

Day 3 Activity File: Protect Your Web Application with Azure's Security Features

Today, you will be protecting your web application. Specifically, you will be working on:

- (1) **Create a front door instance.**
- (2) **Analyze WAF rule sets.**
- (3) **Configure custom WAF rules.**
- (4) **Analyze and remediate Security Center recommendations.**
- (5) **Answer review questions.**
- (6) **Conclude and submit your project.**

Resources

- [Azure Front Door Documentation](#)
- [Azure Front Door Locations by Region](#)
- [Azure Web Application Firewall on Front Door](#)
- [Azure Security Center Documentation](#)
- If Microsoft Support is needed, visit [How to open a support ticket](#)

Getting Started / Pre-requisites

Before you begin Day 3, you are required to have completed the following tasks from Day 2:

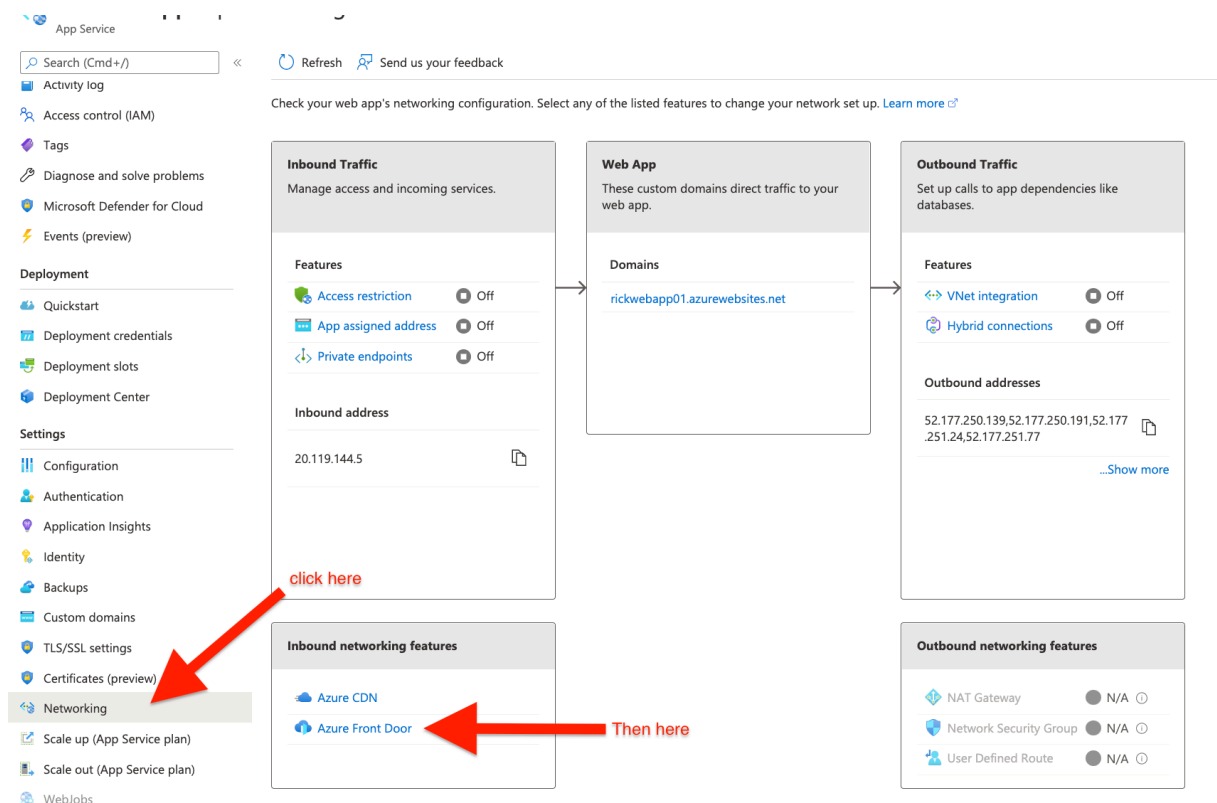
- Created a key vault.
- Created a self-signed certificate.
- Imported and Bound your self-signed certificate to your web app (Paid domains)
- Created and Bound an App Service Managed Certificate (Paid domains)
- Analyzed and compared self-signed certificates and trusted certificates.

