Aviatrix User VPN on the AWS Cloud

Quick Start Reference Deployment

June 2018

Jing Zhou, Sunil Kishen — Aviatrix Systems
Shivansh Singh— Amazon Web Services

This Quick Start deployment guide was created by Aviatrix Systems in partnership with Amazon Web Services (AWS). Aviatrix Systems is an AWS Advanced Technology and Networking Competency Partner.

Quick Starts are automated reference deployments that use AWS CloudFormation templates to deploy key technologies on AWS, following AWS best practices.

Overview

This Quick Start reference deployment guide provides step-by-step instructions for deploying the Aviatrix User VPN service on the AWS Cloud.

This Quick Start uses AWS APIs to automatically deploy an Aviatrix Controller for a User VPN service in a new or existing virtual private cloud (VPC). You can connect to VPCs in the AWS Cloud with enhanced security, and access your Amazon Elastic Compute Cloud (Amazon EC2) instances, applications, and services.

User VPN

Aviatrix provides a cloud-native, feature-rich User VPN solution that enables secure remote access for users to connect to AWS by using the Aviatrix SSL VPN service.

The solution is based on OpenVPN and is compatible with all OpenVPN clients. Aviatrix provides its own client that supports Security Assertion Markup Language (SAML) authentication directly from the client.

Secure remote access enables employees to connect to their AWS Cloud workloads from locations that aren't directly connected to AWS. You can also enable secure remote access for contractors, partners, and their customers. The Aviatrix User VPN service allows you to attach profiles to users, so that they're only allowed to access authorized resources or workloads.

Once you've used this Quick Start to deploy the Aviatrix Controller in one of your VPCs, the User VPN configuration wizard in the controller helps you deploy the Aviatrix gateways that host the User VPN service in high-availability (HA) mode. You can also use the controller to manage users and to configure their authentication mechanisms and access policies.

For more information about the Aviatrix User VPN, see Aviatrix OpenVPN FAQs in the Aviatrix documentation.

Benefits of Aviatrix User VPN

The Aviatrix User VPN includes the following benefits:

- **Centralized controller with User VPN wizard.** Point-and-click, centralized management console (with REST API support) manages distributed gateways that CloudOps and network engineers can operate. No deep networking skills are required, and no network router command-line interface (CLI) knowledge is needed. You can use the Aviatrix Controller to implement changes or customizations quickly and easily.
- **Many authentication options.** Lightweight Directory Access Protocol/Active Directory (LDAP/AD), Duo, Okta, multi-factor authentication (MFA), Client Security Assertion Markup Language (SAML), and other types of authentication.
- **Profile-based access control.** Answers "who can access what VPC?" You can assign each VPN user to a profile that gives access privileges to a multicloud network, even down to the level of hosts, protocols, and ports.
- **Broad client support.** Compatible with all OpenVPN® and Aviatrix SAML clients.
- **Performance at scale.** You can place instances behind a load balancer to handle many users.
- **Logging integration.** You can log sessions, connection history, and bandwidth usage to Splunk, Sumo Logic, Elasticsearch, Logstash, and Kibana (ELK Stack), remote syslog, and Datadog.
- **Cost-effective.** Low connections-per-hour pricing, optionally added to your AWS bill.

Costs and Licenses

You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using this Quick Start.

The AWS CloudFormation template for this Quick Start includes configuration parameters that you can customize. Some of these settings, such as instance type, will affect the cost of deployment. For cost estimates, see the pricing pages for each AWS service you will be using. Prices are subject to change.

Additionally, the solution creates a unique AWS Key Management Service (AWS KMS) customer master key (CMK), which has a low monthly cost, to protect network configuration information. For details, see the AWS KMS pricing webpage.

You are also responsible for the Aviatrix license that is required to deploy the Aviatrix User VPN solution. As explained in Step 2: Subscribe to the Aviatrix AMI of the deployment steps, you subscribe to an Amazon Machine Image (AMI) for Aviatrix software in AWS Marketplace, choosing the Aviatrix Secure Networking Platform PAYG - Metered licensing option. This is an hourly-subscription license based on the prices listed in AWS Marketplace. With this pay-as-you-go license, you can build and scale your User VPN service to any size.

Architecture

This Quick Start sets up a secure Aviatrix User VPN solution that includes the Aviatrix Controller and Aviatrix gateways in a highly available configuration. You can create a new VPC or use an existing VPC.

Deploying this Quick Start for a new VPC with **default parameters** builds the following User VPN solution in the AWS Cloud.

