

How to Configure Azure Cloud Integration Using ARM

<https://campus.barracuda.com/doc/95259336/>

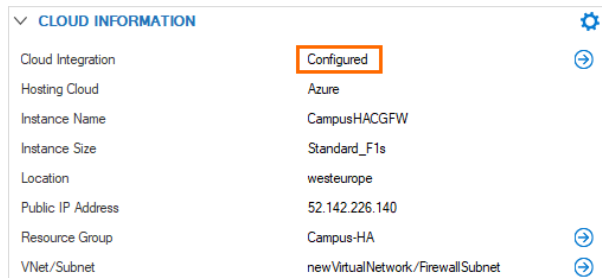
Azure Cloud Integration allows the firewall to connect directly to the Azure service fabric in order to rewrite Azure user-defined routes and to monitor the IP forwarding setting of the NIC of your firewall VM.

There are two methods available for Cloud Integration . The recommended method is Managed Identity because it is easier to maintain and configure.

- **Managed Identity** - For more information, see [Barracuda CloudGen Firewall Managed Identities in Microsoft Azure](#).
- **Service Principal** (User Identity) - Certificate authentication is used to authenticate the firewall when accessing the Azure API endpoints. The certificate must be valid for at least 1 year. The end date of the certificate is used by the setup script to also determine the end date for the Azure AD application. When the certificate or the Azure AD application expires, the firewall can no longer use Azure Cloud Integration features until the Azure AD application and the corresponding certificate have been replaced. If a [global HTTP proxy](#) is configured, all calls to the Azure REST API are sent via the proxy.

Cloud Integration is required for the following features:

- Barracuda Firewall Admin dashboard **Cloud Information** element.



CLOUD INFORMATION		⚙️
Cloud Integration	Configured	➡️
Hosting Cloud	Azure	
Instance Name	CampusHACFW	
Instance Size	Standard_F1s	
Location	westeurope	
Public IP Address	52.142.226.140	
Resource Group	Campus-HA	➡️
VNet/Subnet	newVirtualNetwork/FirewallSubnet	➡️

- UDR route rewriting for CloudGen Firewall high availability clusters
- IP forward protection

Before You Begin

- You need sufficient permissions in Microsoft Azure to create a service principal in Azure Active Directory.
- You need sufficient permissions in Microsoft Azure to assign permissions.
- You need a CloudGen Firewall deployed in the Microsoft Azure cloud. For more information, see [Microsoft Azure Deployment](#).

Step 1. Create the Azure Management Certificate

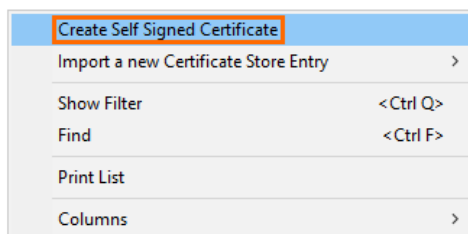
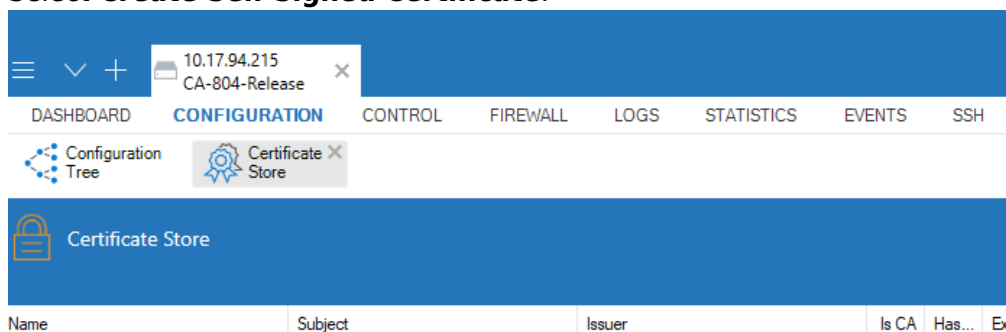
For the firewall to be able to connect to the Azure backend, you must create and upload a management certificate. The certificate must be valid for at least two years.

You can create such a certificate either in Barracuda Firewall Admin or on the CLI using SSH. Follow Step 1.1 to create in Firewall Admin or Step 1.2 to create on the CLI.

