# Appgate SDP® for AWS Deployment Guide

Type: Deployment guide for Amazon Web Services (AWS)
Last Updated: June 26, 2024
Applies to: Appgate SDP v6.0 and newer

| Document Version | Publication Date |
|---|---|
| **Version 1.0** | November 11, 2019 |
| **Version 1.1** | February 3, 2020 |
| **Version 1.2** | February 20, 2020 |
| **Version 1.3** | October 7, 2020 |
| **Version 1.4** | November 16, 2020 |
| **Version 1.5** | December 2, 2020 |
| **Version 2.0** | September 15, 2021 |
| **Version 2.1** | April 1, 2022 |
| **Version 2.2** | June 22, 2022 |
| **Version 2.3** | July 26, 2024 |

# Table of Contents

# Introduction

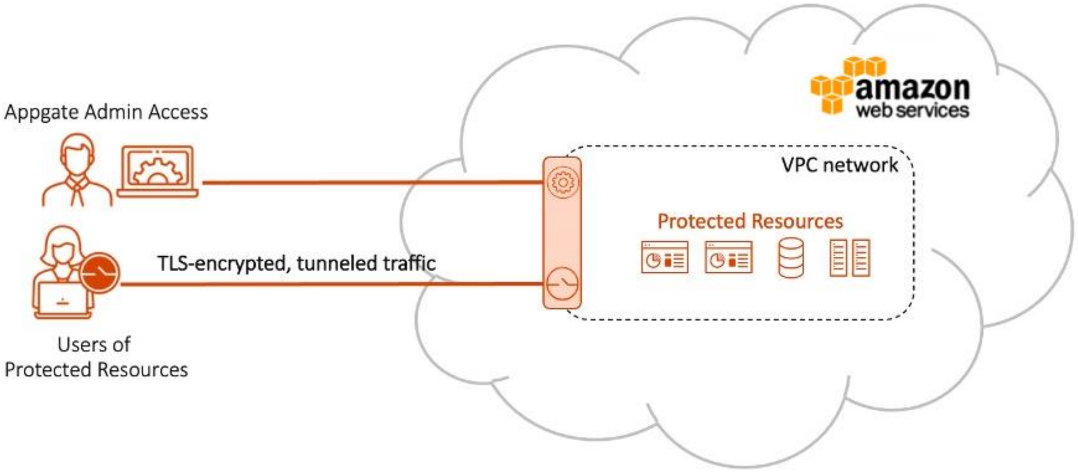
This document serves as a reference guide for deploying Appgate SDP on AWS. It will guide you through the set up and configuration of Appgate SDP to protect your AWS resources. In this document are the AWS-specific steps for deploying a standalone Appgate SDP appliance on AWS. This appliance will function as both a Controller and Gateway. Additional Support Documentation is available at https://sdphelp.appgate.com/

## Overview

Enterprises are rapidly embracing cloud services such as Amazon Web Services (AWS) but do not have an easy way to securely access these resources. Appgate SDP provides a means for security teams to control user access to Amazon EC2 resources efficiently and effectively.

Appgate SDP is purpose-built for AWS and draws on user context to dynamically create a secure, encrypted network ‘segment of one’ that is tailored for each user session. Appgate SDP dramatically simplifies the user access to cloud resource challenge and eliminates IP-based over-entitled network access.

Appgate SDP is known as a software-defined perimeter. Appgate SDP has patented technology which dynamically matches the user and device context with the entitlements to the protected cloud resources to explicitly microsegment access. The Appgate SDP policy engine grants access to and only to the instances defined by policy and current user/device context.  For example, new EC2 server instances are automatically detected, and user access is automatically granted if permitted by policy. No admin intervention is required.



The illustration above provides an example of how Appgate SDP can be deployed (Appgate SDP is designated by the ⊖ icon in the diagram below). The illustration shows all user traffic tunneled from their device (via a virtual network adapter) and passed through the Appgate SDP gateway to the protected resources. All traffic to the Appgate SDP gateway is encrypted with TLS, so these resources can be securely accessed regardless of location.

As you will see, this is much more dynamic and flexible than a firewall. We will be setting policies that control user access based on user attributes and on server attributes (such as AWS tags).

### Root Privileges Not Required

Appgate SDP does not require the use of root privileges for deployment or operation.

### Least Privileged Access

Appgate SDP dynamically creates one-to-one network connections between a user and the resources they access. It is rooted in Zero Trust by applying the principle of least privilege where access rights are limited for users to the bare minimum permissions they need to perform their work. The principle of least privileged access is one of the core tenets of Zero Trust. With least privileged access, users only have network access to resources they need to do their job, and nothing more.

It's important to understand and baseline your server-to-server communications patterns and put in place mechanisms to enforce the principle of least privilege for them. This should apply both to inbound and outbound network calls from servers.

You should not be exposing any enterprise services directly to the Internet and put them behind a dedicated security component. Require authentication and ideally include multiple factors (e.g., device onboarding with out-of-band validation) before permitting access to anything at a network level.

Enforce the principle of *least privilege* – i.e., granting only the permissions required to perform a task – for all access granted as part of the deployment. For broadly accessible services such as email, consider enforcing MFA before allowing the network connection to ensure there's a human operator.

## Browser Compatibility

We recommend using Chrome or Firefox for the administrative steps in the Admin GUI Configuration section below.

## Region Availability

In this section, you'll learn which AWS Regions are supported by Appgate SDP.

| Region Name | Region Code | AWS Marketplace Availability | AWS GovCloud (US) Marketplace Availability |
|---|---|---|---|
| US East (N. Virginia) | `us-east-1` | Yes | |
| US East (Ohio) | `us-east-2` | Yes | |
| US West (N. California) | `us-west-1` | Yes | |
| US West (Oregon) | `us-west-2` | Yes | |
| Canada (Central) | `ca-central-1` | Yes | |
| Europe (Frankfurt) | `eu-central-1` | Yes | |
| Europe (Ireland) | `eu-west-1` | Yes | |
| Europe (London) | `eu-west-2` | Yes | |
| Europe (Paris) | `eu-west-3` | Yes | |
| Europe (Stockholm) | `eu-north-1` | Yes | |
| Europe (Milan) | `eu-south-1` | Yes | |
| Africa (Cape Town) | `af-south-1` | Yes | |
| Asia Pacific (Singapore) | `ap-southeast-1` | Yes | |
| Asia Pacific (Sydney) | `ap-southeast-2` | Yes | |
| Asia Pacific (Mumbai) | `ap-south-1` | Yes | |
| Asia Pacific (Tokyo) | `ap-northeast-1` | Yes | |
| Asia Pacific (Seoul) | `ap-northeast-2` | Yes | |
| Asia Pacific (Osaka) | `ap-northeast-3` | Yes | |
| Asia Pacific (Hong Kong) | `ap-east-1` | Yes | |
| South America (São Paulo) | `sa-east-1` | Yes | |
| Middle East (Bahrain) | `me-south-1` | Yes | |
| AWS GovCloud (US-East) | `us-gov-east-1` | | Yes |
| AWS GovCloud (US-West) | `us-gov-west-1` | | Yes |

# Prerequisites

Deploying the Appgate SDP appliance requires some familiarity with Amazon Web Services. You should be familiar with:

- Amazon EC2, for basic EC2 configuration
- Amazon EBS, for configuring the EC2 instance storage and managing encryption
- Amazon VPC, for configuring a subnet and a security group

This document assumes that you are familiar with AWS EC2, and have some experience creating AMIs, setting up a VPC, subnet, internet gateways, and routing within AWS. Let's briefly explain what you will need in your environment to set up Appgate SDP to protect your resources.

## EC2 Key Pair

Note: Access to Appgate appliances is limited to using an EC2 Key Pair. Password based authentication is not supported.

Amazon EC2 uses public-key cryptography to encrypt and decrypt login information. Public-key cryptography uses a public key to encrypt a piece of data, such as a password, then the recipient uses the private key to decrypt the data. The public and private keys are known as a key pair. For more information, read the Amazon EC2 documentation[1].

Make sure that at least one Amazon EC2 key pair exists in your AWS account in the Region where you are planning to deploy the template. Make note of the key pair name. The EC2 Key Pair will be used to provide SSH access to the appliance, which may be required during the initial setup and for some administrative tasks. Save the PEM key file to your local computer for later use. You'll be prompted for this information during deployment.

If you're deploying for testing or proof-of-concept purposes, we recommend that you create a new key pair instead of specifying a key pair that's already being used by a production instance. To create a key pair, follow the instructions in the Amazon EC2 documentation[2].

## VPC and Subnet

You should have a Virtual Private Cloud (VPC) set up with its own subnet that the Appgate Gateway is going to protect. This can be an existing VPC or a new one. In any case, instances running in this VPC must already be accessible from the internet with an Internet Gateway set up properly. You probably already have multiple VPCs already set up, so just choose one of those to use for testing out Appgate.

We are going to route all traffic to all instances in the VPC through the Appgate SDP security appliance, so the VPC should only be hosting development or test workloads – access will be interrupted during this setup process and will require use of the Appgate SDP Client to access going forward.

In this setup guide, we are assuming that you have a subnet setup with a contiguous address space in which the protected resources will be placed. For example, one can use `172.31.0.0/16` for the VPC and `172.31.16.0/20` for the subnet.

What is important about this network setup is that it has an Internet Gateway set up in AWS with a Route Table that allows traffic into it. If you can currently access resources within the VPC, you are likely already set up.

## Elastic IP Address

Because Appgate SDP provides network security access, the instance requires a fixed/static IP address. A static IP address is important as the IP address is used in Appgate's self-signed certificate generated by the system. This certificate is used to establish trusted communications between appliances (peer-interface) and between client and appliance (client-interface). Additionally, clients also cache the instance's IP address thus a changing address will result in trust and connectivity problems.

If you are using the CloudFormation Template (CFT) fulfillment option, you can choose to automatically create a new Elastic IP address during the provisioning process.

If you are using the Amazon Machine Image (AMI) fulfillment option, make sure that you have an Elastic IP address available to associate to the appliance or be prepared to re-associate one.

