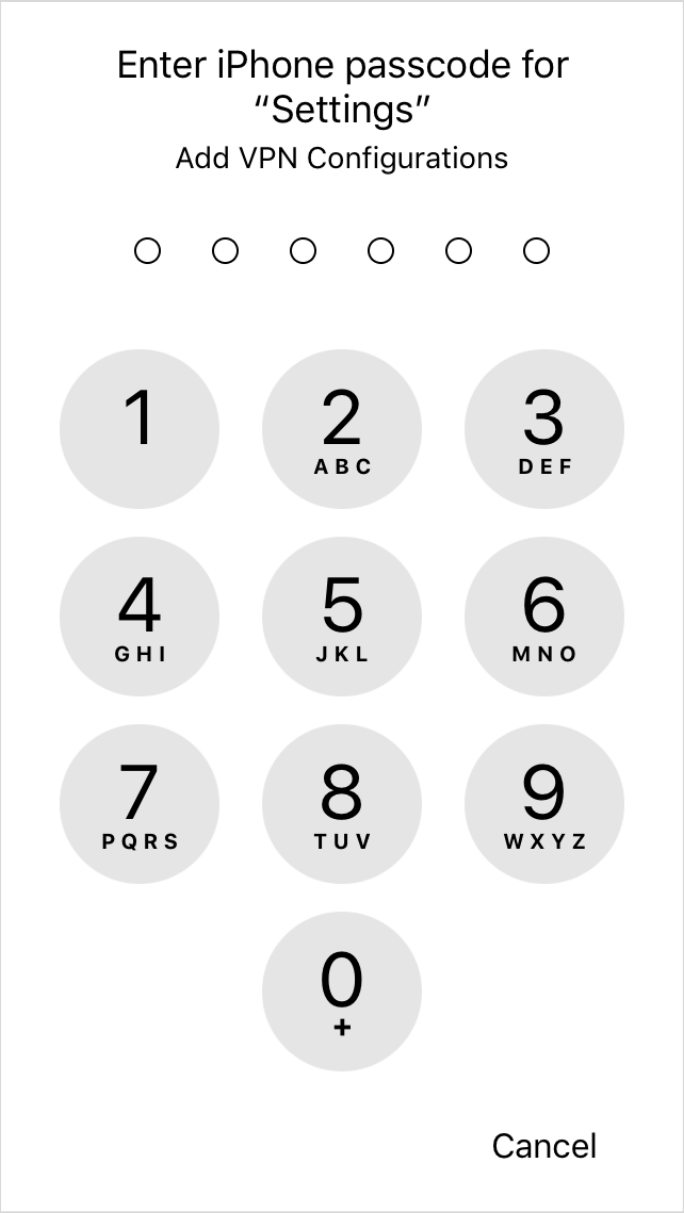
Click “Import” to start the import process



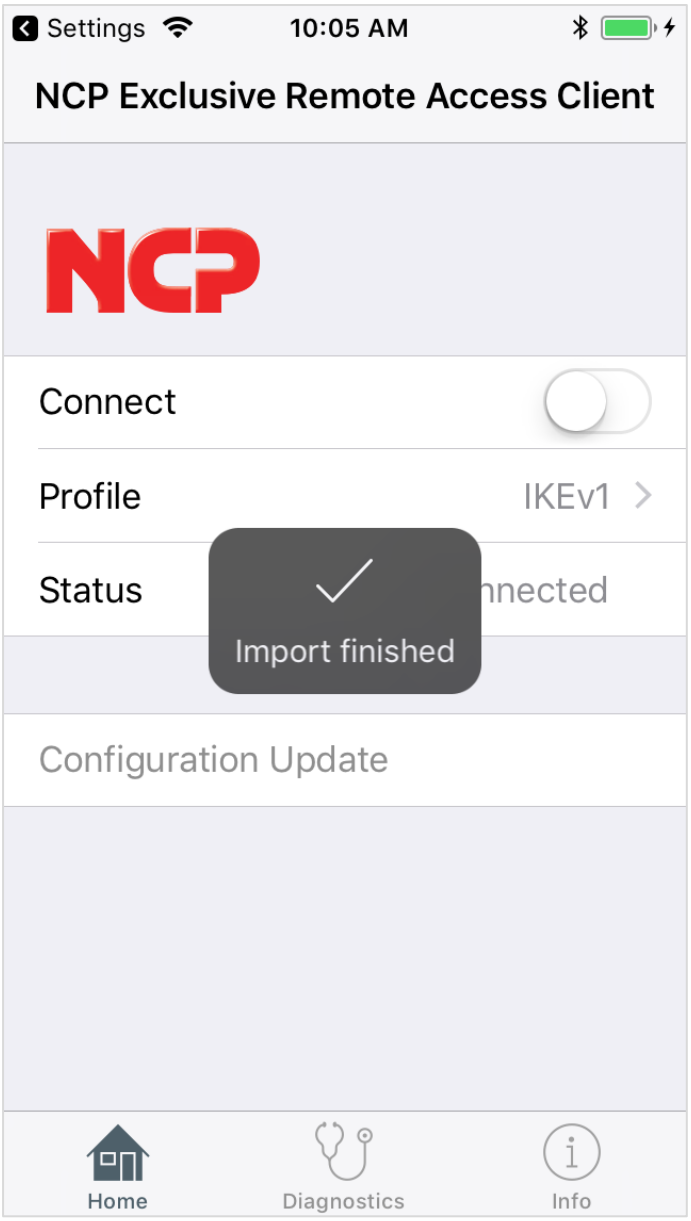
Allow to add a new VPN configuration by clicking on “Allow”