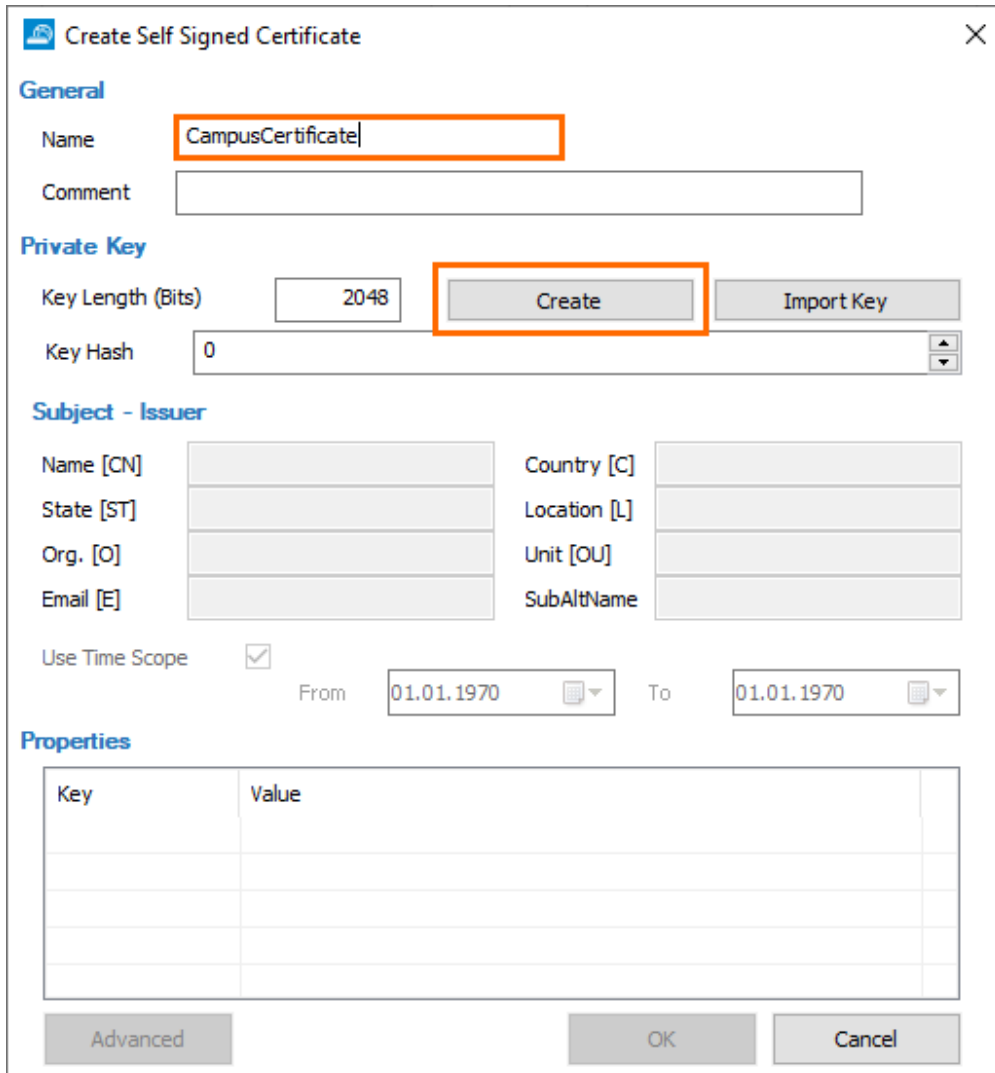
Step 1.1 Create the Azure Management Certificate in Barracuda Firewall Admin

Follow this step to create the management certificate in Barracuda Firewall Admin.

1. Log into the firewall via Firewall Admin.
2. Go to **CONFIGURATION > Configuration Tree > Advanced Configuration > Certificate Store**.
3. Click **Lock**.
4. Right-click in the **Certificate Store** section.
5. Select **Create Self Signed Certificate**.



6. The **Create Self Signed Certificate window** opens.
7. Enter a name and click **Create**.



Create Self Signed Certificate

General

Name: CampusCertificate

Comment:

Private Key

Key Length (Bits): 2048

Key Hash: 0

Subject - Issuer

Name [CN]:

State [ST]:

Org. [O]:

Email [E]:

Country [C]:

Location [L]:

Unit [OU]:

SubAltName:

Use Time Scope:

