



Appgate SDP[®] for Azure Step-by-Step Setup Guide

Type: Technical guide

Date: April 2024

Applies to: v6.3 and newer

© 2024 Appgate

| | |
|--|-----------|
| WELCOME & OVERVIEW | 3 |
| GETTING STARTED | 4 |
| CREATE VIRTUAL MACHINE INSTANCE | 5 |
| CONFIGURE | 5 |
| DEPLOY | 7 |
| VIEW THE RESOURCE GROUP..... | 8 |
| SIGN IN TO THE APPGATE SDP ADMIN UI..... | 8 |
| ADMIN UI..... | 9 |
| THE GATEWAY..... | 9 |
| ADDING AN INTEGRATED GATEWAY (USING THE EXISTING APPLIANCE)..... | 10 |
| ADDING A STAND-ALONE GATEWAY (USING A NEW APPLIANCE) | 11 |
| <i>Defining a new Appgate SDP Gateway.....</i> | <i>11</i> |
| <i>Export the seed for the new Azure appliance</i> | <i>11</i> |
| <i>Create a new Azure appliance</i> | <i>11</i> |
| <i>Deployment.....</i> | <i>12</i> |
| CREATE (OR CHOOSE) A PROTECTED HOST | 12 |
| ACCESSING THE PROTECTED HOST | 12 |
| ABOUT ENTITLEMENTS | 12 |
| ABOUT POLICIES..... | 13 |
| SET UP APPGATE SDP | 14 |
| <i>Create Entitlements – to access the protected host</i> | <i>14</i> |
| <i>Create a User.....</i> | <i>15</i> |
| <i>Create a Policy.....</i> | <i>15</i> |
| <i>Get the Client Profile Link.....</i> | <i>16</i> |
| INSTALL THE CLIENT..... | 16 |
| ADD A CLIENT PROFILE | 16 |
| SIGN IN TO THE CLIENT | 16 |
| TEST OUT ACCESS! | 17 |
| WHAT IF IT DIDN'T WORK? | 17 |
| ADDITIONAL STEP – USING AZURE NAME RESOLUTION..... | 17 |
| MORE THINGS TO TRY | 18 |
| RESOURCES..... | 18 |

Welcome & Overview

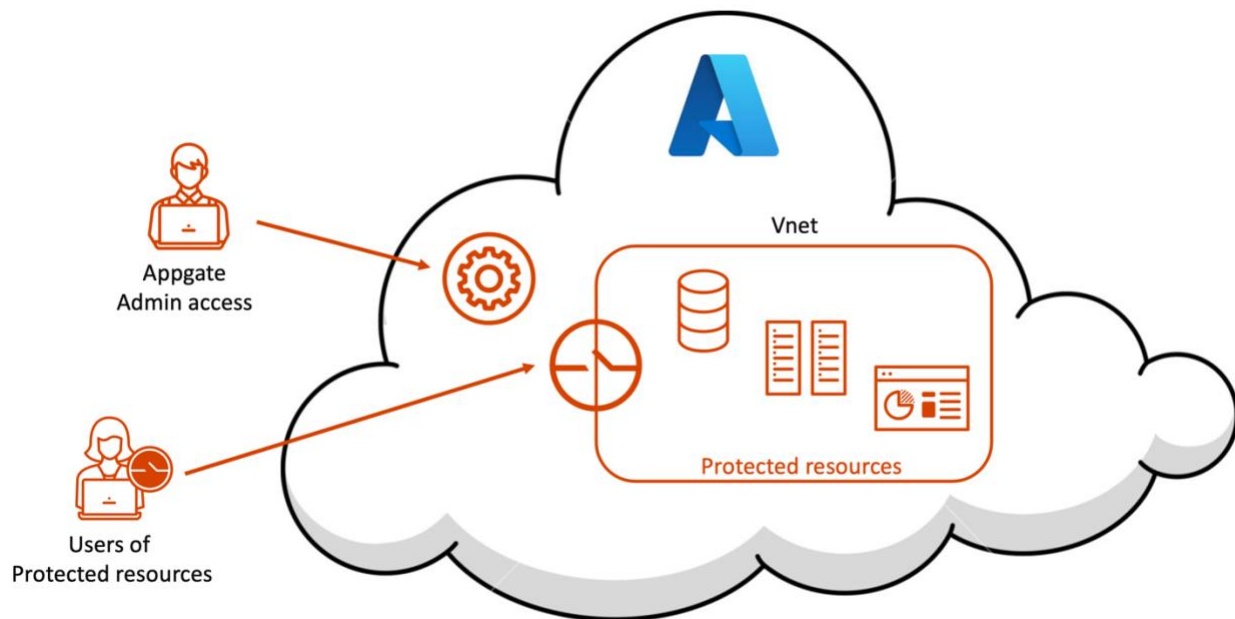
Enterprises continue to embrace Microsoft Azure but securing access to these cloud-based workloads can be a challenge. Appgate SDP is purpose-built for the Azure environment and draws on user context to dynamically create a secure, encrypted network 'segment of one' that's tailored for each user session. It dramatically simplifies the challenge of managing user access to Cloud resources while eliminating IP-based over-entitlement. Appgate SDP provides a means for security teams to efficiently and effectively control user access to Azure resources.

Appgate SDP is a distributed network access control system that creates a unique access profile for each user/device combination. This patented Appgate SDP Policy engine dynamically checks each user/device and along with their context provisions access to an exact set of desired instances.

Certain types of Policies can include information which instructs the Gateways to use real-time information from the cloud provider to automatically adapt access rules as conditions change in the cloud infrastructure. Every new instance that is added or removed will now automatically be identified and added or removed from the access rules, without the need to change the Policies. It becomes an automation-driven network access process that can be very easy to audit because of the much-simplified Policy configuration.

Let's take a look at how we need to configure both Azure and Appgate SDP to be able to use this capability to adapt in real-time to changing conditions in Azure.

All user traffic is tunnelled from their device (via a virtual network adapter, similar to a VPN client), and passed through Appgate SDP gateways to the protected resources. Client traffic to the Appgate SDP gateway is encrypted, so these resources can be securely accessed regardless of location. And the set of protected resources is dynamically adjusted, automatically responding to changes in the Azure environment.