Enter you iPhone/iPad passcode to import the configuration



The import of the configuration was successful



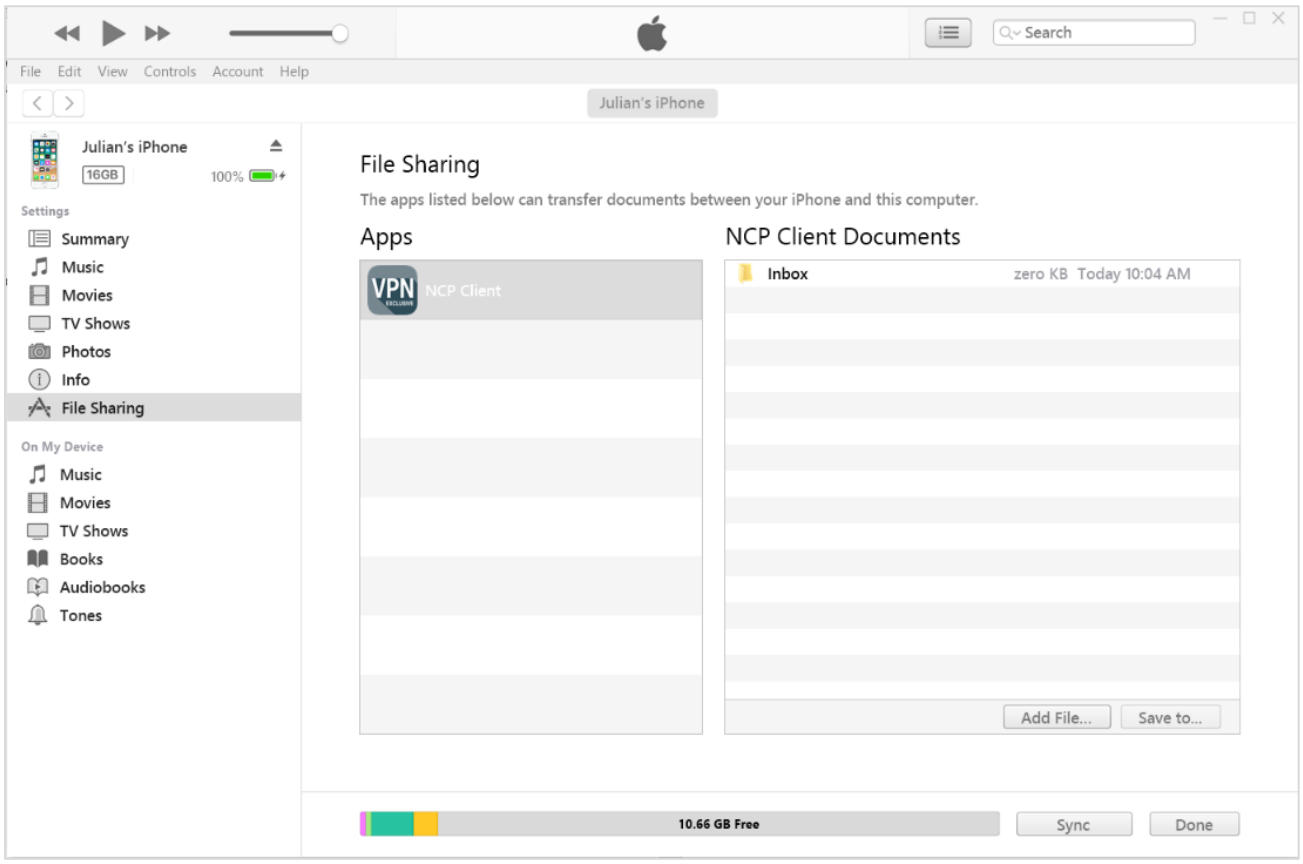
2) Import over iTunes

Connect the iOS devise with your computer

