



# Cybersecurity

## Project 1 Technical Brief

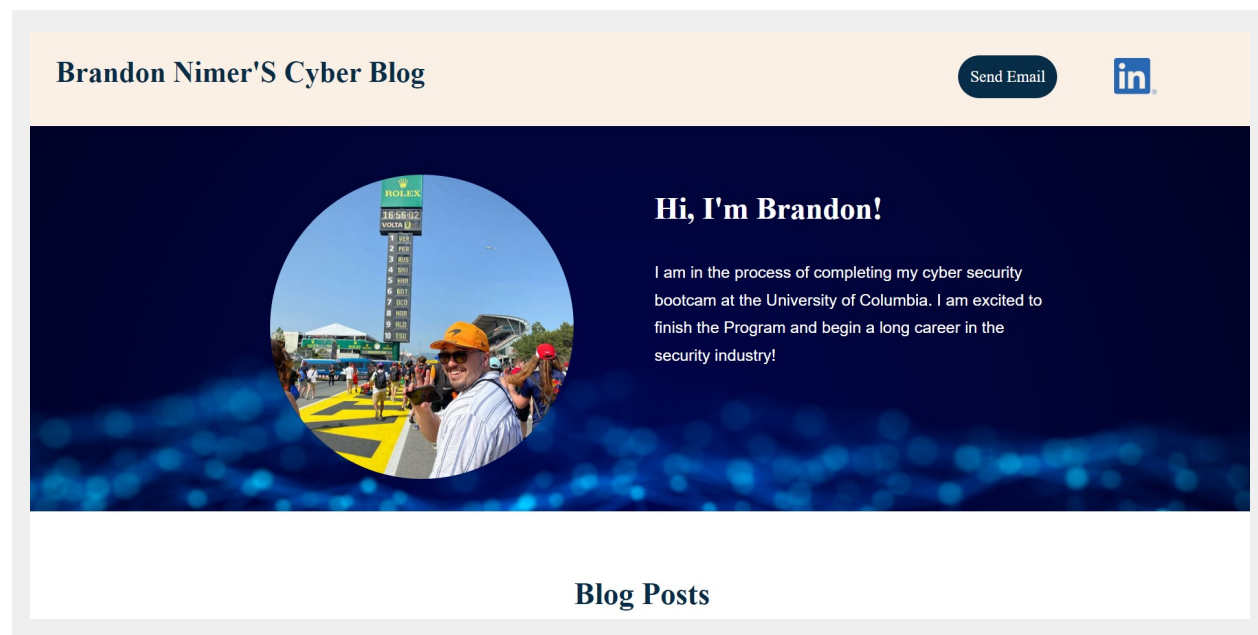
Make a copy of this document before you begin. Place your answers below each question. This completed document will be your deliverable for Project 1. Submit it through Canvas when you're finished with the project at the end of the week.

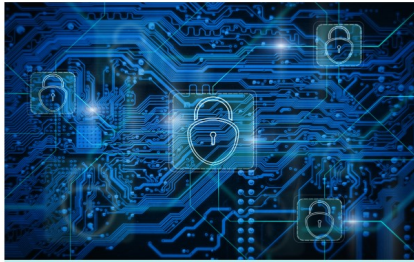
### Your Web Application

Enter the URL for the web application that you created:

<https://brandonsecurityblog2.azurewebsites.net/>

Paste screenshots of your website created (Be sure to include your blog posts):





## CrimeGPT

### AI, ChatGPT

As AI continues to progress, we are seeing more and more processes becoming automated. One of the more recent (and quite frankly scary) creations are tools like "WormGPT" that are now able to write malicious software without having to worry about prohibitions that other AI tools have in place. We got to see this tool in use earlier this year when a security firm asked it to create a phishing lure to trick employees into paying a fake invoice. What resulted was a "persuasive and strategically cunning" email, which demonstrates the capability of such a product. In the right hands this could be a tool for pen testers or ethical hackers, however this does open the door to bad actors being able to craft new and improved schemes to launch on their next victims. It is going to be interesting monitoring this in the weeks/months to come, especially as more of these AI programs become available. While the advancement of the entire machine learning and AI industry is exciting and opens doors to new possibilities, it also creates a lower barrier of entry for cyber criminals, allowing them to create malicious software with the click of a button. With this in mind, cyber security has never been more of a need for businesses everywhere. Making sure your network is secure is only part of the battle now. Proper education for employees is more critical than ever. Being able to spot phishing attempts and knowing the dangers of cyber attacks have to be top of mind for teams everywhere.



