Amazon Web Services EC2 Tiered Appliance Quick Start

Introduction

The Amazon Web Services EC2 appliance (AMI) is a 64-bit based appliance that is based on Ubuntu LTS (Long Term Support) you can quickly launch on your Amazon EC2/VPC in order to quickly setup your VPN server on the web. To make it more convenient for you to deploy your server in the region closest to you, we currently offer the AMI in all of Amazon's publicly available regions.

If you are looking for the specific AMI ID for one of our images on Amazon AWS for automation purposes, you can find it by going to the AWS Marketplace and going through the launch options until you reach the point where you have to select a region to launch the instance. The appropriate AMI ID will then be displayed to you and you can cancel the launch process then.

Important note about licensing on tiered instances

License keys are not required for instance activation. Charges will be automatically billed to your Amazon AWS account. Charges consist of software license costs for the tiered instances, and the cost of running the instance on EC2 itself. The prices are very clearly mentioned on the Amazon AWS Marketplace. Since licensing goes directly through Amazon's systems, you should take care that a custom security group does not block this licensing traffic. If your Amazon tiered instance with a specified amount of allowed connections is not being licensed properly and you only see 2 allowed connections, see our [troubleshooting page for AMI tiered instance licensing](https://docs.openvpn.net/troubleshooting-problems-with-software-licensing/#Licensing_problems_with_Amazon_AWS_tiered_instances).

Another licensing model we have available is the BYOL (Bring Your Own License) licensing model which is also available on Amazon AWS. We have [a separate guide on how to launch an Amazon AWS EC2 BYOL instance](https://docs.openvpn.net/amazon-web-services-ec2-byol-appliance-quick-start-guide/). The BYOL licensing type works on the BYOL instance on Amazon (not the tiered instances with xx amount of connected devices). But it also works on other OpenVPN Access Server installations on other platforms like Linux, ESXi, HyperV, and so on.

Launching the AMI

To get started, visit the Amazon Marketplace site by clicking [here](https://aws.amazon.com/marketplace). In the search bar that appears, enter **OpenVPN Access Server**, and press **Enter.**



On the results that appear, select the instance size you would like to use. Please note that the **HVM** instance is a **BYOL**instance type, and license keys will be required for instance activation.

For convenient instance activation, select instances that contain the ***connected devices*** suffix. Please note that changing instance types will require an instance relaunch, so appropriate planning is encouraged.



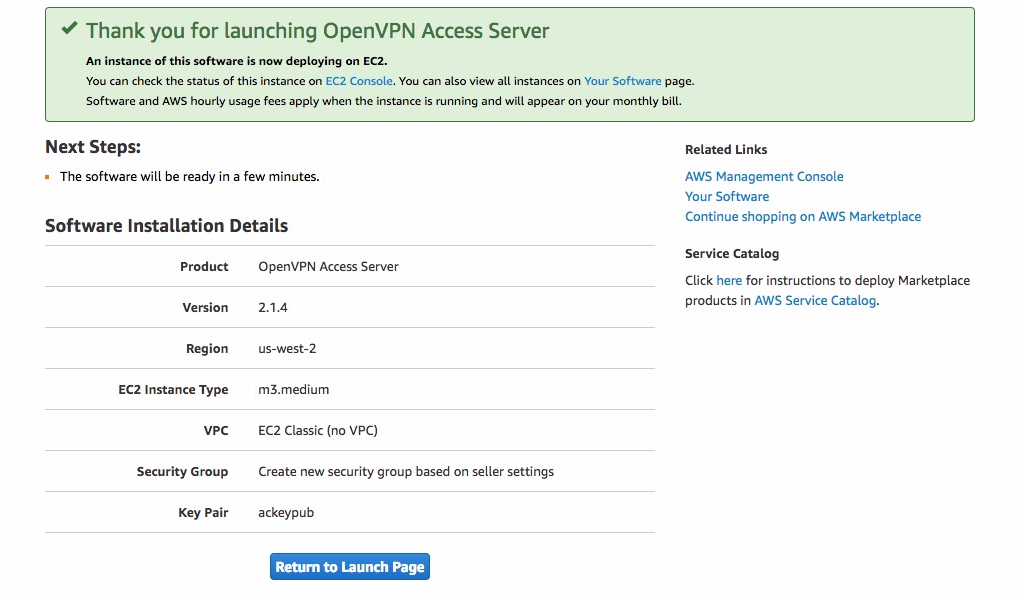
For a simple launch process, follow the instructions below.

