NetXGATE SSL VPN Client (Windows) Installation Guide

Document ver-1.2
15/12/2020

NetXGATE SSL VPN Overview -

A Virtual Private Network (VPN) is a tunnel that carries private network traffic from one endpoint system to another over a public network such as the Internet without the traffic being aware that there are intermediate hops between the endpoints or the intermediate hops being aware they are carrying the network packets that are traversing the tunnel. The tunnel may optionally compress and/or encrypt the data, providing enhanced performance and some measure of security.

For business telecommuters or employees working from home, connecting securely to the corporate intranets or extranets to access files or application is essential.

Hence, whenever users access the organization resources from remote locations, it is essential that not only the common requirements of secure connectivity be met but also the special demands of remote clients. These requirements include:

- Connectivity: The remote users must be able to access the organization from various locations, like Internet cafes, hotels, airport etc. The range of applications available must include web applications, mail, file shares, and other more specialized applications required to meet corporate needs.

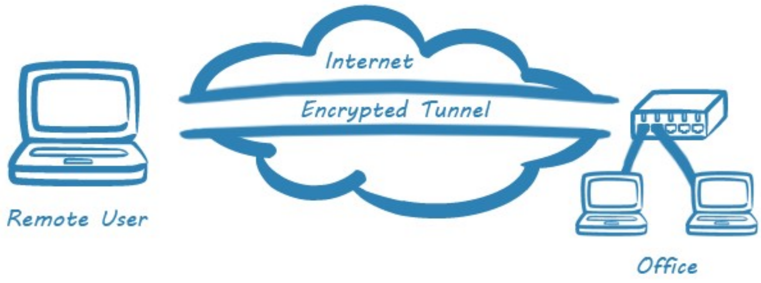
- Secure connectivity: Guaranteed by the combination of authentication, confidentiality and data integrity for every connection.

- Usability: Installation must be easy. No configuration should be required as a result of network modification at the remote user end. The given solution should be seamless for the connecting user.

How it works-

It allows access to the corporate network from anywhere, anytime and provides the ability to create point-to-point encrypted tunnels between remote user and company's internal network, requiring combination of SSL certificates and a password for authentication to enable access to the internal resources.

A VPN Client installed on the Mobile user's PC or Laptop which connects to a NetXGATE Next-Gen FW or VPN Concentrator which installed in the HQ/Corporate network. When the VPN Client is launched by the remote user, it will prompt for a (SMS *OTP / Google Authenticator if enabled*) and Password . The VPN Client then connects to the SSL VPN server in the office and if the password and certificate provided are correct, a secure tunnel is created between the PC and the HQ /office network.



Encrypted ,Authenticated & Authorized Traffic via Internet Line

Pic -1

NetXGATESSL VPN Client Configuration at Remote Users PC / NoteBook

The NetXGATE SSL VPN client is compatible with all versions of MS Windows,

In order to connect to the NetXGATE Secure SSL VPN server you can download VPN Client software from www.netxgate.com or shared over Mail / Link .

Note- SSL VPN is not supported when NetXGATE is deployed as Bridge.

Installing and Running SSL VPN Client

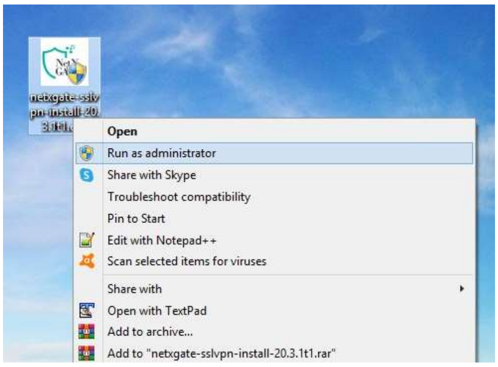
Before you can use SSL VPN Client it must first be installed using the instructions below. You must have administration rights on your computer to be able to install it.

Step -1

Install Secure SSL VPN cleint software in users windows PC –

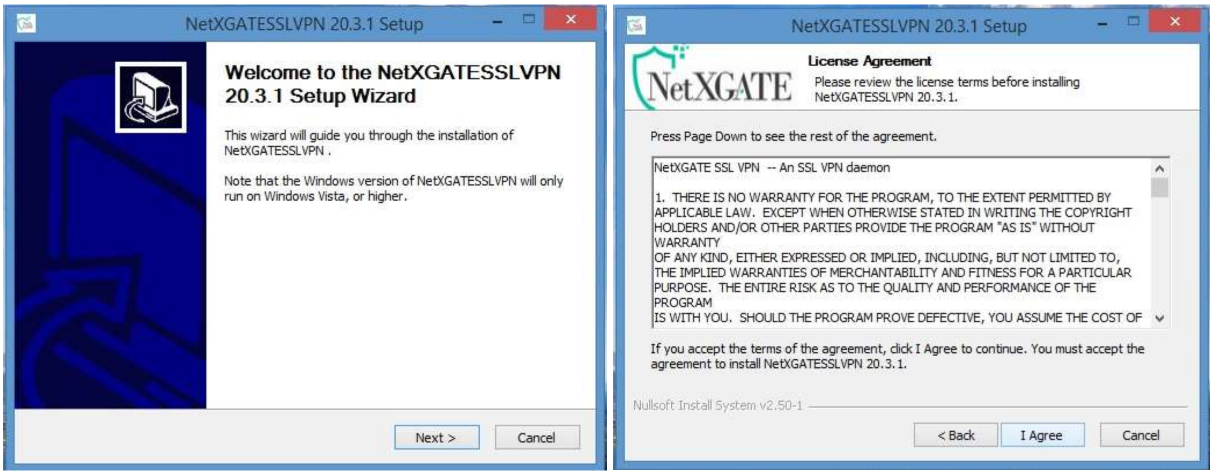
Run NetXGATE SSL VPN Client software usually located in your Desktop , by double-clicking it, or by clicking Run once you have finished downloading it.

You may see a User Access Control window asking "Do you want to allow the following program to make changes to this computer?". If so, click Yes


netxgate-sslvpn-install-20.3.1t1
Open
Run as administrator
Share with Skype
Troubleshoot compatibility
Pin to Start
Edit with Notepad++
Scan selected items for viruses
Share with
Open with TextPad
Add to archive...
Add to "netxgate-sslvpn-install-20.3.1t1.rar"

Pic-2

When you are greeted with the "Welcome to the NetXGATE SSL VPN Client Wizard" window, click Next.