## No Trust These Days

### Zero Trust Architecture

One of the first things we learned in our Cyber Security Bootcamp was the saying, "it's not a matter of if your system can be broken into, but how long it will take". Zero Trust Architecture seems to have emerged with this mindset. It assumes that no device or user whether inside or outside the network should be trusted by default. Access controls and continuous authentication are a must to ensure that only authorized users can access sensitive information. Especially in today's remote and cloud centered environments, this model addresses the challenges posed by increasing numbers of devices and locations where users can connect (i.e. connecting to free wifi from a coffee shop). With the implementation of Zero Trust, it also requires new identity and access management solutions. A shift from reactive security to proactive security is needed to focus on continuous monitoring and real time threat detection. As more and more companies expand to a remote or even hybrid environment this Zero Trust mentality will seemingly become the norm. In a smarter world where AI is making the jobs of cyber criminals easier, it has never been more important to stay on your guard and ensure your data is secure.

## Day 1 Questions

### General Questions

1. What option did you select for your domain (Azure free domain, GoDaddy domain)?

## Azure Free Domain

2. What is your domain name?

`https://brandonsecurityblog2.azurewebsites.net/`

## Networking Questions

1. What is the IP address of your webpage?

`20.211.64.15`

2. What is the location (city, state, country) of your IP address?

`New South Wales, Sydney Australia`

3. Run a DNS lookup on your website. What does the NS record show?

When I run nslookup on my local computer for my website, we can see the server name, the IP address, and any alias for the site:

```
PS C:\Users\brand> nslookup -type=NS brandonsecurityblog2.azurewebsites.net
Server:  G3100.myfiosgateway.com
Address:  2600:4041:54f2:5d00::1

Non-authoritative answer:
brandonsecurityblog2.azurewebsites.net  canonical name = waws-prod-sy3-097.sip.azurewebsites.windows.net
waws-prod-sy3-097.sip.azurewebsites.windows.net canonical name = waws-prod-sy3-097-ef32.australiaeast.cloudapp.azure.com
australiaeast.cloudapp.azure.com
    primary name server = ns1-06.azure-dns.com
    responsible mail addr = msnhst.microsoft.com
    serial = 10001
    refresh = 900 (15 mins)
    retry = 300 (5 mins)
    expire = 604800 (7 days)
    default TTL = 60 (1 min)
PS C:\Users\brand>
```

## Web Development Questions

1. When creating your web app, you selected a runtime stack. What was it? Does it work on the front end or the back end?

The PHP I selected for the runtime stack was php 8.2, which works on the back end

2. Inside the `/var/www/html` directory, there was another directory called `assets`. Explain what was inside that directory.

When looking into the `assets` folder we can see the stock images that will be showing on the website, as well as the `css` file which has all of the font information

```
root@97ef5174c64c:/var/www/html# cd assets
root@97ef5174c64c:/var/www/html/assets# ls
css  images
root@97ef5174c64c:/var/www/html/assets# ls images
Background.jpg Image1.jpg Image2.jpg LinkedIn-logo.png RobertSmith-profile.jpg readme
root@97ef5174c64c:/var/www/html/assets# ls css
style.css style.css.bak
```

3. Consider your response to the above question. Does this work with the front end or back end?

Front-end

## Day 2 Questions

### Cloud Questions

1. What is a cloud tenant?

A cloud tenant is a user of a cloud service provider

2. Why would an access policy be important on a key vault?

An Access policy on a key vault determines who can access the keys, secrets, and certificates and makes sure only you or other authorized personnel have access.

3. Within the key vault, what are the differences between keys, secrets, and certificates?

Keys are used for encryption, secrets are used for authentication and access control, and certificates are used for identity verification/secure communication.

## Cryptography Questions

### 1. What are the advantages of a self-signed certificate?

Some advantages to self-signed certificates are their ease of use and no cost. Self-signed certificates are free to create and relatively quick to setup

### 2. What are the disadvantages of a self-signed certificate?

They are not inherently trusted by the browser because they haven't been validated by a trusted source.

