



Appgate SDP[®] for Azure Using Name Resolvers

Type: Technical guide

Date: April 2024

Applies to: v6.3 and newer

© 2024 Appgate

OVERVIEW 3

CONFIGURE AZURE 4

 ALLOW API ACCESS..... 4

 APP REGISTRATIONS 4

 GIVE THE NEW AZURE API THE RIGHTS TO THE RESOURCE GROUP 5

 ADDING TAGS ETC TO AZURE RESOURCES 5

CONFIGURE APPGATE SDP 6

 ADD RESOLVER TO THE SITE 6

 ADD AN APPGATE SDP ENTITLEMENT 6

RESOURCES 6

Overview

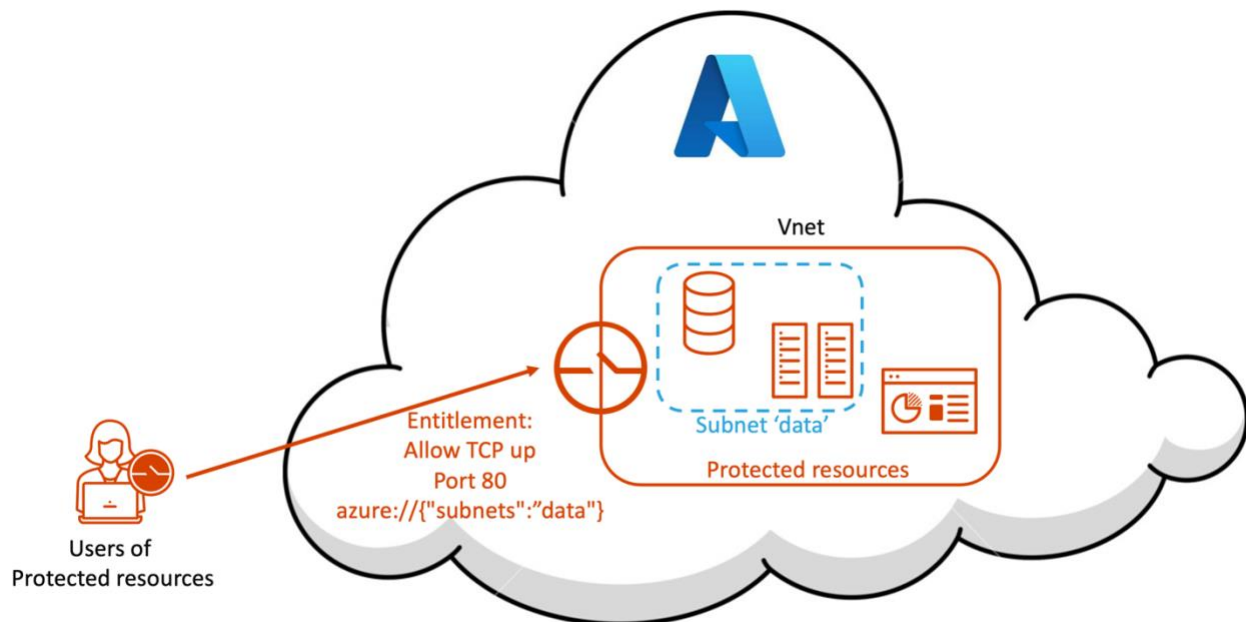
Enterprises continue to embrace Microsoft Azure but securing access to these cloud-based workloads can be a challenge. Appgate SDP is purpose-built for the Azure environment and draws on user context to dynamically create a secure, encrypted network 'segment of one' that's tailored for each user session. 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 the device (via a virtual network adapter, similar to a VPN client), and passed through the Appgate SDP Gateway to the protected resources. The Entitlement in this case does not define an IP address or a host name but instead uses a *resource name*. The Gateway can then make a number of API calls into the Azure environment to discover the IP of hosts or within a subnet or Network Security Group.



This guide will take you through the steps necessary to set up and configure both Azure and Appgate SDP so that these *resource names* can be used and resolved in real time.