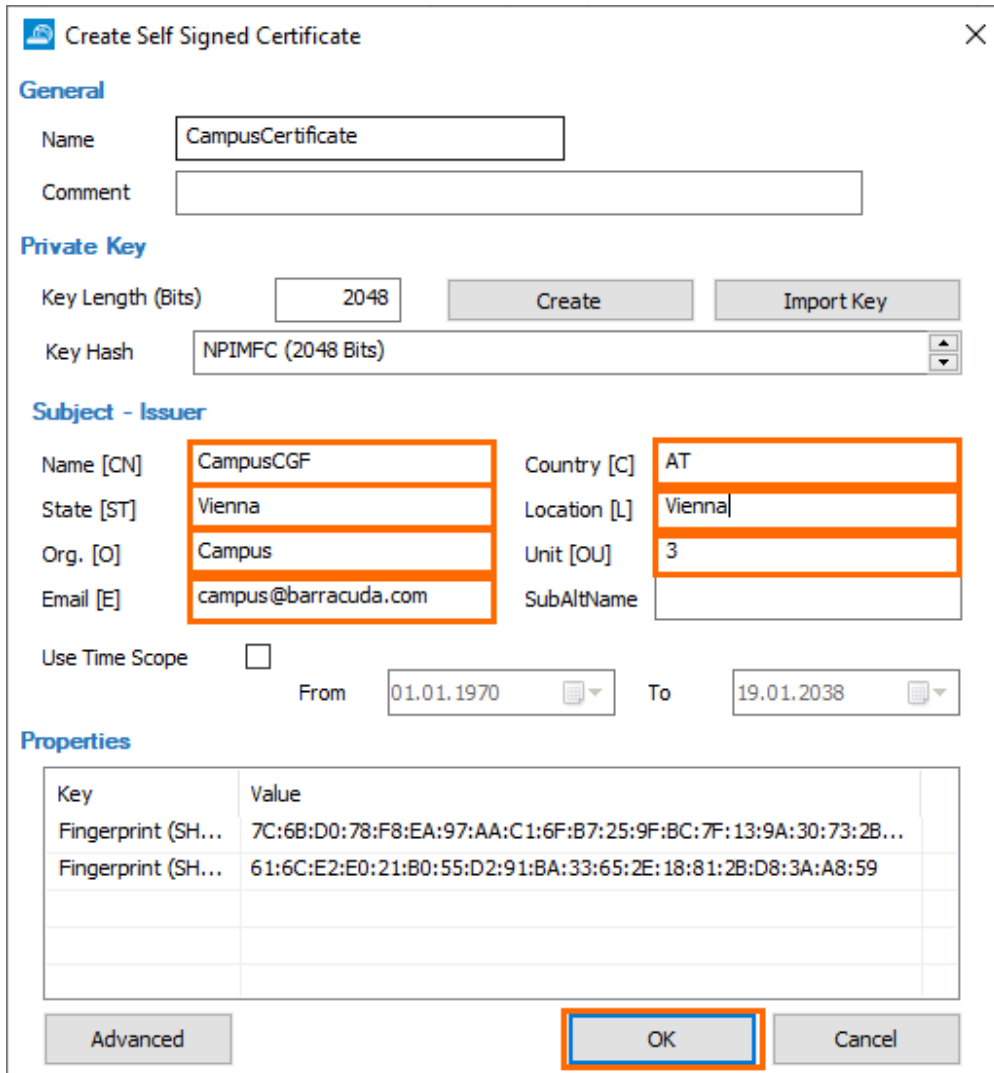
From: 01.01.1970 To: 01.01.1970

Properties

Key	Value

Advanced OK Cancel

8. Specify values for the following:
- **Name** - Enter a name.
 - **State** - Enter your state.
 - **Org.** - Enter your organization name.
 - **Email** - Enter your email address.
 - **Country** - Enter your country.
 - **Location** - Enter your location.
 - **Unit** - Enter your unit.



Create Self Signed Certificate

General

Name: CampusCertificate

Comment:

Private Key

Key Length (Bits): 2048 [Create] [Import Key]

Key Hash: NPIMFC (2048 Bits)

Subject - Issuer

Name [CN]: CampusCGF Country [C]: AT

State [ST]: Vienna Location [L]: Vienna

Org. [O]: Campus Unit [OU]: 3

Email [E]: campus@barracuda.com SubAltName:

Use Time Scope:

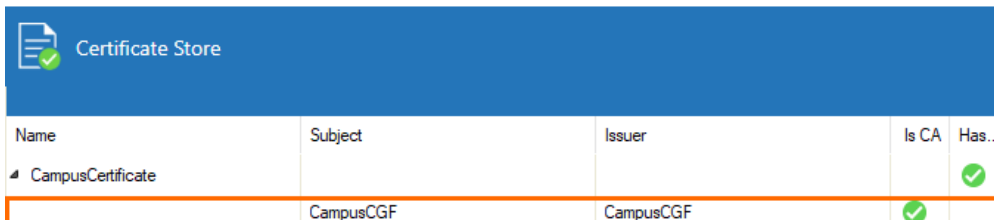
From: 01.01.1970 To: 19.01.2038

Properties

Key	Value
Fingerprint (SH...)	7C:6B:D0:78:F8:EA:97:AA:C1:6F:B7:25:9F:BC:7F:13:9A:30:73:2B...
Fingerprint (SH...)	61:6C:E2:E0:21:B0:55:D2:91:BA:33:65:2E:18:81:2B:D8:3A:A8:59