### 3. What is a wildcard certificate?

A wildcard certificate is a single cert with a wildcard character in the domain name field, allowing the cert to secure multiple sub domain names in relation to the same base domain.

### 4. When binding a certificate to your website, Azure only provides TLS versions 1.0, 1.1, and 1.2. Explain why SSL 3.0 isn't provided.

TLS 1.0, 1.1 and 1.2 have improved cryptographic security. SSL 3.0 is seen as insecure and outdated when compared to TLS, and TLS has become the industry standard.

### 5. After completing the Day 2 activities, view your SSL certificate and answer the following questions:

- a. Is your browser returning an error for your SSL certificate? Why or why not?

It is not returning an error for my SSL Certificate because Microsoft Azure has provided a valid Certificate with my subscription

b. What is the validity of your certificate (date range)?

Thursday, March 9, 2023 at 10:05:55PM to Sunday, March 3, 2024 at 10:05:55PM

c. Do you have an intermediate certificate? If so, what is it?

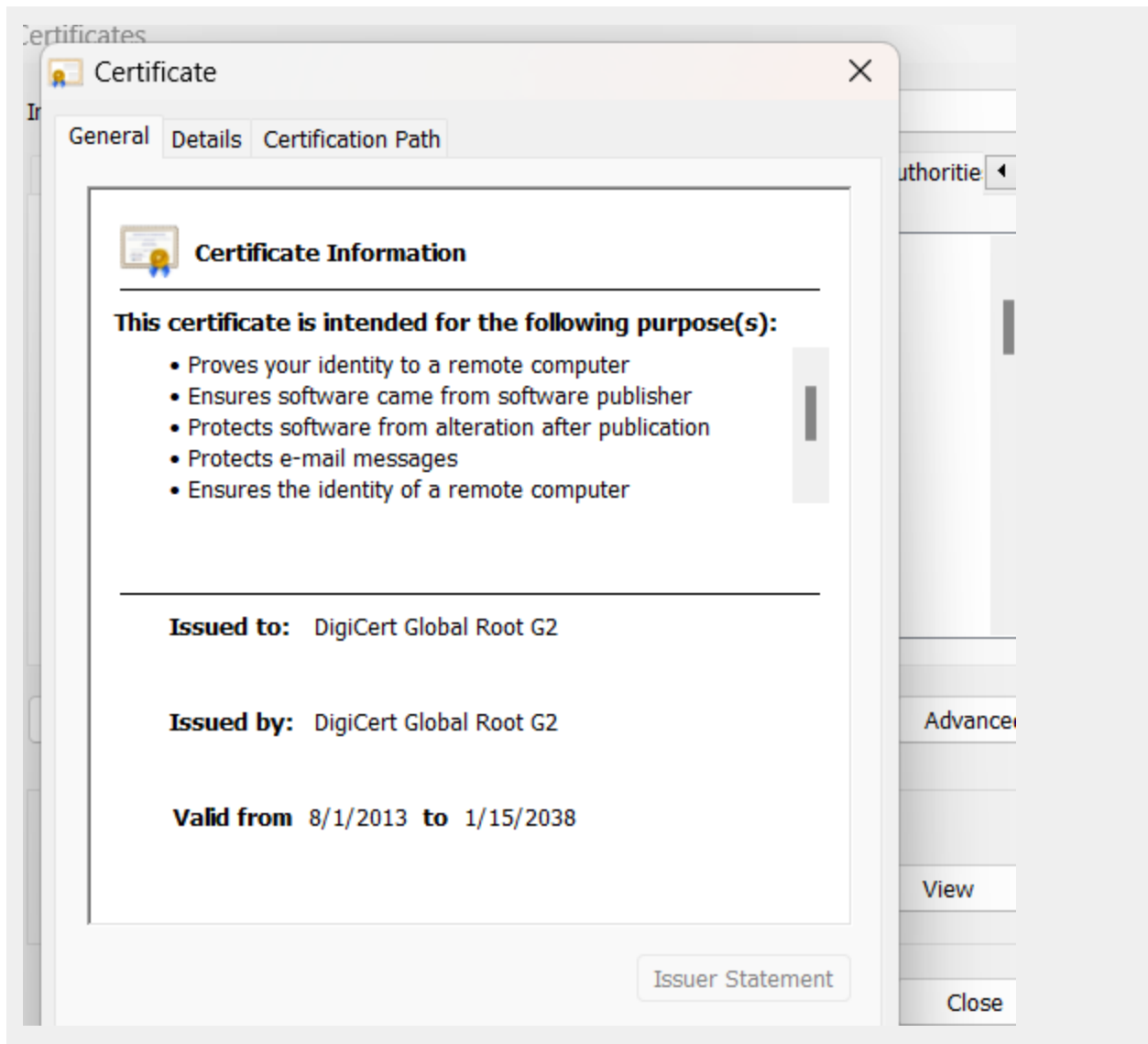
Yes I do have an intermediate certificate, it is Microsoft Azure TLS Issuing CA 02 (Microsoft Corporation)