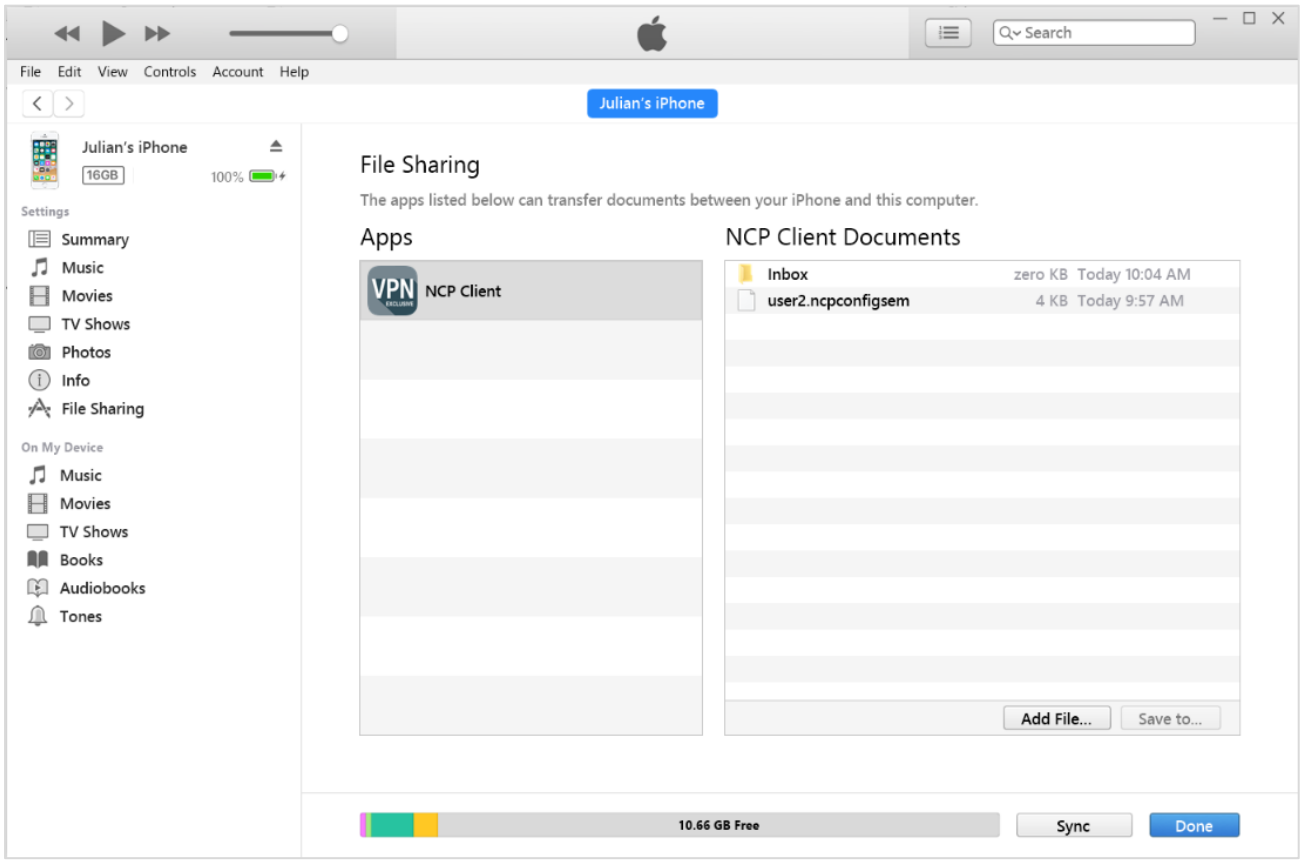
Open iTunes on your computer

Click on the device button

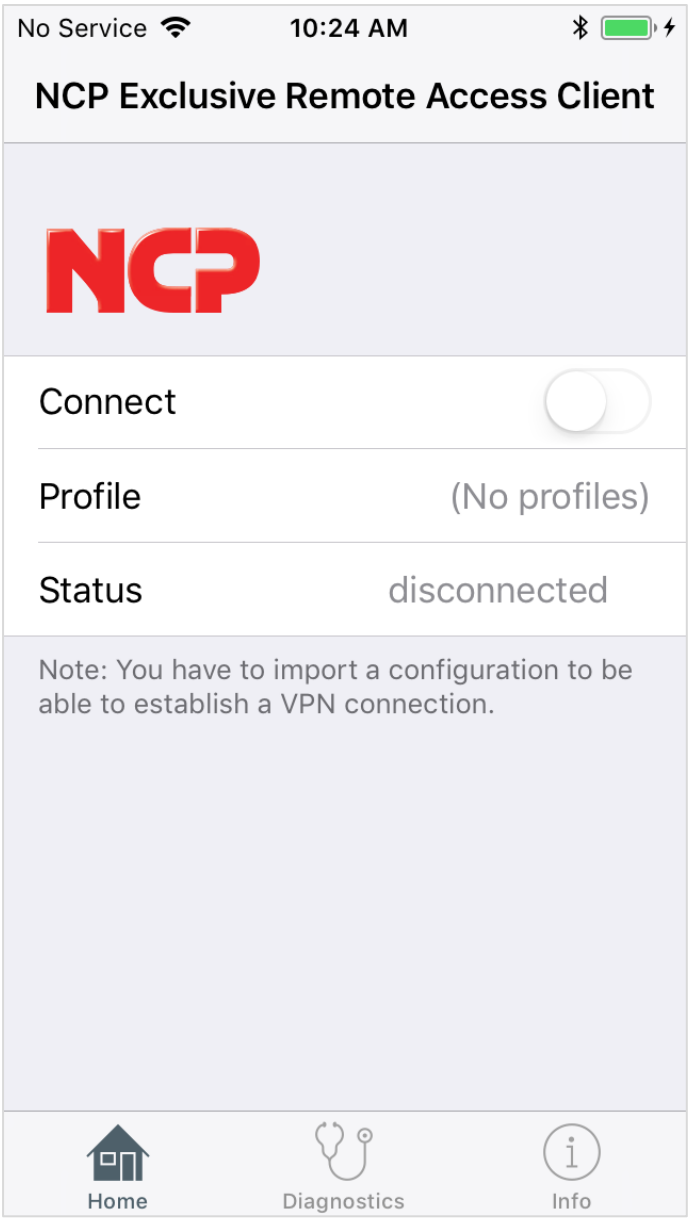
Go to File Sharing and click on NCP Client