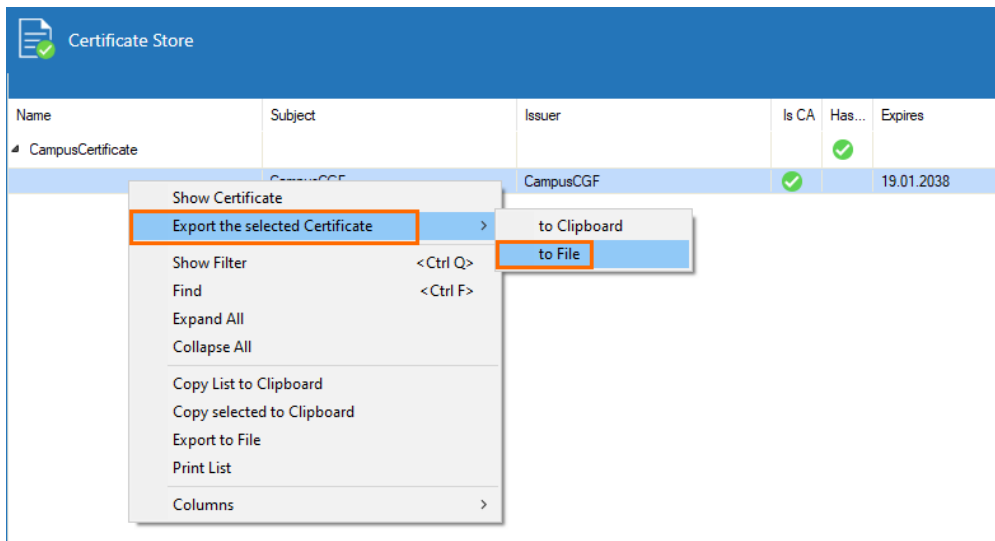
[Advanced] [OK] [Cancel]

9. Click **OK**.
10. The **Certificate Store** section opens.
11. Click **Send Changes**.
12. Click **Activate**.
13. In the **Certificate Store** section, double-click on the certificate you just created to expand it.
14. Select the first entry and right-click it.

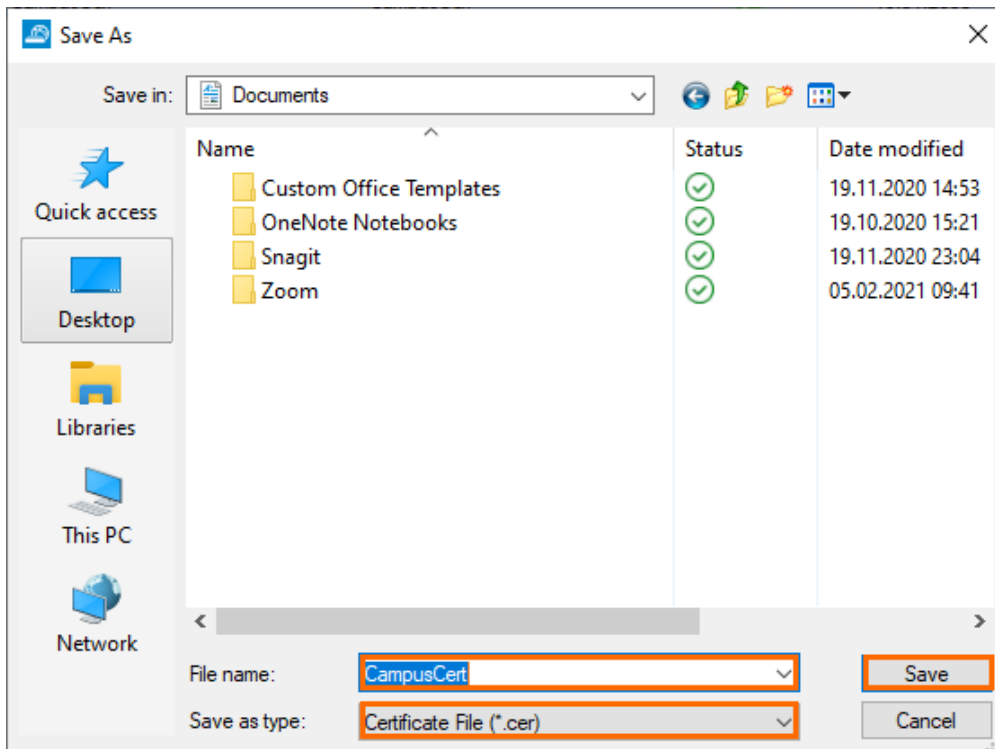


Name	Subject	Issuer	Is CA	Has...
CampusCertificate	CampusCGF	CampusCGF	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