Configure Azure

Allow API access

By default, Appgate SDP (Gateway) is not allowed to use any Azure APIs, so we need to configure Azure to allow this. As we go there are a number of pieces of information we need to be able to configure Appgate SDP make these API calls to Azure.

Begin by logging into your Azure Portal.

App registrations

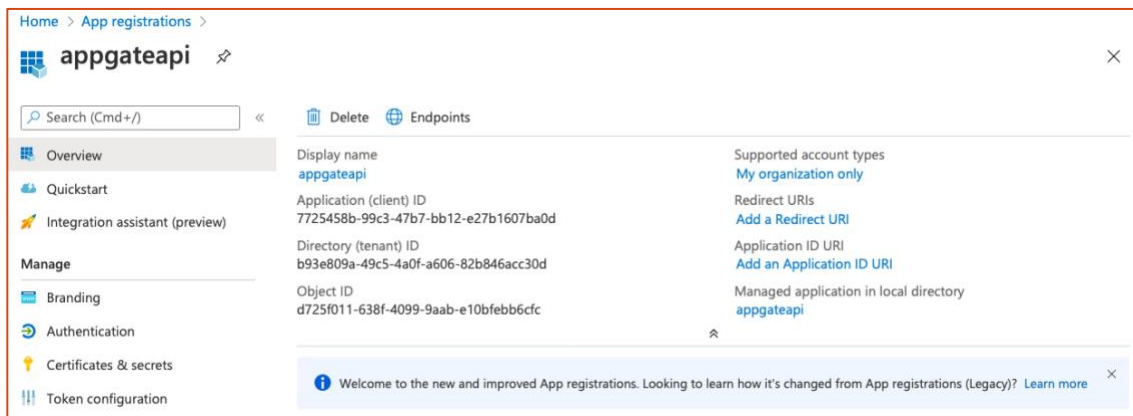
From the start page search for **App registrations** then click on <+New registration> and a new page will open.

Name - enter a name such as *Appgateapi*

Supported account types - change if required

Redirect URI (optional) – n/a

Then click on <Register>. The page will then close and the App registrations summary screen is shown:

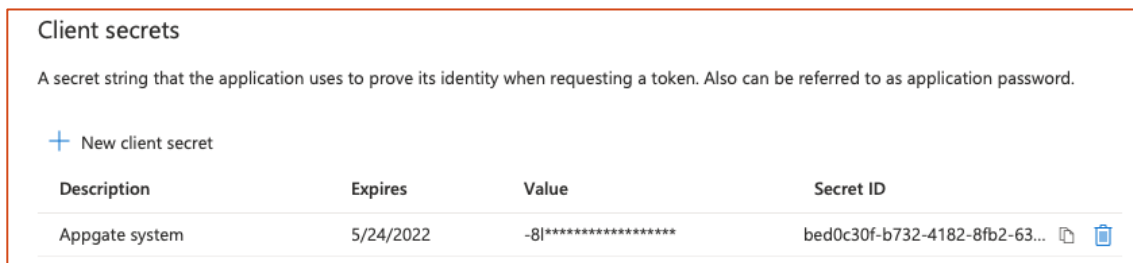


There are two things from this screen we need to set up the name resolver in Appgate SDP; (client) ID and (tenant) ID.

Certificates and secrets

From the menu Click on **Certificates and secrets**. Then click on <+ New client secret>. A dialogue will open where you can provide a description and an expiration. You might want to select *Never* if you want to avoid the Appgate system breaking in a year or two's time!

Then click on <Add>.



Copy the *Value* before you move on as it will become obfuscated - so don't lose it! We will need the client secret value to set up the name resolver in Appgate SDP

Give the new Azure API the rights to the Resource Group

From the Azure portal start page click **Resource groups** from the left side menu. Select the Resource group where the protected resources behind the Appgate Gateway reside. In the first block in the menu click on **Access control (IAM)**.