Instructions

Part 1: Create a Front Door Instance

In this first part, you will create an Azure Front Door instance. To do so, complete the following steps:

1. Begin by logging in to the Azure portal: <https://portal.azure.com>.
 - Make sure that you're logged in to your personal Azure account (not @Cyberxsecurity), where your Cloud Security–unit VMs are located.
2. Next, access the app service resource that you created on Day 1.
3. From the menu on the left side of the screen, select "Networking."
4. From this page, select "Azure Front Door" under "Inbound networking features," as the following image shows:



5. On the next page, since you haven't created your Front Door resource yet, select "Create new" next to "Front Door profile."
6. This will open a pane on the right side of your screen.
 - In this pane, name your Front Door "project1-FrontDoor".
 - Add "Project1-FD" for the Endpoint name.
 - Make the Origin group name "Red Team".
 - Change the pricing tier to "Premium".

- Click the "Create" button at the bottom of the pane, as the following image shows:

The screenshot shows the 'Create a new Front Door' pane in the Azure portal. It includes fields for 'Front Door profile name', 'Endpoint name', 'Endpoint hostname', 'Origin group name', and 'Pricing tier'. A 'Create new' link is visible next to the 'Front Door profile' field. Red arrows and numbers indicate the following steps:

1. Click here (points to the 'Create new' link).
2. Then here (points to the 'Front Door profile name' field).
3. And then here (points to the 'Pricing tier' field).
4. Finally, click here (points to the 'Create' button at the bottom of the pane).

7. This will return you to the Azure Front Door page.

- Click "OK" to update the Front Door instance to your application, as the following image shows:

The screenshot shows the 'Azure Front Door' page in the Azure portal. It displays the 'Front Door profile' as '(New) Project1-FrontDoor' and the 'Endpoint' as '(New) Project1-FD-ezdhabe4e4ghbthk.z01.azurefd.net'. A red arrow points to the 'Create' button at the bottom of the page.

8. To verify that your Front Door instance has been set up correctly, select "Azure Front Door" (from Step 4) again.
9. The message "Azure Front Door is configured for your web app" should display as confirmation, as shown in the following image:



Azure Front Door

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](#)

✓ 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.

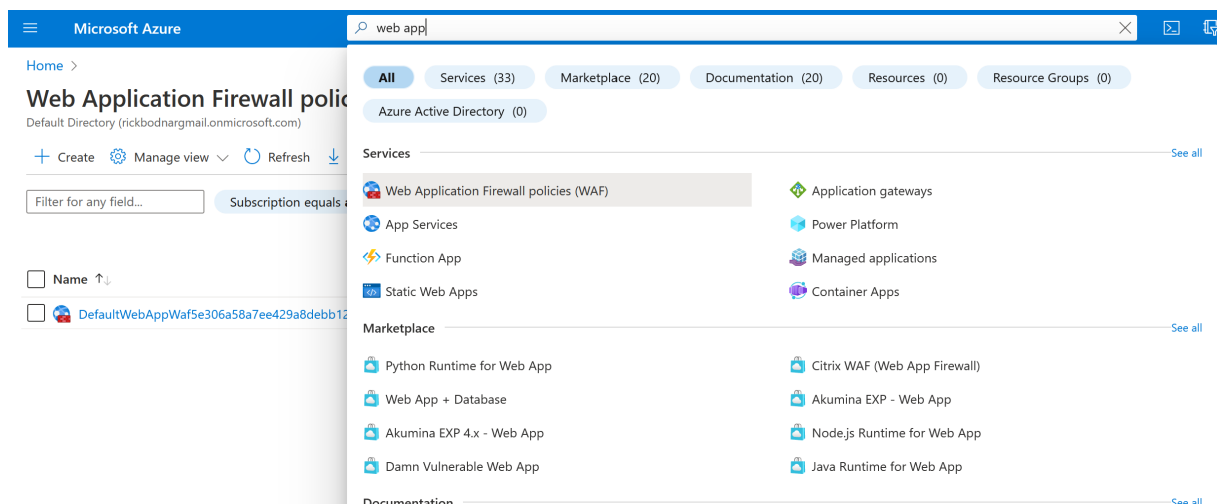
Name ↑↓	Type ↑↓	Endpoint name ↑↓	Origin group name ↑↓
Project1-FrontDoor	Azure Front Door Premium	Project1-FD-ezdhabe4e4ghbthkz0...	Red-Team