15. Select **Export the selected Certificate** and **to File**.



16. Save the certificate as a *.cer file.



17. Repeat the last step and save the file as *.pem file as well.

Step 1.2 Create the Azure Management Certificate on the CLI via SSH

Follow this step to create the management certificate using the CLI via SSH. Note: Skip this step if you already created a certificate in Barracuda Firewall Admin.

1. Log into the firewall via ssh.
2. Create the certificate:

```
openssl req -x509 -nodes -days 1095 -newkey rsa:2048 -keyout arm.pem -
out arm.pem
```

3. Answer the questions at the prompt. The **Common Name** is used to identify this certificate in the Azure web interface.
4. Convert the certificate to CER, as required by Azure:

```
openssl x509 -inform pem -in arm.pem -outform der -out arm.cer
```

5. Extract the RSA key:

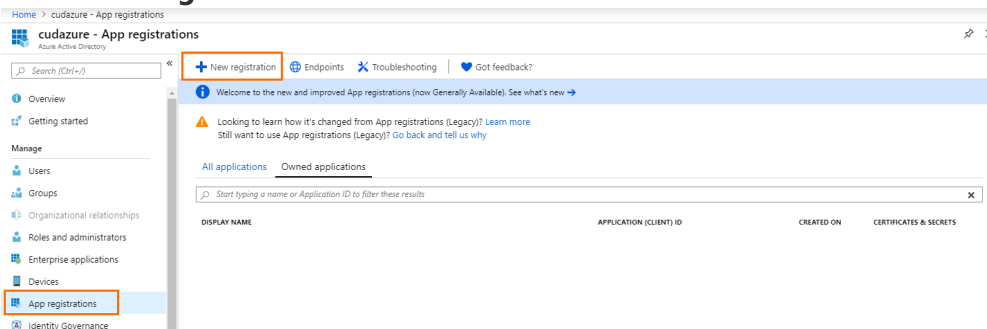
```
openssl rsa -in arm.pem -out arm.key.pem
```

You now have three certificates: *arm.pem*, *arm.key.pem* and *arm.cer*. Use the download function to save these somewhere safe on your device.

Step 2. Create a Microsoft Azure Service Principal

Create a service principal in Microsoft Azure and configure to authenticate with a certificate.

1. Go to the Azure portal: <https://portal.azure.com>
2. In the left menu, click **All services** and search for **Azure Active Directory**.
3. Click **Azure Active Directory**.
4. In the left menu of the **Azure Active Directory** blade, click **App registrations**.
5. Click **New registration**.



6. The **Register an application** blade opens. Specify values for the following:
 - o **Name** – Enter a name for the application registration.
 - o **Supported account types** – Select **Accounts in this organizational directory only (<your_directory_name> only - Single tenant)**. If you have multiple Azure Active Directory accounts, select **Accounts in any organizational directory (Any Azure AD directory - Multitenant)**.
 - o **Redirect URI (optional)** – Leave this field blank.

[Home](#) > [cudazure](#) >

Register an application ...

×

* Name

The user-facing display name for this application (this can be changed later).

BarracudaCGFApp ✓

Supported account types

Who can use this application or access this API?

- Accounts in this organizational directory only (cudazure only - Single tenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant)
- Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
- Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web e.g. https://example.com/auth

By proceeding, you agree to the [Microsoft Platform Policies](#)

Register

8. Click **Register**.
9. The newly registered application opens automatically when it is finished.
10. In the left menu, click **Certificates & secrets**.

Home > cudazure >

BarracudaCGFApp ⚙️ ...

Search (Ctrl+/) <<

Overview
Quickstart
Integration assistant

Manage

Branding
Authentication
Certificates & secrets
Token configuration

Delete Endpoints

Got a second? We would (developer).