[1] https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/ec2-key-pairs.html

[2] https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/create-key-pairs.html

## IAM Role

Appgate SDP instances will assume an IAM Role. This role needs a policy attached to it to grant read access within Amazon EC2 and to meter usage. This IAM role must be associated with your EC2 instance at the time of launch. The instances will inherit the rights from the IAM role which are needed for the AWS name-resolver and AWS Marketplace Metering Service to work properly.

If you choose the CloudFormation fulfillment option, CloudFormation will automatically create the IAM role for you; therefore, you can safely ignore this prerequisite.

If you choose the Amazon Machine Image fulfillment option, you must create an IAM role that will be used later when launching the instance.

**To create an IAM role using the AWS Management Console:**

1. Navigate to the IAM console at https://console.aws.amazon.com/iam/
2. In the navigation pane of the console, choose **Roles** and then choose **Create role**
3. From the Select trusted entity page:
    3.1. Under Trusted entity type, select AWS Service
    3.2. Under **Use Case**, select **EC2**
    3.3. Click **Next**
4. From the **Add permissions** page:
    4.1. Choose the following policies from the list to attach them to the IAM role:

| Policy Name | Policy Description |
|---|---|
| **`AmazonEC2ReadOnlyAccess`** | Grants permissions that allow read-only access to Amazon EC2. This is needed for Appgate SDP's AWS name resolver to work properly. |
| **`AWSMarketplaceMeteringFullAccess`** | Grants contributor permissions that allow reporting metered usage that corresponds to products with flexible consumption pricing on AWS Marketplace. |
| **`AWSMarketplaceMeteringRegisterUsage`** | Grants contributor permissions that allow reporting metered usage that corresponds to products with hourly pricing on AWS Marketplace. |

    4.2. Under **Set permissions boundary - optional**, leave the default **Create role** without a permissions boundary selected
    4.3. Click **Next**
5. From the **Name, review, and create** page:
    5.1. For **Role name**, enter a meaningful name to identify this IAM role. Role names must be unique within your AWS account. Because other AWS resources might reference the role, you cannot edit the name of the role after it has been created.
    5.2. (Optional) For **Description**, enter a description for the IAM role.
    5.3. (Optional) Under **Add tags**, add metadata to the role by attaching tags as key–value pairs.
    5.4. Click **Create role**

## Security Groups

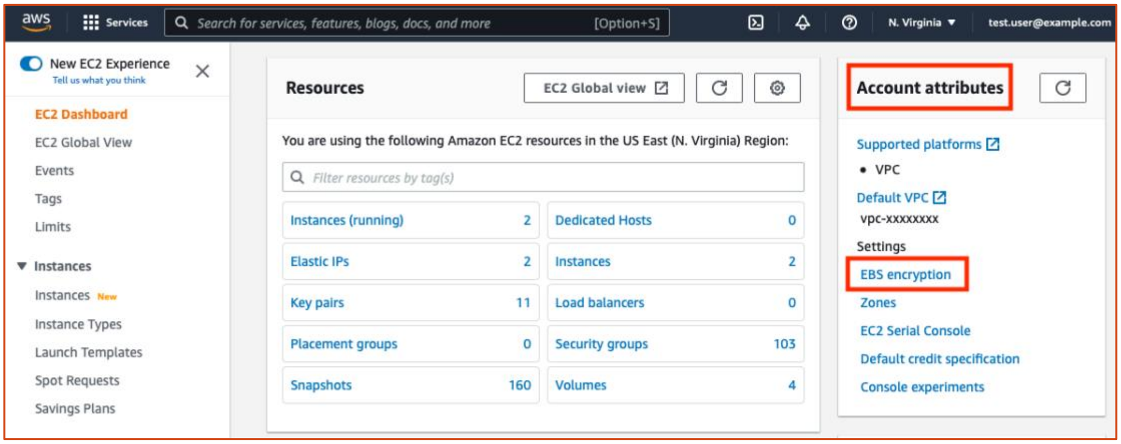
Both the Appgate server and the protected resources will need properly configured security groups. We will create these during the setup process below.

## Enable EBS Encryption

We recommend you enable default encryption for your EBS Volumes.

**How to enable default encryption for your Amazon EBS Volumes:**

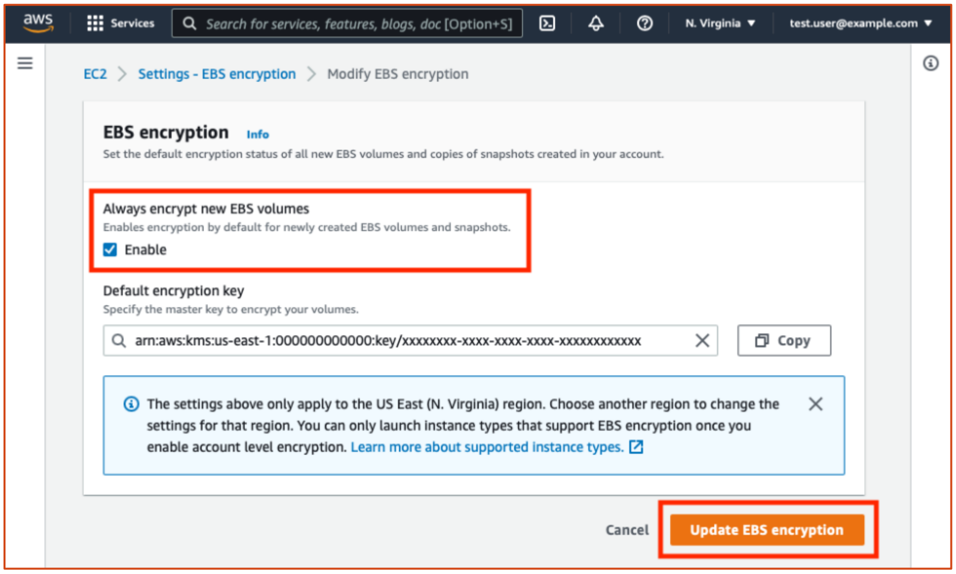
1. Open the Amazon EC2 console at [https://console.aws.amazon.com/ec2/](https://console.aws.amazon.com/ec2/)
2. From the navigation pane, select **EC2 Dashboard**
3. In the upper-right corner of the page, choose **Account Attributes**, click **EBS encryption** under **Settings**



You are using the following Amazon EC2 resources in the US East (N. Virginia) Region:

| | | | |
|---|---|---|---|
| Instances (running) | 2 | Dedicated Hosts | 0 |
| Elastic IPs | 2 | Instances | 2 |
| Key pairs | 11 | Load balancers | 0 |
| Placement groups | 0 | Security groups | 103 |
| Snapshots | 160 | Volumes | 4 |

4. If **Always encrypt new EBS volumes** is disabled, click **Manage** to modify EBS encryption
5. Select **Enable**. You can keep the AWS managed key with the alias **alias/aws/ebs** created on your behalf as the default encryption key, or choose the symmetric customer managed key that you created
6. Click **Update EBS encryption**


aws
Services
Search for services, features, blogs, doc [Option+S]
N. Virginia ▾
test.user@example.com ▾
EC2 > Settings - EBS encryption > Modify EBS encryption
Info
Copy
Cancel
Update EBS encryption

**EBS encryption**

Set the default encryption status of all new EBS volumes and copies of snapshots created in your account.

Always encrypt new EBS volumes

Enables encryption by default for newly created EBS volumes and snapshots.

☑ Enable

Default encryption key

Specify the master key to encrypt your volumes.

arn:aws:kms:us-east-1:000000000000:key/xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

The settings above only apply to the US East (N. Virginia) region. Choose another region to change the settings for that region. You can only launch instance types that support EBS encryption once you enable account level encryption. Learn more about supported instance types.

## AWS Service Limits

Before you proceed, your AWS account must have resource quotas as specified in the following table.

| AWS Resource | Quota Usage for this deployment |
|---|---|
| **Amazon Elastic Compute Cloud (EC2) instances** | 2 |
| **Amazon Elastic Block Store (EBS) volumes** | 2 |
| **Amazon Virtual Private Cloud (VPC)** | 1 |
| **Amazon Elastic IP addresses (EIP)** | 1 |
| **Amazon CloudFormation (CFT)** | Optional |

If required, you may need to request a quota increase from AWS for the resources in the above table. You will need to do this if you might exceed the default AWS service limit quotas with this Appgate SDP deployment. You can view and manage your usage and quotas in the AWS Service Quotas Console[3]. For more details, see the AWS Service Quotas User Guide[4]

# Getting Started

In about 20 minutes you will have the system up and running and will be playing with different polices and user access rights!

**There are four steps to bringing an Appgate SDP environment online, plus a few prerequisites:**

Step 1: Provision AWS resources for a new Appgate appliance
We are including this step because there are a couple of security group details that are important to properly configure.

Step 2: Setup first Controller by seeding the Appgate appliance from the SSH command line
After securely logging in to the server through SSH, we will seed the appliance with basic configuration details such as DNS servers and administrative passwords. Note that the metered versions of Appgate SDP do not support more than one Controller. If you require a multi-Controller configuration, please contact us at channelteam@appgate.com to arrange for an AWS Private Offer.

Step 3: Configure Gateway from the Admin GUI
This step is where you will login to the Appgate SDP admin GUI to configure policies, resources, and users. This is the bulk of the setup work, as we will be introducing you to the Appgate policy and entitlement model.

[3] https://console.aws.amazon.com/servicequotas/home
[4] https://docs.aws.amazon.com/servicequotas/latest/userguide/intro.html

Step 4: Install the client and test connectivity
This is where it all comes together, and you can see Appgate SDP in action dynamically protecting your AWS resources.

## Fulfillment Options

Appgate SDP is pre-configured for 1-Click launch capability on AWS infrastructure. There are two ways to deploy Appgate SDP on the AWS Marketplace, which are referred to as fulfillment options.

**Two Fulfillment Options for Appgate SDP products on the AWS Marketplace:**

1. **CloudFormation Template** — this is the preferred fulfillment option, which uses AWS CloudFormation to launch a single standalone SDP appliance. CloudFormation takes care of provisioning and configuring the required AWS resources, such as EC2 and EBS.
2. **Amazon Machine Image** — this is the alternative fulfillment option containing an image of a server, including an operating system and the Appgate SDP software. You can launch an instance from the product's AMI using the Amazon EC2 launch wizard.