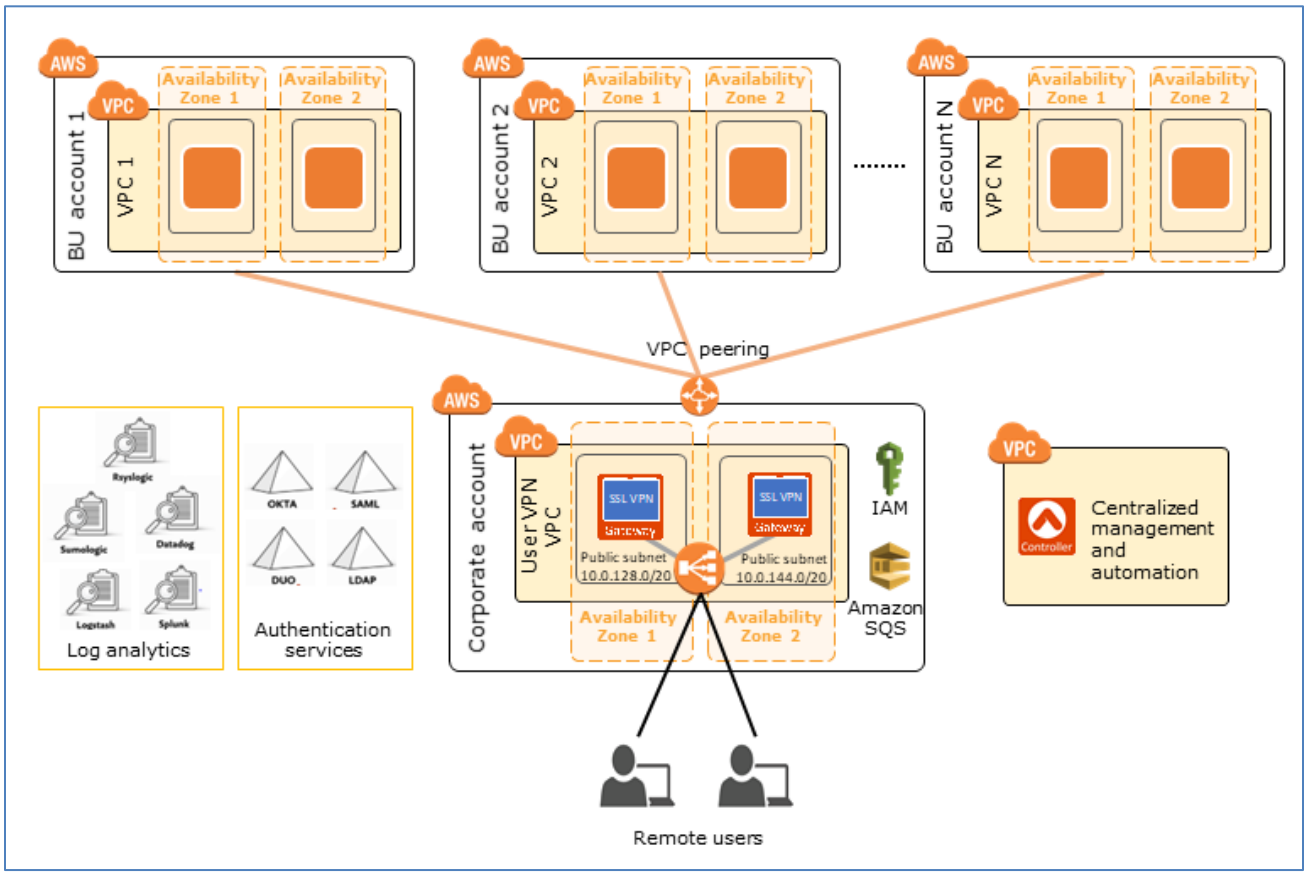


Figure 1: Aviatrix User VPN architecture

This architecture diagram shows the end to end solution, which includes:

- The Aviatrix Controller
- Aviatrix gateways (deployed behind an AWS Elastic Load Balancing load balancer for scaling out and high availability)
- Log analytics
- Authentication services

The gateways allow for SSL VPN termination, routing, and security policies. The Aviatrix Controller also provides a user-friendly interface for further customizing User VPN services, and enables monitoring and cloud network visualization.

Quick Start Components

The Quick Start sets up the functional and automation components shown in Figure 2.

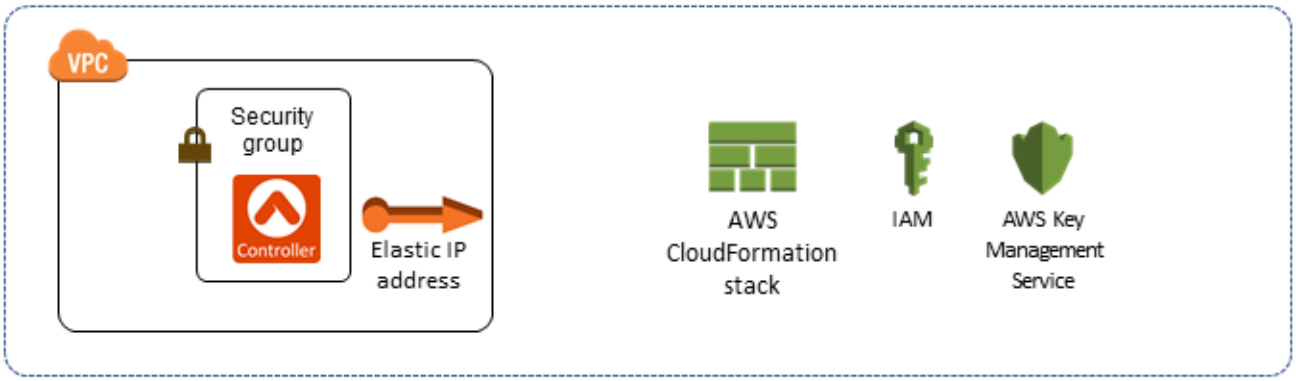


Figure 2: Quick Start components of the Aviatrix User VPN on AWS

It creates, deploys, and configures the following components and services, mapped to Figure 2:

1. An EC2 instance for the Aviatrix Controller
2. An Aviatrix security group (named **AviatrixSecurityGroup**)
3. An Elastic IP (EIP) assigned to the Aviatrix Controller
4. An Aviatrix IAM EC2 role and attached policy
5. An Aviatrix IAM App role and attached policy
6. AWS Key Management Service (KMS)

Additional Functionality

After you deploy the Quick Start and take advantage of the User VPN Wizard to establish your User VPN service, you can extend the environment beyond the AWS Cloud. By using the Aviatrix Controller, you can configure VPN access to other VPCs, other network providers, on-premises infrastructure, or even other public cloud providers. See Configuring Aviatrix User SSL VPN for detailed documentation.

Prerequisites

Specialized Knowledge

Before you deploy this Quick Start, we recommend that you become familiar with the following AWS services. (If you are new to AWS, see Getting Started with AWS.) You don't need advanced networking skills to deploy and maintain the Aviatrix environment on AWS.

- Amazon EC2
- Amazon SQS
- Amazon VPC

License Requirements

By default, this Quick Start deploys an Aviatrix Controller with Metered license included in the AWS Marketplace AMI for Aviatrix Secure Networking Platform PAYG - Metered

Technical Requirements

AWS Accounts

You will need an AWS account to deploy this Quick Start. Once the Quick Start deploys the Aviatrix Controller, you can add one or more AWS accounts, and connect spoke VPCs in those AWS accounts. You can also connect spoke VPCs across different AWS Regions.

> **Note** The Aviatrix Controller supports multiple AWS accounts. Use the Aviatrix Controller to add multiple accounts. For more information, see the Aviatrix Onboarding and Account FAQs documentation.

IAM Requirements

This Aviatrix User VPN Quick Start requires the following IAM roles to be created in the primary AWS account:

- An Aviatrix role for EC2 (`aviatrix-role-ec2`) with a corresponding role policy (`aviatrix-assume-role-policy`). See policy details.
- An Aviatrix role for apps (`aviatrix-role-app`) with a corresponding role policy (`aviatrix-app-policy`). See policy details.

You can configure the IAM roles for the primary AWS account in one of the following ways:

- If this is the first time you're launching the Aviatrix Controller, this Quick Start creates the required IAM roles. See Quick Start Deployment Option 1 and Option 2.
- If the required IAM roles already exist, select **aviatrix-role-ec2** in the Quick Start Deployment Option 1 and Option 2.

> **Important** If you have existing Aviatrix IAM roles, make sure they are up to date by checking the preceding links for policy details.