Add a role assignment

Click on <+Add > & pick **Add role assignment**

Role – select *Reader*

The generic *read* permission should work fine; but permissions can be further minimized if required. However, the resolver needs access to all possible resource types (that can be used to resolve hosts), which are:

"Microsoft.Resources/subscriptions/read",

"Microsoft.Network/networkSecurityGroups/read",

"Microsoft.Network/virtualNetworks/read",

"Microsoft.Network/networkInterfaces/read",

"Microsoft.Network/loadBalancers/read",

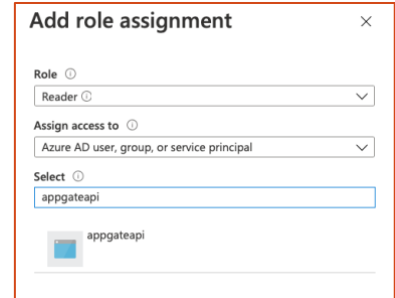
"Microsoft.Compute/virtualMachines/read",

"Microsoft.Network/publicIPAddresses/read"

Assign access to - *Azure AD user, group, or service principal*

Select – search for the new app we created earlier and select that.

Then click <Save>.



Adding tags etc to Azure resources

In the Azure UI we might want to add some extra information for our resolver to use. This may not be required if the information is already available in the current configuration.

The full set of *resource name* syntax can be found in the [admin guide](#).

These normally involve resolving resources from NSGs, Vnets, subnets, tags, etc. If we want to use tags to resolve hosts then we need to update our target hosts/networks/etc with a tag NAME:VALUE we can look for.

Open the resource and click on Tags. In the Tags blade add *Name* and *Value*. The Appgate API call will now use these to resolve the related IP addresses when a user connects.

Now it is time to move on to configure the Appgate side of things.

Configure Appgate SDP

Add resolver to the Site

Name resolvers are configured on a per Site basis:

Open your Azure **Sites** and click on the **Name Resolution** tab.

Find **Azure Resolvers** and click <+ Add New>.

Make the Name reflect the Resource Group in Azure. Leave the update interval at its default (this is how frequently the Appgate server calls into Azure to check for server changes). Then enter these pieces of information:

Subscription ID:	now deprecated
Tenant ID:	Use the Directory (tenant) ID from the App registration summary screen
Client ID:	Use Application (client) ID from the App registration summary screen
Secret:	Use the client secret value you copied earlier

Add an Appgate SDP Entitlement

Configure the Entitlement with a *resource name* in place of an IP/hostname is the final step.

Add an **Entitlement** and select an Azure Site where you have configured the resolver.

Add an **Actions**; you will see an Azure link which is there to help configure the *resource name* syntax you will require for Target/Source.

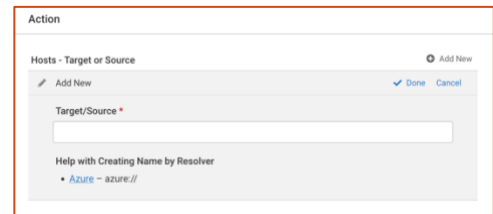
Pick a Resource Type and then the Name/Id you want to use to select the Target(s) or Source(s). This will generate the some basic syntax for you automatically. For this example:

```
azure://{ "network-security-groups": "thomas-testNSG" }
```

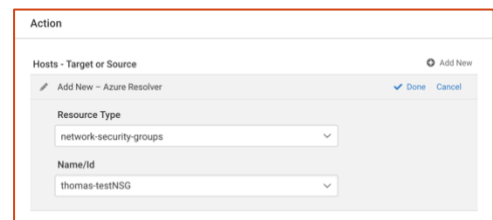
This will return all the IPs of hosts in the NSG named *thomas-testNSG*.



The screenshot shows a form with a dropdown menu for 'Site' set to 'Azure North Europe' and a text field for 'Actions' set to 'None'.



The screenshot shows an 'Action' configuration form with a 'Target/Source' field and a link for 'Help with Creating Name by Resolver' pointing to 'Azure - azure://'.



The screenshot shows an 'Action' configuration form with 'Resource Type' set to 'network-security-groups' and 'Name/Id' set to 'thomas-testNSG'.

Resources

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

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](#).