All Appgate SDP for AWS Marketplace products run within a customer's AWS account.

## Instance Sizing

For the latest instance sizing guidelines, go to SDP Admin Guide: Instance sizing[5]

# Step 1: Provision appliance with CloudFormation

This section covers the CloudFormation Template fulfillment option, which uses AWS CloudFormation to provision a standalone Appgate SDP appliance. If you wish to use the alternative fulfillment option, see AMI deployment using the EC2 Launch Wizard.

The Standalone Appgate Deployment CloudFormation template deploys a single Amazon EC2 instance with a 100 GiB EBS volume. The AWS CloudFormation template for this deployment 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.

**To deploy Appgate SDP using the CloudFormation Template fulfillment method:**

1. Go to the **AWS Marketplace: Appgate** seller profile at https://aws.amazon.com/marketplace/seller-profile?id=96f40b35-0171-4557-b9ee-a96f1949a5d1
   (Alternative) For GovCloud, go to the **AWS Marketplace: Appgate Federal** seller profile at https://aws.amazon.com/marketplace/seller-profile?id=75244fa0-365c-4921-9a2d-e47b3f30994b
2. Select a product type. For this walkthrough, you can choose any of the product types.
3. On the Product Detail page:
   3.1. Click **Continue to Subscribe**
4. On the Subscribe to this software page:
   4.1. Review the Terms and Conditions
   4.2. Click **Continue to Configuration**
5. On the Configure this software page:

[5] https://sdphelp.appgate.com/adminguide/instance-sizing.html

   - 5.1. Choose the **CloudFormation Template** fulfillment option from the list
   - 5.2. Verify **Standalone Appgate SDP Deployment** is selected
   - 5.3. Choose the **Software Version** of Appgate SDP you wish to deploy
   - 5.4. Choose the **AWS Region** containing the EC2 instances to which Appgate SDP will control access
   - 5.5. Click **Continue to Launch**

6. On the Launch this software page:
   - 6.1. Under Choose Action, select **Launch CloudFormation**
   - 6.2. Click **Launch**. The AWS CloudFormation Console opens.
7. On the Create stack page:
   - 7.1. Verify **Template is ready** is selected
   - 7.2. Verify **Amazon S3 URL** is selected. Keep the default pre-populated Amazon S3 URL.
   - 7.3. Click **Next**
8. On the Specify stack details page, enter the following information, and then click **Next**:

   **Stack name**
   Give your stack a name

   **KeyName**
   Select an existing EC2 key pair for SSH access on port 22

   **VpcId**
   Select a VPC containing the EC2 instances to which Appgate SDP will control access

   **SubnetID**
   Choose a subnet within the selected VPC

   **SourceLocationSSH**
   Enter a valid CIDR-format IP address range (e.g., 0.0.0.0/0) that can access SSH on port 22. SSH access should be limited to admin networks and should only be used during the initial setup, after which access to port 22 should be restricted. Allowing access from the internet is NOT recommended!

   **SourceLocation443**
   Enter a valid CIDR-format IP address range (e.g., 0.0.0.0/0) that can access port 443, which is used for Client connections and appliance-to-appliance traffic. Port 443 should be open to all IP addresses from which your users will attempt to access your protected resources (i.e., it can be open to the Internet)

   **SourceLocation8443**
   Enter a valid CIDR-format IP address range (e.g., 0.0.0.0/0) that can access port 8443, which is used to access the Admin UI and for API calls. Access should be limited to admin networks and the LogServer

   **UdpTcpSpaEnabled**
   Choose a SPA protocol. The default is TCP SPA. If UDP-TCP SPA is selected, then two additional security group rules are created for UDP port 53 and UDP port 443 to allow access from the IP address range set in the SourceLocation443 parameter.
   Keep the default TCP SPA selected.

   **UserData**
   Leave blank

   **InstanceType**
   Choose an EC2 instance size. For sizing guidelines, see Instance Sizing

   **AllocateElasticIP**
   Yes

> **Warning**: In a production environment, you would most likely want to carefully control which devices can reach port 8443 and port 22 on your instance as they are administrative ports.

9. On the **Configure stack options** page, enter the following information, and then click **Next**:

   **Tags**

   (Optional) Tag your AWS CloudFormation Stack using the key and value fields.

   **Permissions**

   Leave blank. CloudFormation will create the appropriate IAM role. The role will have the correct EC2 read-only permissions so that Appgate can query EC2 for newly created server instances.

   **Stack failure options**

   Leave the default selection.

   **Advanced Options**

   Leave the default selection.

10. On the Review stack options page:

    10.1. Review the stack options

    10.2. Select the **I acknowledge that AWS CloudFormation might create IAM resources** checkbox at the bottom of the page.

    10.3. Click **Create stack** to deploy the AWS CloudFormation stack. This will take you to the AWS CloudFormation Console.

CloudFormation begins creating the resources that are specified in the template. While your stack is being created, it's listed on the **Stacks** page with a status of **`CREATE_IN_PROGRESS`**.

Click on the **Stack Name** to view the stack creation progress. After your stack has been successfully created, its status changes to **`CREATE_COMPLETE`**.

Once status changes to **`CREATE_COMPLETE`**, go to Step 2: Setup first Controller

## Step 1: (Alternative) AMI deployment using the EC2 Launch Wizard

This section covers the alternative fulfillment option, which uses an Amazon Machine Image (AMI) and the Amazon EC2 Launch Instance Wizard to provision the appliance. This fulfillment option is considered the alternative because it is a more manual process. If you completed Step 1: Provision appliance with CloudFormation, then you can safely skip this section and move on to Step 2: Setup first Controller.

Before you begin, make sure that you have completed the Prerequisites. More specifically, you must create an IAM Role to use with this appliance before proceeding to the next step. For more information, see Prerequisites: IAM Role

**To deploy Appgate SDP using the Amazon EC2 Launch Instance Wizard:**

1. Go to the **AWS Marketplace: Appgate** seller profile at https://aws.amazon.com/marketplace/seller-profile?id=96f40b35-0171-4557-b9ee-a96f1949a5d1
   (Alternative) For GovCloud, go to the **AWS Marketplace: Appgate Federal** seller profile at https://aws.amazon.com/marketplace/seller-profile?id=75244fa0-365c-4921-9a2d-e47b3f30994b
2. Select a product type. For this walkthrough, you can choose any of the product types.
3. From the Product Detail page:

   3.1. Click **Continue to Subscribe**

4. From the Subscribe to this software page:
    - 4.1. Review the Terms and Conditions
    - 4.2. Click **Continue to Configuration**
5. From the Configure this software page:
    - 5.1. Choose the **Amazon Machine Image** fulfillment option from the list
    - 5.2. Choose the **Software Version** of Appgate SDP you wish to deploy
    - 5.3. Choose the **AWS Region** containing the EC2 instances to which Appgate SDP will control access
    - 5.4. Click **Continue to Launch**
6. From the Launch this software page:
    - 6.1. Under Choose Action, select **Launch through EC2**
    - 6.2. Click **Launch**. The Amazon EC2 Launch Instance Wizard opens in a new tab
7. From the Launch an Instance page:
    - 7.1. Under **Name and tags**, enter a descriptive name for your instance
    - 7.2. Under **Application and OS Images (Amazon Machine Image),** verify the AMI by Appgate SDP is selected from the AWS Marketplace AMIs catalog
    - 7.3. Under **Instance type**, select the hardware configuration for your EC2 instance from the list. For sizing guidelines, see SDP Admin Guide: Instance Sizing[6].
    - 7.4. Under **Key pair (login)**, choose an existing key pair that you have on hand or create a new key pair for SSH access to this EC2 instance (see Prerequisites: EC2 Key Pair).
8. Next to Network settings, click **Edit**
    - 8.1. Under **VPC**, select the VPC containing the EC2 instances to which Appgate SDP will control access
    - 8.2. Under **Subnet**, choose a subnet within the selected VPC or create a new subnet
    - 8.3. Under **Auto-assign public IP**, keep the default selection, **Enable**
    - 8.4. For **Security group name**, you'll see that the wizard created a security group for you. You can use this security group, or alternatively you can edit the Inbound security groups rules as following:

| Description | Type | Protocol | Port Range | Source |
|---|---|---|---|---|
| Security group rule 1 | SSH | TCP | 22 | My IP |
| Security group rule 2 | Custom TCP | TCP | 8443 | My IP |
| Security group rule 3 | HTTPS | TCP | 443 | 0.0.0.0/0 |
| Security group rule 4 | DNS (UDP) | UDP | 53 | 0.0.0.0/0 |
| Security group rule 5 | Custom UDP | UDP | 443 | 0.0.0.0/0 |

TCP port 443, UDP port 53, and UDP port 443 are used for Client connections and appliance-to-appliance traffic. These ports should be open to all IP addresses from which your users will attempt to access your protected resources (i.e., they can be open to the Internet).

**Warning:** In a production environment, you would most likely want to carefully control which devices can reach TCP port 8443 and TCP port 22. SSH access on TCP port 22 should be limited to admin networks and

[6] https://sdphelp.appgate.com/adminguide/instance-sizing.html

should only be used during the initial setup, after which access to TCP port 22 should be restricted. TCP port 8443 is used to access the Admin UI and for API calls. Access to TCP port 8443 should be limited to admin networks and the LogServer.

9. Under Configure storage, click **Add new volume**
    - 9.1. Enter **100 GiB** for EBS Volume Size
    - 9.2. Choose **General purpose SSD (gp3)** for EBS Volume Type
10. Under Advanced details, select the **IAM instance profile** that you created in the Prerequisites: IAM Role outlined above.
11. Keep the default selections for the other configuration settings for your instance.
12. Review a summary of your instance configuration in the Summary panel, and when you're ready, click **Launch instance**. A confirmation page lets you know that your instance is launching.
13. Choose **View all instances** to close the confirmation page and return to the EC2 console.

It can take a few minutes for the instance to be ready for you to connect to it. To check if the instance has passed its status checks, review the **Status check** column of the Amazon EC2 Console[7]. Once the instance has finished launching, proceed to Step 2: Setup first Controller.