10. Take a screenshot of this confirmation.

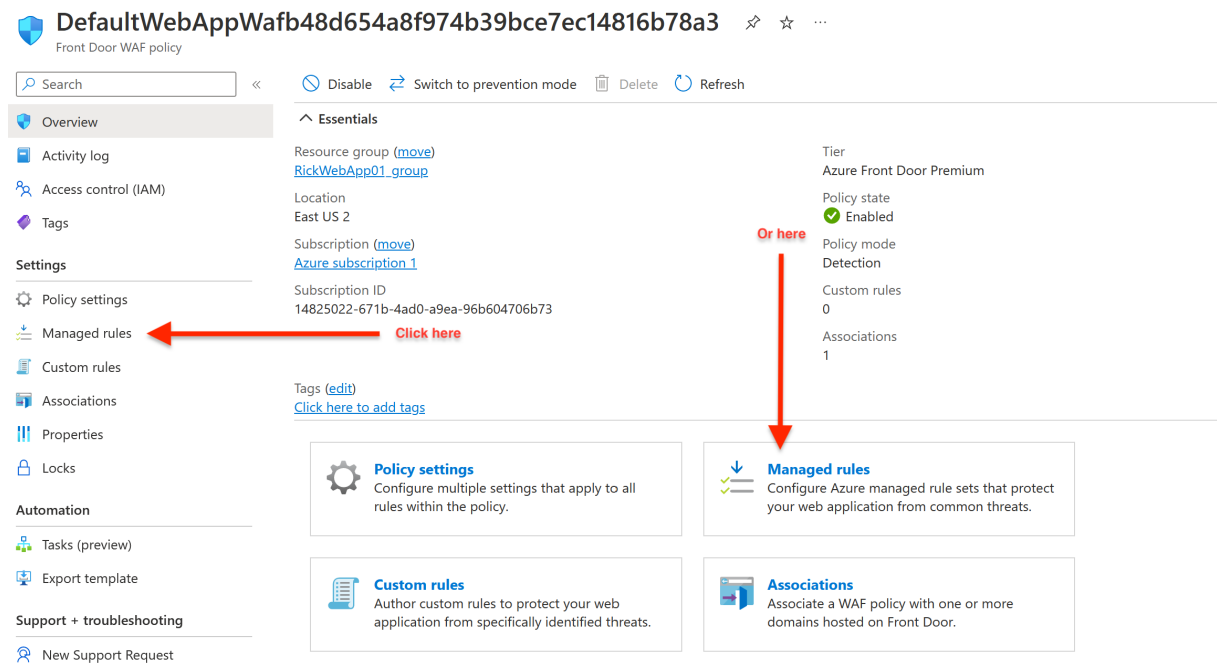
Part 2: Analyze WAF Rule Sets

In this second part, you will view the features that are provided by your web application firewall. To do so, complete the following steps:

