

OPENVPN INSTALLATION ON AWS IN VPC


Create an Ubuntu 14 Linux instance with the following security group rules.


Description	Inbound	Outbound	Tags
<div>Edit</div>			
Type <small>i</small>	Protocol <small>i</small>	Port Range <small>i</small>	Source <small>i</small>
Custom UDP Rule	UDP	1194	0.0.0.0/0
SSH	TCP	22	0.0.0.0/0
Custom TCP Rule	TCP	943	0.0.0.0/0
HTTPS	TCP	443	0.0.0.0/0


Then go to the openvpn access server downloads page and download the package for respective Linux server.


Download URL: <https://openvpn.net/index.php/access-server/download-openvpn-as-sw.html>


Download the software package for your OS platform:



Select


Select


Select


Select


Select


Select

```
root@ip-10-100-2-121:~# wget http://swupdate.openvpn.org/as/openvpn-as-2.1.2-Ubuntu14.amd_64.deb
--2016-09-18 19:54:55-- http://swupdate.openvpn.org/as/openvpn-as-2.1.2-Ubuntu14.amd_64.deb
Resolving swupdate.openvpn.org (swupdate.openvpn.org)... 104.24.0.59, 104.24.1.59
Connecting to swupdate.openvpn.org (swupdate.openvpn.org)|104.24.0.59|:80... connected.
HTTP request sent, awaiting response... 200 OK
Length: 31902098 (30M) [application/octet-stream]
Saving to: 'openvpn-as-2.1.2-Ubuntu14.amd_64.deb'

100%[=====]
2016-09-18 19:54:57 (16.8 MB/s) - 'openvpn-as-2.1.2-Ubuntu14.amd_64.deb' saved [31902098/3190209]
```

Once downloaded use dpkg command to install the openvpn access server.

```
root@ip-10-100-2-121:~# dpkg -i openvpn-as-2.1.2-Ubuntu14.amd_64.deb
Selecting previously unselected package openvpn-as.
(Reading database ... 51172 files and directories currently installed.)
Preparing to unpack openvpn-as-2.1.2-Ubuntu14.amd_64.deb ...
Unpacking openvpn-as (2.1.2-Ubuntu14) ...
Setting up openvpn-as (2.1.2-Ubuntu14) ...
The Access Server has been successfully installed in /usr/local/openvpn_as
Configuration log file has been written to /usr/local/openvpn_as/init.log
Please enter "passwd openvpn" to set the initial
administrative password, then login as "openvpn" to continue
configuration here: https://10.100.2.121:943/admin
To reconfigure manually, use the /usr/local/openvpn_as/bin/ovpn-init tool.

Access Server web UIs are available here:
Admin UI: https://10.100.2.121:943/admin
Client UI: https://10.100.2.121:943/
```

Once installed, change the password for openvpn user.

```
root@ip-10-100-2-121:~# passwd openvpn
Enter new UNIX password:
Retype new UNIX password:
passwd: password updated successfully
```

Then open vpn admin console by opening like below.

<https://server-ip-address/admin>

specify username as openvpn and password as which you have just changed above and click login.

Once logged in, go to the Server Network Settings from the left pane, change the Hostname or IP Address to the Public IP address which you got from AWS.



Logout Help

Status

Status Overview
Current Users
Log Reports

Configuration

License
SSL Settings
Server Network Settings
VPN Mode
VPN Settings
Advanced VPN
Web Server
Client Settings

Server Network Settings

VPN Server

Warning: Changing the Hostname, Protocol or Port Number after VPN clients are deployed will cause the existing clients to be unusable (until a new client configuration or VPN installer is downloaded from the Client Web Server)

Hostname or IP Address: 52.32.212.96

Interface and IP Address

- Listen on all interfaces
- eth0: 10.100.2.121

Protocol

- TCP
- UDP
- Both (Multi-daemon mode)

At a glance

Server Status: on More

License: 2 users Info

Current Users: 0 List

Next, go to below the page, and choose save settings to save the settings.

Client Web Server

Users login to the Client Web Server to obtain an auto-generated VPN config or customized VPN Client Installer.

☒ Use the same address and port as the Admin Web Server

☐ Use a different IP address or port:

Save Settings

Next, click on Update Running Server to take in to effect the changes which you saved.

Status

Status Overview
Current Users
Log Reports

Configuration

License

Settings Changed

The active profile 'Default' has been modified and saved.
Press the button below to propagate the changes to the running server.

Update Running Server

VPN Settings

At a glance

Server Status: on More

License: 2 users Info

Current Users: 0 List

Next go to VPN settings page from the left pane. Go to Routing settings and specify all your Public and Private subnet IP Address ranges in the text box. Next go to end of the page choose save settings.

Server Network Settings

VPN Mode

VPN Settings

Advanced VPN

Web Server

Client Settings

Failover

User Management

User Permissions

Group Permissions

Revoke Certificates

Authentication

General

PAM

RADIUS

LDAP

Tools

Profiles

Connectivity Test

Documentation

Support

172.27.224.0 / 20

Static IP Address Network (Optional)

Any static VPN IP addresses specified for particular users on the [User Permissions](#) page must be within this network. It must be different than the Dynamic IP Address Network above.