NetXGATESSLVPN 20.3.1 Setup
Next >
Cancel
NetXGATESSLVPN 20.3.1 Setup
NetXGATE
Nullsoft Install System v2.50-1
< Back
I Agree
Cancel

Welcome to the NetXGATESSLVPN 20.3.1 Setup Wizard

This wizard will guide you through the installation of NetXGATESSLVPN .

Note that the Windows version of NetXGATESSLVPN will only run on Windows Vista, or higher.

License Agreement

Please review the license terms before installing NetXGATESSLVPN 20.3.1.

Press Page Down to see the rest of the agreement.

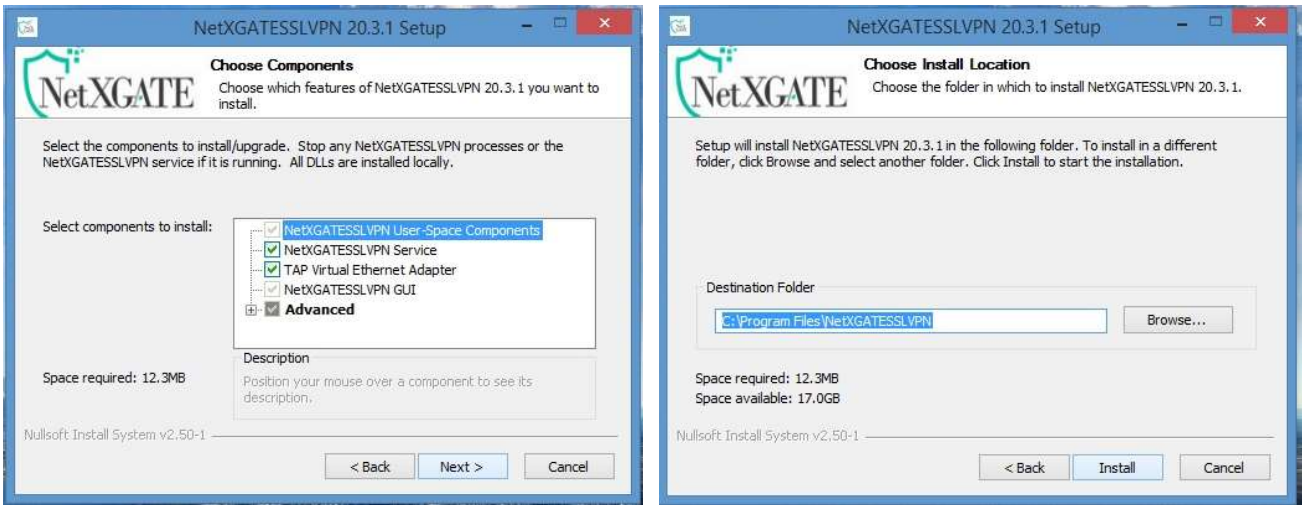
NetXGATE SSL VPN -- An SSL VPN daemon

1. THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY
OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM
IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF

If you accept the terms of the agreement, click I Agree to continue. You must accept the agreement to install NetXGATESSLVPN 20.3.1.

Pic-3 & 4

Click Next –



Choose Components

Choose which features of NetXGATESSLVPN 20.3.1 you want to install.

Select the components to install/upgrade. Stop any NetXGATESSLVPN processes or the NetXGATESSLVPN service if it is running. All DLLs are installed locally.

Select components to install:

- ☑ NetXGATESSLVPN User-Space Components
- ☑ NetXGATESSLVPN Service
- ☑ TAP Virtual Ethernet Adapter
- ☑ NetXGATESSLVPN GUI
- ☑ Advanced

Space required: 12.3MB

Description

Position your mouse over a component to see its description.

Choose Install Location

Choose the folder in which to install NetXGATESSLVPN 20.3.1.

Setup will install NetXGATESSLVPN 20.3.1 in the following folder. To install in a different folder, click Browse and select another folder. Click Install to start the installation.

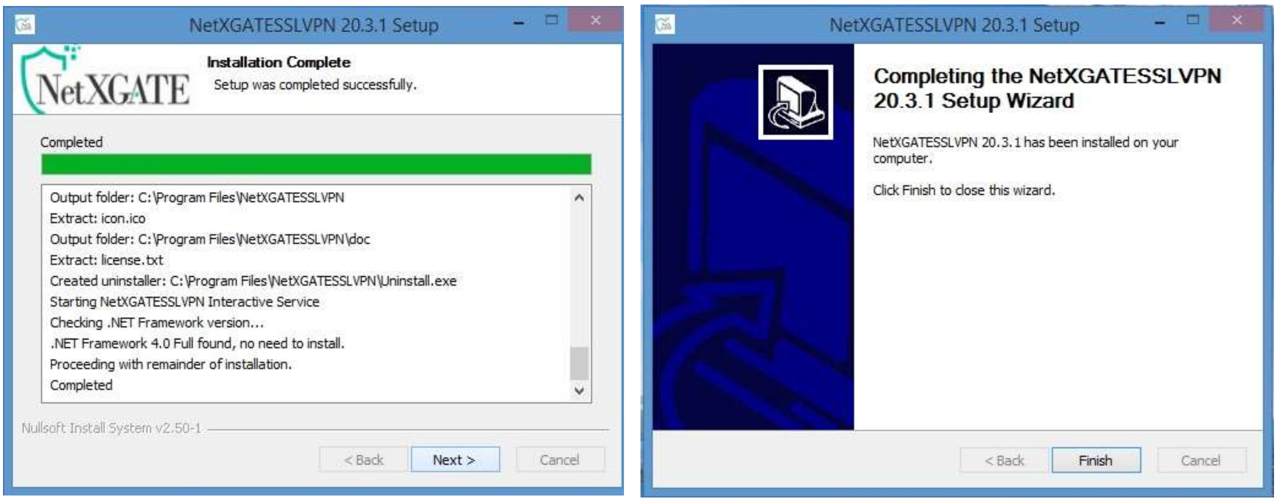
Destination Folder: C:\Program Files\NetXGATESSLVPN

Space required: 12.3MB
Space available: 17.0GB

Pic-5 & 6

Select where you would like SSL VPN Client to be installed, then click Next. We highly recommend you use the default install location that the installer selects for you.