As you'll see, this is much more dynamic and flexible than a firewall – we'll be setting policies that control user access based on user attributes, and on server attributes (such as Azure tags).

This step-by-step guide will take you through the steps necessary to set up and configure Appgate SDP to protect your Azure resources.

Getting Started

In Azure there plenty of defaults which make it relatively painless to quickly spin up instances. This means two things, firstly Appgate SDP is an important component for locking down and managing user access; and secondly it is very easy to get Appgate SDP up and running in the first instance, you will only need a Subscription to Azure and everything else is created on the fly. This document assumes that you're familiar with Azure, and have some experience creating VMs, and setting up the networking features within Azure. If not, or if you need a refresher, please take a look readily available online resources, such as the Azure networking documentation here: <https://docs.microsoft.com/en-us/azure/networking/fundamentals/networking-overview>

Azure has mostly automated the set up and will (optionally) choose to use default network components for our Appgate SDP instance(s).

All VMs in the same Virtual network (VNet) can access each other, this will allow an Appgate SDP Gateway to easily forward all the users traffic to any of the protected resources. But since VNets are logically isolated from each other, an Appgate SDP Gateway would be required for each VNet (unless VNet-to-VNet links exist).

The chosen VNet must be accessible from the internet – as a minimum port 443 should be allowed. A public IP is typically required for most Appgate SDP appliances.

Keep in mind that you will probably now route all traffic to the protected resources running in the protected sub-net through the Appgate SDP. The rules in the Network Security Group must be changed to allow external access to ONLY the Appgate SDP Gateway. Users will then be required to use the Appgate SDP Client for access.

There are 3 steps to getting your Appgate SDP system running.

1. Create one or more instances for the Appgate SDP system – this is probably very similar to the instances you have launched before.
2. Configure the Appgate SDP system using the admin UI to configure Policies, Entitlements and identity providers. This will take the bulk of the time - introducing you to the Appgate SDP Policy and Entitlement model.
3. Install the Client and test it out! – this is where it all comes together, and you can see Appgate SDP in action, dynamically protecting your Azure resource.

So, let's get started – in less than 20 minutes you'll have the system up and running, and will be playing with different Polices and user access rights!

Create Virtual Machine Instance

In this Step, we're going to launch the VHD for the Appgate SDP appliance. The information that follows, details the launch process from within the Azure using a custom template.

There is one thing you do need to have done first on your device. You will need to create and SSH key pair. You will need the public key during the set up.

Search for Appgate SDP in the Azure Marketplace then...

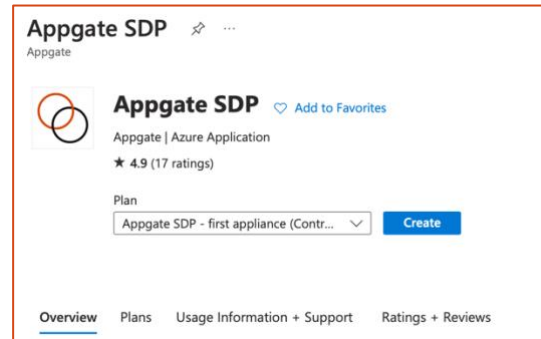
Select *Appgate SDP* and click <Create>.

Create

You don't need to have set anything up within your Azure subscription first, we will create all you need to get your Appgate SDP up and running.

Search for Appgate SDP in the Marketplace then...

Select *Appgate SDP - first appliance (Controller)* and click <Create>.



Configure

The template used within the Azure Console has 3 screens:

Basics:

A screenshot of the "Basics" configuration screen in the Azure console. The screen has three tabs: "Basics", "Select VM settings", and "Review + create". Under "Project details", there is a description: "Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources." There are two dropdown menus: "Subscription" (selected as "Microsoft Azure Enterprise...") and "Resource group" (empty). Below the "Resource group" dropdown is a "Create new" link. Under "Instance details", there are three fields: "Region" (selected as "UK South"), "Appliance name" (empty), and "SSH public key" (empty). At the bottom, there is a link: "Learn more about creating and using SSH keys in Azure".

- **Subscription** – select one and then for Resource Group select <Create new>, and specify a resource group name of your choice. You can only use an existing Resource group if it is empty (Azure limitation).
- **Region** - choose a suitable Location for the Resource Group to be hosted. This could for instance be close to your user community.
- **Appliance name** – provide a suitable name.
- **SSH public key** – paste the public key from earlier.

Select VM Settings:

The screenshot shows the 'Select VM settings' page with the following fields and values:

- AppGate SDP version: 5.4
- Virtual network: (new) VirtualNetwork (with 'Create new' link)
- Subnet: (new) Subnet (10.0.4.0/24)
- Public IP Address for the VM: (new) PublicIP (with 'Create new' link)
- DNS Prefix for the public IP Address: controller190a3440933 (with a green checkmark)
- Password for admin user: (empty text box)
- Confirm Password: (empty text box)
- Profile Hostname (only version >= 5.4): (empty text box)
- VM size: 1x Standard B2s (2 vcpus, 4 GB memory) (with 'Change size' link)

- **Appgate SDP version** – pick the version you want to use.
- **Virtual network** - the template allows from /16 to /24 if creating a new virtual network. The associated Subnet allows from /22 to /29 if creating a new subnet. You don't need to enter anything - you will get a /24 v-net called *Virtual network* with a /24 subnet called *Subnet*.
- **Public IP Address for the VM** – one will be created.
- **DNS Prefix for the public IP address** - first part of the FQDN.
- **Password for the admin user** - which you will need later when using the admin UI.
- **Profile Hostname** – the Profile DNS Name the Clients will use to connect to the Controller(s). Enter a full FQDN.
- **VM size** - We have set a default of B2s. This is only suitable for set-up and small use cases. Production environments should be sized according to function, anticipated user load and network throughput requirements. For further information there is guidance about sizing of cloud appliances in the [Appgate SDP Admin Guide](#).

Review and create

The summary screen is presented once validation has passed. Click <Create> if the summary looks OK.

✓ Validation Passed

Basics Select VM settings **Review + create**

PRODUCT DETAILS

Appgate SDP
by AppGate
[Terms of use](#) | [Privacy policy](#)

TERMS

By clicking "Create", I (a) agree to the legal terms and privacy statement(s) associated with the Marketplace offering(s) listed above; (b) authorize Microsoft to bill my current payment method for the fees associated with the offering(s), with the same billing frequency as my Azure subscription; and (c) agree that Microsoft may share my contact, usage and transactional information with the provider(s) of the offering(s) for support, billing and other transactional activities. Microsoft does not provide rights for third-party offerings. See the [Azure Marketplace Terms](#) for additional details.