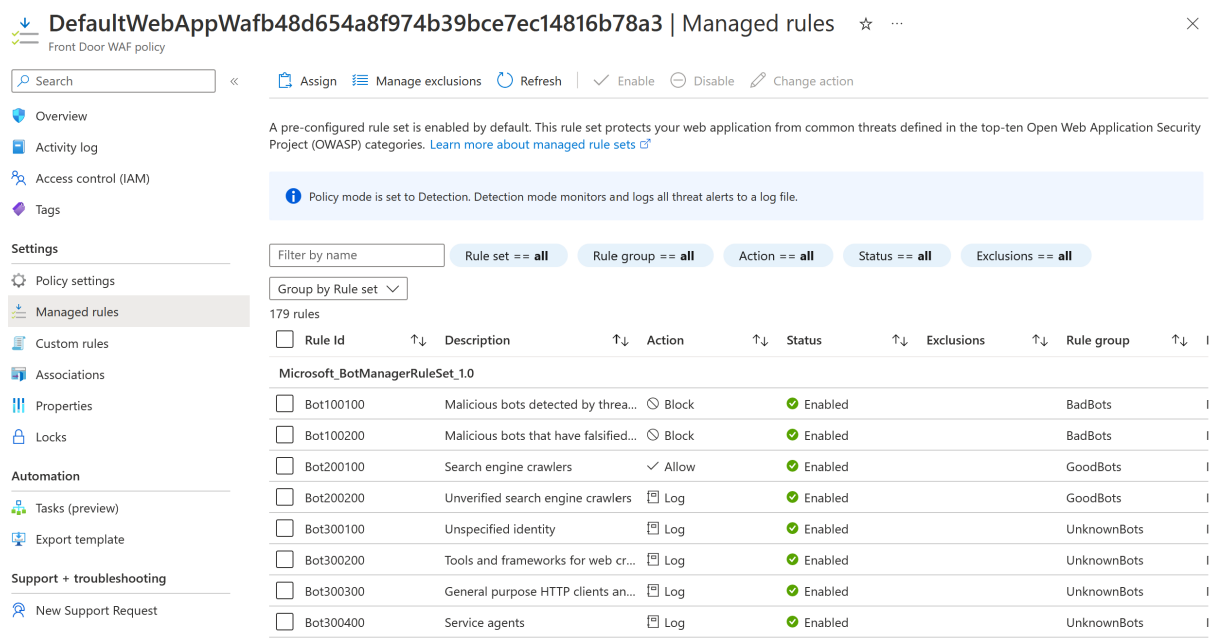
1. From your Azure portal, enter "web app" until "Web Application Firewall policies (WAF)" appears as one of the choices in the dropdown.
2. Select that option. The WAF that you created during the previous step should display on the "Web Application Firewall policies (WAF)" page.
 - Note: It will begin with "project1frontdoor" and end with several random letters and numbers.
3. Select your WAF, as the following image shows:



- When your WAF policies page opens, notice the options on the left side of your screen.
- Select "Managed rules" either from the left-hand toolbar or from the box on the bottom of the page, as the following image shows:



- When the "Managed rules" page appears, scroll through the page to view the various rules, as shown in the following image:



- Note the following about these rules:

- This is the list of the application vulnerabilities that the WAF will protect against (we will explore these vulnerabilities in further detail in the Web Vulnerabilities unit).
- While it's unlikely that your web application would be impacted by these vulnerabilities, this exercise illustrates the Azure WAF feature, which identifies and blocks the application attacks indicated on this page.
- These managed rules can be individually enabled or disabled, and a variety of actions can be taken if an attack is identified, such as:
 - Allow the request.
 - Block the request.
 - Log the request.
 - Redirect the request to another webpage.

Part 3: Configure Custom WAF Rules

In this part, you will configure a custom WAF rule to protect against a potential security attack.

Let's assume for this project that you have been experiencing a variety of attacks from international IP addresses, and you need to only accept traffic from the locations where your business partners reside: the United States, Canada, and Australia.

Now, you'll learn how to create a custom rule on your web application to protect against these attacks. To do so, complete the following steps:

1. Select "Custom rules" from the toolbar on the left-hand side of the screen, as the following image shows:

DefaultWebAppWafb48d654a8f974b39bce7ec14816b78a3 | Managed rules ☆ ...