## Step 2: Setup first Controller

In this step, we'll log in to the AWS EC2 instance via SSH and run a simple menu-driven setup tool called **`cz-setup`**. Once the instance has finished initializing and passed its status checks (typically under 5 minutes), connect to it via SSH using its Elastic IP address and the EC2 key pair you associated in the prior step.

**To connect to the appliance using SSH and setup the appliance as the first Controller:** [8]

1. In a terminal window, use the **ssh** command to connect to the instance. Specify the path and file name of the private key (.pem), the username "**`cz`**", and the public DNS name as shown below:

```
ssh -i "/path/key-pair.pem" cz@ec2-54-84-124-154.compute-1.amazonaws.com
```

where…

`"/path/key-pair.pem"` = The PEM file for the key pair you used when launching this instance, including it's absolute path if the file is not in the current directory. The PEM file must have permissions of 400, which can be set by running '**`chmod 400 /path/to/key.pem`**'

`cz` = The standard user for all Appgate SDP AMIs

`ec2-54-84-124-154.compute-1.amazonaws.com` = Public Elastic IPv4 address of your instance

[7] https://console.aws.amazon.com/ec2/#Instances
[8] To connect to your EC2 instance from Windows using PuTTY, see https://docs.aws.amazon.com/AWSEC2/latest/UserGuide/putty.html

2. After entering the SSH command above, you'll likely see a response like the following:

```
The authenticity of host 'ec2-54-84-124-154.compute-1.amazonaws.com (54-84-124-154)' can't be established.
ECDSA key fingerprint is l8PLB/nR59WgrgzEimkgJeBad9tvf1QZWxheQmCG6kZY.
Are you sure you want to continue connecting (yes/no)?
```

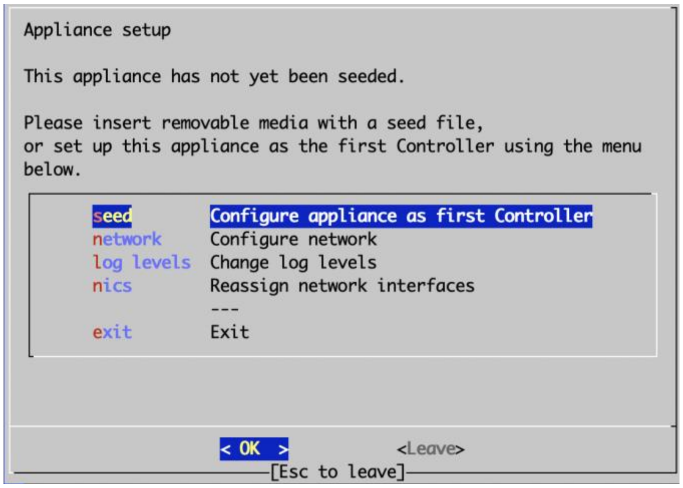
3. Type **`yes`** and click **Enter**. Once connected, you see the following login message:

```
Hint: run 'sudo cz-setup' for appliance management.
```

4. Once connected to your instance via SSH, run the following command to launch the interactive setup tool:

```
sudo cz-setup
```

You will see the following screen:



```
Appliance setup

This appliance has not yet been seeded.

Please insert removable media with a seed file,
or set up this appliance as the first Controller using the menu
below.

      seed        Configure appliance as first Controller
      network     Configure network
      log levels  Change log levels
      nics        Reassign network interfaces
                  ---
      exit        Exit

                  < OK  >            <Leave>
                        [Esc to leave]
```

Use the up ↑ **and down ↓ arrow keys** to highlight items and "**Enter**" to select items.

5. Select **Configure appliance as first Controller**

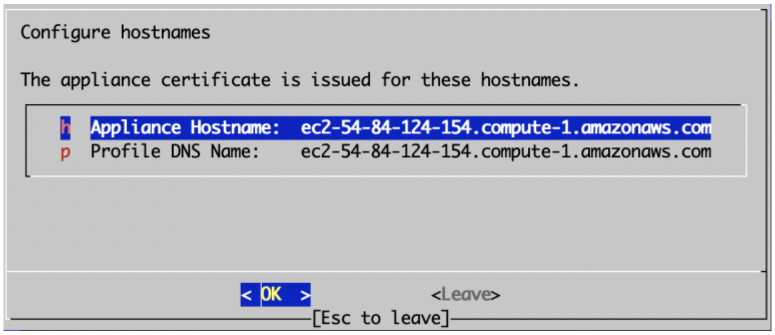
6. Select **Hostnames** and enter the following information:

    **Appliance Hostname**
    `yourElasticIP`[9]

    **Profile DNS Name**
    `yourElasticIP`[10]

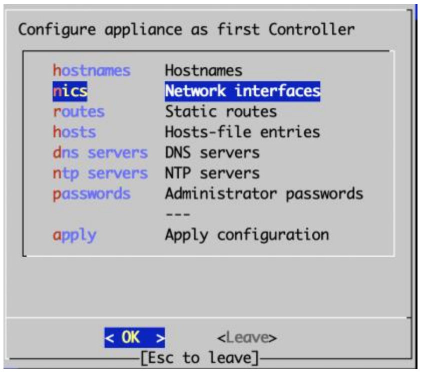
7. Click **Esc** to return to the top-level menu.

[9] For example: `ec2-54-84-124-154.compute-1.amazonaws.com`
[10] For example: `ec2-54-84-124-154.compute-1.amazonaws.com`



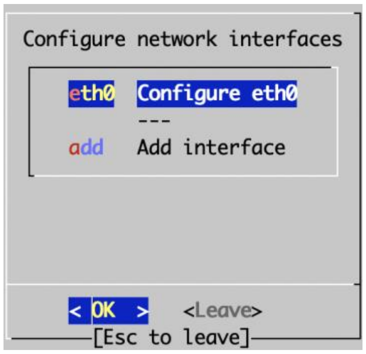
```
Configure hostnames

The appliance certificate is issued for these hostnames.

  h  Appliance Hostname:   ec2-54-84-124-154.compute-1.amazonaws.com
  p  Profile DNS Name:     ec2-54-84-124-154.compute-1.amazonaws.com

                 < OK >              <Leave>
                       [Esc to leave]
```

8. Select **Network interfaces**



```
Configure appliance as first Controller

  hostnames     Hostnames
  nics          Network interfaces
  routes        Static routes
  hosts         Hosts-file entries
  dns servers   DNS servers
  ntp servers   NTP servers
  passwords     Administrator passwords
                ---
  apply         Apply configuration

          < OK >        <Leave>
            [Esc to leave]
```

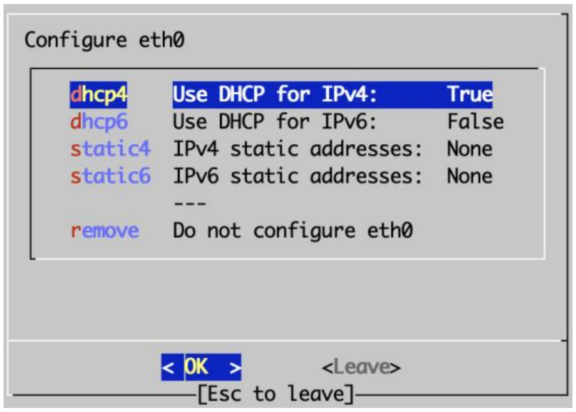
9. Select **Configure eth0**



```
Configure network interfaces

   eth0   Configure eth0
          ---
   add    Add interface

      < OK >   <Leave>
      [Esc to leave]
```

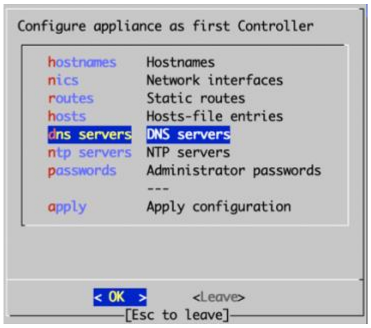
10. Verify the settings match the following and then click **Esc** twice to return to the top-level menu.

| | |
|---|---|
| Use DHCP for IPv4: | True |
| Use DHCP for IPv6: | False |
| IPv4 static addresses: | None |
| IPv6 static addresses: | None |



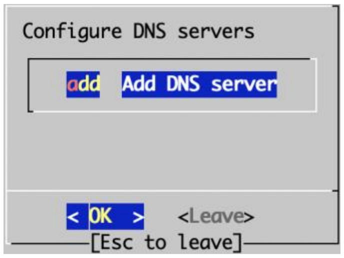
```
Configure eth0

  dhcp4    Use DHCP for IPv4:        True
  dhcp6    Use DHCP for IPv6:        False
  static4  IPv4 static addresses:    None
  static6  IPv6 static addresses:    None
           ---
  remove   Do not configure eth0

          < OK  >        <Leave>
              [Esc to leave]
```

11. Select **DNS Servers**



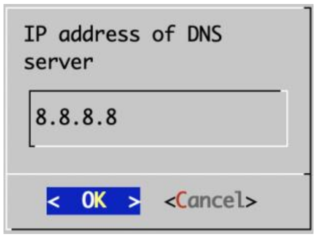
```
Configure appliance as first Controller

  hostnames    Hostnames
  nics         Network interfaces
  routes       Static routes
  hosts        Hosts-file entries
  dns servers  DNS servers
  ntp servers  NTP servers
  passwords    Administrator passwords
               ---
  apply        Apply configuration

          < OK  >        <Leave>
              [Esc to leave]
```

12. Select **Add DNS server**



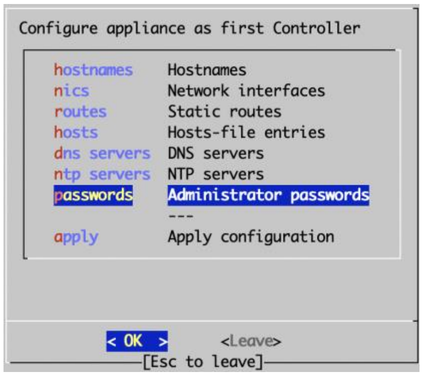
```
Configure DNS servers

  add  Add DNS server

     < OK  >    <Leave>
        [Esc to leave]
```

13. Enter `8.8.8.8` to use Google’s DNS or you may use your preferred provider’s DNS. Click **Esc** twice to return to the top-level menu.