Deployment Options

This Quick Start provides two deployment options:

- **Deploy Aviatrix into a new VPC** (end-to-end deployment). This option builds a new AWS environment consisting of a VPC, subnets, internet gateway, default route, and other infrastructure components, and then deploys an Aviatrix Controller.
- **Deploy Aviatrix into an existing VPC**. This option provisions an Aviatrix Controller into an existing VPC.

The Quick Start provides separate templates for these options. It also lets you configure CIDR blocks, instance types, and Aviatrix settings, as discussed later in this guide.

> **Note** The Aviatrix Controller is normally deployed in a Shared Services VPC where your DevOps and management tools and services are hosted.

Deployment Steps

Step 1. Prepare Your AWS Account

1. If you don't already have an AWS account, create one at https://aws.amazon.com by following the on-screen instructions.
2. Use the region selector in the navigation bar to choose the AWS Region where you want to deploy the Aviatrix User VPN service on AWS.
3. Create a key pair in your preferred region.
4. If necessary, request a service limit increase for the EC2 instance type that you want to use for the Aviatrix Controller (by default, t2.large. You might need to do this if you already have an existing deployment that uses these instance types, and you think you might exceed the default limit with this deployment.

Step 2. Subscribe to the Aviatrix AMI

1. Log in to the AWS Marketplace at https://aws.amazon.com/marketplace.
2. Open the page for Aviatrix Secure Networking Platform PAYG - Metered. For more information about this option, see License Requirements earlier in this guide.
3. Choose **Continue to Subscribe**, as shown in Figure 3.

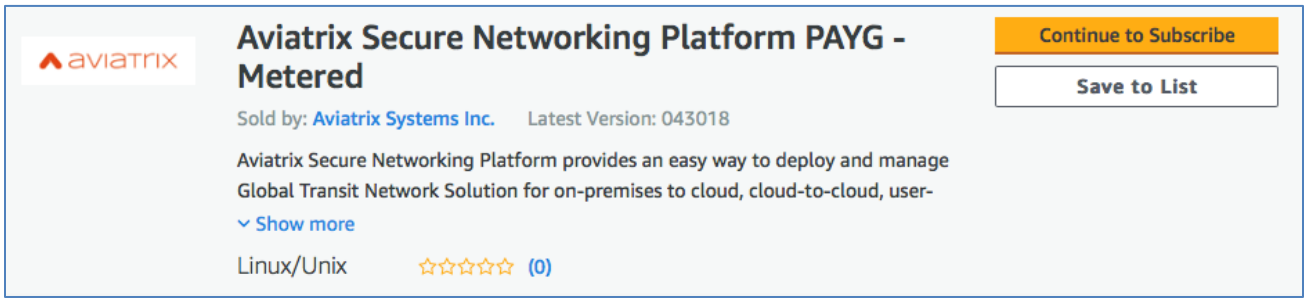


Figure 3: Subscribing to the AMI, with the required license

4. On the **Subscribe to this software** page, read the license agreement, and then choose **Accept Terms**, as shown in Figure 4.

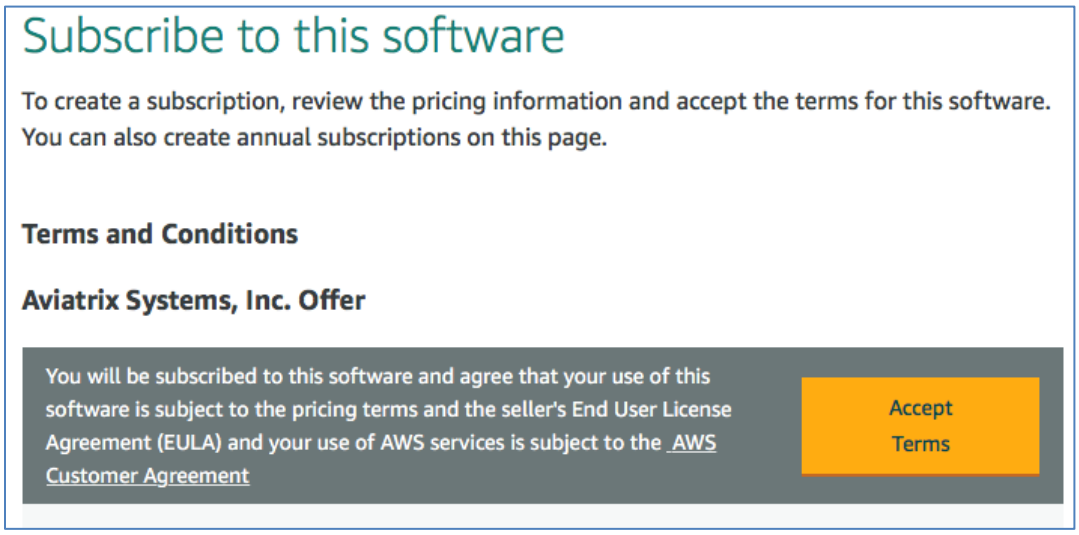


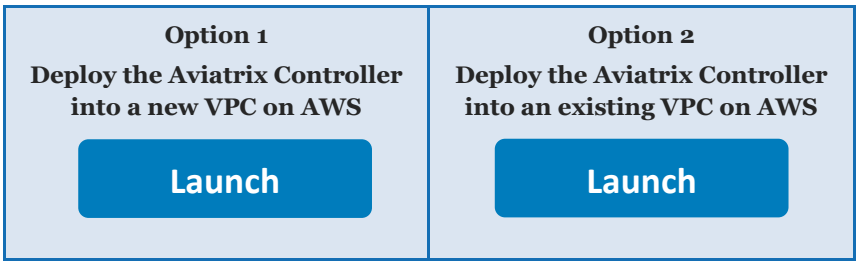
Figure 4: Subscribing to the AMI—Accept Terms

> **Important** After you've finished subscribing in step 4, do not choose **Continue to Configuration**. The Quick Start will handle this.

Step 3. Launch the Quick Start

> **Note** You are responsible for the cost of the AWS services used while running this Quick Start reference deployment. There is no additional cost for using this Quick Start. For full details, see the pricing pages for each AWS service you will be using in this Quick Start. Prices are subject to change.

1. Choose one of the following options to launch the AWS CloudFormation template into your AWS account. For help choosing an option, see deployment options earlier in this guide.



   This deployment takes about 10-15 minutes to complete.