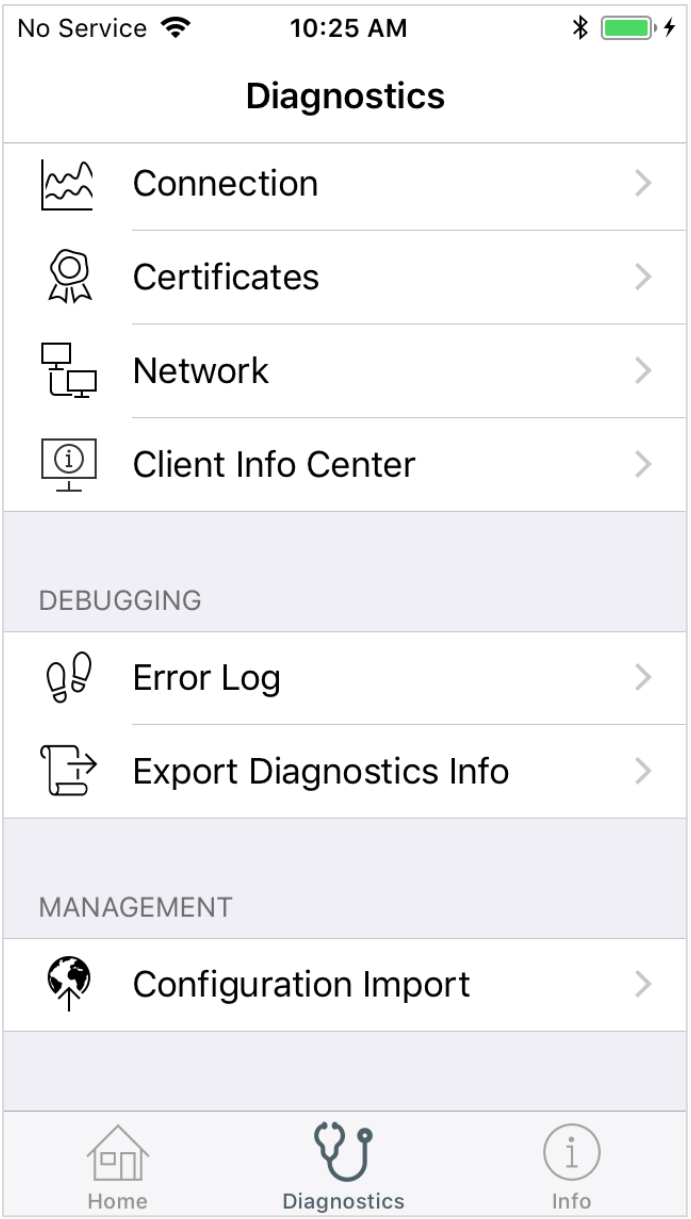
Add the configuration via “Add File…” and click “Sync” to synchronize the information with the iOS device


Search
File Edit View Controls Account Help
Julian's iPhone
Julian's iPhone
16GB
100%
Settings
Summary
Music
Movies
TV Shows
Photos
Info
File Sharing
On My Device
Music
Movies
TV Shows
Books
Audiobooks
Tones
File Sharing
The apps listed below can transfer documents between your iPhone and this computer.
Apps
NCP Client
NCP Client Documents
Inbox zero KB Today 10:04 AM
user2.ncpconfigsem 4 KB Today 9:57 AM
Add File...
Save to...
10.66 GB Free
Sync
Done