Review the instance information on the page, select the region you would like the instance in and click **Continue** to launch the instance.

Instance Launch Options:

* **Version:**The default should launch the latest version available on Amazon Marketplace. It's strongly recommended that you always run the latest version of the software to ensure that security and stability fixes are in place.
* **Region:**Select the region you would like to launch your instance in. The default is US East (N. Virginia).
* **EC2 Instance Type:**Select the instance type you would like to use for your newly launched instance. The micro or small instances should be appropriate for most small workloads, however, you may want to change the instance type to a higher tier if a higher demand is to be expected. Note that some instance types are not available for use when launching into a EC2 network. Please select a VPC network for all instance type availability.
* **VPC Settings:**Select the VPC network or EC2 network you would like to launch the instance in.
* **Security Group:**Select the security group you would like to use for this instance. The seller settings contain all of the default ports you would need in order to configure and access your instance. If you are using a custom security group, please ensure that all of the ports are listed properly so access can be granted appropriately.
* **TCP 22** - SSH, used to remotely administrate your appliance. It is recommended that you restrict this port to trusted IP addresses. If you do not want to do this, leave the source as **0.0.0.0/0**. To restrict ports to a specific subnet, enter the port number, then the subnet in CIDR notation (e.g. **12.34.56.0/24**). For single IP addresses, **/32** will need to be appended at the end (e.g. **22.33.44.55/32** for IP address **22.33.44.55**).
* **TCP 943** - The port number used by the Admin Web UI. By default, the Admin Web UI is also served on port **443**. For security reasons, you can turn this setting off and restrict the Admin Web UI port to trusted IP addresses only.
* **TCP 443** - HTTPS, used by OpenVPN Access Server for the Client Web Server. This is the interface used by your users to log on to the VPN server and retrieve their keying and installation information. It is recommended that you leave this open to the world (i.e. leaving the source as 0.0.0.0/0). The OpenVPN Admin Web UI by default is also enabled on this port, although this can be turned off in the settings. In multi-daemon mode, the OpenVPN TCP daemon shares this port alongside with the Client Web Server, and your clients will initiate TCP based VPN sessions under this port number.
* **UDP 1194** - OpenVPN UDP port, used by your clients to initiate UDP based VPN sessions to the VPN server. This is the preferred way for your clients to communicate and this port should be open to all of your clients. You may change this port number in the settings to a non-standard port in the Admin Web UI if desired.

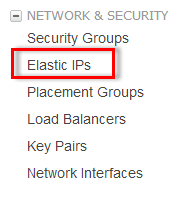
After verifying the instance pricing details, click the **Launch with 1-Click** button to initiate the launching process. The following dialog should appear. You should then be able to access the instance on the EC2 console.



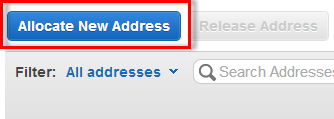
**Important:**The ***Access Software***link in the software subscription portal will ***not*** work until the setup wizard is complete. Please see instructions towards the end of this guide for setup wizard instructions. If the instance was manually launched from the EC2 console with user data information, the setup wizard will be automatically complete upon instance instantiation.

To confirm that the instance has successfully launched, watch the **Instances** section for status. You should see the newly created instance with the same security group and AMI ID you have selected previously.

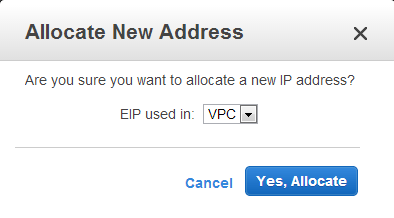
Although not strictly necessary, you should allocate a static IP address for your appliance so the IP address can be reclaimed in case of machine failure/shutdown/reboot. To do so, visit the **Elastic IPs** section in the left navigation panel.