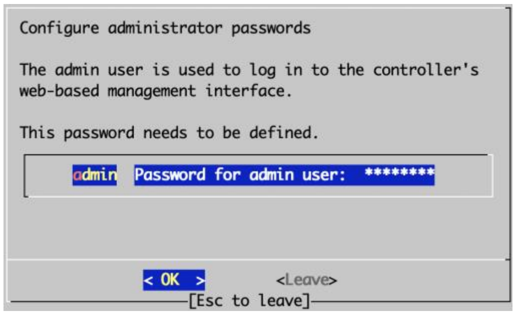
```
IP address of DNS
server

 8.8.8.8

  <  OK  >   <Cancel>
```

14. Select **Administrator passwords**.



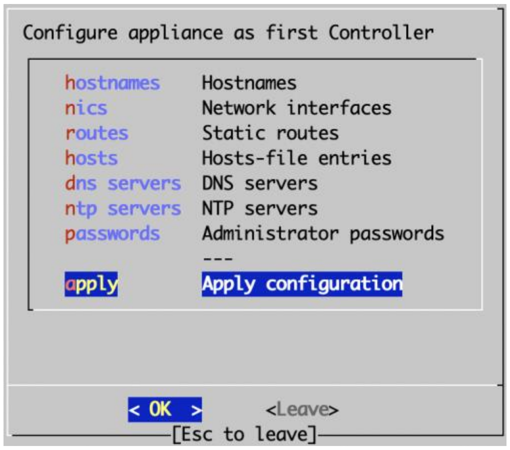
```
Configure appliance as first Controller

  hostnames     Hostnames
  nics          Network interfaces
  routes        Static routes
  hosts         Hosts-file entries
  dns servers   DNS servers
  ntp servers   NTP servers
  passwords     Administrator passwords
                ---
  apply         Apply configuration

          < OK  >         <Leave>
              [Esc to leave]
```

15. Set the password for the **admin** user. We will need the admin password to access the Admin GUI in the next step.



```
Configure administrator passwords

The admin user is used to log in to the controller's
web-based management interface.

This password needs to be defined.

      admin  Password for admin user:  ********

          < OK  >         <Leave>
              [Esc to leave]
```

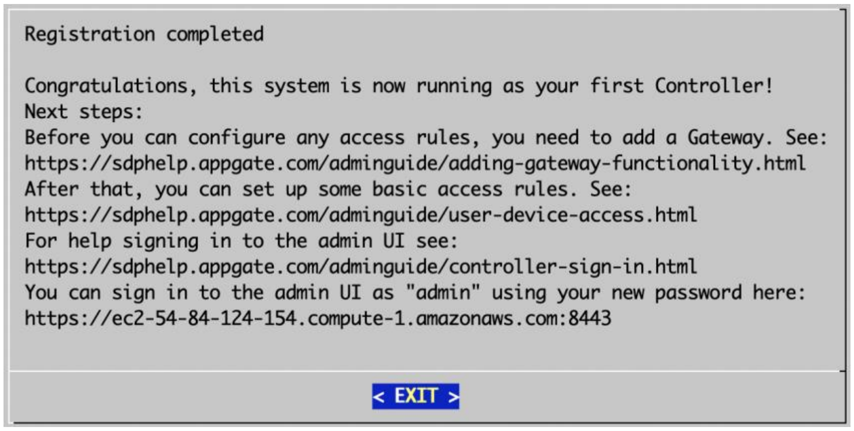
16. Hit **Esc** to return to the top-level menu, and then select **Apply configuration**. Confirm **Yes** when prompted.



```
Configure appliance as first Controller

  hostnames     Hostnames
  nics          Network interfaces
  routes        Static routes
  hosts         Hosts-file entries
  dns servers   DNS servers
  ntp servers   NTP servers
  passwords     Administrator passwords
                ---
  apply         Apply configuration

          < OK  >         <Leave>
              [Esc to leave]
```

17. Once the appliance configuration is complete, you'll see a confirmation message like the one below.

**Copy the admin UI URL**, which we'll use in the next step.



```
Registration completed

Congratulations, this system is now running as your first Controller!
Next steps:
Before you can configure any access rules, you need to add a Gateway. See:
https://sdphelp.appgate.com/adminguide/adding-gateway-functionality.html
After that, you can set up some basic access rules. See:
https://sdphelp.appgate.com/adminguide/user-device-access.html
For help signing in to the admin UI see:
https://sdphelp.appgate.com/adminguide/controller-sign-in.html
You can sign in to the admin UI as "admin" using your new password here:
https://ec2-54-84-124-154.compute-1.amazonaws.com:8443
```

18. Exit `cz-setup` and log out of SSH. Proceed to Step 3: Configure Gateway using Admin GUI

## Step 3: Configure Gateway using Admin GUI

Once the appliance configuration is complete, you can access the Controller's admin UI through the admin/API TLS connection on port 8443.

**To sign into the Controller's Admin UI:**

1. In your browser, open the Admin UI URL that you copied in the previous step.

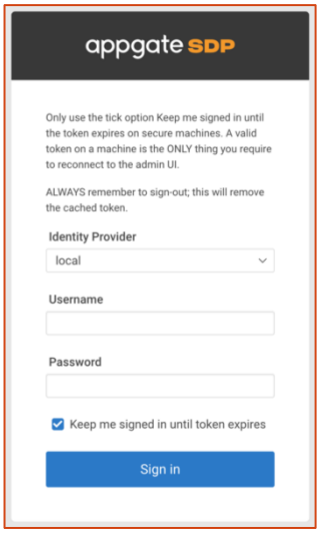
```
https://ec2-54-84-124-154.compute-1.amazonaws.com:8443
```

Remember, add `https://` to the front and `:8443` to the end of the URL

Your browser will likely display a security warning since the connection uses HTTPS into an AWS domain, while the server uses a self-signed certificate. You can safely ignore this warning and proceed to the login screen.

2. Enter the following information and click **Sign in**.

| | |
|---|---|
| **Identity Provider:** | local |
| **Username:** | admin |
| **Password:** | Enter the admin password you chose in Step 2: Setup first Controller of this deployment guide. |



appgate SDP

Only use the tick option Keep me signed in until the token expires on secure machines. A valid token on a machine is the ONLY thing you require to reconnect to the admin UI.

ALWAYS remember to sign-out; this will remove the cached token.

Identity Provider: local

Username

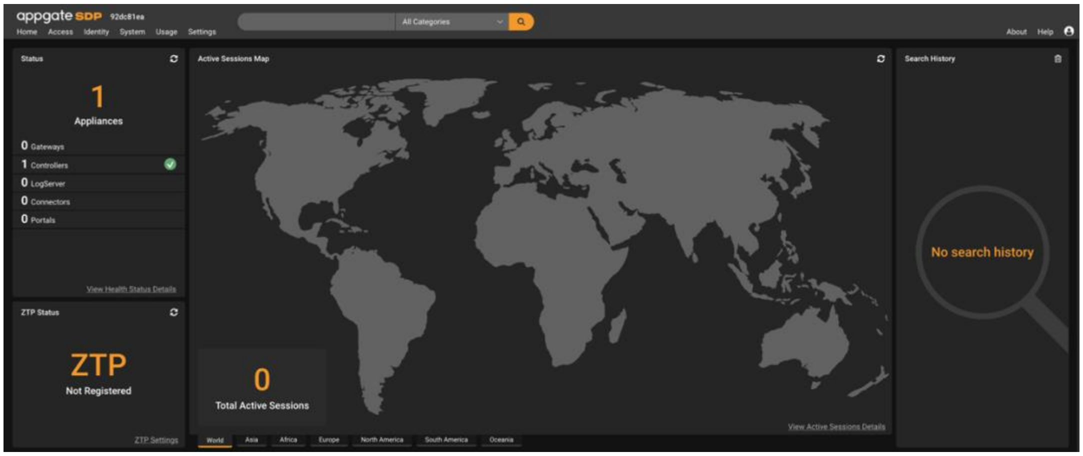
Password

☑ Keep me signed in until token expires

Sign in

## Admin GUI Overview

Let’s look at the Admin Dashboard.



The left-hand side of the dashboard shows the current system status, including the number of appliances in the overall Appgate SDP system.

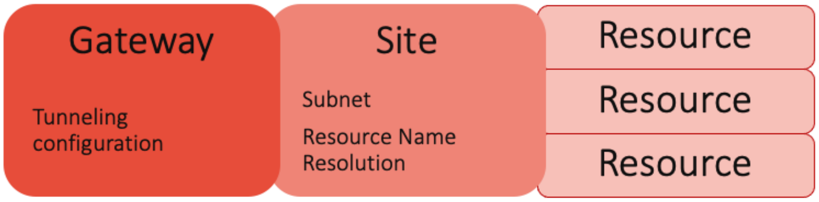
The menu at the top provides the controls for administrative management of the appliance itself and to manage user access to protected resources.

In the center is a map which shows active sessions. The search bar (at the top) can be used to quickly take you to items you have already configured.

Under **Status**, you should see **1 Appliance**, which is the **1 Controller**. The Controller is the “brain” of the system, acting as the Policy Decision Point (PDP).

To get started, we need to configure a Gateway, which you’ll need to access your SDP-protected AWS instances. The Gateway acts as Policy Enforcement Point (PEP) where policy decisions are carried out or enforced. All Client traffic to and from the SDP-protected resources is managed by the Gateways.

As shown below, each Gateway is associated with one Site, and within each Site are multiple SDP-protected Resources.



The Site is also where the resource name resolution is set up, to enable dynamic detection of newly created AWS EC2 instances. Next, let's get started with the Site.

## Configure a Site

**To create a Site:**

1. From the Admin UI, go to **System > Sites** and click **Default Site**.
2. From the **General** tab, rename the Site to **AWS VPC Site**.
3. From the **Name Resolution** tab, under Name Resolvers, select **Add New > AWS Resolver**.
4. Configure the AWS Name Resolver:
    - 4.1. Enter a **Name** for the AWS Resolver (e.g., **`AWS Resolver 1`**).
    - 4.2. Next to **Regions**, click **Add New**.
        - 4.2.1. Enter the AWS region used when creating the EC2 instance using the compact region format (for example, **`us-east-1`**) [11]
        - 4.2.2. Click the **Check Mark** to finish editing.
    - 4.3. Click **Done**.
5. Click **Save**.