d. Do you have a root certificate? If so, what is it?

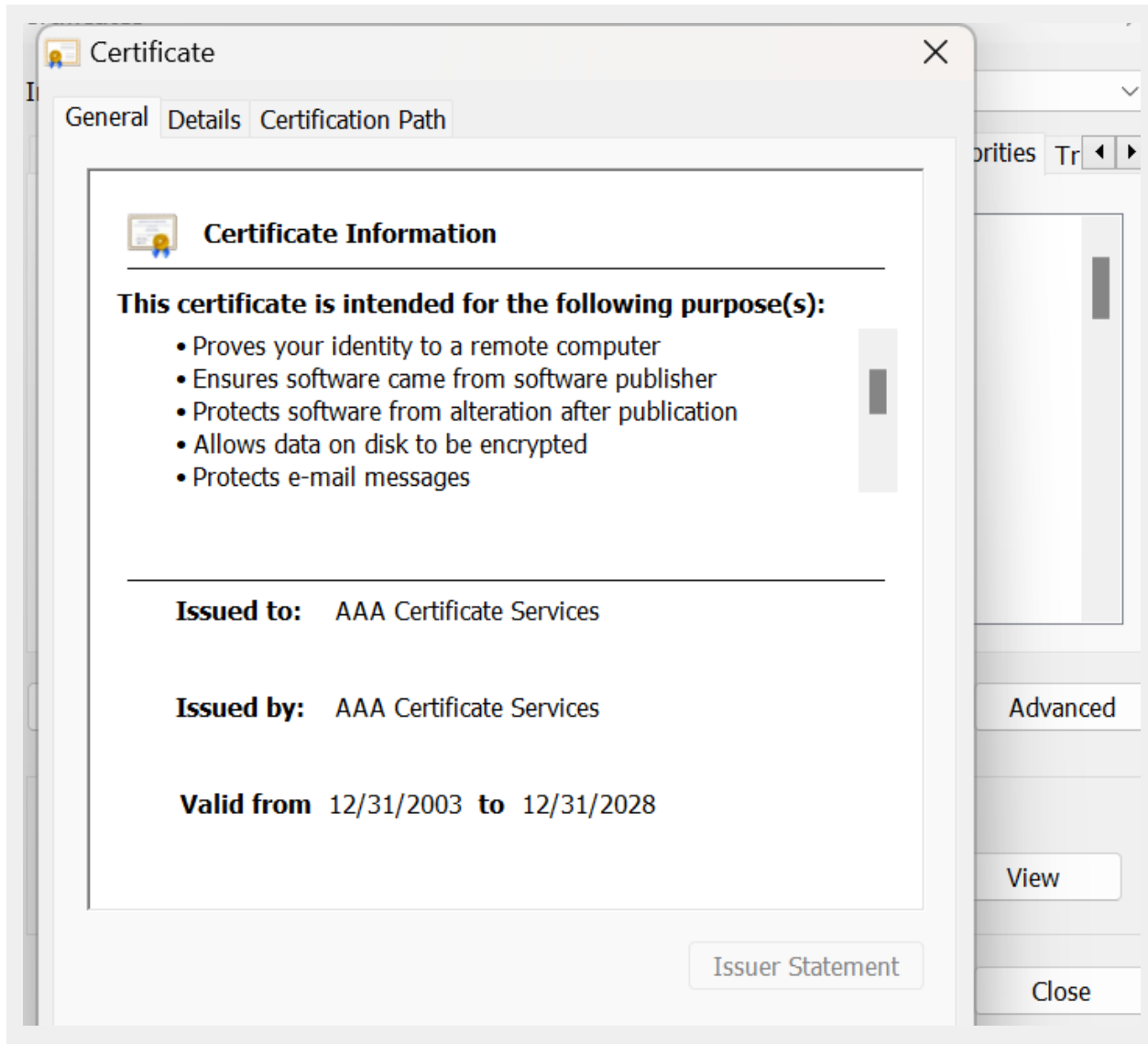
Yes, the DigiCert Global Root G2

e. Does your browser have the root certificate in its root store?

Yes



f. List one other root CA in your browser's root store.



## Day 3 Questions

### Cloud Security Questions

1. What are the similarities and differences between Azure Web Application Gateway and Azure Front Door?

Both Azure Web App Gateway and Azure Front Door offer advanced security and load balancing, however the Gateway primarily acts to secure the web applications whereas the Front Door acts as the global entry point for the web applications.



2. A feature of the Web Application Gateway and Front Door is “SSL Offloading.” What is SSL offloading? What are its benefits?

SSL Offloading is the process in which SSL encrypted incoming traffic is decrypted by an intermediate tool to relieve the web server from having to decrypt the data. This frees up the backend servers which can improve performance and response time, as well as provides an added layer of security.