Note- The installation will now proceed. However, you may be warned about suspicious behavior of the installation process. In this case, warning may be ignored, so just close the window .



Installation Complete

Setup was completed successfully.

Completed

```
Output folder: C:\Program Files\NetXGATESSLVPN
Extract: icon.ico
Output folder: C:\Program Files\NetXGATESSLVPN\doc
Extract: license.txt
Created uninstaller: C:\Program Files\NetXGATESSLVPN\Uninstall.exe
Starting NetXGATESSLVPN Interactive Service
Checking .NET Framework version...
.NET Framework 4.0 Full found, no need to install.
Proceeding with remainder of installation.
Completed
```

Completing the NetXGATESSLVPN 20.3.1 Setup Wizard

NetXGATESSLVPN 20.3.1 has been installed on your computer.

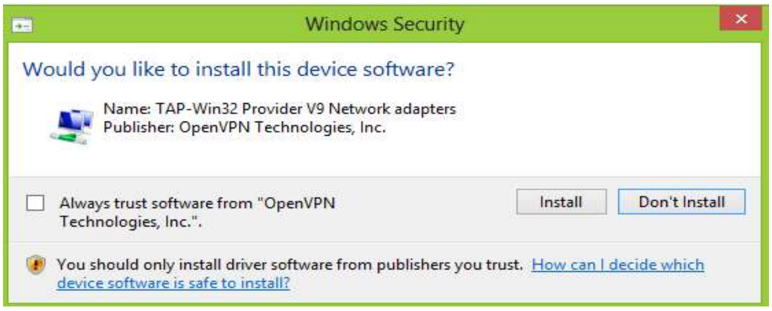
Click Finish to close this wizard.

Pic-7 & 8

Once installation has completed, click Finish .

During installation, you may be asked if you wish to install a SSL Device driver (TAP –Win32" . Allow this by clicking "Install" or "Continue".

If pop-up below windows , Click to Install



Windows Security

Would you like to install this device software?

Name: TAP-Win32 Provider V9 Network adapters
Publisher: OpenVPN Technologies, Inc.

☐ Always trust software from "OpenVPN Technologies, Inc.".

You should only install driver software from publishers you trust. How can I decide which device software is safe to install?

Pic-9

You have now successfully installed the NetXGATE SSL VPN client on PC.

Creating Your First Connection:-

NetXGATE SSL VPN Client can be launched from your Start menu by going to Start->All Programs-> **NetXGATE SSL VPN** -> **NetXGATE SSL VPN GUI** (if you selected the default location), or if you selected to have a desktop icon during install, you will see the NetXGATE SSL VPN GUI Icon on your desktop.

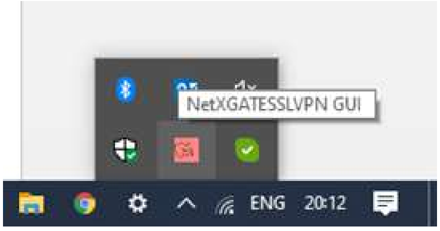
<u>Running NetXGATE SSL VPN Client –</u>

Before Configuring the below part , Pls obtain the details you need to setup your connection. Your IT Team may provide you with the settings and files you need to manually enter into SSL VPN Client , Like Certificate , Username and Its Password .

STEP-2-

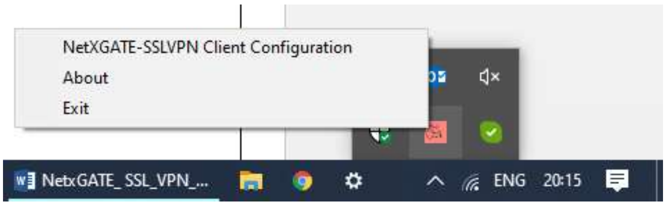
Go to The desktop > NetXGATE SSL VPN GUI > double click.

An icon for the NetXGATE SSL VPN GUI will appear in the lower-right corner "System Tray " of the screen .



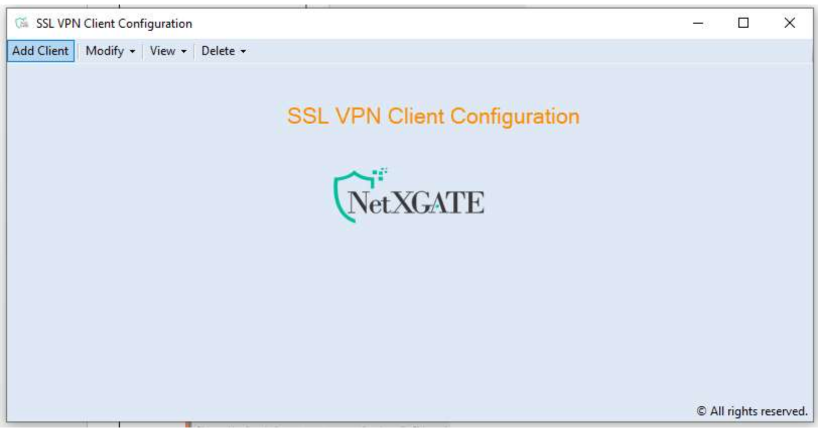
Pic-10

Right click on the ***NetXGATESSL VPN GUI Icon*** (in system-tray applet), and a menu should appear and giving you the option to "***NetXGATE –SSLVPN Client Configuration*** ".*Click Over it* ..