2. Check the region that's displayed in the upper-right corner of the navigation bar, and change it if necessary. *This is where the network infrastructure for your Aviatrix User VPN solution will be built*. The template is launched in the US East (N. Virginia) Region by default.
3. On the **Select Template** page, keep the default setting for the template URL, and then choose **Next**.
4. On the **Specify Details** page, the stack name field is pre-populated; change it if needed. Review the parameters for the template. Provide values for the parameters that require input. For all other parameters, review the default settings and customize them as necessary. When you finish reviewing and customizing the parameters, choose **Next**.
5. In the following tables, parameters are listed by category and described separately for the two deployment options:
   - Parameters for deploying Aviatrix Controller into a new VPC
   - Parameters for deploying Aviatrix Controller into an existing VPC

- **Option 1: Parameters for deploying Aviatrix Controller into a new VPC**

View template

Network Configuration:

Parameter label (name)	Default	Description
VPC CIDR (VPCCIDR)	10.0.0.0/16	The CIDR block for the VPC.
Public Subnet 1 CIDR (PublicSubnet1CIDR)	10.0.10.0/24	The CIDR block for the public (DMZ) subnet located in Availability Zone 1. This is where the Aviatrix Controller will be deployed.
Public Subnet 2 CIDR (PublicSubnet2CIDR)	10.0.20.0/24	The CIDR block for the public (DMZ) subnet located in Availability Zone 2. This is where the high availability hub gateway will be deployed.
Availability Zones (AvailabilityZones)	*Requires input*	The list of Availability Zones to use for the subnets in the VPC. The Quick Start uses two Availability Zones from your list and preserves the logical order you specify.

Amazon EC2 Configuration:

Parameter label (name)	Default	Description
Key Pair (KeyNameParam)	*Requires input*	A public/private key pair, which allows you to connect securely to the Aviatrix Controller instance after it launches. When you created an AWS account, this is the key pair you created in your preferred region.
Aviatrix Controller Instance Type (InstanceTypeParam)	t2.large	The instance size for the controller. The default is t2.large.

IAM Roles:

Parameter label (name)	Default	Description
Create the IAM Roles (IAMRoleParam)	**New**	Determine if IAM roles aviatrix-role-ec2 and aviatrix-role-app should be created. Select **New** if an Aviatrix IAM role has not been created (first-time launch). Select **aviatrix-role-ec2** if there is already an Aviatrix IAM role created.

AWS Quick Start Configuration:

Parameter label (name)	Default	Description
Quick Start S3 Bucket Name (QSS3BucketName)	aws-quickstart	The S3 bucket you have created for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. The bucket name can include numbers, lowercase letters, uppercase letters, and hyphens, but should not start or end with a hyphen.
Quick Start S3 Key Prefix (QSS3KeyPrefix)	quickstart-aviatrix-controller/	The S3 key name prefix used to simulate a folder for your copy of Quick Start assets, if you decide to customize or extend the Quick Start for your own use. This prefix can include numbers, lowercase letters, uppercase letters, hyphens, and forward slashes.

- **Option 2: Parameters for deploying Aviatrix Controller into an existing VPC**

View template

Network Configuration:

Parameter label (name)	Default	Description
VPC ID (VPCID)	*Requires input*	The ID of your existing VPC where the Aviatrix Controller will be deployed.(e.g., vpc-0343606e)
Public Subnet ID (SubnetID)	*Requires input*	The Aviatrix Controller must be launched on a public subnet.

Amazon EC2 Configuration:

Note Make sure you have subscribed to the Aviatrix PAYG (Metered) AMI on AWS Marketplace.

Parameter label (name)	Default	Description
Key Pair (KeyNameParam)	*Requires input*	A public/private key pair, which allows you to connect securely to the Aviatrix Controller instance after it launches. When you created an AWS account, this is the key pair you created in your preferred region.
Aviatrix Controller Instance Type (InstanceTypeParam)	t2.large	The instance size for the controller. The default is t2.large.

IAM Roles:

Parameter label (name)	Default	Description
Create the IAM Roles (IAMRoleParam)	New	Determine if IAM roles aviatrix-role-ec2 and aviatrix-role-app should be created. Select **New** if an Aviatrix IAM role has not been created (first-time launch). Select **aviatrix-role-ec2** if there is already an Aviatrix IAM role created.

6. On the **Options** page, you can specify tags (key-value pairs) for resources in your stack and set advanced options. These are all options and can be configured later. When you're done, choose **Next**.
7. On the **Review** page, review and confirm the template settings. Under **Capabilities**, select the check box to acknowledge that the template will create IAM resources.
8. Choose **Create** to deploy the stack. You may need to refresh the browser or console to see the status.
9. Monitor the status of the stacks. A primary stack and other nested stacks will be created. When the statuses are **CREATE_COMPLETE**, the Aviatrix User VPN is ready.

> **Note** This Quick Start creates the EC2 instance that runs the Aviatrix Controller AMI. This instance is termination-protected. If you delete the Quick Start stack, you must manually turn off Termination Protection on the Aviatrix Controller EC2 instance before you delete the CloudFormation stack. You can change Termination Protection by using the Amazon EC2 console.

10. Click the primary stack, and then click the **Outputs** tab to view the AWS account ID, and the public and private IPs of the Aviatrix Controller, as shown in Figure 4. You will need these IP addresses to access the Controller console in the next step.

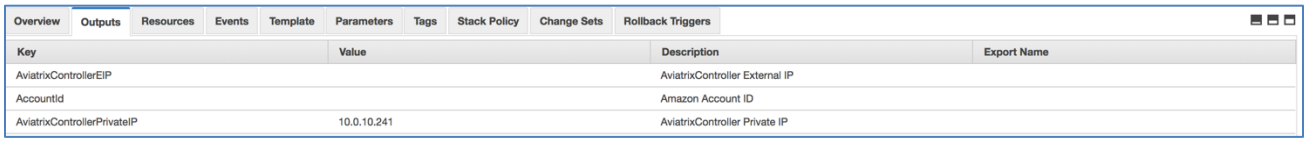


Figure 4: Stack outputs

Step 4. Initial Setup of the Aviatrix Controller

1. Use the public address of the controller (**AviatrixControllerEIP**=*x.x.x.x*) in your web browser to access the Aviatrix Controller console (https://*x.x.x.x*/). You can see the public address of the controller in the **Outputs** tab (shown in Figure 4).

   Note To access the site, you must prefix the IP address with https://.

   Also, because a new instance was just created, you will see a browser message that "Your connection is not private." This message appears because there is a self-signed SSL certificate on your new instance. You may ignore this warning. Depending on your browser, you may need to select **Advanced** > **Proceed** or **Show Details** > **Visit this website**. Later, you can remove this warning by uploading your own signed certificates.