Basics

| | |
|----------------|---|
| Subscription | Microsoft Azure Enterprise_jamiebs |
| Resource group | c-test |
| Region | UK South |
| Appliance name | controller1 |
| SSH public key | ssh-rsa AAAAB3NzaC1yc2EAAAADAQABAAQDKfbmAcC76+/7BrEAr1c8... |

Select VM settings

| | |
|--|---------------------|
| AppGate SDP version | 5.4 |
| Virtual network | VirtualNetwork |
| Subnet | Subnet |
| Address prefix (Subnet) | 10.0.4.0/24 |
| Public IP address | PublicIp |
| Domain name label | controller1-main |
| Password for admin user | ***** |
| Profile Hostname (only version >= 5.4) | controller1-profile |
| VM size | Standard_B2s |

The template we used will have created all the required components within Azure - so there is nothing more to do.

Deploy

✓ Your deployment is complete

Deployment name: `cyxtera.appgatesdp-20210521111229` Start time: 5/21/2021, 11:33:43 AM
Subscription: [Microsoft Azure Enterprise_](#) Correlation ID: `de67ae3b-590f-479f-896b-8e219356c842`
Resource group: `c-test`

∨ Deployment details ([Download](#))

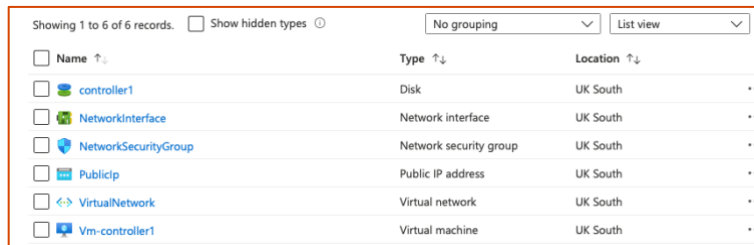
∧ Next steps

[Go to resource group](#)

Once your deployment is complete then you can view or manage all the components within Azure. The appliance will be started and be ready for use after a short while.

View the resource group

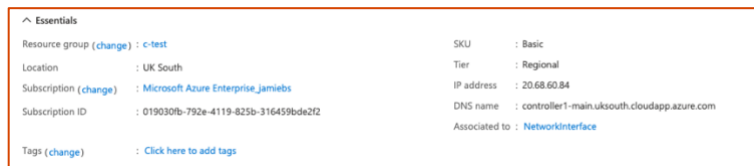
In the new Resource group you should find the following components:



| Name | Type | Location |
|----------------------|------------------------|----------|
| controller1 | Disk | UK South |
| NetworkInterface | Network interface | UK South |
| NetworkSecurityGroup | Network security group | UK South |
| PublicIp | Public IP address | UK South |
| VirtualNetwork | Virtual network | UK South |
| Vm-controller1 | Virtual machine | UK South |

There is no *Availability set* configured for these template-driven marketplace instances. If this is required, then the instances will need to be launched using the (generic) VM option instead.

In the PublicIp component you can find the DNS name of the Controller - so copy this:

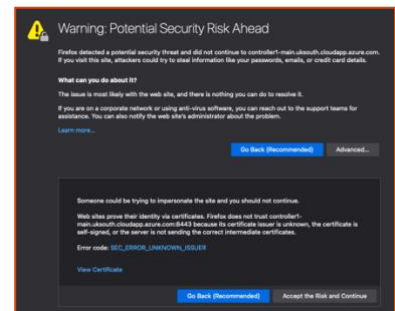


| | | | |
|-------------------------|--|---------------|---|
| Resource group (change) | : c-test | SKU | : Basic |
| Location | : UK South | Tier | : Regional |
| Subscription (change) | : Microsoft Azure Enterprise_jamiebs | IP address | : 20.68.60.84 |
| Subscription ID | : 019030fb-792e-4119-825b-316459bde2f2 | DNS name | : controller1-main.uksouth.cloudapp.azure.com |
| Tags (change) | : Click here to add tags | Associated to | : NetworkInterface |

Sign in to the Appgate SDP admin UI

Enter the address of the Controller in your browser in the format: [https:<DNS name>:8443](https://<DNS name>:8443). Even though we use https our admin UI lives on port 8443.

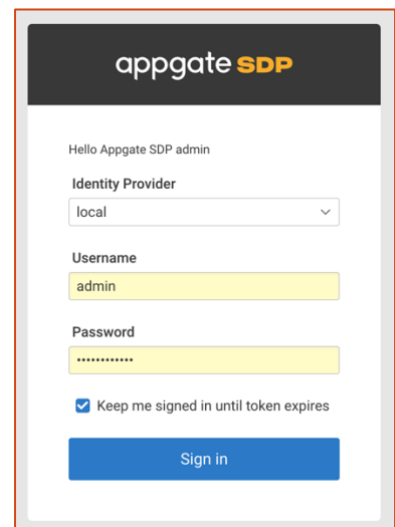
When the Controller is ready and you open this URL, you'll see a security warning since the connection to the Appgate SDP Controller uses HTTPS. The reason for this is that the appliance uses a self-signed certificate that is not known to the browser.



However, it is safe to proceed if the DNS name is the one you specified when creating the Controller.

Next, you should see the sign-in screen for the admin console. Select the "local" Identity Provider and then proceed to sign in using the username "admin", and the admin password you entered in the template earlier.

Click <Sign in> and you should be taken to the Appgate SDP dashboard.