Essentials

Display name
BarracudaCGFApp

Application (client) ID
[Redacted]

Directory (tenant) ID
[Redacted]

Object ID
[Redacted]

11. In the **Certificates & secrets** blade, click **Upload certificate**.

Home > cudazure > BarracudaCGFApp

BarracudaCGFApp | Certificates & secrets ⚙️ ...

Search (Ctrl+/) << Got feedback?

Overview
Quickstart
Integration assistant

Manage

Branding
Authentication
Certificates & secrets
Token configuration
API permissions
Expose an API

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires	ID
No certificates have been added for this application.			

12. The **Upload Certificate** window opens. Select the *.cer file created in Step 1 and click **Add**.

13. After the upload is complete, the certificate is displayed in the list.

Home > cudazure > BarracudaCGFApp

BarracudaCGFApp | Certificates & secrets ✨ ...

Search (Ctrl+/) << Got feedback?

- Overview
- Quickstart
- Integration assistant

Manage

- Branding
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- App roles | Preview

Certificates

Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web addressable location (using an HTTPS scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public keys.

Upload certificate

Thumbprint	Start date	Expires	ID
69A132B4CB4300063400FB1BB0330...	1/1/1970	1/19/2038	2bcf87c7-7

14. Click **Overview** .

15. In the **Overview** blade, copy the **Application (client) ID** and the **Directory (tenant) ID** and insert both into a text editor. You will need this information later.

Home >

BarracudaCGFApp ✨ ...

Search (Ctrl+/) << Delete Endpoints Preview features

- Overview**
- Quickstart
- Integration assistant

Manage

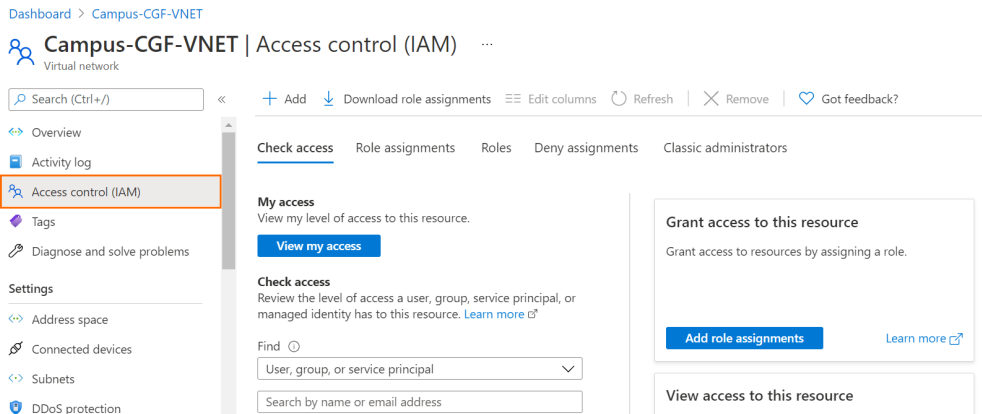
- Branding
- Authentication
- Certificates & secrets**
- Token configuration

Essentials

- Display name : BarracudaCGFApp
- Application (client) ID :
- Directory (tenant) ID :
- Object ID :
- Supported account types : My organization only
- Redirect URIs : Add a Redirect URI
- Application ID URI : Add an Application ID URI
- Managed application in local directory : BarracudaCGFApp