   Use the default user name **admin** and your controller's private IP address "x.x.x.x" (AviatrixControllerPrivateIP) as the password to log in to your controller. You can see the private IP address of the controller in the primary **Outputs** tab (shown in Figure 4).

2. Enter your email address, as shown in Figure 5. This email is used for alerts and password recovery (if needed).

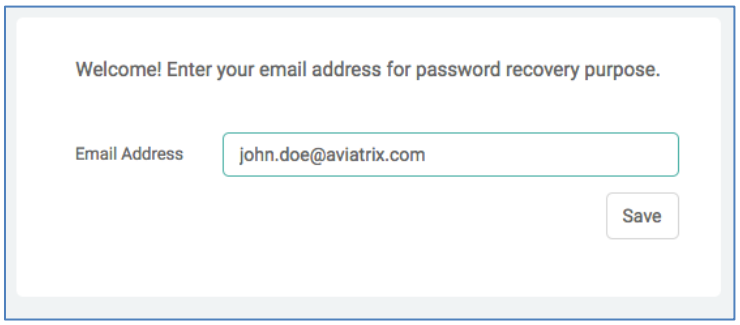


Figure 5: Entering the email address for password recovery

3. Change your admin password, as shown in Figure 6.

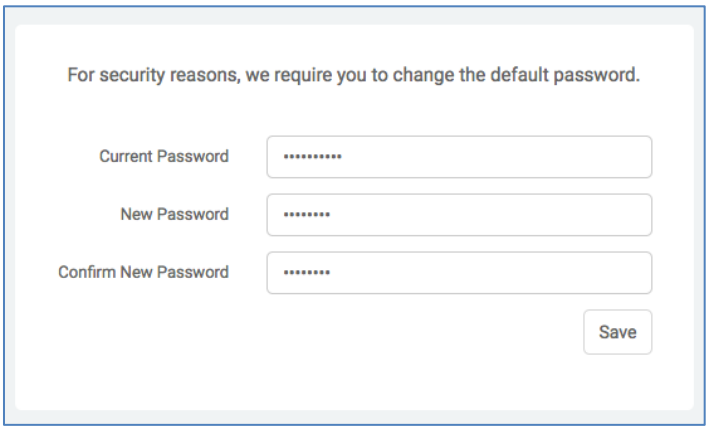


Figure 6: Changing the default password

4. Click **Skip**, as shown in Figure 7, unless the controller instance VPC has an HTTP or HTTPS proxy configured for internet access.

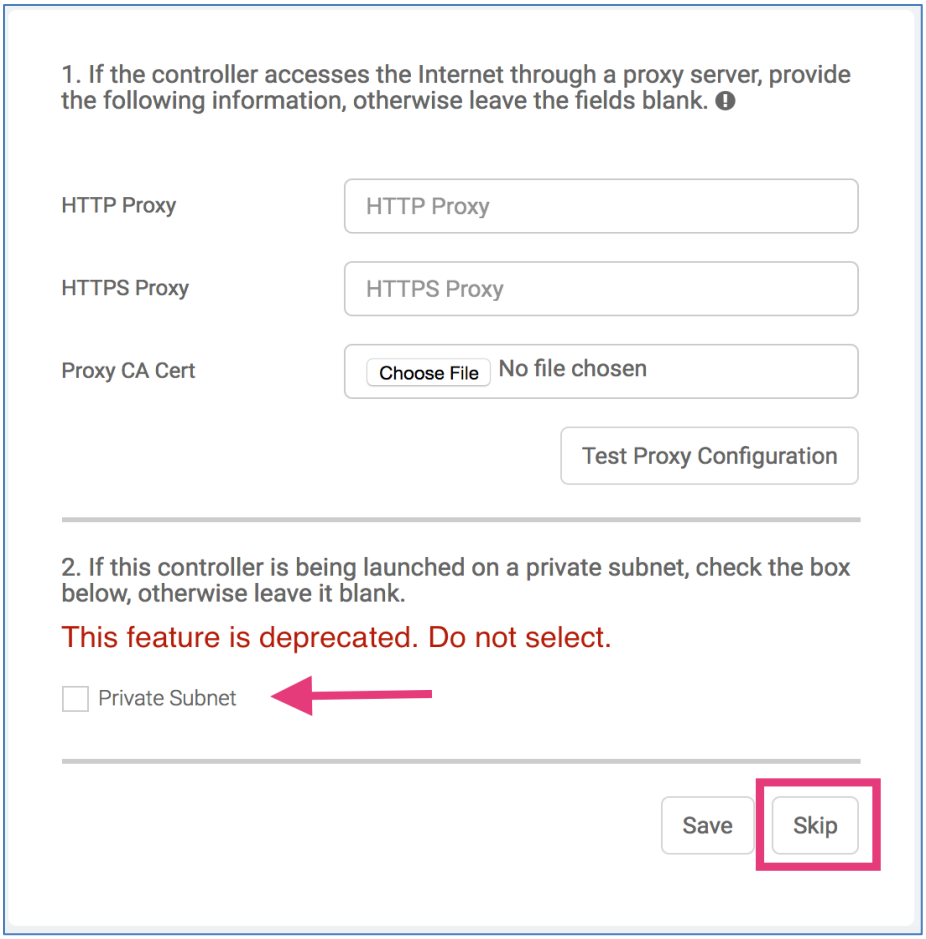


Figure 7: Configuring the proxy server

5. Click **Run**, as shown in Figure 8. The controller will upgrade to the latest software version. Wait for about 3-5 minutes for the process to finish.

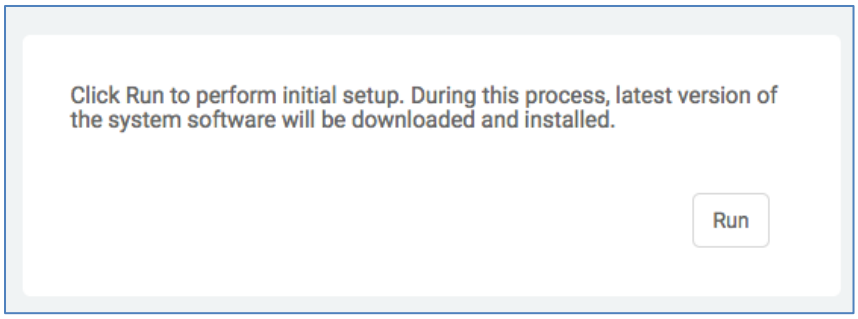


Figure 8: Performing initial setup

> **Note** Once the controller upgrade is complete, the login prompt will appear. Use the user name "admin" and your new password to log in.