Front Door WAF policy

Search « Assign Manage exclusions Refresh Enable Disable Change action

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

A pre-configured rule set is enabled by default. This rule set protects your web application from common threats defined in the top-ten Open Web Application Security Project (OWASP) categories. [Learn more about managed rule sets](#)

Policy mode is set to Detection. Detection mode monitors and logs all threat alerts to a log file.

Filter by name Rule set == all Rule group == all Action == all Status == all Exclusions == all

Group by Rule set

179 rules

<input type="checkbox"/>	Rule Id	Description	Action	Status	Exclusions	Rule group
Microsoft_BotManagerRuleSet_1.0						
<input type="checkbox"/>	Bot100100	Malicious bots detected by threa...	Block	Enabled		BadBots
<input type="checkbox"/>	Bot100200	Malicious bots that have falsified...	Block	Enabled		BadBots
<input type="checkbox"/>	Bot200100	Search engine crawlers	Allow	Enabled		GoodBots
<input type="checkbox"/>	Bot200200	Unverified search engine crawlers	Log	Enabled		GoodBots
<input type="checkbox"/>	Bot300100	Unspecified identity	Log	Enabled		UnknownBots
<input type="checkbox"/>	Bot300200	Tools and frameworks for web cr...	Log	Enabled		UnknownBots
<input type="checkbox"/>	Bot300300	General purpose HTTP clients an...	Log	Enabled		UnknownBots
<input type="checkbox"/>	Bot300400	Service agents	Log	Enabled		UnknownBots

2. To create a custom rule, select "+ Add custom rule."

- When the pane pops up on the right, name your custom rule "Project1rule."
- Leave the status and rule type at the default options.
- Set the priority to 100.
- Set the following terms for the rule's condition:
 - Match type: Geo location
 - Operation: is not
 - Select the three countries (USA, Canada, Australia)
 - Then: Deny traffic
- Then, click "Add."
- The following image shows these steps:

The screenshot shows the 'Add custom rule' dialog in the Azure WAF console. Red arrows and numbers indicate the following steps:

- Click the '+ Add custom rule' button in the main panel.
- Click the 'Add custom rule' button in the dialog header.
- Select 'Rule type' in the dialog header.
- Select 'Is not' under the 'Operation' section.
- Select 'U.S., Canada, Australia' under the 'Country/Region' dropdown.
- Select 'Deny traffic' under the 'Then' section.
- Click the 'Add' button at the bottom right.

3. Your custom rule should now display on the page, as the following image shows:

The screenshot shows the 'Custom rules' page in the Azure WAF console. A blue banner at the top indicates 'There are pending changes, click 'Save' to apply.' Below this, a table lists the custom rules:

Priority	Name	Rule type	Action	Status
100	Project1rule	Match	Block	Enabled

4. Take a screenshot of your custom rule. Press "Save".

5. Congratulations! You have configured the WAF to restrict traffic from accessing your webpage unless the source IP is from the US, Canada, or Australia.

:warning: Checkpoint :warning:

Before continuing, make sure that you have completed the following critical tasks:

:heavycheckmark: Created your Azure Front Door instance.

:heavycheckmark: Created a WAF and analyzed your rule sets.

:heavycheckmark: Created a custom WAF rule to protect against international traffic.