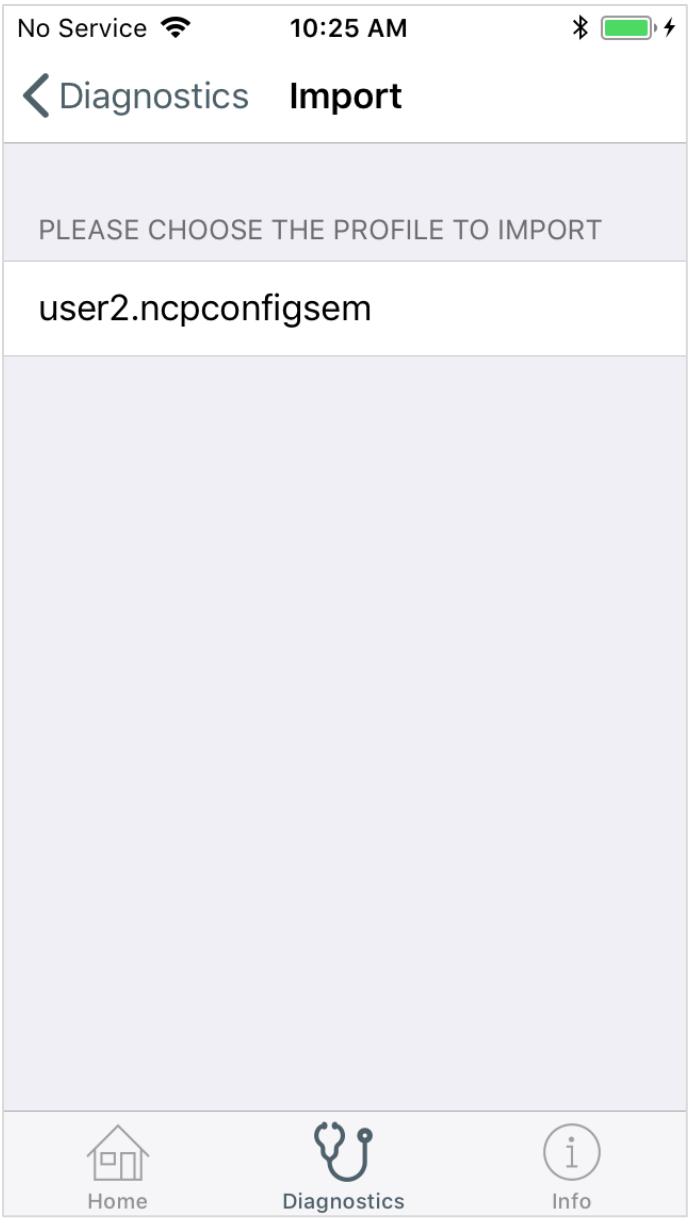
Open the App on the iOS device



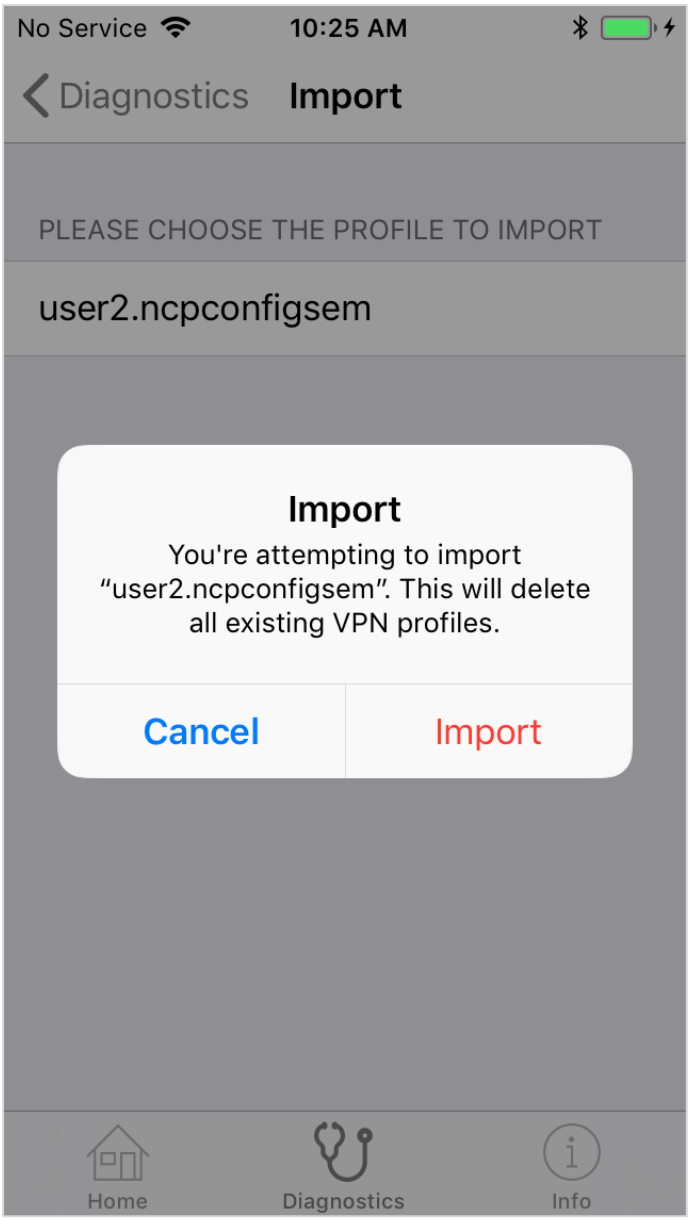
Go to “Diagnostics” and “Configuration Import”