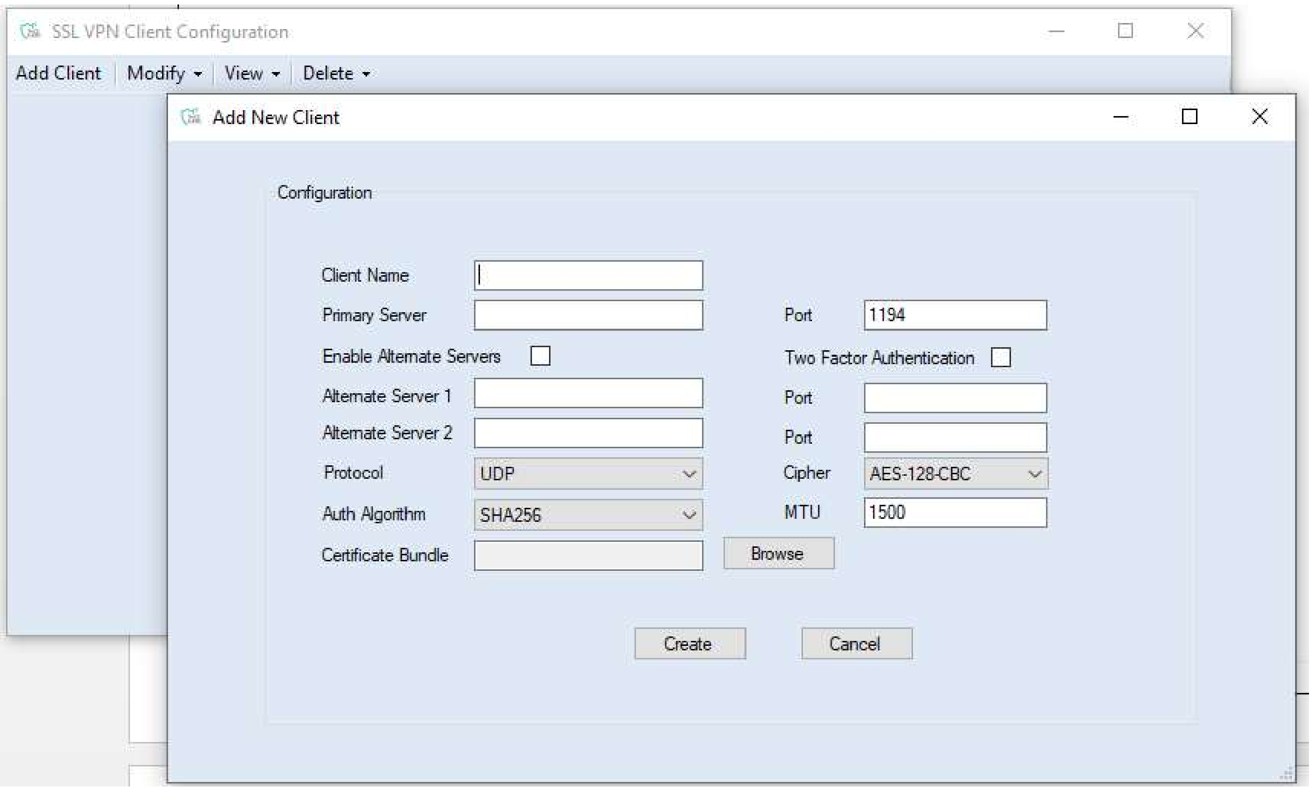
Pic-11

Will open below New window for **'SSL VPN Client Configuration'**-



Pic 12

Navigate to Add Client , will Open a New Configuration window for Creating new Client profile “.



Port: 1194

Enable Alternate Servers ☐

Two Factor Authentication ☐

Protocol: UDP

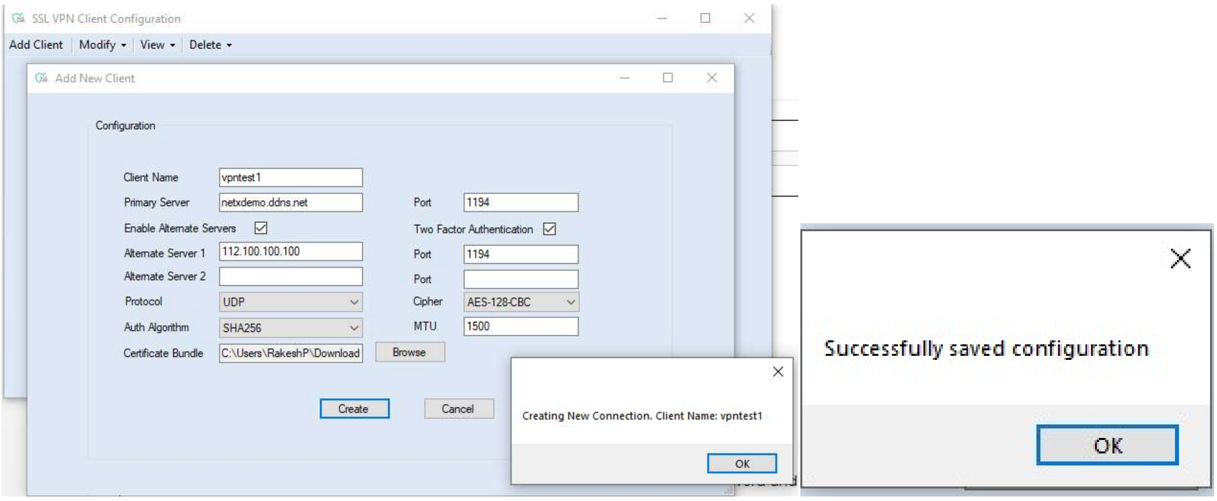
Cipher: AES-128-CBC

Auth Algorithm: SHA256

MTU: 1500

Pic 13

1. Here Configure the ***Client Name*** details provided By IT team.
2. ***Primary Server*** – Public IP which configured In NetXGATE device or. &
3. ***Port*** – Default : 1194 or Shared by IT Team
4. ***Protocol*** – Default: UDP or Shared by IT Team
5. ***Two Factor Authentication*** – If Using any “Two Factor” Like SMS OTP or Google Authenticator- Check it , if Not leave it Blank
6. ***Authentication*** – Default :SHA 256 or Shared by IT Team
7. ***Cipher Type*** - Default: AES-128-CBC or Shared by IT Team
8. ***Certificate Bundle*** – Upload Certificate File (.zip) shared by IT Team
9. Click on “*Create*” to save the configuration.