Network Address / Number of Bits in Netmask

Group Default IP Address Network (Optional)

When a group does not have a specific Dynamic IP Address pool setting, the dynamic IP address pool for the group will be allocated from this list of subnets.

172.27.240.0/20

Routing

Should VPN clients have access to private subnets (non-public networks on the server side)?

☐ No

☒ Yes, using NAT

☐ Yes, using routing (advanced)

Specify the private subnets to which all clients should be given access (as 'network/netmask_bits', one per line):

10.100.2.0/24
10.100.0.0/24
10.100.1.0/24
10.100.3.0/24

Specify all your subnet ranges.

Default Domain Suffix (optional)

Setting a default suffix here will enable Windows clients to resolve host names to FQDN names. This is especially useful if your organisation uses a Windows Domain or Active Directory. Only one default suffix can be defined here.

Default domain suffix:

Save Settings

Next, click on Update Running Server to make changes to take in to effect.

The screenshot shows the 'VPN Settings' page. On the left is a sidebar with 'Status' (Status Overview, Current Users, Log Reports) and 'Configuration' (License). A central blue box contains a green 'Settings Changed' notification: 'The active profile 'Default' has been modified and saved. Press the button below to propagate the changes to the running server.' Below this is a button labeled 'Update Running Server', which is highlighted with a red box and a green arrow. On the right, an 'At a glance' section shows 'Server Status: on' with a 'More' link, 'License: 2 users' with an 'Info' link, and 'Current Users: 0' with a 'List' link.

Next, we will go with user creation and giving users VPN access.

Go to User Permissions from the left pane.

The screenshot shows the 'User Management' sidebar. The 'User Permissions' option is highlighted with a red box and a red arrow. Other options listed are 'Group Permissions' and 'Revoke Certificates'.

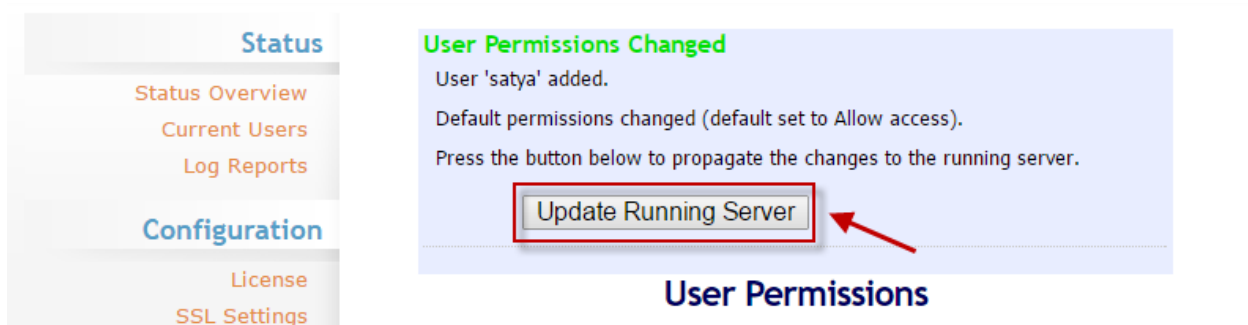
Create a user in Linux and add a password to the user.

Specify a username, click Allow Auto login, and click on save settings.

The screenshot shows the 'Configuration' page. On the left is a sidebar with 'License', 'SSL Settings', 'Server Network Settings', 'VPN Mode', 'VPN Settings' (highlighted with a green arrow), 'Advanced VPN', 'Web Server', 'Client Settings', and 'Failover'. The main content area has a table with columns: Username, Group, More Settings, Admin, Allow Auto-login, Deny Access, and Delete. The first row shows 'openvpn' with group 'No Default Group' and 'Show' link. The second row is for a 'New Username' with the value 'satya' (highlighted with a green box), group 'No Default Group', and 'Show' link. The 'Allow Auto-login' checkbox for the 'satya' user is checked and highlighted with a blue box. Below the table is a checkbox labeled 'Require user permissions record for VPN access'. At the bottom, a 'Save Settings' button is highlighted with a red box and a red arrow.