3. What OSI layer does a WAF work on?

Layer 7

4. Select one of the WAF managed rules (e.g., directory traversal, SQL injection, etc.), and define it.

Rule 99031003 is a default Microsoft managed rule that attempts to block all instances of SQL injection attacks

<input type="checkbox"/> 99031003	SQL Injection Attack	⊖ Block on Anomaly	✔ Enabled
-----------------------------------	----------------------	--------------------	-----------

5. Consider the rule that you selected. Could your website (as it is currently designed) be impacted by this vulnerability if Front Door wasn't enabled? Why or why not?

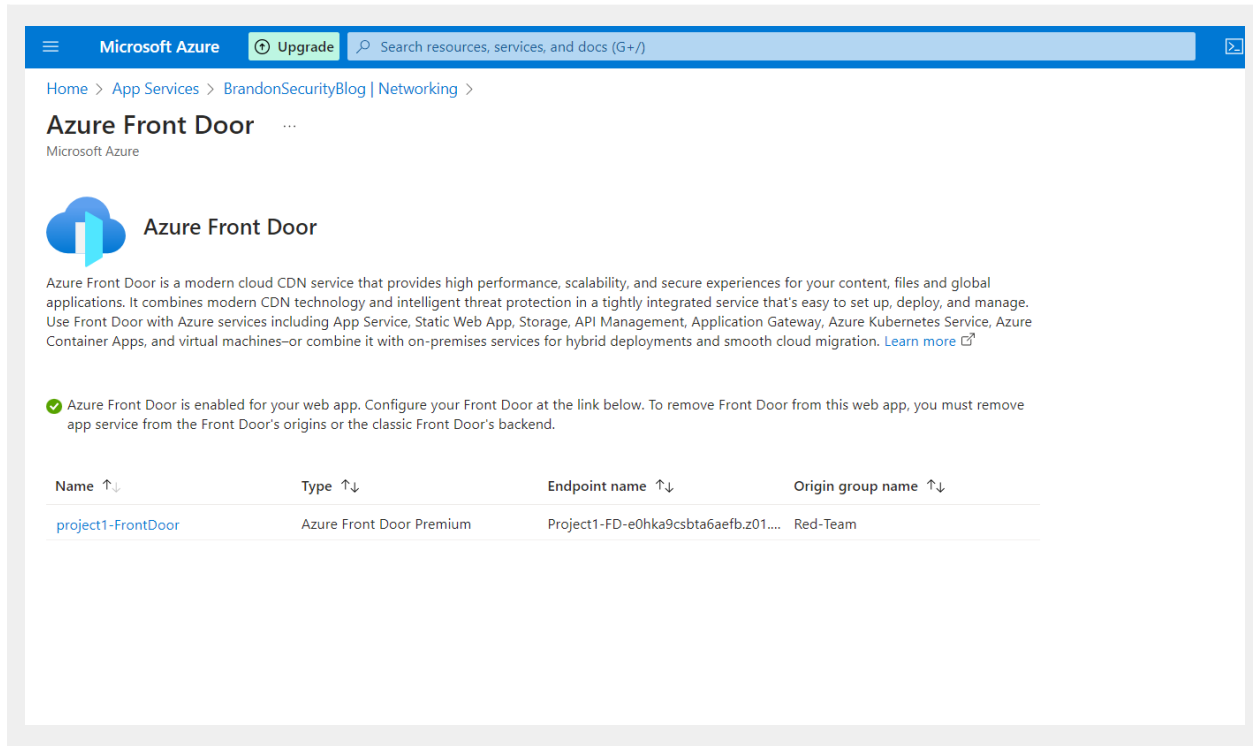
Because the Front Door provides the extra layer of security, if it were not enabled my website would most likely be much more vulnerable to SQL injection.