SSL VPN Client Configuration
Add Client | Modify ▾ | View ▾ | Delete ▾
Add New Client
Configuration
Browse
Create
Cancel
OK
OK

Client Name: vpntest1

Primary Server: netxdemo.ddns.net Port: 1194

Enable Alternate Servers ☑ Two Factor Authentication ☑

Alternate Server 1: 112.100.100.100 Port: 1194

Alternate Server 2: Port:

Protocol: UDP Cipher: AES-128-CBC

Auth Algorithm: SHA256 MTU: 1500

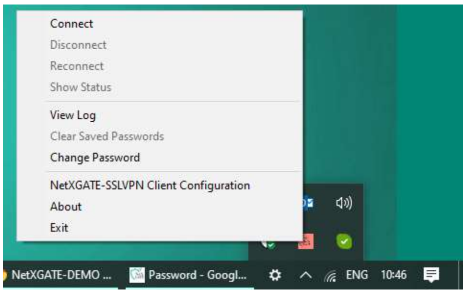
Certificate Bundle: C:\Users\RakeshP\Download

Creating New Connection. Client Name: vpntest1

Successfully saved configuration

Pic 14 & 15

This finished the installation and configuration of SSL VPN client on the user’s machine.



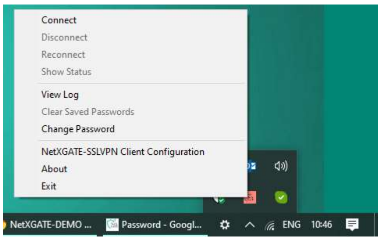
Pic 16

Establish connection

Step 3.-

Login to access network resources or Internet

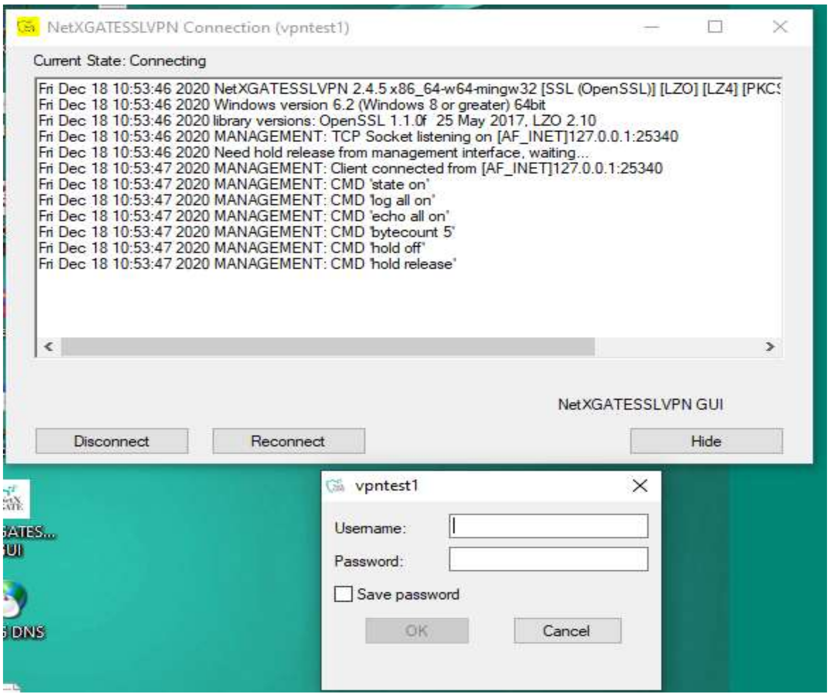
Right click on the ***NetXGATE SSL VPN GUI Icon*** (in system-tray applet), and Your connection will now appear in the NetXGATE SSL VPN Client menu and giving you the option to "***Connect***".



Pic 17

Double click on ***"Connect*** " and it will appear new Window for Password .

Enter here the SSL VPN Passwords which provided by your IT Team .



Current State: Connecting

```
Fri Dec 18 10:53:46 2020 NetXGATESSLVPN 2.4.5 x86_64-w64-mingw32 [SSL (OpenSSL)] [LZO] [LZ4] [PKCS
Fri Dec 18 10:53:46 2020 Windows version 6.2 (Windows 8 or greater) 64bit
Fri Dec 18 10:53:46 2020 library versions: OpenSSL 1.1.0f  25 May 2017, LZO 2.10
Fri Dec 18 10:53:46 2020 MANAGEMENT: TCP Socket listening on [AF_INET]127.0.0.1:25340
Fri Dec 18 10:53:46 2020 Need hold release from management interface, waiting...
Fri Dec 18 10:53:47 2020 MANAGEMENT: Client connected from [AF_INET]127.0.0.1:25340
Fri Dec 18 10:53:47 2020 MANAGEMENT: CMD 'state on'
Fri Dec 18 10:53:47 2020 MANAGEMENT: CMD 'log all on'
Fri Dec 18 10:53:47 2020 MANAGEMENT: CMD 'echo all on'
Fri Dec 18 10:53:47 2020 MANAGEMENT: CMD 'bytecount 5'
Fri Dec 18 10:53:47 2020 MANAGEMENT: CMD 'hold off'
Fri Dec 18 10:53:47 2020 MANAGEMENT: CMD 'hold release'
```

Username:

Password:

□ Save password

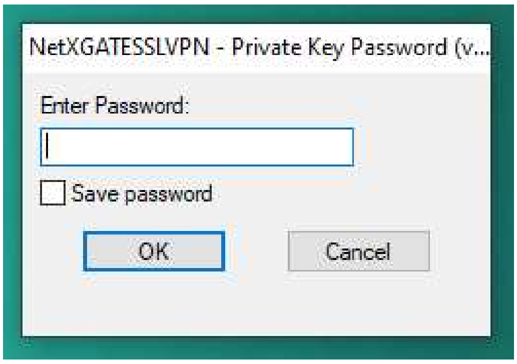
.

Pic-18

Note – *If you Using Dual Authentication – For **SMS OTP**- User name as "SMS" and Password – which shared over OTP and For **Google Authenticator**- User name as "VPN" and Password as shown in Google Authenticator*

Click ***"OK"*** Button.

Again You will get window for master Password .



NetXGATESSLVPN - Private Key Password (v...