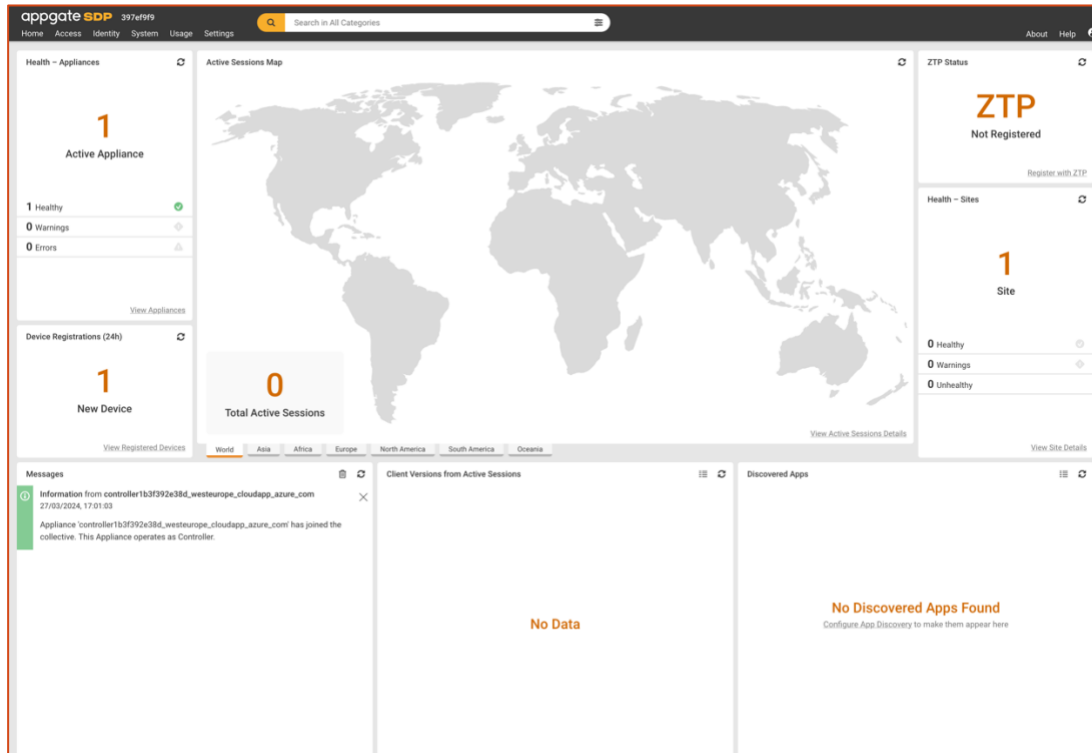


Admin UI

Take a moment to look at the interface, and we'll take you through it one step at a time.

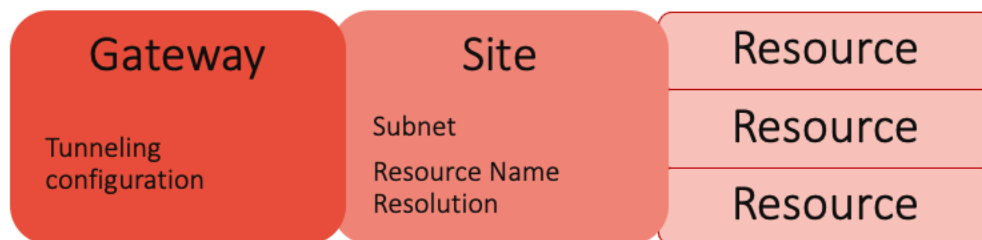
The dashboard shows the current system status, including the number of appliances in the overall Appgate SDP system. At the top are the menu controls for Operations, which is for management of user access to protected resources, for System, which is for the components within the Appgate SDP system itself as well as Scripts, Users & Service and Settings.

You can see that we have one appliance, which currently functions as a Controller. The Controller is the "brain" for the system, Gateways manage traffic to/from protected resources, LogServer/LogForwarder/Metrics Aggregator handles logs and metrics, Connectors collect traffic from network devices (where the Client can't be easily installed, while Portals allow browser-based access for users.



The Gateway

To move forward, we need to configure a Gateway for the system, which belongs to a Site, which in turn protects resources (other Azure instances). As shown below, each Gateway is associated with one Site, and within each Site are multiple Resources.



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

The Site

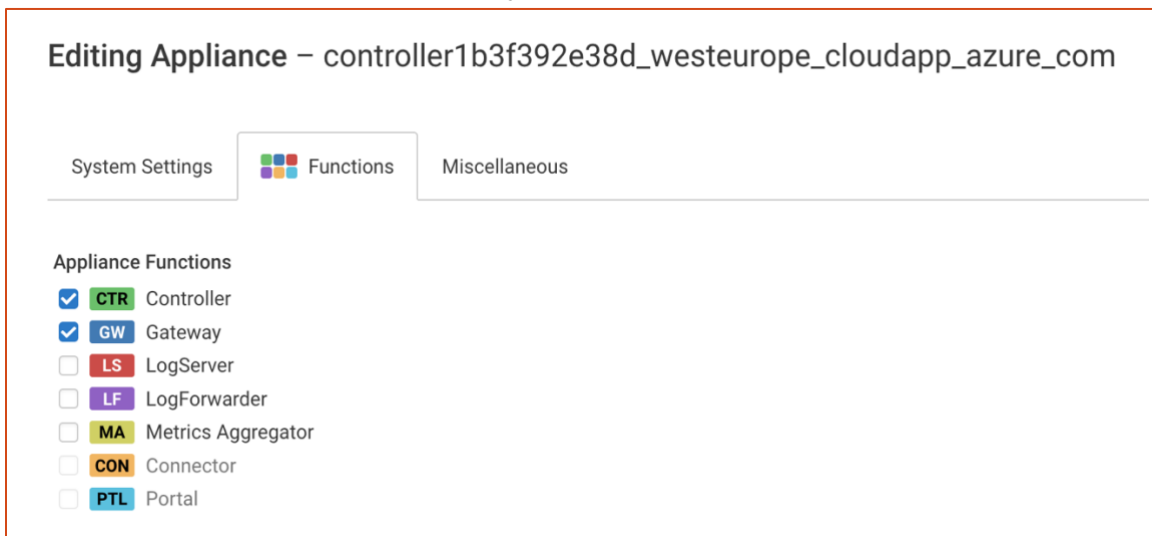
Under **System>Sites** there should already be a Default Site so we will use that. There is nothing to configure however the Name Resolvers tab is interesting. We will for now access the protected Azure instance(s) by IP address. However, Appgate SDP integrates with Azure using what is called an Azure resolver. This will allow Appgate SDP to query Azure to find the servers that need Appgate SDP firewall rules configuring automatically. There is an 'Additional things to try' section later on where we will explain the use of name resolvers.