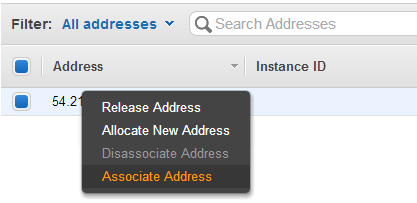
Click the **Allocate New Address** button.



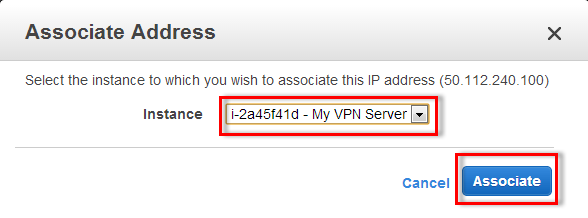
Select the IP address type you would like to allocate. This should match the type of instance you have launched previously. Afterward, click the **Yes, Allocate** button.



Right click the IP address that was created, and then click **Associate Address**.



Select the instance ID this IP address should be associated to. The instance ID can be found in the **Instances** section, and right next to the instance name. In our case, our instance name is **i-99a04ffe**.



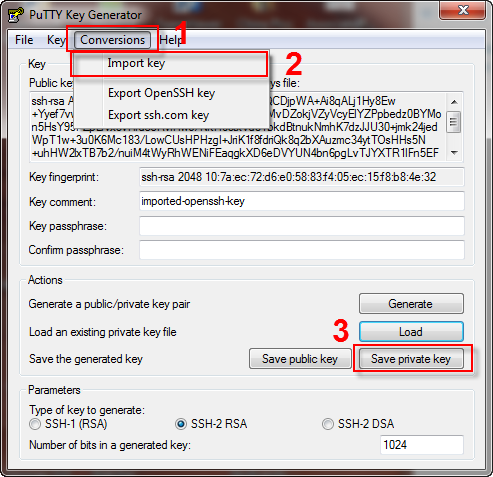
Connecting to your new AMI

Once your new AMI is successfully launched, you will need to SSH into the console using a SSH client software and the private key pair you have used/created previously.  
In this section, we will cover the most common case for users using the **Windows** operating system, and the **PuTTY** SSH client. If you have a different configuration, please follow Amazon's specific instructions on how to connect to your instance.

If you have not done so already, download the **PuTTY** and the **PuTTYgen** tools from this page: http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html

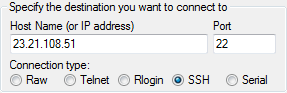
Launch the **PuTTYgen** tool. click **Conversions -> Import Key**. Select the key file you have previously used or generated, and click **Open**.

After **PuTTYgen** has successfully loaded your key file, click the **Save Private Key** button, and save the private key to a safe place. (You may want to protect your private key with a passphrase, although this is not strictly necessary.)

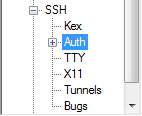


The **PuTTYgen** tool will no longer be needed at this point. To continue, open the **PuTTY** client you have downloaded earlier.

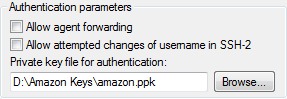
In the **Host name (or IP address)** section, enter the static IP address you have allocated previously. In our case, this is **23.21.108.51**.



Then, on the left navigation panel, navigate to **SSH->Auth**.

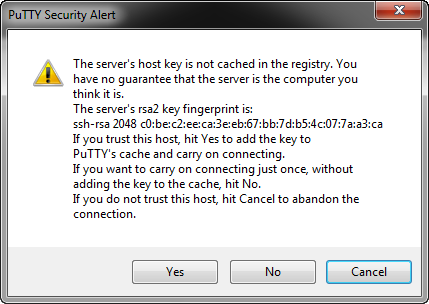


Under the **Private key file for authentication:** section, click **Browse...** and select the private key file that **PuTTYgen** has generated in the previous step.