Enter Password:

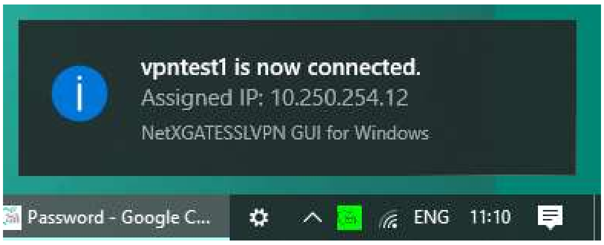
□ Save password

Pic-19

Enter the password and click ***"OK"*** Button.

The icon turns yellow indicating that connection is in progress and turns green the moment connection is established and IP is leased.

When you have successfully connected, you will see a similar bubble message like 'VPNtest1' is now connected'

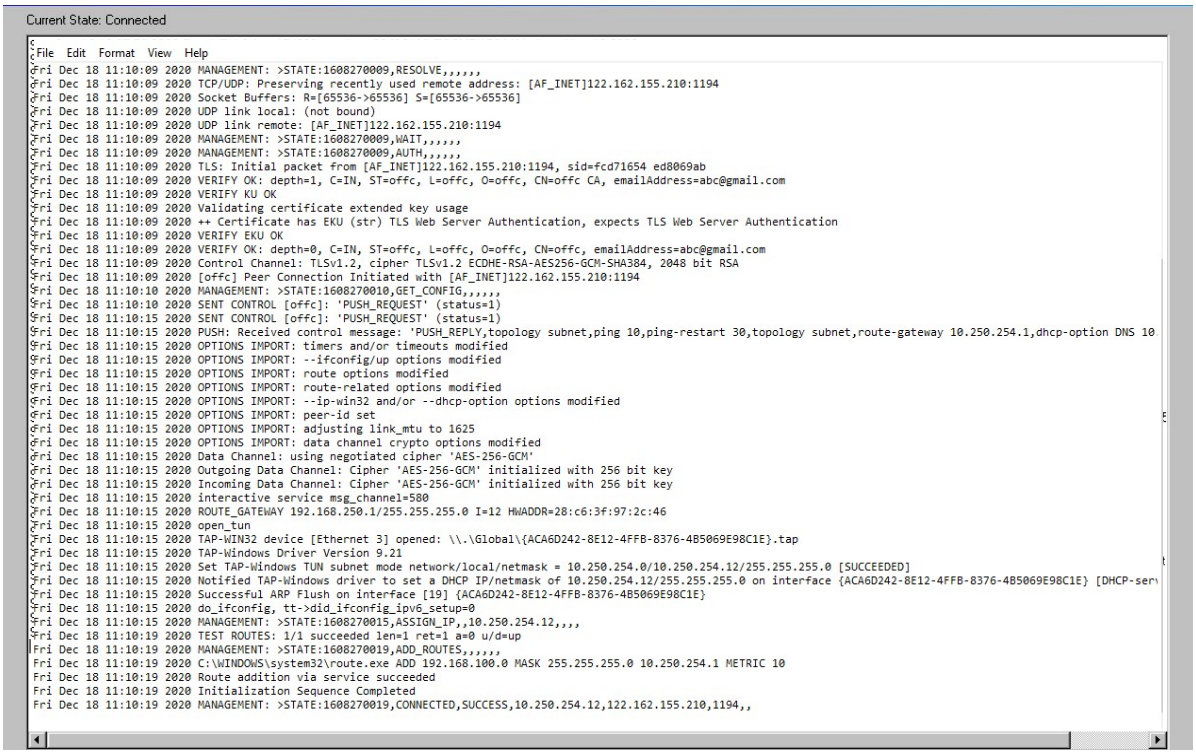


vpntest1 is now connected.
Assigned IP: 10.250.254.12
NetXGATESSLVPN GUI for Windows

Pic-20

Now you successfully connected the Secure VPN .

Similarly you will get also "CONNECTED,SUCCESS" msg like Below window.