Adding an integrated Gateway (using the existing appliance)

Next up, we configure the Gateway on the existing Controller appliance (and then later as a stand-alone appliance).

In **System>Appliances** click the only appliance in the list to edit it.

Then on the **Functions** tab enable *Gateway*



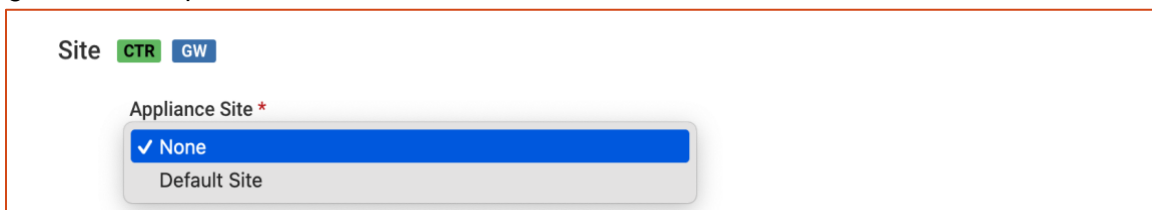
Editing Appliance – controller1b3f392e38d_westeurope_cloudapp_azure_com

System Settings **Functions** Miscellaneous

Appliance Functions

- CTR** Controller
- GW** Gateway
- LS** LogServer
- LF** LogForwarder
- MA** Metrics Aggregator
- CON** Connector
- PTL** Portal

Using the **Site** dropdown, select the *Default Site*.



Site **CTR** **GW**

Appliance Site *

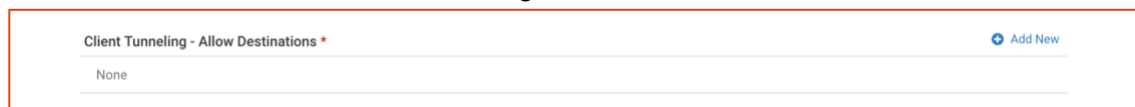
None

Default Site

Under Secure Tunnel Settings:

Client Hostname/IP – this field tells the Client how to set up the secure tunnel to the Gateway. The hostname shown is inherited from the Appliance Hostname.

Client Tunneling - Allow Destinations – is required so the tunnel can forward traffic, so click <+ Add new> to create a new destination - against **Network Interface** enter *eth0*.



Client Tunneling - Allow Destinations *

None

[Add New](#)

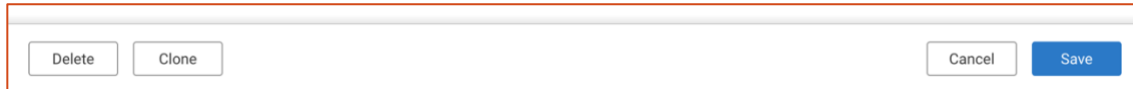
Then click **Save Changes** to complete this step. The Gateway will now be added to the appliance.

Adding a stand-alone Gateway (using a new appliance)

The alternative is to create a new appliance in Azure which will host the Gateway.

Defining a new Appgate SDP Gateway

To define an appliance that functions as a Gateway you can follow the instructions in the [admin guide](#). However, the easiest way to do this is to clone the existing Controller/Gateway appliance.



Click <Clone> at the bottom of the appliance and then change the **Name** and the **Appliance Hostname/IP** to suit. In this example it is best to make sure the hostname follows the same Azure format already in use. Then click <Save>. NOTE: The Controller function will have been dropped from the configuration, as that can only be enabled on active appliances.

Export the seed for the new Azure appliance

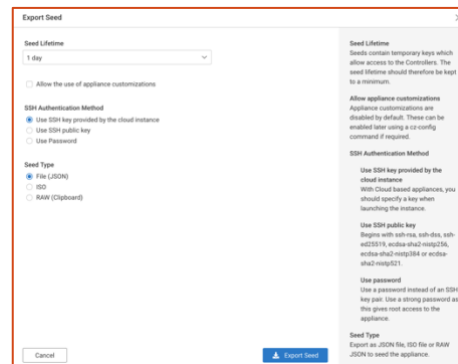
The next task is to [get the seed file](#) from the Appliances page.

| Appliances | | | | | | | Total Appliances: 2 | Auto-Refresh | Refresh | Settings | Bulk Actions | Add New |
|---|------------|---|---------------------|--------------|------|----------------------|---------------------|--------------|---------|----------|--------------|---------|
| Name | Status | Hostname | Functions | Site | Tags | Modified | | | | | | |
| controller1b3f392e38d_westeurope_cloudapp_azure_com | Healthy | controller1b3f392e38d.westeurope.cloudapp.azure.com | Controller, Gateway | Default Site | | 28/03/2024, 11:03:58 | | | | | | |
| gateway1b3f392e38d_westeurope_cloudapp_azure_com | Not Active | gateway1b3f392e38d.westeurope.cloudapp.azure.com | Gateway | Default Site | | 28/03/2024, 11:20:18 | | | | | | |

Click on the ... to the right and click on <Export Seed File/ISO>.

Choose the option “Use SSH key provided by the cloud instance”.

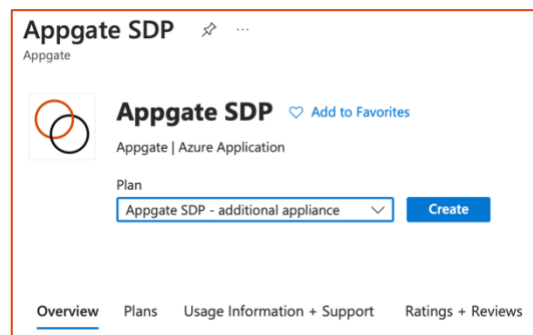
When you click <Export Seed> the JSON file will be downloaded (to your downloads folder).



Create a new Azure appliance

The next step is to create the Azure appliance which will become the Gateway and join itself to the Collective.

Start as before (for making the first Controller), but this time select *Appgate SDP – additional appliance* and click <Create>.



Basics

Same as previous

VM Settings

Similar to previous

- **DNS Prefix for the public IP address** – ensure this is the same as you used in the Gateway configuration.
- **Seed configuration** – upload the seed file you exported.