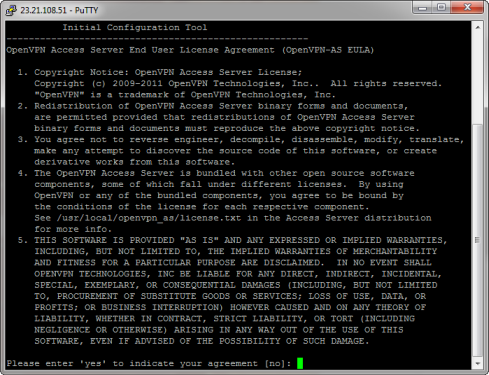
To connect to the server, simply click the **Open** button. However, to simplify the process in the future, you may want to save these settings as a profile. To do so, return to the **Session** category on the top, select a name for your session under the **Saved Sessions** box, and then click the **Save** button. The settings then can be loaded back by double clicking the profile, or by selecting the profile, and then clicking the **Load** button.

Upon connecting, you will receive a warning that **PuTTY** has not seen this server before. It is safe to simply click **Yes** on this dialog.



When prompted, login as **openvpnas**, and then press **Enter**. (**NOTE:** If you are using previous versions of our appliance, the username used is **root** instead of **openvpnas**)

If the private key you have specified was correct, you should now be logged in and the **OpenVPN Access Server Setup Wizard** should now be started. Follow the instructions below to begin configuring your server.



Running the OpenVPN Access Server Setup Wizard

(required, if no Amazon user-data was specified)

The OpenVPN Access Server Setup Wizard runs automatically upon your initial login to the appliance. If you would like to run this wizard again in the future, issue the **sudo ovpn-init --ec2** command in the terminal.

Read through the EULA, and enter **yes** to indicate your agreement.

> Will this be the primary Access Server node?  
**Explanation:** If this is your initial Access Server node, press **Enter** to accept the default setting. Otherwise, if you are setting up your failover node, change this to say **no**.

> Please specify the network interface and IP address to be used by the Admin Web UI:  
**Explanation:** This will be the interface where OpenVPN Access Server will listen to Admin Web UI requests. Make sure you have access to the interface listed otherwise you will be unable to login to your server. If you are uncertain on what interface to use, select option **1** for all interfaces. Do note that if your network did not assign your appliance a DHCP lease or if you are planning to use a static IP for your server, you will need to specify all interfaces here and follow the instructions for assigning a Static IP in the later section of this article. This option may be changed any time after the completion of the wizard in the Web Admin UI.

> Please specify the port number for the Admin Web UI.  
**Explanation:** This is the port you will use to access the web-based administration area. It is usually safe to leave this at the default port unless customization is desired.

> Please specify the TCP port number for the OpenVPN Daemon  
**Explanation:** This is the port clients will use to connect to your VPN server. This port will have to be forwarded to the Internet if your server is behind a NAT-based router. By default, the web-based administration area also runs on this port for your convenience, although this setting can be disabled in the Admin Web UI interface.

> Should client traffic be routed by default through the VPN?  
**Explanation:** If you only have a small network you would like your remote users to connect to over the VPN, select **no**. Otherwise, if you would like everything to go through the VPN while the user is connected (especially useful if you want to secure data communications over an insecure link), select **yes** for this option.

> Should client DNS traffic be routed by default through the VPN?  
**Explanation:** If you would like your VPN clients to able to resolve local domain names using an on-site DNS server, select **yes**for this option. Otherwise, select **no**. Do note that if you selected **yes** for the previous option, all traffic will be routed over the VPN regardless what you set for this option here.

> Use local authentication via internal DB?  
**Explanation:** If you would like OpenVPN Access Server to keep an internal authentication database for authenticating your users, select **yes** for this option. When this option is turned on, you will be able to define and/or change username and passwords within the Admin Web UI. If you select **no** for this option, Linux PAM authentication will be used and you will need to add/change/delete users within the Linux operating system itself. If you would like to use LDAP or RADIUS as your authentication method, you will need to change this after you login to the Web Admin UI.

> Should private subnets be accessible to clients by default?  
**Explanation:** This option defines the default security setting of your OpenVPN Access Server. When **Should client traffic be routed by default through the VPN?** is set to **no**, it defines the list of subnets that your VPN clients are able to access. You are able to add more entries to this list once you login to the Admin Web UI area. This option will have no effect if **Should client traffic be routed by default through the VPN?** is set to **yes**.