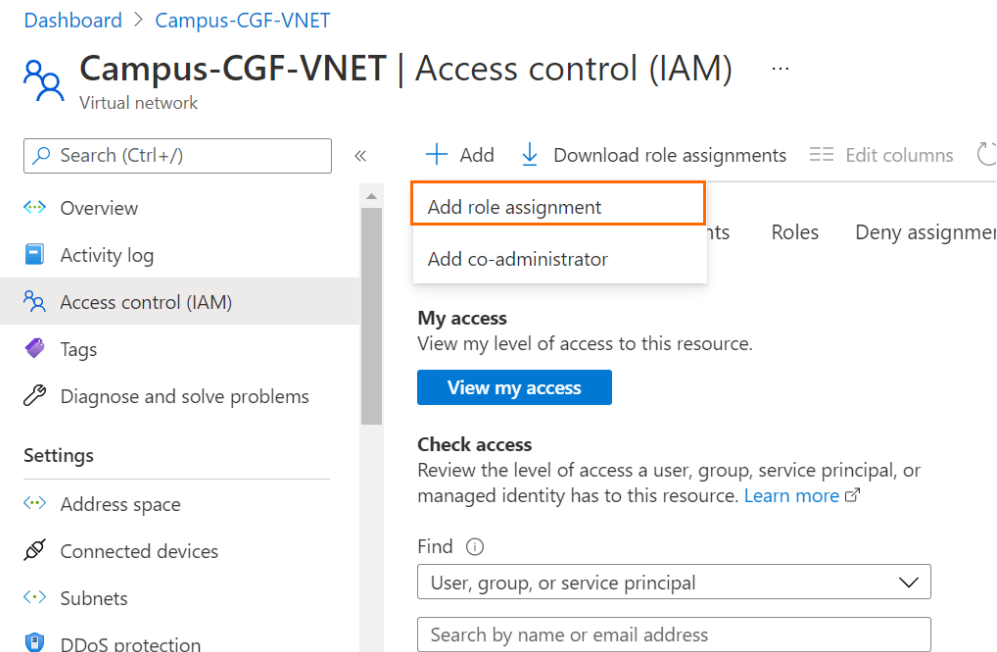
Step 3. Assigning the Permissions

1. Go to the Azure portal: <https://portal.azure.com>
2. Go to the Resource Group that contains the VNET and User Defined Routes of the CloudGen Firewall.
3. In the left menu, select **Access Control (IAM)**.



4. Click **+ Add**.

5. Select **Add role assignment**.



6. The **Add role assignment** window opens. Specify values for the following:

- **Role** - Select **Network Contributor**.
- **Assign Access to** - Select **User, group, or service principal**.
- **Select** - Enter the name of the application created in Step 2 and click on its entry in the list.

Add role assignment ✕

Role ⓘ

Network Contributor ⓘ

Assign access to ⓘ

User, group, or service principal

Select ⓘ

barracudaCGFApp

No users, groups, or service principals found.

Selected members:



BarracudaCGFApp

Remove

Save

Discard

7. Click **Save**.

This role is sufficient for the firewall to manage the route tables. If you want the firewall to monitor the IP Forwarding setting of its network interfaces as well, you must add the role **Virtual Machine Contributor**. Repeat Step 3 and select **Virtual Machine Contributor**.

Add role assignment ×

Role ⓘ

Virtual Machine Contributor ⓘ

Assign access to ⓘ

User, group, or service principal

Select ⓘ

Barracudacgf

No users, groups, or service principals found.

Selected members:



BarracudaCGFApp

Remove

Save

Discard

Step 4. Get the Subscription ID

1. Log into the Azure portal: <https://portal.azure.com>
2. In the left menu, click **Subscriptions**.
3. Copy the **Subscription ID** in the **Subscription ID** column.

Home > Subscriptions

Subscriptions 🔍 ✕

Subscriptions in cudazure

[+ Add](#)

Showing subscriptions in cudazure. Don't see a subscription? [Switch directories](#)

My role ⓘ Status ⓘ

[Apply](#)

Show only subscriptions selected in the [global subscriptions filter](#) ⓘ











SUBSCRIPTION	SUBSCRIPTION ID	MY ROLE	CURRENT COST	STATUS	
EngineeringTeam	XXXXXXXXXXXXXXXXXXXXXXXXXXXX	Owner		✔ Active	...

4. Insert the **Subscription ID** in the text editor where you already inserted the **Application (client) ID** and the **Directory (tenant) ID**. You will need these 3 IDs in the Step 5.

Step 5. Configure Cloud Integration on the Firewall

1. Log into the firewall via Firewall Admin.
2. Go to **CONFIGURATION > Configuration Tree > Cloud Integration**.
3. Click **Lock**.
4. In the left menu, click **Azure Networking**.
5. In the Azure Networking section, specify values for the following:
 - **Azure Deployment Type** - Select **Azure Resource Manager**.
 - **Subscription ID** - Enter your Subscription ID, retrieved in Step 4.
 - **Tenant ID** - Enter your Tenant ID, retrieved in Step 2.
 - **Application ID** - Enter your Application ID, retrieved in Step 2.
 - **Resource Group** - Enter the name of the resource group containing the VNET and the UDR route table.
 - **Virtual Network Name** - Enter the name of the virtual network.
 - **Select Certificate** - Select the certificate created in Step 1 from the drop-down list.
 - **Management Key** - Click on the settings icon. Select **Import from File** and select the *.pem file created in Step 1.
 - **Protect IP forward settings** - Select **yes**.