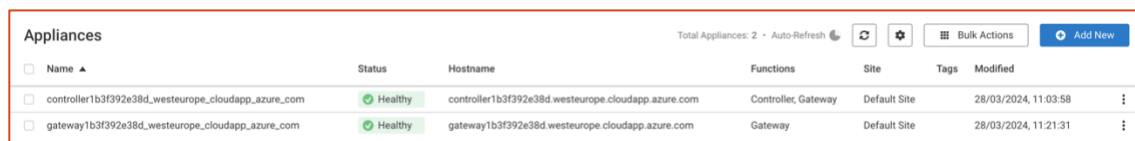
Review and create

Same as previous

Deployment

Now it may take up to two minutes for the Gateway to fully add itself to the Collective. You can verify this in the Appgate SDP admin UI Appliances form which will now show the **Status** as Active.

The Appgate SDP admin UI Dashboard will be showing 'healthy' for the new Gateway.



The screenshot shows the 'Appliances' dashboard in the Appgate SDP admin UI. It features a table with columns for Name, Status, Hostname, Functions, Site, Tags, and Modified. Two appliances are listed, both with a 'Healthy' status. The dashboard also includes a 'Total Appliances: 2' indicator, an 'Auto-Refresh' button, and a 'Bulk Actions' menu.

| Name | Status | Hostname | Functions | Site | Tags | Modified |
|---|---------|---|---------------------|--------------|------|----------------------|
| controller1b3f392e38d_westeurope_cloudapp_azure_com | Healthy | controller1b3f392e38d.westeurope.cloudapp.azure.com | Controller, Gateway | Default Site | | 28/03/2024, 11:03:58 |
| gateway1b3f392e38d_westeurope_cloudapp_azure_com | Healthy | gateway1b3f392e38d.westeurope.cloudapp.azure.com | Gateway | Default Site | | 28/03/2024, 11:21:31 |

Create (or choose) a protected host

Now, select a VM to test out access via Appgate SDP. The simplest thing to do is to create one just for testing. The easiest to try is an Ubuntu instance. Use the same resource group and VNet, select no External IP address when creating this instance. Also give it the name target1 and add a tag on the VM instance Type:target which we will use later.

We need to check the instances IP address. The VM instances summary will show you the internal IP address. We will use SSH to connect to this IP address on port 22 using the Client later on.

Accessing the protected host

About Entitlements

Each Entitlement defines the rules for controlling access to network resources on a particular Site. The main settings for an Entitlement are the Site, Actions (traffic protocols, target hosts, ports), and any Access Controls that must be applied to those Actions to be allowed by the Gateway. Entitlements are provisioned to users via Policies.

Example of a user Entitlement to allow IP Access to 10.0.0.1 server on port 80 only if the time is between 09.00 and 17.00:

```
<Site> "Net01" <Actions> "TCP up to 10.0.0.1 on port 80" <Conditions> "Office Hours"
```

The default Access Control setting in an Entitlement is '*Always Allow Action(s)*'.

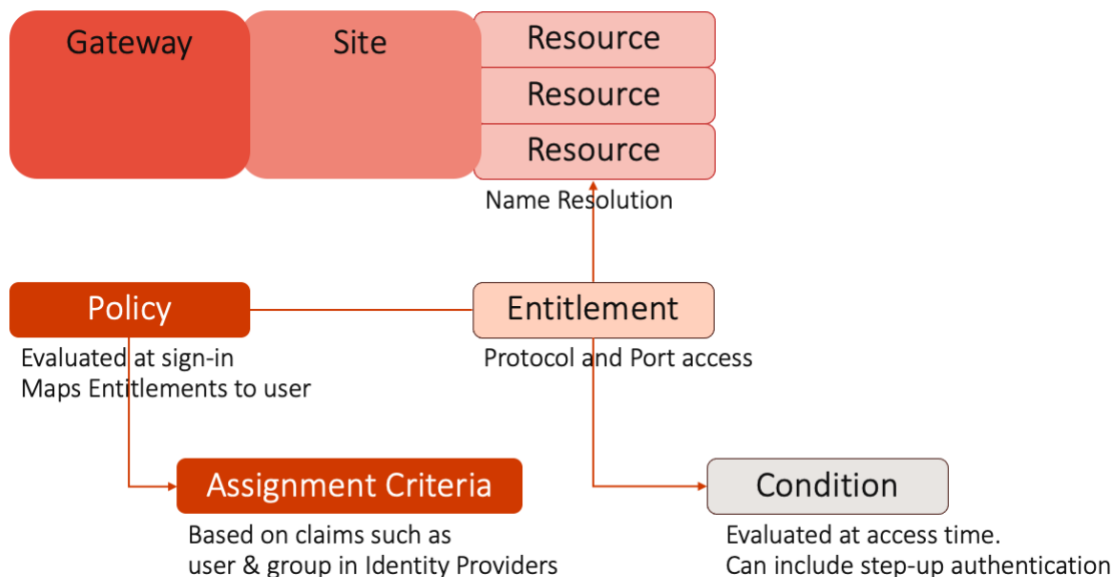
Under normal circumstances, Actions will be set to <ALLOW> user traffic to a host. However, an Action can <BLOCK> traffic to a resource, trigger an <ALERT> if traffic is sent to a particular host or <EXCLUDE> traffic from that Site.

About Policies

Policies are used to assign rights to a user or group of users. These can include a blend of Entitlements (inc. DNS), Device Security settings and any Admin Roles. Policy assignment is done using claims-based expressions identifying who the Policy should be assigned to. The Controller manages this process and the resulting configurations are then granted to the user in the form of:

- Site based Entitlement token(s), comprising the list of Entitlements.
- Device Security settings, which are pushed to the connected Client (Advanced Ringfence and Tamper Proofing)
- Admin token (for an administrator), comprising the list of Admin Roles allowed

When an Entitlement is created, the Site where this resource lives has to be specified. This Site information is normally used to collect all the Entitlements together in order to create a single Entitlement token for that Site.



The diagram above shows the components we're going to be creating:

- The Entitlement allows SSH access to our Ubuntu instance in our VNet.
- In this example, we chose not to set any Access Controls (which is an additional restriction that's checked at time of access). This 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!)
- The Policy binds this Entitlement to the user using assignment criteria which defines the set of users who can access this Entitlement. In our example, we're going to let any user with a tag *employee* get access. (The user tag is metadata within the Appgate SDP system, and is completely separate from any Azure tags).