> Do you wish to login to the Admin UI as "openvpn"?  
**Explanation:** This defines the initial username in which you would use to login to the Access Server Admin UI area. This username will also serve as your **"lockout"** administrator username shall you ever lock yourself out of your own server. If you would like to specify your own username, select **no**. Otherwise, accept **yes**for the default.  
> > Specify the username for an existing user or for the new user account:  
**Explanation:** Enter the initial username you would like to use instead of the default '**openvpn**'.  
> Type the password for the 'user' account:  
> Confirm the password for the 'user' account:  
**Explanation:** Specify the password you would like to use for the account.

> > Please specify your OpenVPN-AS license key (or leave blank to specify later):  
**Explanation:** If you have purchased a license key for your OpenVPN Access Server software, enter it here. Otherwise, leave it blank. OpenVPN Access Server includes two free licenses for testing purposes.

***After you complete the setup wizard, you can access the Admin Web UI area to configure other aspects of your VPN. Please note that as Amazon does not reveal the elastic/external IP inside the machine, the links displayed within the setup wizard will not work in accessing the web interfaces. For this reason, you will need to replace the internal IP address with the external IP that Amazon has given you. As mentioned previously, you will be able to access the Admin Web UI on both the VPN port and the Admin port unless you disable this behavior in the Admin Web UI.***

Note: If you selected **yes** to the **Do you wish to login to the Admin UI as "openvpn"?**option in the setup wizard, you will need to define the password for this account by running:  
**sudo passwd openvpn**  
and press **Enter**.

Changing Default Hostname

If you did not assign an elastic IP prior to launching the instance, or you have a custom hostname you would like to use, you will need to login to the Web Admin UI and configure the **Hostname** parameter manually (inside the Server Settings section). You may either use an IP address or a hostname here, although it is strongly recommended that you use a hostname since your clients will depend on this setting to be able to know where to connect to, and updating a DNS record is much easier than reinstalling all clients to update the IP address they need to connect to. Also, SSL certificates require a proper FQDN hostname in order to function properly.

**Note: If you leave this setting as the default, NONE of your clients will be able to connect to your VPN server since by default it is set to a non-routable (private) IP address!**

Changing Default Timezone

The default timezone is set to **US (Pacific - Los Angeles)**. If you reside at another timezone and you would like to change this setting, run the following command (you will be asked what timezone you would like to set):

sudo dpkg-reconfigure tzdata

The system will show the new local time after this setting is configured.

Install NTP client for automatic time synchronization

This is recommended for all situations but especially for people that want to use Google Authenticator.

apt-get install ntp

Disabling Source/Dest checking (recommended)

If your VPN setup consists of a site-to-site setup between your cloud instances and your machines on-premises, you will need to disable source destination check protection on Amazon, otherwise routing will not function properly. To do this, right click on the VPN instance, select **Change Source/Dest. Check** and make sure the status is **Disabled**. This setting must also be used if for for example want traffic from your VPC to go directly to the IP addresses of your VPN clients in the VPN client subnet or this security feature will block the traffic.

Set up static routes if necessary

By default, the OpenVPN Access Server gives VPN clients access to your VPC by using the NAT method (Network Address Translation). Using this method, traffic originating from the VPN clients will appear to be coming from the local IP address of the Access Server. For that reason, routing is not necessary and is much easier to implement. However, one drawback of using such method is that traffic from the VPC itself cannot directly access a VPN client as the NAT engine prevents such direct contact. In order to allow a VPN client to be directly addressable via the VPC, you will need to configure the Access Server to use the routing method instead of NAT. Once that is done, the source IP address of packets coming from the VPN clients is kept intact, and direct access from the VPC network to the VPN client subnet is then possible. However, because the VPC does not automatically recognize the VPN subnet within the VPN instance, it does not know how to send the return traffic back to the instance. To correct this problem, you will need to add a static route in the Amazon routing table for your VPC so that the return traffic flows properly. To learn how to do this see this document on Amazon AWS VPC routing:

* <https://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/VPC_Route_Tables.html>

Updating Operating System Software (recommended)

From the time we have generated the appliance and the time you have downloaded and are using the appliance, operating system updates might have become available. To make sure your appliance operating system is up to date, execute the following commands:

sudo apt-get update

sudo apt-get upgrade