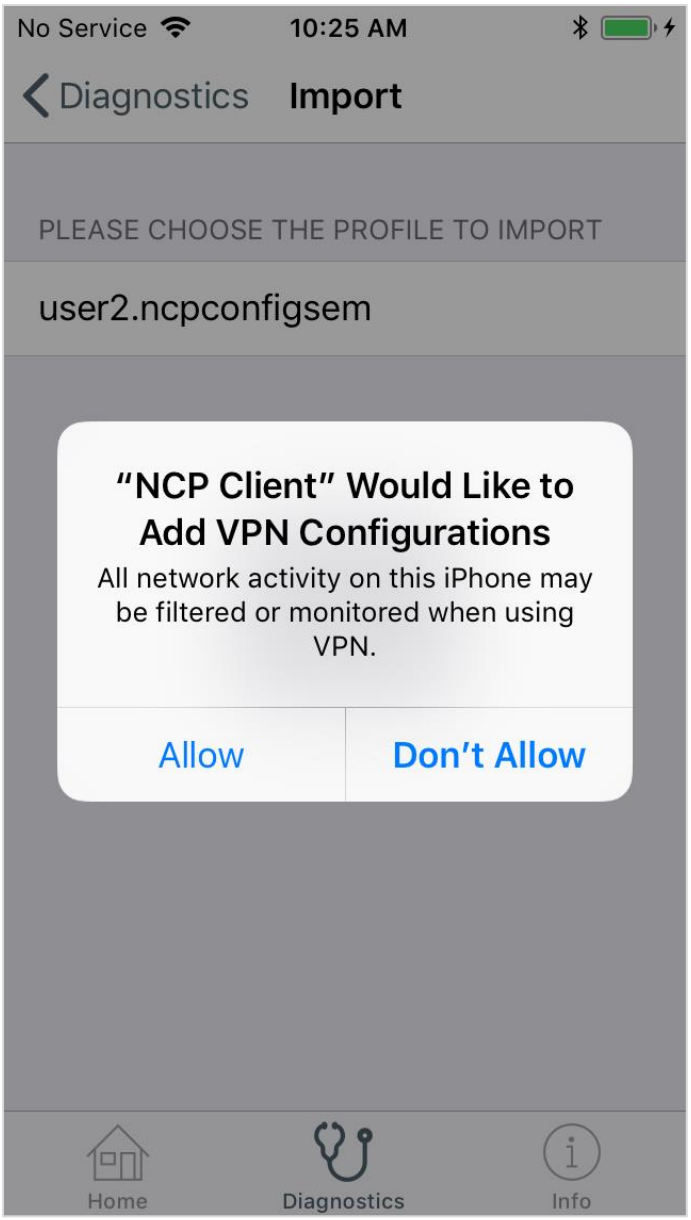
Click on the .ncpconfigsem file to start the import process



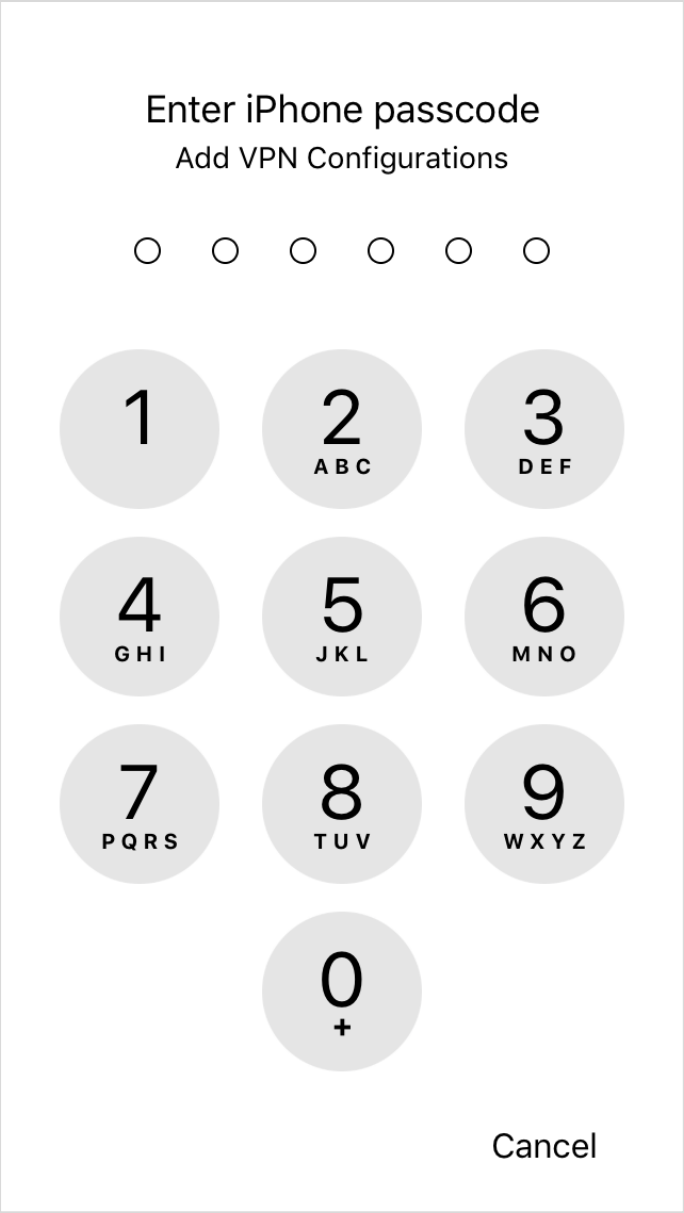
Click on “Import”