Set up Appgate SDP

Create Entitlements – to access the protected host

Appgate SDP supports many types of IP access.

From the Appgate SDP main Menu, select **Access>Entitlements** and click on <+Add New>.

Give it a name – in this case let's use the name *target*.

Next, we'll link the Entitlement to a Site. Pick the Default Site from earlier.

Now we specify the Entitlement Action.

Actions:

Click the <+ Add new> button for **Actions** to create a new action.

Configure the Action as shown:

Hosts – Target or Source should be the internal interface IP address of the of the Ubuntu instance.

Note that each Entitlement can include a number of Entitlement Actions, so you can group Actions that relate to a particular Site. For this example, let's just keep it simple with our one port 22 Action.

Rule should be *Allow*.

Protocol should be *tcp up* (TCP traffic *from* the Client up to the server. Return traffic is subsequently allowed).

Ports should be 22 since we're permitting SSH traffic.

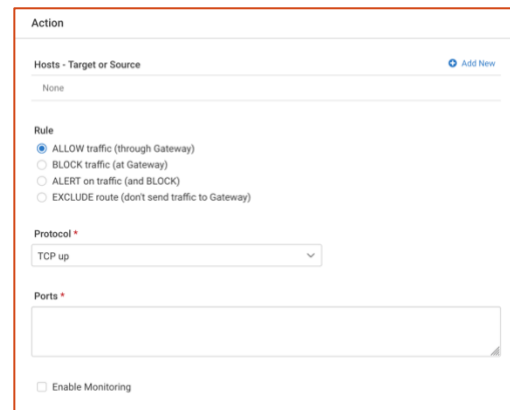
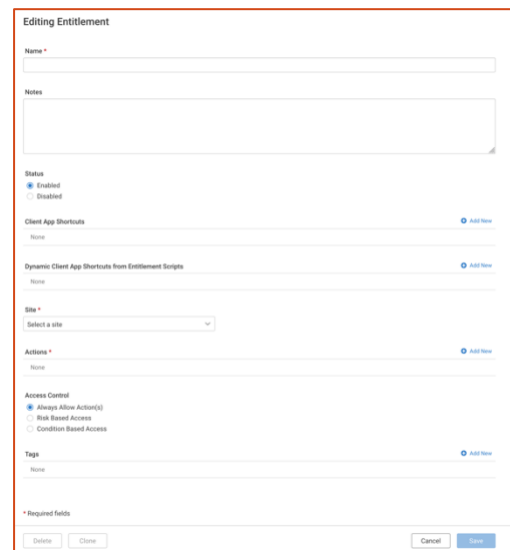
Access Control:

Each Entitlement can include one or more conditions to provide real-time control over when the Entitlement is used. Access decisions are taken at the time a user attempts to access a resource. Examples include only allowing access to a service during working hours, or requiring the user to re-enter their password before gaining access to sensitive resources.

If *Always Allow Action(s)* is set, the Entitlement is **Always** available (the default).

Click <Save>.

From the Entitlements list, if you click <Show Details> then you should see a summary like this:



| Entitlements | | | | | | | Total Entitlements: 157 | Refresh | Settings | Bulk Actions | Add New |
|---------------------------|---------|--------------|------------------------|------|----------------------|-------------------------|-------------------------|---------------|----------|--------------|---------|
| Name | Status | Site | Access Control | Tags | Modified | | | | | | |
| Test - Whatismyip dot com | Enabled | Gothenburg 1 | Always Allow Action(s) | | 31/05/2022, 20:00:03 | | | | | | |
| APP SHORTCUT | | | | | | | URL | | | | |
| Whatismyip | | | | | | https://whatismyip.com | | | | | |
| ACTION | | | | | | | HOSTS | PORTS & TYPES | | | |
| allow tcp-up | | | | | | domain://whatismyip.com | 443 | | | | |

Create a User

In order to create a User, select **Identity>Local Users**. Click on <+ Add New>.

| Local Users | | | | | | Total Local Users: 23 | ⌂ | ⚙ | + Add New |
|-------------|---------|-----------------------|-----------------|---------|----------------------|-----------------------|---|---|-----------|
| Username | Status | Name | E-mail | Tags | Modified | | | | |
| admin | Enabled | Builtin Administrator | admin@email.com | builtin | 15/03/2022, 11:39:39 | | | | |

Proceed to add a new user by completing the fields required.

Note:

- Make note of the username and password, since we'll be using that to sign in from the Appgate SDP client in a later step.
- The email address is required as a unique identifier, but the Appgate SDP system doesn't send any email to the address.

Important: Make sure to add the **employee** tag to the user! This tag is how the Policy will know to grant Joe access to our Entitlements. To do this, type "employee" where it says "None" or click on <+ Add New>.

Create a Policy

Next, we create a Policy that picks the **employee** tag and allows our employee users to access **target** Entitlements. From the main menu, select Access **Access>Policies** click <+Add New>.

| Policies | | | | | | Total Policies: 108 | ⌂ | ⚙ | ⌵ Bulk Actions | + Add New |
|--------------------------|----------------------|---------|--------|------|----------------------|---------------------|---|---|----------------|-----------|
| <input type="checkbox"/> | Name | Status | Type | Tags | Modified | | | | | |
| <input type="checkbox"/> | ZTP Test Environment | Enabled | Access | | 15/03/2023, 17:01:37 | | | | | |

Give it a name – in this case we have chosen the name Employee Access to External Apps.

Next, in the Policy Assignment section, click <+Add new>. Select tags from the drop down and then enter 'employee'.

Next, we'll link the Entitlement. Under **Entitlements by name** click <+ Add New>. Enter or select the name *target* from earlier.

Once you are done, click <save>.

Editing Policy – Access

Name *
Employee Access to External Apps.

Notes

Status
 Enabled
 Disabled

Assignment – Active when all below are true

Editing Done Cancel

tags

Operator
match

Value
employee

Entitlements by name + Add New

target

Get the Client Profile Link

The last thing to do before leaving the Admin UI is to get the profile link from the Controller. From the Appgate SDP main Menu, go to **Identity>Client Profiles**.

Normally Controllers should use a shared FQDN hostname and not the appliance's own hostname. This will be the Profile DNS Name you entered when you created the Controller – this ensures that it is already baked into the appliance's certificate.