Azure Networking

Azure Deployment Type	Azure-Resource-Manager-(ARM) ▼	
Subscription ID	[Redacted]	
Tenant ID	[Redacted]	
Application ID	[Redacted]	
Resource Group	catamaniuk-RG-CGF	
Virtual Network Name	catamaniukCGF-VNET	
Route Check Interval	300	
Select certificate	CampusCGF ▶	
Management Key	Hash: FMDJGQ 2048 Bits 	
Protect IP forwarding settings	yes	

6. Click **Send Changes**.
7. Click **Activate**.

Step 6. Configure Azure Environment

If your firewall is running in a non-default Azure environment, such as Azure Germany, govcloud, Azure China, or Azure Stack, you must configure the Azure environment. Otherwise, you can skip this step.

1. Log into the firewall via Firewall Admin.
2. Go to **CONFIGURATION > Configuration Tree > Cloud Integration**.
3. Click **Lock**.
4. In the left menu, click **Configuration mode** and click **Switch to Advanced**.
5. In the left menu, click **Azure Networking**. Then, specify values for the following:
6. **Azure Environment** - Select the Azure Environment from the drop-down menu. Select **Explicit** if your environment is not listed in the drop-down menu. If you have selected **Explicit**, you must provide the following configuration:
 - **Service Management URL** - Enter the Service Management URL.
 - **Resource Manager URL** - Enter the Resource Manager URL.
 - **Active Directory Authority** - Enter the Active Directory Authority.
 - **Token Issuer Service URL** - Enter the Token Issuer Service URL.
 - **Resource** - Enter the resource identifier.

Configuration

- ✔ **Azure Networking**
- Azure Event Hub
- Azure OMS
- Azure Virtual WAN
- AWS Integration
- AWS Cloudwatch
- AWS Autoscaling

Configuration Mode

Switch to Basic View

Azure Networking

Azure Deployment Type: Azure-Resource-Manager-(ARM)

Subscription ID: [Redacted]

Tenant ID: [Redacted]

Application ID: [Redacted]

Resource Group: catamaniuk-RG-CGF

Virtual Network Name: catamaniukCGF-VNET

Route Check Interval: 300

Select certificate: CampusCGF

Management Key: Hash: [Redacted] ⚙️

Protect IP forwarding settings: yes

Azure Environment: ✔ **Germany**

Service Management URL: https://management.core.windows.net

Resource Manager URL: https://management.azure.com

Active Directory Authority: https://login.windows.net

Token Issuer Service URL: https://sts.windows.net

Resource: [Redacted]

7. Click **Send Changes**.
8. Click **Activate**.

Monitoring

Go to **NETWORK > Azure UDR** to see the UDR routing table for all subnets in the firewall's VNET. Routes using the firewall VM as the next hop are marked with a green icon. This icon changes to red during the UDR HA failover process.

Table / Route	Prefix	Next Hop Type	Next Hop Gateway	Mode
DOC-Routetable				
✔ Backend-2-VNET	0.0.0.0/0	VirtualAppliance	10.8.1.10	ARM

All activity is logged to the **Box\Control\daemon** log file.

Box\Control\daemon <new Log>

Select Log File Box\Control\daemon Reload Log File Tree

Time	Type	TZ	Message
2016 01 22 10:12:17	Notice	+00:00	control: UDP Handler: Server/Service state changed
2016 01 22 10:12:21	Notice	+00:00	----- Server State Changed -----
2016 01 22 10:12:21	Info	+00:00	----- Server State for VSNGFHA: this=down other=secondary
2016 01 22 10:12:21	Notice	+00:00	-----
2016 01 22 10:12:21	Notice	+00:00	Public Key for secondary boxIP 10.8.1.20 server VSNGFHA present
2016 01 22 10:12:32	Info	+00:00	control: Send session poll request status to master 10.8.10.10
2016 01 22 10:12:35	Notice	+00:00	control: UDP Handler: Server/Service state changed
2016 01 22 10:12:35	Info	+00:00	control: Send status poll request status to master 10.8.10.10
2016 01 22 10:12:35	Info	+00:00	control: Send session poll request status to master 10.8.10.10
2016 01 22 10:12:36	Info	+00:00	control: route Backend-2-INET in route table DOC-Routetable successfully updated (old gateway IP: 10.8.1.20 new gateway IP: 10.8.1.10)

Figures

1. dashboard_Cl.png
2. create_cert.png
3. create2.png
4. cert3.png
5. export1.png
6. export2.png
7. export3.png
8. app_registrations.png
9. register_app.png
10. cert_sec.png
11. upload_cer.png
12. upload_success.png
13. ids.png
14. IAM1.png
15. add_ra.png
16. add_role1.png
17. add_role2.png
18. vwan_sp_06.png
19. cloud_integration.png
20. azure_env.png
21. ARM-UDR_01.png
22. ARM-UDR_02.png

© Barracuda Networks Inc., 2022 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.