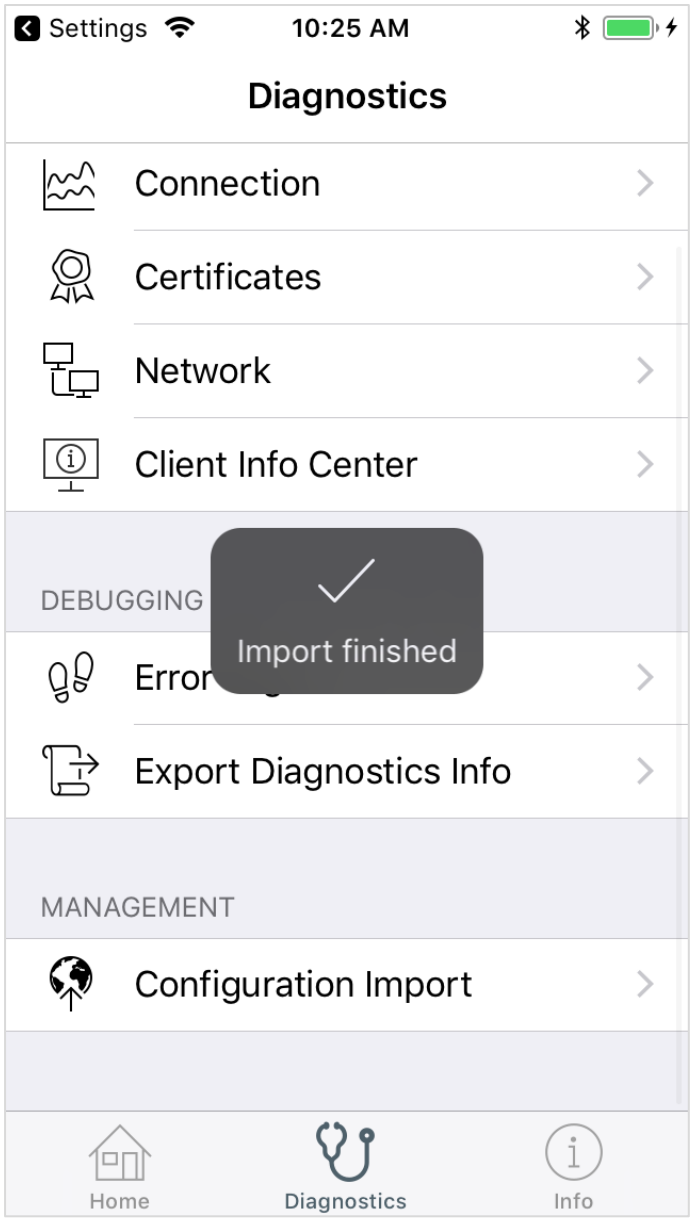
Click “Allow” to add another VPN configuration