- Create a new name for the profile.
- Choose the *local* IdP
- <Save> the form

| | | | | | |
|---------------------------|---------|---------------------------|----------------------|----------------------|--------------------------------------|
| temptest | Profile | AppGate Azure AD SAML OTP | 07/12/2023, 13:21:34 | 09/02/2023, 14:17:58 | |
| Test | Profile | local | Unknown | 27/03/2024, 16:14:21 | |
| testing | Group | | | 30/01/2024, 10:00:00 | |
| AppGate Azure AD SAML OTP | Profile | service | 23/10/2023, 08:54:34 | 28/02/2024, 10:00:00 | Copy to clipboard |
| Test | Profile | service | 21/03/2024, 14:11:02 | 28/02/2024, 10:00:00 | Download QR code for mobile clients |
| testing | Profile | service | 22/02/2024, 20:01:20 | 28/02/2024, 10:00:00 | Download Client on-boarding web page |
| | | | | | Copy email template |

Now use the actions menu on the right-hand side to <Copy to Clipboard> and paste it somewhere for the next step.

Install the Client

The next step is to install the Client. Recall that the Appgate SDP client installs as 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. It will run automatically after the installation completes.

The Client installers are available from <https://www.appgate.com/software-defined-perimeter/support>


Add a Client Profile

The Client needs to be told about the Controller. This allows it to make a trusted and secure connection without the user having to get involved. Once opened just click on the **USE PROFILE LINK** and enter the Profile Link we copied earlier. And then press **ADD PROFILE**.

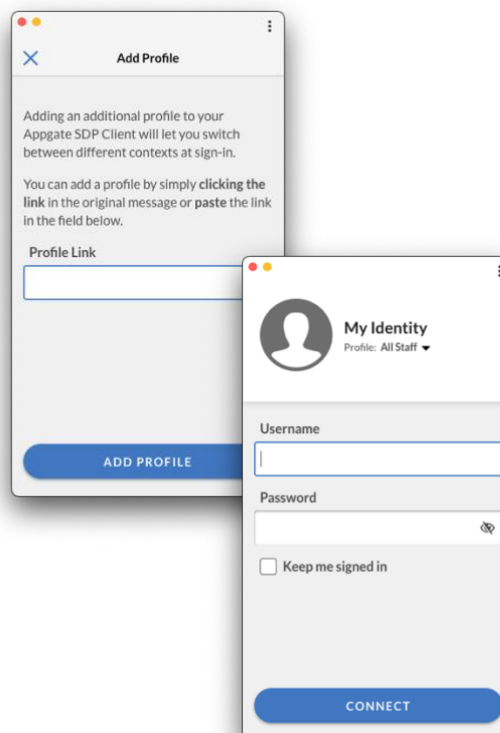
Sign in to the Client

Now you are ready to sign-in.

Now enter the username and password and click on **CONNECT**.

When minimized, the client will show as an Appgate SDP  icon in the taskbar.

Now, you're ready to access the protected server through Appgate SDP!



Test out Access!

Go ahead and open the protected resource, using the private IP address. It should work!

Open your terminal and enter:

```
ssh joe@10.0.250.5
```

You are now using Appgate SDP to provide access to your protected Azure resource!

What if it didn't work?

If you're unable to login to the Ubuntu instance (or the equivalent in your protected resource):

- Double-check that it's running, and has an IP address in the subnet that the Gateway is protecting
- Make sure the Site and Gateway configurations are correct, as shown above
- SSH into the Appgate SDP server, and try pinging the protected resource (because this isn't going through the Appgate SDP Gateway, there's no need to set up a Policy/Entitlement)
- Make sure your user has the tag *employee* within Appgate SDP, and that your Policy uses this in the assignment criteria.

If you're still stuck, or have questions or comments, feel free to connect with us via the support pages <https://www.appgate.com/software-defined-perimeter/support>.

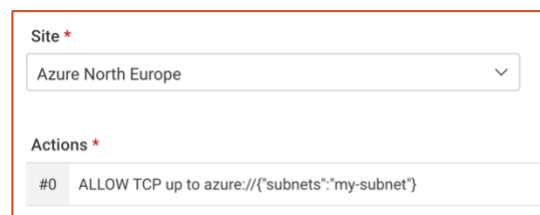
Additional step – Using Azure Name Resolution

With more advanced settings in place, network access automatically adapts in real time to changing conditions on the Client as well as the resources in the cloud environment. You can be assured every new instance that is added or removed will automatically be traced and added or removed from the access rules, without the need for changing any Entitlements. It is now an automation-driven network access process that can be audited by the simple Policies you created. This means less work for you and the right protection for your resources!

This process for setting up name resolvers is quite straight forward – however it does involve some specific steps both on the Azure and Appgate side of things. There is a specific guide relating to [Using name resolvers in Azure](#).

The main steps are summarised below:

- Configure Azure to accept API calls from the Appgate SDP system
- Configure the Appgate SDP Site with the required information to be able to issue API calls
- Modify the Entitlement to use Azure resolver syntax to resolve the hosts dynamically.



The screenshot shows a configuration interface with two main sections: 'Site *' and 'Actions *'. The 'Site *' section has a dropdown menu currently set to 'Azure North Europe'. The 'Actions *' section contains a table with one row: '#0 ALLOW TCP up to azure://{subnets:*my-subnet}'.

Once configured go to the user's session details on the dashboard. Here you will see the actual resolved IP address(s) that are being used for the firewall rule.

| Firewall Rules | Rule Name | Ports | Hosts |
|----------------|-------------------|-------|--------------|
| | #0 - allow TCP-UP | 22 | 10.0.55.4/32 |
| | #1 - allow TCP-UP | 22 | 10.0.55.6/32 |

More things to try

Now that you have Appgate SDP working with your first access Policy, have some fun. Here are a few things to try out:

- Add an ICMP Entitlement so that our user, can ping the SSH server
- Try choosing a few more Azure instances and add them to the Entitlement, to see how user access is automatically assigned
- Try creating different Entitlements and Policies

Resources

You'll find additional resources on the [Appgate website](#)

There is another [step-by-step guide](#) for the VM which is also available in the marketplace. This is a universal image suitable for scripted deployments.

The Appgate SDP product documentation is available here:

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

Access to our support services (including further articles) is via the [customer portal](#).