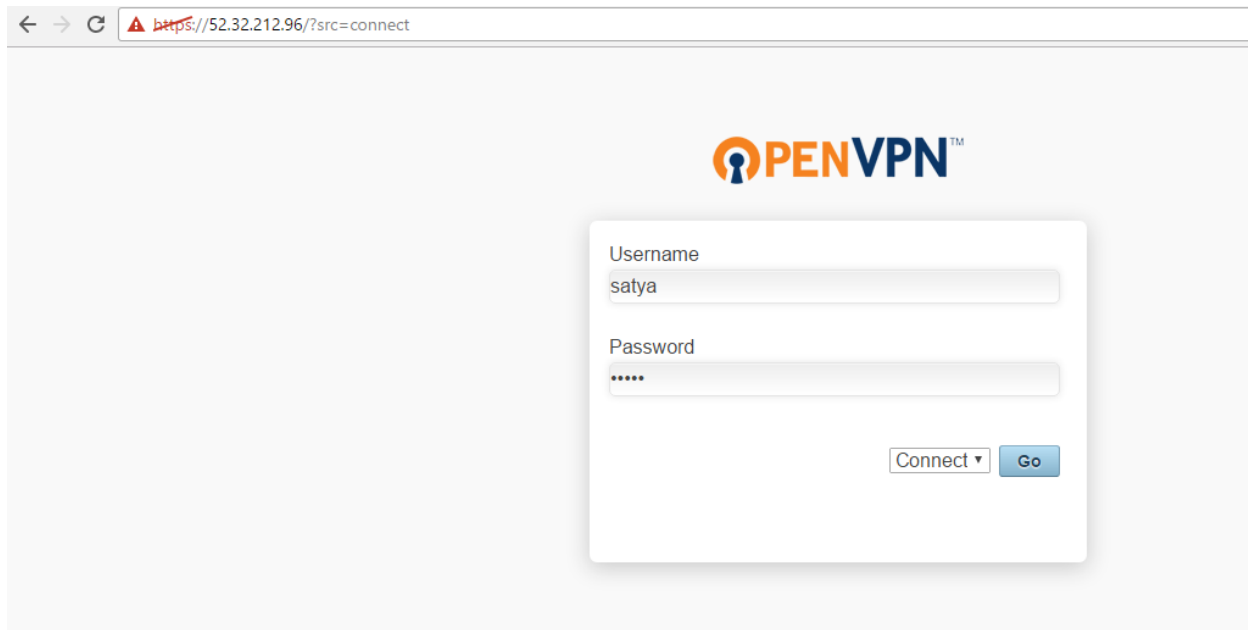
Username	Group	More Settings	Admin	Allow Auto-login	Deny Access	Delete
openvpn	No Default Group	Show	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	
New Username: satya	No Default Group	Show	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>	

Run Update Running Server to effect changes which you saved.



Next, Open below URL and specify user and password credentials then choose Go to connect.

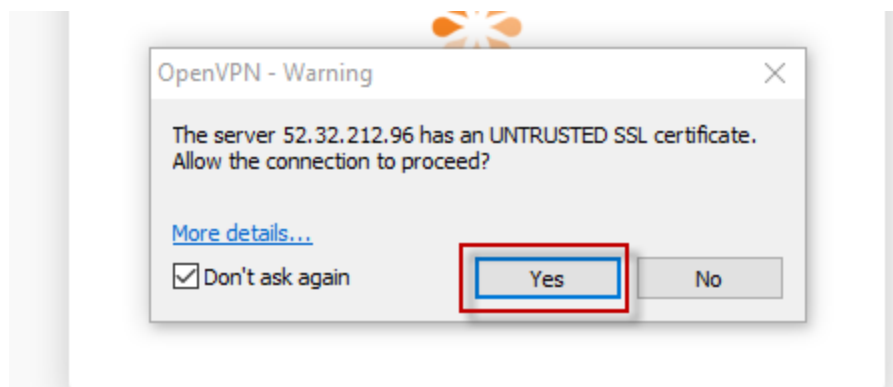
Web URL: <https://your-server-ip-here/>



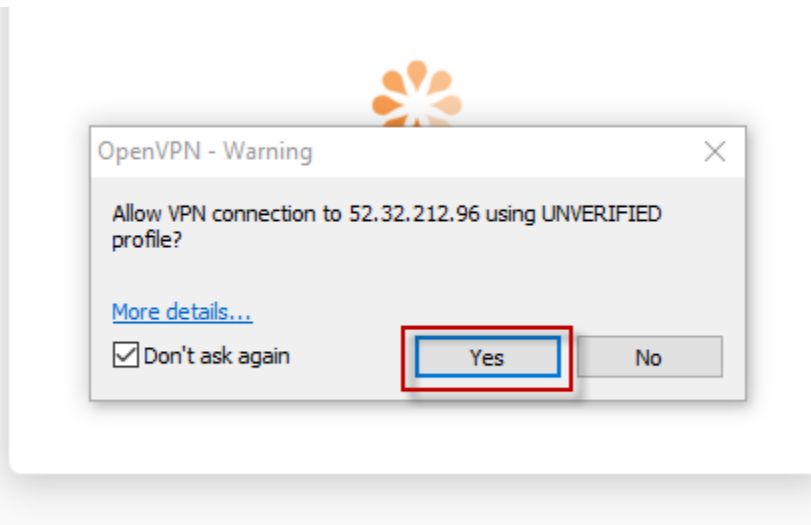
Next choose Yes to allow connection.



Next, choose yes to use untrusted SSL cert.



Next, choose yes to Allow VPN connection.



Once done, you will be presenting with page like below.

Now you can connect to the Private subnet instances over VPN secure connection.