Step 5. Create a Primary Access Account

1. Once logged back in to the Aviatrix Controller, you should be on the **Onboarding** page. Otherwise, on the navigation bar, click **Onboarding**.

   The Aviatrix primary access account is set up in the **Onboarding** page. This setup gives permissions to the Aviatrix Controller to configure the cloud networking within that public cloud provider, including deploying Aviatrix gateways. You then operate the Aviatrix Controller via the console or REST APIs. For more information about Aviatrix accounts, see Onboarding and Account FAQs in the Aviatrix documentation.

2. Select AWS.

3. Set up a primary access account. The Aviatrix primary access account contains the AWS account credential of the controller instance.

   For more information about the Aviatrix access account, see What is an Aviatrix access account on the Controller? in the Aviatrix documentation.

   a. Fill out the fields as shown in the following table:

Field	Expected Value
Account Name	Enter a unique name—for example, *AWSOpsTeam*.
Controller's AWS Account Number	The controller instance's 12 digit AWS account number. You can find this in the Outputs section (as shown in Figure 4).
IAM role-based	Select this box.

b. At the bottom of the **Create Primary Access Account** form, click **Create**, as shown in Figure 9.

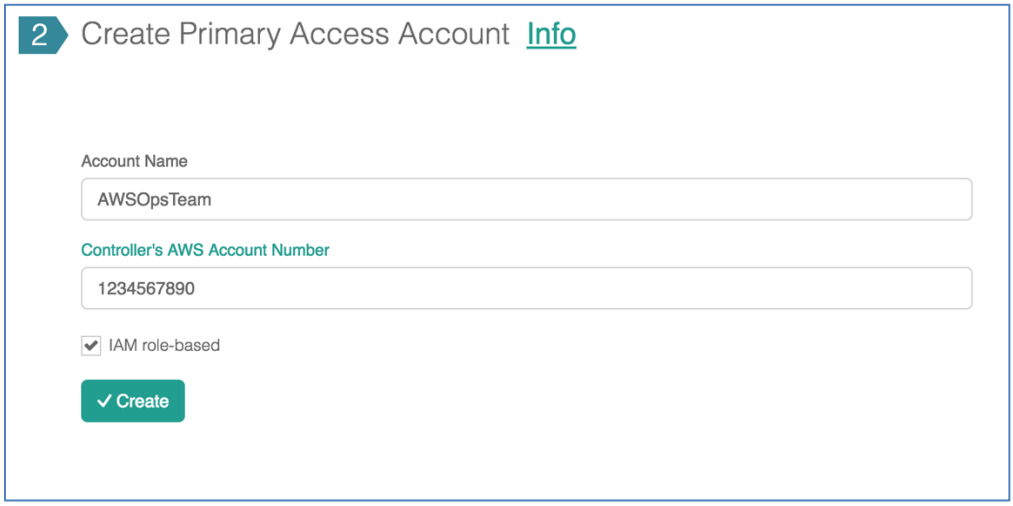


Figure 9: Creating the account

Note If the Aviatrix Controller needs to build connectivity in AWS accounts that are different from the Aviatrix Controller instance's AWS account, you must create secondary access accounts. To create a secondary access account on the controller and to create IAM roles, policies, and establish trust relationship to the primary AWS account, see IAM Roles for Secondary Access Accounts.

Step 6: Deploy the User VPN Service

Planning and Prerequisites

Identify a VPC that will become your remote access VPC, in a region where you want to launch the Aviatrix gateways that will host the SSL VPN service.

Important This document assumes you have set up an Aviatrix Controller. See Configuring Aviatrix User SSL VPN in the Aviatrix documentation for more details.

There are three main steps to setting up User VPN connectivity:

1. Create a VPN gateway
2. (Optional) Create user profiles and add policies to those profiles
3. Add a user and (optionally) associate users with profiles

You can also watch a video to learn how to set up the User VPN.

1. Create a VPN Gateway

> **Note** The description in the following steps indicates critical fields you need to select; it may not include all fields.

1. Log in to the Aviatrix Controller.
2. Launch a gateway with VPN capability.
   a. In the left navigation bar, click **Gateway**.
   b. At the top of the page, select **New Gateway**, as shown in Figure 10.

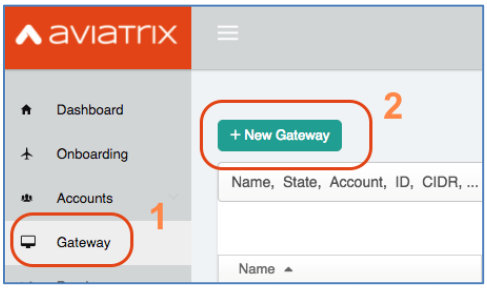


Figure 10: Launching a gateway

> **Important** You will need a public subnet in the VPC where you provision the gateway. Before starting this step, be sure to provision a new one or identify the correct one.

   c. Select the cloud type and enter a gateway name, as shown in Figure 11.
   d. Select the account name, region, and VPC.
   e. Select the VPC ID and the public subnet where the gateway will be provisioned.
   f. Select the gateway size (t2.micro is sufficient for most test use cases).

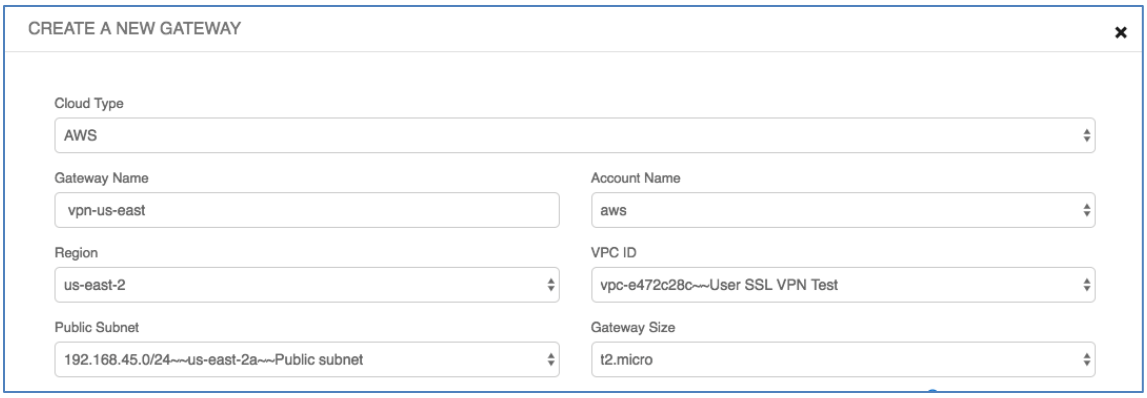


Figure 11: Configuring the gateway

g. Select **VPN Access**, as shown in Figure 12. More fields will appear.