## Configure the Gateway appliance

Once you have set up the Controller, the same appliance can also be used as a Gateway.

**To configure the Controller appliance to also be a Gateway:**

1. From the Admin UI, go to **System > Appliances**. From the list of appliances, click the appliance you created earlier to edit it.
2. Click the **Functions** tab:
    - 2.1. Under Appliance Functions, select the **Gateway checkbox**.
    - 2.2. Under Appliance Site, choose the Site you previously created (for example, **`AWS VPC Site`**).
    - 2.3. Under Secure Tunnel Settings, next to **Client Tunneling - Allow Destinations**, click **Add New**. The Target pop-up window opens.

[11] For the full list of AWS Regions, see https://docs.aws.amazon.com/general/latest/gr/rande.html

3. From the **Target** pop-up window, enter the following information to add a target destination.

| | |
|---|---|
| **Address** | `<Leave Blank>` |
| **Netmask Length** | `<Leave Blank>` |
| **Network Interface** | `eth0` |

4. Click **Done**.
5. Click **Save**, then a confirmation window appears.
6. Click **Confirm** to push the changes to the appliance.

## Create (or Choose) an AWS Instance to Protect

You can either create a new EC2 instance or select an existing instance to test out access via Appgate SDP. The instance you choose should have a web server running on port 80, since that's what we'll be configuring our first policy to allow access to with the SDP Client, which we will setup later in this deployment guide.

We recommend creating a new EC2 instance running a simple preconfigured web server, such as AWS Marketplace: Apache Tomcat packaged by Bitnami.[12] Assuming you're familiar with launching EC2 instances, we're not going to take you through this step-by-step, but we are going to point out a few things that are important to set up correctly, see below.

**To launch an EC2 instance to protect using Apache Tomcat packaged by Bitnami's AWS Marketplace AMI, configure the following instance details in the EC2 Launch Wizard:**

1. **Name and tags**
   We will be using AWS tags to resolve this instance, so you must tag the instance:
   1.1. Click **Add additional tags > Add tag**
   1.2. For Key, enter **`app-type`**
   1.3. For Value, enter **`employee-app`**
   1.4. For Resource types, select **Instances** from the list
   Without this tag, Appgate SDP's name resolver will not be able to find this instance.
2. **Subnet and VPC**
   Choose the subnet and VPC that we configured Appgate SDP to protect in the previous steps.
3. **Auto-assign public IP**
   Do NOT allocate a public IP address, so the instance will only accessible from the Appgate SDP network. Choose **Disable** from the list
4. **AWS Security Group**
   Create a new security group that allows all TCP traffic, but only from the private IPv4 address belonging to the Appgate SDP instance we had setup in Step 1 of this deployment guide. You can use the Amazon EC2 console[13] to find the instance's private IPv4 address. This private IPv4 address must be in the same subnet as your Apache Tomcat web server.

[12] https://aws.amazon.com/marketplace/pp/prodview-f23upzzjwznxm
[13] https://console.aws.amazon.com/ec2/#Instances

For example, if the private IPv4 address of the Appgate SDP instance is `172.31.29.70`, add the following inbound rule to the security group using CIDR notation:

| Description | Type | Protocol | Port Range | Source |
|---|---|---|---|---|
| Security group rule 1 | All TCP | TCP | 0-65535 | `172.31.29.70/32` |

Remember to replace the **Source** IP address in the above example with your Appgate SDP instance's private IPv4 address using CIDR notation.

5. Review the instance details, and when you're ready, click **Launch Instance** to complete the launch process for the resource.

   The Apache Tomcat web server will be assigned a private IPv4 address within the same subnet as the Appgate SDP instance we had setup in Step 1 of this deployment guide.

   You should not be able to access the Apache Tomcat server at this time since there is no network route for you yet. In the next steps, we'll create the policy that will grant you access to the Apache Tomcat server.

## Create an Entitlement

Policies and Entitlements are the primary tools for provisioning and controlling user access to resources protected by Appgate SDP Gateways.

An *Entitlement* is the primary mechanism for defining what resources a user will have access to on the protected network.

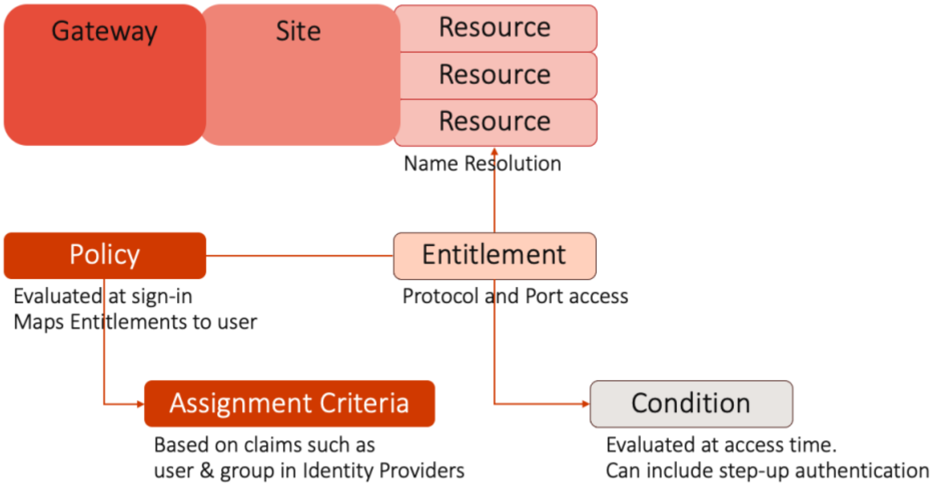
Entitlements contain *Actions*, which define the exact (firewall) rules that will be implemented for the user.

A *Condition* is an optional component within an Entitlement. Defining a Condition allows you to implement Actions, which depend on attributes, such as, the status of the network, which may change while the Entitlement is active.

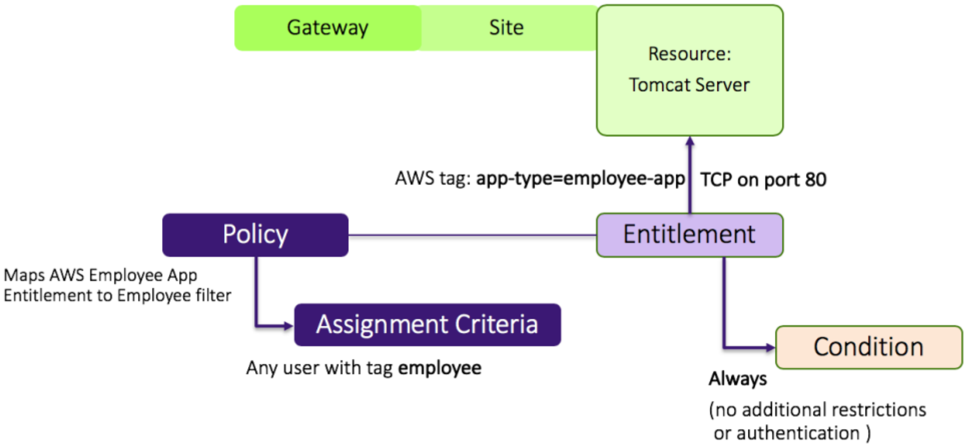
Example transient statuses include:

- Laptop moved from corporate environment to a non-trusted network connection (for example, to a hotspot or cafe WIFI).
- Contractor only needing access to resources during working hours.
- Anti-Virus protection is disabled.

As shown in the diagram below, Entitlements are grouped together in *Policies*. Policies use *Assignment Criteria* to control which Entitlements are available to which users.



**The diagram below shows the Policy and Entitlement that we're going to be creating:**



- The Entitlement allows HTTP access to any server in our site that has the tag **`app-type=employee-app`**. Appgate's dynamic AWS name resolver will automatically detect new EC2 instances created in our VPC, and grant access if they have this tag.
- In our example Entitlement, we chose not to define a Condition. Again, Conditions can be used to enforce restrictions on network location, time of day, or to apply step-up authentication (we're keeping it simple for this example and not using any of those!). In our example, you can think of the lack of a Condition being defined to mean "*Always apply this Entitlement*".
- Assignment criteria selects the Policy, which in turn binds the Entitlements to the set of allowed users. In our example, we're going to let any user with a tag **`employee`** get access. (The user tag is metadata within the Appgate system and is separate from the AWS tag used for EC2 instances).

Next, we need to create an Entitlement with the AWS resolver format.

**To create an Entitlement to access the Apache Tomcat web server:**

1. From the Admin UI, navigate to **Access > Entitlements**
2. Click **Add New** and enter the following information:

2.1. **Name**
`AWS employee app type`

2.2. **Site**
`AWS VPC Site` (select the site we created above)

2.3. **Actions**

2.3.1. Click **Add New** and enter the following information:

| | |
|---|---|
| **Host(s) – target or source:** | `aws://tag:app-type=employee-app` |
| **Rule:** | `ALLOW traffic (through Gateway)` |
| **Protocol:** | `TCP up`[14] |
| **Ports:** | `0-65535` |

2.3.2. Click **Done**.

2.4. **Access Control**
Verify that **Always allow Action(s)** is selected, so the Entitlement Action will always be evaluated

3. Click **Save**

## Create a User

The customer can choose to use either the built-in local identity provider or an external identity provider of their choice. In this deployment guide, we cover setting up the local identity provider for simplicity. For production systems, it is recommended that you configure an external identity provider. For details on setting up an identity provider, see SDP Admin Guide: Configure identity providers[15]

**To create a user:**

1. From the Admin UI, navigate to **Identity > Local Users**

[14] By setting the Protocol to TCP up, we are allowing TCP traffic initiated from the client up to the server; return traffic is automatically allowed.
[15] https://sdphelp.appgate.com/adminguide/identity-providers-configure.html

2. Click **Add New** and enter the following information to add a new local user:

| | |
|---|---|
| **Username:** | `test-user` |
| **Password:** | Choose a password that we'll use to sign in to the Appgate SDP Client |
| **First Name:** | `Test` |
| **Last Name:** | `User` |
| **Tags:** | Click **Add New** and enter the following tag:<br>`employee`<br>Click the **Check Mark** to finish editing. |

3. Click **Save**

> **Important:** Make sure to add the **`employee`** tag to the user. This tag is how the Policy will assign access to the Entitlements.