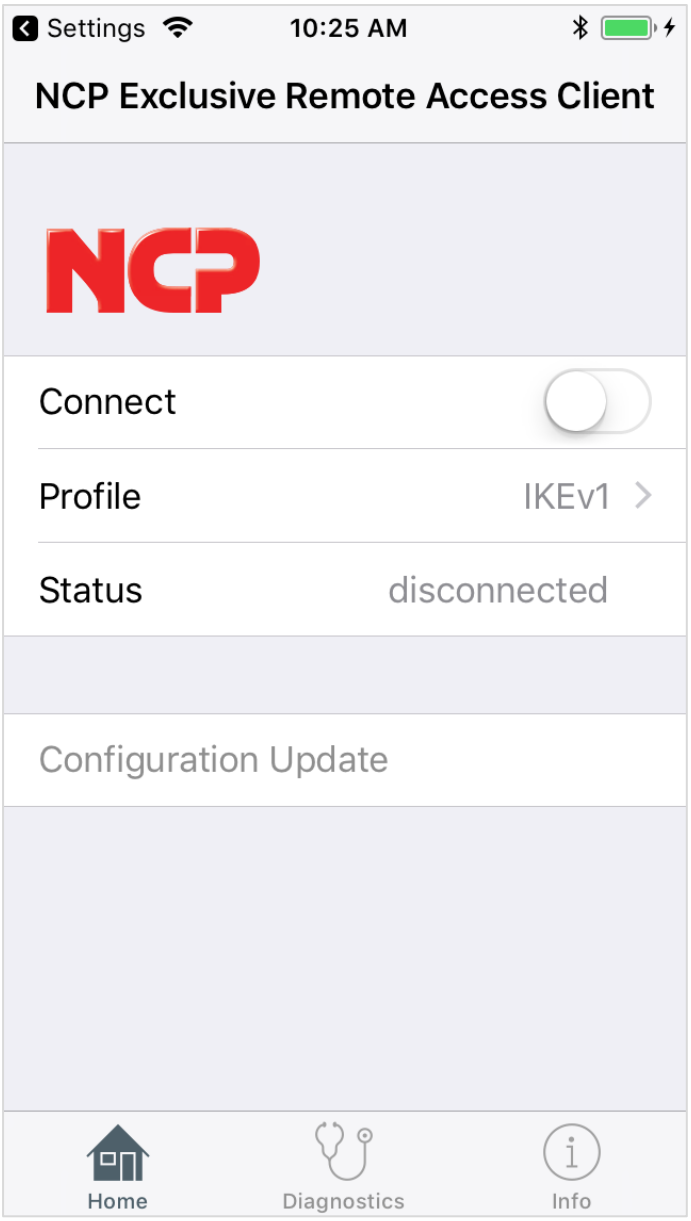
Enter your iPhone/iPad passcode to import the configuration

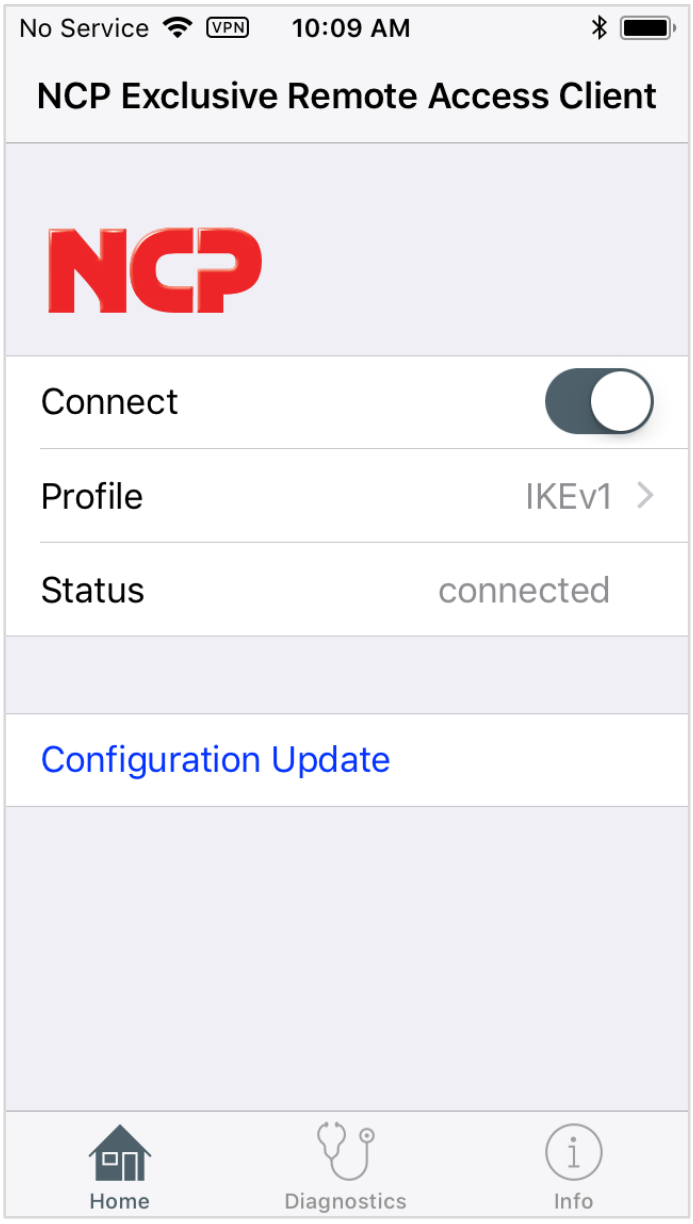


The import of the configuration was successful



Click the slide button to establish the VPN connection




No Service
VPN
10:09 AM
NCP Exclusive Remote Access Client
Connect
Profile
IKEv1
Status
connected
Configuration Update
Home
Diagnostics
Info