6. Hypothetically, say that you create a custom WAF rule to block all traffic from Canada. Does that mean that anyone who resides in Canada would not be able to access your website? Why or why not?

In theory yes it would block users who reside in Canada with the exception being people using a VPN. We already created a similar rule where we are blocking all traffic that is not from the US, Canada and Australia, so if we were to do the opposite we could limit the traffic from specific countries as well.

7. Include screenshots below to demonstrate that your web app has the following:

a. Azure Front Door enabled



The screenshot shows the Microsoft Azure portal interface. At the top, there's a navigation bar with the Microsoft Azure logo, an 'Upgrade' button, and a search bar. Below the navigation bar, the breadcrumb trail reads: Home > App Services > BrandonSecurityBlog | Networking >. The main heading is 'Azure Front Door' with a subheading 'Microsoft Azure'. Below this is the Azure Front Door logo and a description: 'Azure Front Door is a modern cloud CDN service that provides high performance, scalability, and secure experiences for your content, files and global applications. It combines modern CDN technology and intelligent threat protection in a tightly integrated service that's easy to set up, deploy, and manage. Use Front Door with Azure services including App Service, Static Web App, Storage, API Management, Application Gateway, Azure Kubernetes Service, Azure Container Apps, and virtual machines—or combine it with on-premises services for hybrid deployments and smooth cloud migration. [Learn more](#)'.

A green checkmark icon indicates that Azure Front Door is enabled for the web app. The text below the icon states: 'Azure Front Door is enabled for your web app. Configure your Front Door at the link below. To remove Front Door from this web app, you must remove app service from the Front Door's origins or the classic Front Door's backend.'

Below the text is a table with the following columns: Name, Type, Endpoint name, and Origin group name. The table contains one row with the following data:

Name	Type	Endpoint name	Origin group name
<a href="#">project1-FrontDoor</a>	Azure Front Door Premium	Project1-FD-e0hka9csbta6aefb.z01....	Red-Team

b. A WAF custom rule

> DefaultWebAppWaf33a9574aadb642959da4970d7707c1e6

DefaultWebAppWaf33a9574aadb642959da4970d7707c1e6 | Custom rules ☆ ...

Front Door WAF policy

Search << Save Discard Refresh

Overview

Activity log

Access control (IAM)

Tags

Settings

Policy settings

Managed rules

Custom rules

Associations

Properties

Locks

Automation

Tasks (preview)

Export template

Support + troubleshooting

New Support Request

Configure a policy with custom-authored rules. Once a rule is matched, the corresponding action defined in the rule is applied to the request. Once such a match is processed, rules with lower priorities are not processed further. A smaller integer value for a rule denotes a higher priority. [Learn more](#)

+ Add custom rule

Priority	Name	Rule type	Action	Status
100	Project1rule	Match	Block	Enabled

## Disclaimer on Future Charges

Please type “**YES**” after one of the following options:

- **Maintaining website after project conclusion:** I am aware that I am responsible for any charges that I incur by maintaining my website. I have reviewed the [guidance](#) for minimizing costs and monitoring Azure charges.
- **Disabling website after project conclusion:** I am aware that I am responsible for deleting all of my project resources as soon as I have gathered all of my web application screen shots and completed this document.