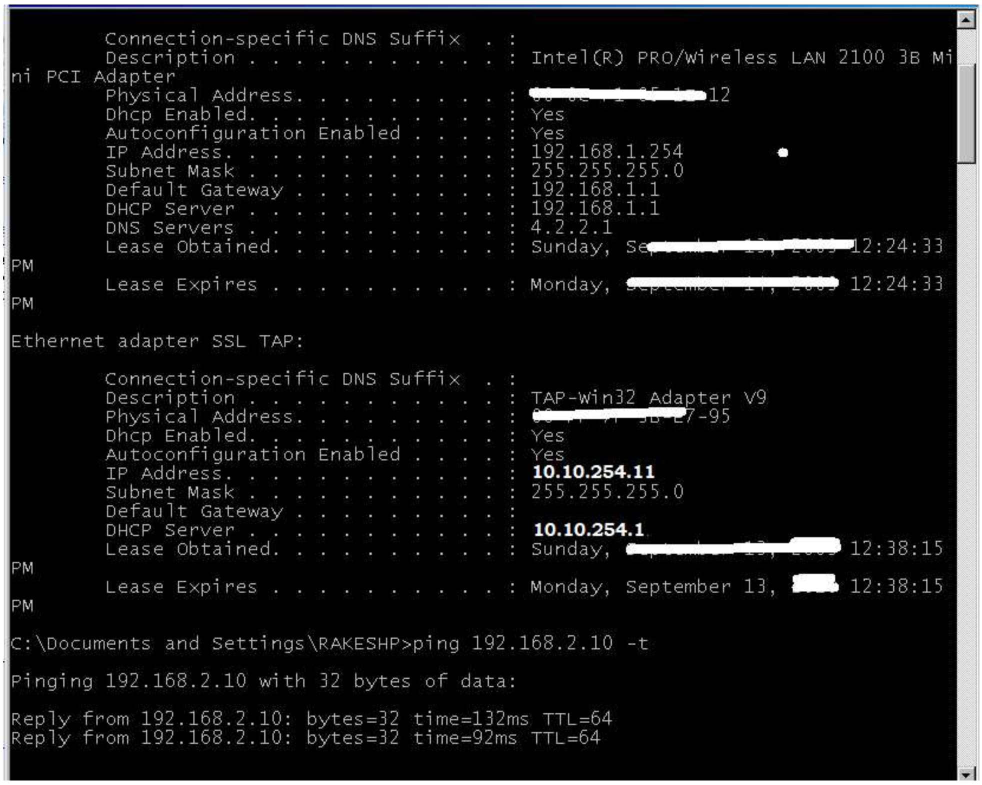


```
Fri Dec 18 11:10:09 2020 MANAGEMENT: >STATE:1608270009,RESOLVE,,,,,,
Fri Dec 18 11:10:09 2020 TCP/UDP: Preserving recently used remote address: [AF_INET]122.162.155.210:1194
Fri Dec 18 11:10:09 2020 Socket Buffers: R=[65536->65536] S=[65536->65536]
Fri Dec 18 11:10:09 2020 UDP link local: (not bound)
Fri Dec 18 11:10:09 2020 UDP link remote: [AF_INET]122.162.155.210:1194
Fri Dec 18 11:10:09 2020 MANAGEMENT: >STATE:1608270009,WAIT,,,,,,
Fri Dec 18 11:10:09 2020 MANAGEMENT: >STATE:1608270009,AUTH,,,,,,
Fri Dec 18 11:10:09 2020 TLS: Initial packet from [AF_INET]122.162.155.210:1194, sid=fcd71654 ed8069ab
Fri Dec 18 11:10:09 2020 VERIFY OK: depth=1, C=IN, ST=offc, L=offc, O=offc, CN=offc CA, emailAddress=abc@gmail.com
Fri Dec 18 11:10:09 2020 VERIFY KU OK
Fri Dec 18 11:10:09 2020 Validating certificate extended key usage
Fri Dec 18 11:10:09 2020 ++ Certificate has EKU (str) TLS Web Server Authentication, expects TLS Web Server Authentication
Fri Dec 18 11:10:09 2020 VERIFY EKU OK
Fri Dec 18 11:10:09 2020 VERIFY OK: depth=0, C=IN, ST=offc, L=offc, O=offc, CN=offc, emailAddress=abc@gmail.com
Fri Dec 18 11:10:09 2020 Control Channel: TLSv1.2, cipher TLSv1.2 ECDHE-RSA-AES256-GCM-SHA384, 2048 bit RSA
Fri Dec 18 11:10:09 2020 [offc] Peer Connection Initiated with [AF_INET]122.162.155.210:1194
Fri Dec 18 11:10:10 2020 MANAGEMENT: >STATE:1608270010,GET_CONFIG,,,,,,
Fri Dec 18 11:10:10 2020 SENT CONTROL [offc]: 'PUSH_REQUEST' (status=1)
Fri Dec 18 11:10:15 2020 SENT CONTROL [offc]: 'PUSH_REQUEST' (status=1)
Fri Dec 18 11:10:15 2020 PUSH: Received control message: 'PUSH_REPLY,topology subnet,ping 10,ping-restart 30,topology subnet,route-gateway 10.250.254.1,dhcp-option DNS 10.
Fri Dec 18 11:10:15 2020 OPTIONS IMPORT: timers and/or timeouts modified
Fri Dec 18 11:10:15 2020 OPTIONS IMPORT: --ifconfig/up options modified
Fri Dec 18 11:10:15 2020 OPTIONS IMPORT: route options modified
Fri Dec 18 11:10:15 2020 OPTIONS IMPORT: route-related options modified
Fri Dec 18 11:10:15 2020 OPTIONS IMPORT: --ip-win32 and/or --dhcp-option options modified
Fri Dec 18 11:10:15 2020 OPTIONS IMPORT: peer-id set
Fri Dec 18 11:10:15 2020 OPTIONS IMPORT: adjusting link_mtu to 1625
Fri Dec 18 11:10:15 2020 OPTIONS IMPORT: data channel crypto options modified
Fri Dec 18 11:10:15 2020 Data Channel: using negotiated cipher 'AES-256-GCM'
Fri Dec 18 11:10:15 2020 Outgoing Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Fri Dec 18 11:10:15 2020 Incoming Data Channel: Cipher 'AES-256-GCM' initialized with 256 bit key
Fri Dec 18 11:10:15 2020 interactive service msg_channel=580
Fri Dec 18 11:10:15 2020 ROUTE_GATEWAY 192.168.250.1/255.255.255.0 I=12 HWADDR=28:c6:3f:97:2c:46
Fri Dec 18 11:10:15 2020 open_tun
Fri Dec 18 11:10:15 2020 TAP-WIN32 device [Ethernet 3] opened: \\.\Global\{ACA6D242-8E12-4FFB-8376-4B5069E98C1E}.tap
Fri Dec 18 11:10:15 2020 TAP-Windows Driver Version 9.21
Fri Dec 18 11:10:15 2020 Set TAP-Windows TUN subnet mode network/local/netmask = 10.250.254.0/10.250.254.12/255.255.255.0 [SUCCEEDED]
Fri Dec 18 11:10:15 2020 Notified TAP-Windows driver to set a DHCP IP/netmask of 10.250.254.12/255.255.255.0 on interface {ACA6D242-8E12-4FFB-8376-4B5069E98C1E} [DHCP-serv
Fri Dec 18 11:10:15 2020 Successful ARP Flush on interface [19] {ACA6D242-8E12-4FFB-8376-4B5069E98C1E}
Fri Dec 18 11:10:15 2020 do_ifconfig, tt->did_ifconfig_ipv6_setup=0
Fri Dec 18 11:10:15 2020 MANAGEMENT: >STATE:1608270015,ASSIGN_IP,,10.250.254.12,,,,
Fri Dec 18 11:10:19 2020 TEST ROUTES: 1/1 succeeded len=1 ret=1 a=0 u/d=up
Fri Dec 18 11:10:19 2020 MANAGEMENT: >STATE:1608270019,ADD_ROUTES,,,,,,
Fri Dec 18 11:10:19 2020 C:\WINDOWS\system32\route.exe ADD 192.168.100.0 MASK 255.255.255.0 10.250.254.1 METRIC 10
Fri Dec 18 11:10:19 2020 Route addition via service succeeded
Fri Dec 18 11:10:19 2020 Initialization Sequence Completed
Fri Dec 18 11:10:19 2020 MANAGEMENT: >STATE:1608270019,CONNECTED,SUCCESS,10.250.254.12,122.162.155.210,1194,,
```