## Create a Policy

Next, we'll create the Policy that uses the **`employee`** tag to assign the **`employee-app`** Entitlement.

**To create the Policy:**

1. From the Admin UI, navigate to **Access > Policies**
2. Click **Add New > Access Policy** and enter the following information:

| | |
|---|---|
| **Name:** | `Policy Employee Access to Employee Apps` |
| **Status:** | `Enabled` |
| **Assignment:** | Click **Add New**.<br>For **Assignment Criteria**, choose **tags** from the list.<br>For **Operator**, choose **match** from the list.<br>For **Value**, enter **`employee`**.[16]<br>Click the **Check Mark** to finish editing. |
| **Entitlements (by name):** | Click **Add New**.<br>Choose **AWS employee app type** from the list.<br>Click the **Check Mark** to finish editing. |

3. Click **Save**.

[16] This is how the Policy will pick up our newly created user to whom we applied the employee tag earlier.

# Step 4: Deploy the Client to End Users

The last step is to install the Client on end user devices. The Appgate SDP Client installs a virtual network adapter, which provides remote, encrypted access to resources. Because it works like a network adapter, it requires local admin privileges to install. Client installation is a straightforward process and is not shown here.

**Download the Appgate Client:**

- The Windows, MacOS, and Linux clients are in the Appgate SDP User Guide.[17]
- The iOS client is available from the Apple App Store.[18]
- The Android client is available from the Google Play Store.[19]

Select the download link for your operating system and install the software on your device.

## Copy the Client Profile URL

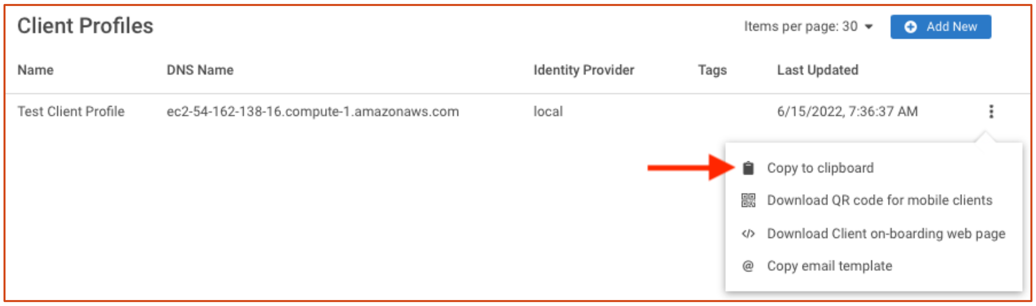
Any new Appgate SDP system will use Single Packet Authorization in TCP mode by default. This means the servers are cloaked and the Clients need to present a special pre-shared packet containing a key to make a connection. The connection to the Controller also requires the Client to check the server's certificate before establishing a TLS connection. Both requirements get fulfilled by copying a URL from the Controller and using this in the Client when making the first connection.

**To get the Client Profile URL from the Admin UI:**

1. Go to **Identity > Client Profiles**.
2. Click **Add New** and enter the following information:
   **Profile name** [20]
   `Test Client Profile`
   **Identity Provider**
   `Local`
3. Click **Save**. When adding a Client Profile, you must save before you can export it.

[17] https://sdphelp.appgate.com/userguide/getting-started/installation/index.html
[18] https://itunes.apple.com/us/app/appgate-sdp/id1295622462?mt=8
[19] https://play.google.com/store/apps/details?id=com.cryptzone.appgate.xdp&hl=en
[20] The name of the Client Profile will appear in the Client, so choose a name that is meaningful to users.

4. Click the 3-dots hamburger icon next to the **Test Client Profile** that we created above (see below), and then click the **Clipboard icon <** 📋 **>** to copy the Client Profile URL to the clipboard.



Client Profiles

Items per page: 30

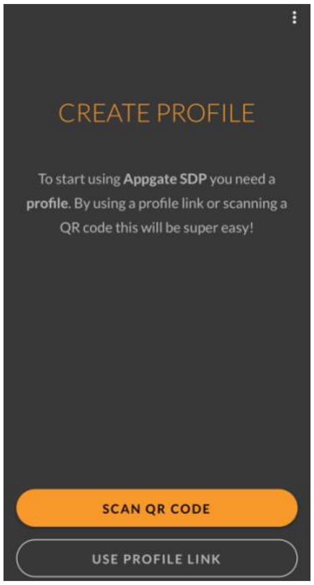
| Name | DNS Name | Identity Provider | Tags | Last Updated |
|---|---|---|---|---|
| Test Client Profile | ec2-54-162-138-16.compute-1.amazonaws.com | local |  | 6/15/2022, 7:36:37 AM |

Add New
Copy to clipboard
Download QR code for mobile clients
Download Client on-boarding web page
Copy email template

## Log in to the Client

**To log in to the Client to connect to your protected resources:**

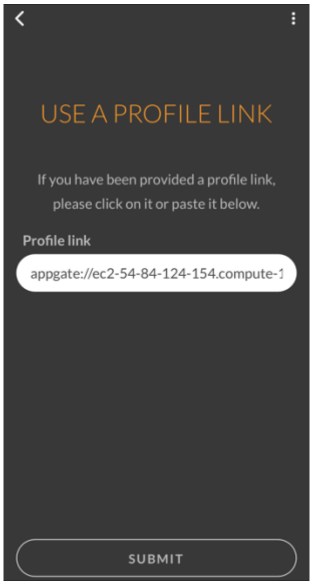
1. Open the Appgate SDP Client.
2. Click **USE PROFILE LINK**.



CREATE PROFILE

To start using **Appgate SDP** you need a **profile**. By using a profile link or scanning a QR code this will be super easy!

3. For **Profile link**, paste the **Client Profile URL** from the previous step, then click **SUBMIT**.

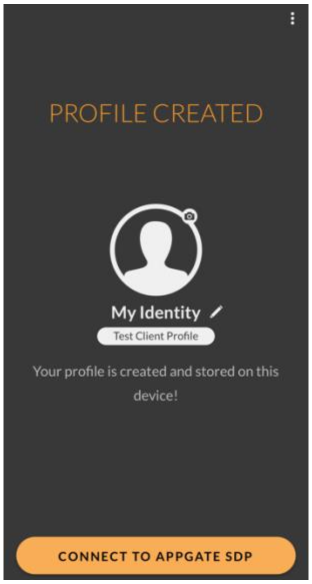


USE A PROFILE LINK

If you have been provided a profile link, please click on it or paste it below.

Profile link: appgate://ec2-54-84-124-154.compute-1

4. Once the profile is created, click **CONNECT TO APPGATE SDP**.



PROFILE CREATED

My Identity

Test Client Profile

Your profile is created and stored on this device!

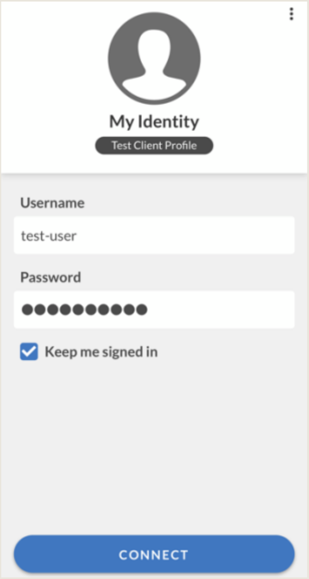
4. Enter your login details and click **CONNECT**.

   **Username**

   `test-user`

   **Password**

   Enter the password you had previously created.



My Identity

Test Client Profile

Username

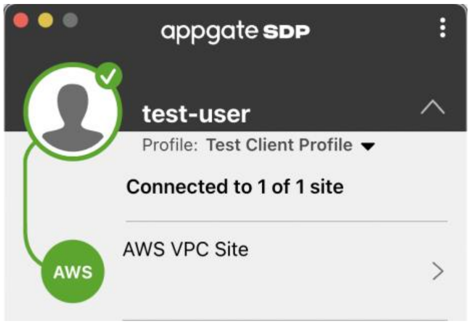
test-user

Password

●●●●●●●●●●●

☑ Keep me signed in

5. Once connected, the client visually displays the connection to your AWS VPC Site, as shown below.



test-user

Profile: Test Client Profile

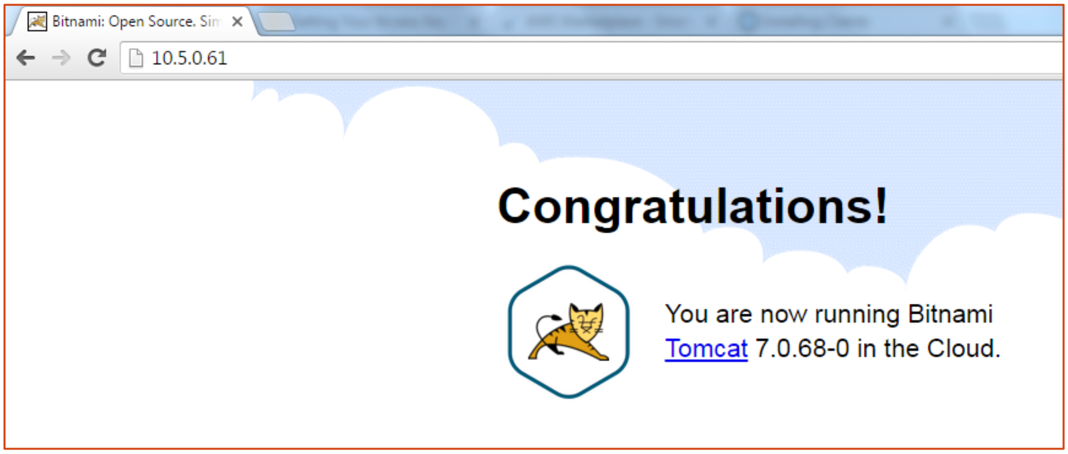
Connected to 1 of 1 site

AWS VPC Site

Congratulations, you are now ready to access the protected instance with Appgate SDP!