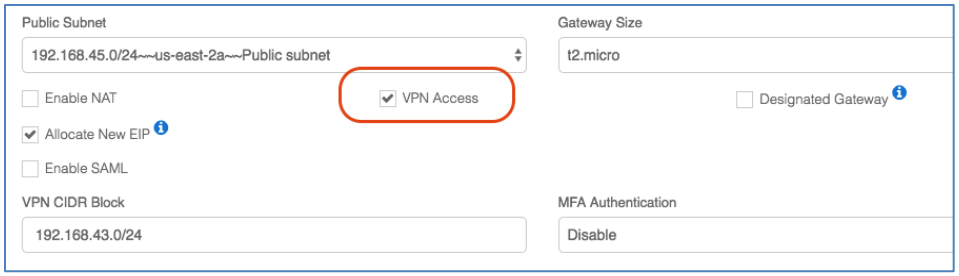


Figure 12: Setting up VPN access

> **Note** If you just want a basic user VPN solution without multi-factor authentication, you can skip the rest of the VPN-related fields.

h. Use the default VPN CIDR Block. The VPN CIDR Block is the virtual IP address pool that the VPN user will be assigned.

i. If you use Duo or Okta for multi-factor authentication, select one of them at **Two-step Authentication**, and more fields will appear. For details on Okta authentication, see Okta Authentication in the Aviatrix documentation.

j. If you select Split Tunnel Mode, only the VPC CIDR traffic will go through the tunnel. If you specify Additional CIDRs, these CIDRs and the VPC CIDR will go through the VPN tunnel. You can modify the Split tunnel settings later, when more VPCs are created. (Go to **OpenVPN** -> **Edit Config** -> **MODIFY SPLIT TUNNEL** to make changes. Specify all the CIDRs, separated by commas.) You can leave **Nameservers** and **Search Domains** blank, if you don't have any.

> **Note** If you plan to support Chromebook, you must configure full-tunnel mode because Chromebook only supports full tunnel.

k. By default, ELB is enabled. As a result, you can create more VPN gateways that are load balanced by ELB. (Aviatrix automatically creates the ELB.)

> **Important** If you disable ELB, your VPN traffic runs on UDP port 1194. When ELB is enabled, your VPN traffic runs on TCP 443. TCP 443 makes it easier to go through the corporate firewall.

l. Click LDAP if the VPN user should be authenticated by AD or the LDAP server. After you fill out the LDAP fields, run **Test LDAP Configuration** to test that your configuration is valid.

m. If you want to create more VPN gateways (for example, behind ELBs for load balancing), select **Save Template**. This saves your LDAP and multi-factor authentication credentials.

n. To create the gateway, select **OK**.

> **Note** Once you select **OK**, the gateway will be provisioned and configured. This will take a minute or two.

2. (Optional) Add VPN Profiles

A VPN user profile is defined by a list of access policies with allow or deny rules. When a VPN user is connected to a VPN gateway, the user's profile is pushed dynamically to the VPN gateway, and the user can only access resources defined in the profile. When a VPN user disconnects from the gateway, the policies are deleted.

> **Important** A VPN user who has no profile association has full access to all resources.

1. Log in to the Aviatrix Controller.
2. Expand **OpenVPN**, and then select **Profiles**, as shown in Figure 13.

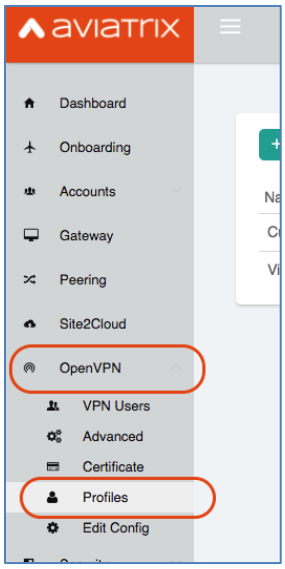


Figure 13: Adding VPN profiles

Create a profile

1. Select + **New Profile.**
2. Enter a profile name, select the appropriate base policy, and then click **OK**, as shown in Figure 14.

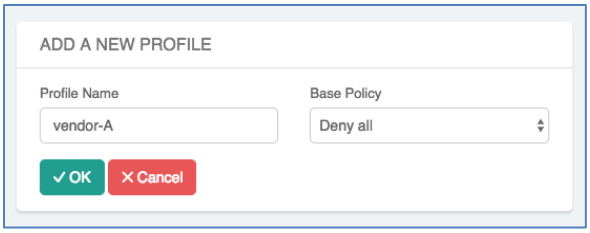


Figure 14: Creating a profile

Attach policies to a profile

Once you have created one or more profiles, you will need to attach policies to the profile. There can be any number of policies that apply to each profile.

1. Next to the profile name, click **Edit/View**, as shown in Figure 15.

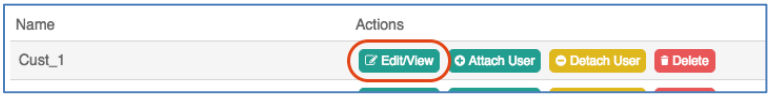


Figure 15: Attaching policies to a profile

2. To create a new policy, click + **Add New**.
3. Select the protocol, target CIDR block, port, and action, and then click **Save**, as shown in Figure 16.

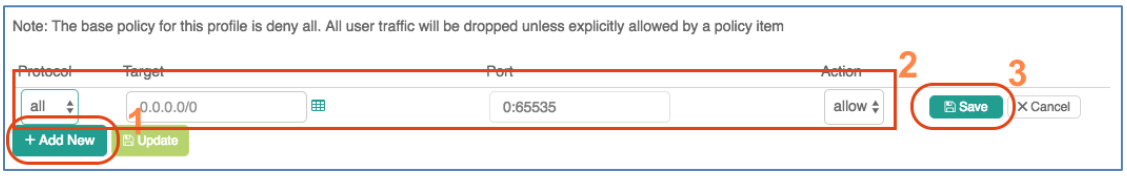


Figure 16: Adding policies to a profile

3. VPN users

You can add users manually or sync from an existing LDAP server:

1. Log in to the Aviatrix Controller.
2. Expand OpenVPN, and then select **VPN Users**, as shown in Figure 17.

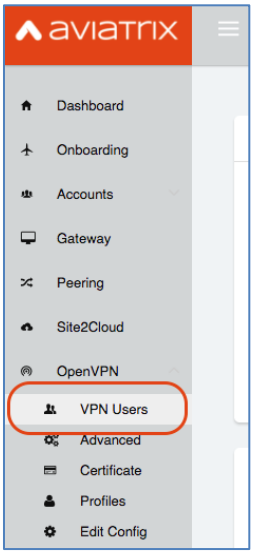


Figure 17: Adding VPN users

Create VPN users

1. Click + **Add New**.
2. Select the VPC ID where this user should be attached. The associated load balancer will appear in the LB/Gateway Name.
3. Enter the user name and user email.