Pic-21

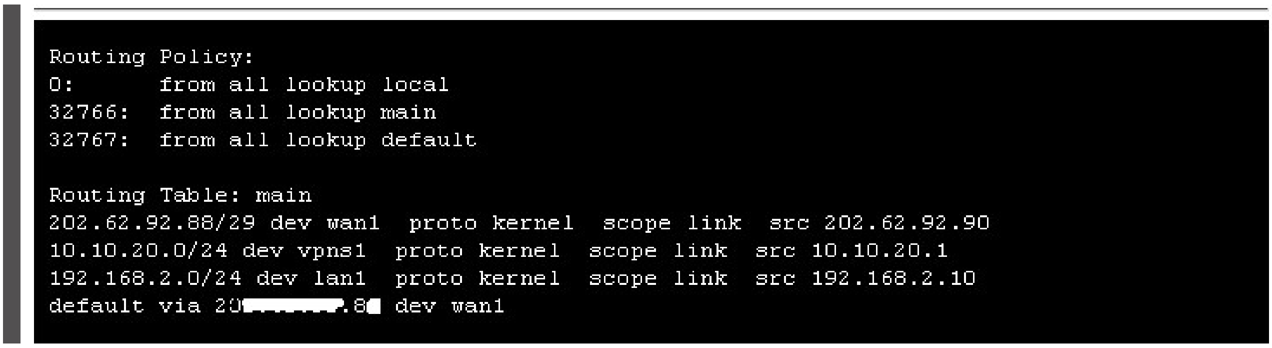
You also Right click the Client icon and click "Disconnect" to disconnect the connection.

After successful connection of Host PC .IPConfig/all will show the below type of details include virtual IP Report-



```
        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Intel(R) PRO/Wireless LAN 2100 3B Mi
ni PCI Adapter
        Physical Address. . . . . . . . . : [redacted]
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.1.254
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.1.1
        DHCP Server . . . . . . . . . . . : 192.168.1.1
        DNS Servers . . . . . . . . . . . : 4.2.2.1
        Lease Obtained. . . . . . . . . . : Sunday, [redacted]12:24:33
PM
        Lease Expires . . . . . . . . . . : Monday, [redacted] 12:24:33
PM

Ethernet adapter SSL TAP:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : TAP-Win32 Adapter V9
        Physical Address. . . . . . . . . : [redacted]7-95
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 10.10.254.11
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . :
        DHCP Server . . . . . . . . . . . : 10.10.254.1
        Lease Obtained. . . . . . . . . . : Sunday, [redacted] 12:38:15
PM
        Lease Expires . . . . . . . . . . : Monday, September 13, [redacted] 12:38:15
PM

C:\Documents and Settings\RAKESHP>ping 192.168.2.10 -t

Pinging 192.168.2.10 with 32 bytes of data:

Reply from 192.168.2.10: bytes=32 time=132ms TTL=64
Reply from 192.168.2.10: bytes=32 time=92ms TTL=64
```

Routing table –At NetXGATE Server end.



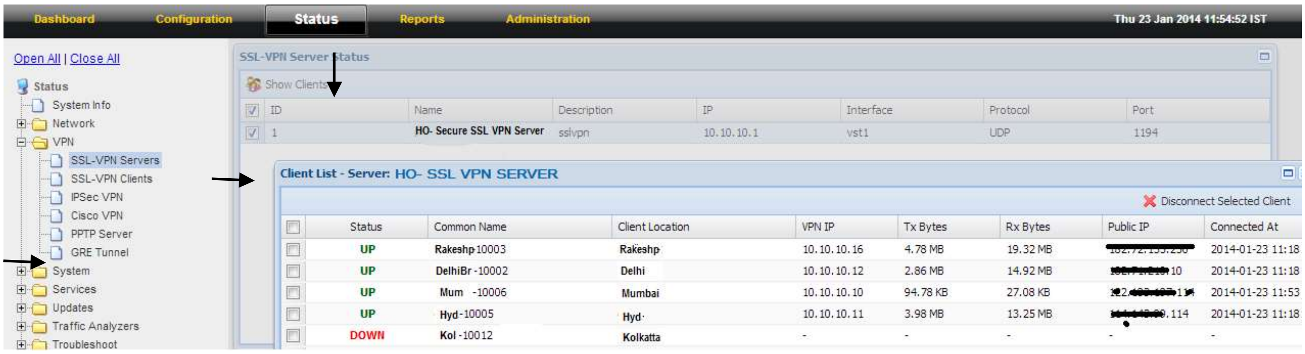
```
Routing Policy:
0:      from all lookup local
32766:  from all lookup main
32767:  from all lookup default

Routing Table: main
202.62.92.88/29 dev wan1  proto kernel  scope link  src 202.62.92.90
10.10.20.0/24 dev vpns1  proto kernel  scope link  src 10.10.20.1
192.168.2.0/24 dev lan1  proto kernel  scope link  src 192.168.2.10
default via 20[redacted].8[redacted] dev wan1
```

Pic- 22

Verifying Client connection state- At SSL VPN Server End (For Admin Only)

Go to Status> VPN> SSL VPN Servers > Select the VPN server then click on Show Client.

Check SSL VPN server connection, here it will show the Active and Inactive Clients.



☑	ID	Name	Description	IP	Interface	Protocol	Port
☑	1	HO- Secure SSL VPN Server	sslvpn	10.10.10.1	vst1	UDP	1194

Client List - Server: HO- SSL VPN SERVER

□	Status	Common Name	Client Location	VPN IP	Tx Bytes	Rx Bytes	Public IP	Connected At
□	UP	Rakeshp 10003	Rakeshp	10.10.10.16	4.78 MB	19.32 MB	[redacted]	2014-01-23 11:18
□	UP	DelhiBr -10002	Delhi	10.10.10.12	2.86 MB	14.92 MB	[redacted]	2014-01-23 11:18
□	UP	Mum -10006	Mumbai	10.10.10.10	94.78 KB	27.08 KB	[redacted]	2014-01-23 11:53
□	UP	Hyd -10005	Hyd·	10.10.10.11	3.98 MB	13.25 MB	[redacted]	2014-01-23 11:18
□	DOWN	Kol -10012	Kolkatta	-	-	-	-	-

Pic-23