## Step 5: Testing Access

Try to access the protected resource using its private IP address. It should work as shown below:



Congratulations!

You are now running Bitnami Tomcat 7.0.68-0 in the Cloud.

With these simple policies in place, network access dynamically adapts in real-time to changing conditions on both the client and cloud infrastructure. You can be assured every new instance that is added or removed into the protected VPC will be discovered by Appgate and assigned to the appropriate policies, without any administrative intervention. This results in significantly less operational maintenance with a much higher degree of security for your cloud resources!

### Troubleshooting

If you are unable to load the protected resource using its private IP address:

- Verify that it's running and has an IP address in the subnet that the Gateway is protecting
- Verify the Site and Gateway configurations are correct
- Check the Security Group settings
- SSH into the Appgate server again, and try pinging the protected resource
- Verify the resource has the appropriate tag and the Entitlement resolver uses the same tag (**`app–type=employee–app`**)
- Verify the user has the **`employee`** tag and the Policy has the corresponding Assignment Criteria set up correctly

For more information on handling fault conditions, see SDP Admin Guide: Troubleshooting[21]

## Monitoring Appliance Health

Appgate SDP provides an SNMP MIB (Management Information Base) which includes a rich set of metrics that can be used to monitor the health of the appliances in the Collective. For more details on how to properly monitor and manage your deployment, see SDP Admin Guide: SNMP MIB.[22] You can also monitor the health and check the appliance status in the Amazon EC2 console.

[21] https://sdphelp.appgate.com/adminguide/troubleshooting-guide.html

[22] https://sdphelp.appgate.com/adminguide/snmp-mib.html

**To view status checks in the EC2 console:**

1. Open the Amazon EC2 console at https://console.aws.amazon.com/ec2/
2. In the navigation pane, choose **Instances**.
3. On the Instances page, the **Status check** column lists the operational status of each instance.
4. To view the status of an instance, select the instance, then switch to the **Status checks** tab.

# Backup and Recovery

There are a few ways to create a backup file:

- Use the Appgate Backup script, which creates a backup file of the entire Appgate SDP Collective. (We strongly recommend the use of the Appgate Backup script.)
- Create a snapshot of the virtual machine, which saves the entire appliance configuration and file system.

Use the `cz-restore` utility and the backup file created by the Appgate Backup script on a fresh non-activated appliance to recreate an equivalent system. We recommend performing recovery testing on a regular basis. For more details, check out SDP Admin Guide: Backup and restore.[23]

# Upgrading Appliances

Appgate regularly enhances its software products, periodically releasing software patches, updates, and upgrades to deliver new product features and software fixes. An active paid Software Subscription License is required to receive software updates and upgrades. Each release has a unique set of AMIs, which will be made available to existing subscribers of the product through the AWS Marketplace at no additional cost. For more details on software patches and upgrades, see SDP Admin Guide: Upgrading appliances[24]

## Version Availability

| Version | Support Level Status | Support Resources |
|---|---|---|
| **Appgate SDP v6.0** | Full Support | https://www.appgate.com/support/software-defined-perimeter-support/sdp-v6-0 |
| **Appgate SDP v5.5** | Full Support | https://www.appgate.com/support/software-defined-perimeter-support/sdp-v5-5 |
| **Appgate SDP v5.4** | Full Support | https://www.appgate.com/support/software-defined-perimeter-support/sdp-v5-4 |
| **Appgate SDP v5.3** | Support until 30 July 2022.<br>No Support thereafter. | https://www.appgate.com/support/software-defined-perimeter-support/sdp-v5-3 |

[23] https://sdphelp.appgate.com/adminguide/backup-and-restore.html

[24] https://sdphelp.appgate.com/adminguide/upgrading-appliances.html

# Product Support

**Support documentation is available online:**

- SDP Admin Guide: https://sdphelp.appgate.com/adminguide
- Client User Guide: https://sdphelp.appgate.com/userguide

## Support Terms

A paid Appgate SDP Subscription Licenses, excluding BYOL, entitles the user to receive product support. All paid products will be supported through the Appgate Support Terms found at https://appgate.com/legal/product-and-service-terms-and-conditions

The Appgate Support Terms are subject to the product End User License Agreement (EULA).

Upgrading to the latest version of Appgate SDP indicates your acceptance of any new terms that may be applicable for the new version.

## Contact Customer Support

For product-related support inquiries, send your question(s) along with your AWS Account ID to"

AppgateSDP.Support@appgate.com

Please be sure to include your AWS Account ID in the body of your email.

## Support Level Definitions

| Support Level | Definition |
|---|---|
| **Full Support** | Support will be provided such as with troubleshooting or installation/configuration problems. The most recent patch version of the Software [Appgate SDP] must be used which will be updated with feature packs, product enhancements and bug fixes. All Associated systems [such as host OS] must be fully patched and manufacturer supported. Where specified versions are shown, these must be used. Full support for any newer versions of Associated systems will be provided in the first subsequent release of the Software unless otherwise stated. |
| **Support** | Support will be provided such as with troubleshooting or installation/configuration problems. The most recent patch version of the Software must be used and even though the Software is no longer being actively developed, it may still occasionally receive bug fixes and security patches. For new feature packs, product enhancements and the most recent security fixes, customers must upgrade. Where specified, the Associated systems version compatibility is frozen, however the Software may run on newer versions of Associated systems. Customers may be asked to upgrade their Associated systems and/or Software to resolve any issues. |
| **Qualified Support** | Support may be provided such as with troubleshooting or installation/configuration specifically related to the Software on a best effort basis. The Software is frozen, so in problem situations customers must upgrade. Software used on Associated systems that no longer have manufacturer support, automatically fall under qualified support and the Software is used at the customers own risk. |

| | |
|---|---|
| **No Support** | When specified, the Software (version) is no longer in support. For any Associated systems specified and all others not specifically mentioned elsewhere, the Software (version) will not run on these Associated systems, customers must upgrade their Software and/or Associated systems. |

# Software Pricing Details

Charges associated with your use of the Appgate SDP for AWS software fall into two categories:

- **AWS Infrastructure** – All AMI-based products incur associated AWS infrastructure charges depending on the services and infrastructure used. These rates and fees are defined and controlled by AWS and can vary between AWS Regions. For more information, see https://aws.amazon.com/pricing/
- **Appgate SDP Software Usage** – The charges incurred for your use of the Appgate SDP software. These rates and fees are defined and controlled by Appgate and can vary between the Licensing Models as defined in Software Licensing.

## Billable Services

The following table lists the AWS resources used by Appgate SDP and if they are required and billable.

| Service | Required | Billable | Notes |
|---|---|---|---|
| Amazon EC2 | Yes | Yes | |
| Amazon EBS | Yes | Yes | |
| Amazon VPC | Yes | Yes | Additional services are billable (e.g., Elastic IP, AWS Network Egress) |
| AWS CloudFormation | No | No | |
| Software Usage: Appgate SDP | Yes | Yes | See Software Licensing |

All Appgate SDP for AWS Marketplace products run within a customer's AWS account. The total price is a combination of the Appgate SDP software usage charge and the AWS infrastructure costs for the resources running in the customer's AWS account. Buyers are responsible for all the AWS infrastructure costs. These costs are set by AWS and are available at https://aws.amazon.com/pricing/

## Licensing

The following table provides general information about the licensing models available for Appgate SDP products on the AWS Marketplace and shows pricing information for each product. You can choose from several available licensing models. All pricing is based on US dollars (USD).

| Licensing Model | Description |
|---|---|
| **Hourly or Annual Pricing with Free Trial** | **Appgate SDP**<br>https://aws.amazon.com/marketplace/pp/prodview-sshqbmjhlrx6o<br>Appgate SDP's paid version comes with a 15-day Free Trial. This product includes a 25-user license and should be deployed as a single standalone SDP appliance. The buyer pays either on an hourly basis or hourly with an annual contract.<br>**Free Trial –** Hourly and Annual subscriptions include a **15-day Free Trial** allowing customers to run one instance of the software without incurring a charge for 15 days. The free trial applies to the most expensive instance type that is running, and any concurrent usage outside the one instance is billed at the hourly rate.<br>**Hourly –** Software is charged by the hour at a rate of **$0.70** per EC2 instance hour, and usage is rounded up to the nearest whole hour.<br>**Annual –** Customers have the option to purchase a year's worth of usage upfront for one EC2 instance of any instance type at a rate of **$5,500.00** per year. Annual subscriptions provide a **10 percent savings** compared to running the same product hourly for extended periods. Any customer usage above the number of annual subscriptions purchased is billed at the hourly rate. |
| **Metered Pricing (Per Provisioned User)** | **Appgate SDP – Metered**<br>https://aws.amazon.com/marketplace/pp/prodview-2fhzg7bqt225u<br>Appgate SDP's Metered version is a pay-as-you-go model enabling customers to only pay for what they consume. Each hour, the customer is charged for the total number of provisioned users at a rate of **$0.015** per user (per hour). All usage is calculated monthly and billed monthly through AWS Marketplace. |
| **Bring Your Own License (BYOL)** | **Appgate SDP – BYOL**<br>https://aws.amazon.com/marketplace/pp/prodview-pher4gyrq4pky<br>Appgate SDP's BYOL version requires a separate software license. AWS Marketplace doesn't charge customers for usage of the Appgate SDP software, but customers must supply a separate license key to activate the product.<br>A license key must be purchased outside of AWS Marketplace to use this product. Without this license key, the product is limited to **2 Users** and **1 Site**.<br>To obtain a license for the product, go to https://www.appgate.com/support/software-defined-perimeter-support/sdp-additional-licenses |

## Managing Licenses

You can view and manage your Appgate SDP licenses in the AWS Marketplace subscription manager by signing into the AWS Marketplace console at https://console.aws.amazon.com/marketplace and then choosing **Manage subscriptions**. For information on how to view and manage your Appgate SDP licenses from within the application itself, see SDP Admin Guide: Licenses[25]

[25] https://sdphelp.appgate.com/adminguide/licenses.html