4. (Optional) If associating this user with an existing profile, select the checkmark next to **Profile**, select the appropriate profile name, and then click **OK**, as shown in Figure 18.

> **Note** When a user is added to the database, an email with .ovpn file or .onc (for Chromebooks) will be sent to the user with detailed instructions.

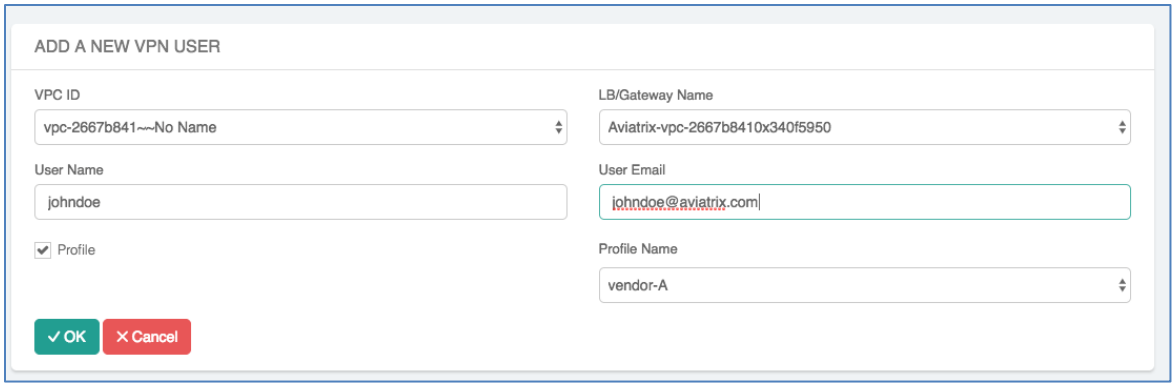


Figure 18: Adding VPN users

You now have a working Aviatrix VPN gateway. Users can connect and gain access to their cloud resources. Detailed audit logs are maintained and available in various logging platforms.

> **Note** Audit reports are best viewed in Splunk App for Aviatrix.

Best Practices Using Aviatrix on AWS

Gateway Sizing

For complete information about how to correctly size your gateway, see the Aviatrix documentation.

Backups

When you deploy the Aviatrix User VPN service in a cloud environment, the Aviatrix Controller is not in the data path because packet processing and encryption are handled by the Aviatrix gateways.

When the Aviatrix Controller is down or out of service, your network will continue to be operational, and encrypted tunnels and OpenVPN users will stay connected. Because most of the data logs are forwarded directly from the gateways, the loss of log information from

the Aviatrix Controller is minimal. However, you won't be able to build new tunnels or add new OpenVPN users.

This loosely coupled relationship between the Aviatrix Controller and gateways reduces the impact of controller availability issues and simplifies your infrastructure. The Aviatrix Controller stores configuration data and should be periodically backed up to the appropriate AWS account. If a replacement controller is launched, you can restore the configuration data from your backup. For more information, see the Aviatrix documentation.

Security

The Aviatrix Controller is secured by exposing only the necessary ports (TCP 443). Each gateway created by the Aviatrix Controller is able to communicate only with other gateways (using UDP 500 and 4500) and the Aviatrix Controller (using TCP 22 and 443). Software and patch updates are provided by Aviatrix. For more information, contact Aviatrix at info@aviatrix.com.

All peering connections are secured by using IPsec encryption.

Troubleshooting

Q. I encountered a CREATE_FAILED error when I launched the Quick Start.

A. If AWS CloudFormation fails to create the stack, we recommend that you relaunch the template with **Rollback on failure** set to **No**. (This setting is under **Advanced** in the AWS CloudFormation console, **Options** page.) With this setting, the stack's state will be retained and the instance will be left running, so you can troubleshoot the issue. (Look at the log files in `%ProgramFiles%\Amazon\EC2ConfigService` and `C:\cfn\log`.)

> **Important** When you set **Rollback on failure** to **No**, you will continue to incur AWS charges for this stack. Please make sure to delete the stack when you finish troubleshooting.

For additional information, see Troubleshooting AWS CloudFormation on the AWS website.

Q. I encountered a size limitation error when I deployed the AWS CloudFormation templates.

A. We recommend that you launch the Quick Start templates from the links in this guide or from another S3 bucket. If you deploy the templates from a local copy on your computer or

from a non-S3 location, you might encounter template size limitations when you create the stack. For more information about AWS CloudFormation limits, see the AWS documentation.

Support

Aviatrix provides customer support for all the Aviatrix components of the Aviatrix User VPN service, including the automation scripts. Contact support@aviatrix.com for assistance.

GitHub Repository

You can visit our GitHub repository to download the templates and scripts for this Quick Start, to post your comments, and to share your customizations with others.

Additional Resources

AWS services

- Amazon EC2
  https://aws.amazon.com/documentation/ec2/
- Amazon VPC
  https://aws.amazon.com/documentation/vpc/
- AWS CloudFormation
  https://aws.amazon.com/documentation/cloudformation/

Aviatrix documentation

- Aviatrix website
  https://www.aviatrix.com/
- Aviatrix documentation
  https://www.aviatrix.com/docs/

Quick Start reference deployments

- AWS Quick Start home page
  https://aws.amazon.com/quickstart/

Document Revisions

Date	Change	In sections
June 2018	Initial publication	—

Notices

This document is provided for informational purposes only. It represents AWS's current product offerings and practices as of the date of issue of this document, which are subject to change without notice. Customers are responsible for making their own independent assessment of the information in this document and any use of AWS's products or services, each of which is provided "as is" without warranty of any kind, whether express or implied. This document does not create any warranties, representations, contractual commitments, conditions or assurances from AWS, its affiliates, suppliers or licensors. The responsibilities and liabilities of AWS to its customers are controlled by AWS agreements, and this document is not part of, nor does it modify, any agreement between AWS and its customers.

The software included with this paper is licensed under the Apache License, Version 2.0 (the "License"). You may not use this file except in compliance with the License. A copy of the License is located at http://aws.amazon.com/apache2.0/ or in the "license" file accompanying this file. This code is distributed on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied. See the License for the specific language governing permissions and limitations under the License.