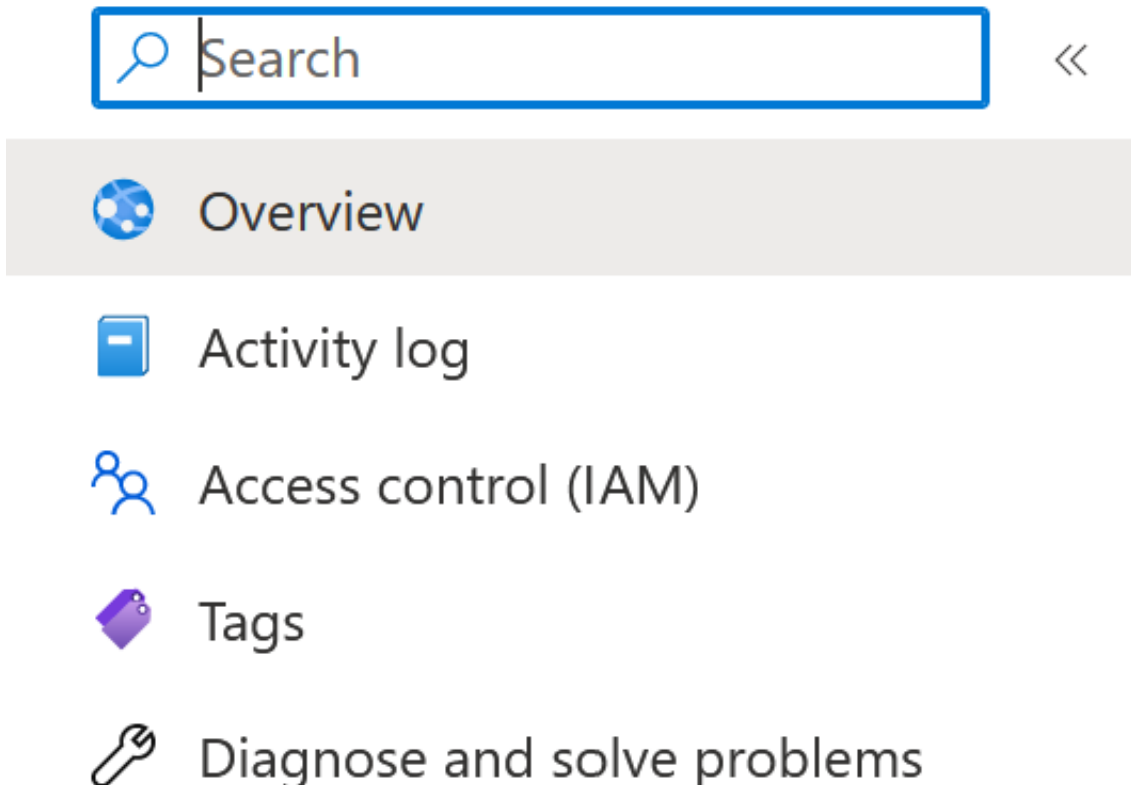
Part 4: Analyze and Fix a Security Center Recommendation

Azure Security Center is a management system that provides best practices and recommendations to enhance the security of your cloud resources.

While Azure provides tools to protect your cloud resources, it is up to you to apply the correct configurations and best practices to protect your web application.

In this part, you will learn how to use Microsoft Defender for Cloud to analyze and fix a recommendation from the dashboard. To do so, complete the following steps:

1. To access Defender for Cloud, from your web app, select "Microsoft Defender for Cloud" from the toolbar, as the following image shows:





Microsoft Defender for Cloud



Events (preview)

Deployment



Quickstart



Deployment credentials




Deployment slots



Deployment Center

Settings

2. When the Security page opens, it should display counts for both recommendations and alerts (note that your counts may vary).
 - Review the recommendations, and note that Azure describes the recommendations in this way: "Defender for Cloud continuously monitors the configuration of your app services to identify potential security vulnerabilities and recommends actions to mitigate them."
 -  **Important:** Your security recommendations may vary, or may not show up at all. If there are no security recommendations, skip ahead to Part 5, and return in a few hours to complete this section. If you have any, most security recommendations will appear within 24 hours.
3. Select the recommendation "Web apps should request an SSL certificate for all incoming

requests," as shown in the following image:


For enhanced security with just-in-time access, adaptive application controls and more, upgrade your subscription's Microsoft Defender for Cloud plan →


Visit [Microsoft Defender for Cloud](#) to manage security across your virtual networks, data, apps, and more

Recommendations

Security alerts

Microsoft Defender for App Services **Off**




3 

0 

Learn more
[About Microsoft Defender for Cloud](#)
[Protect App services](#)

Recommendations




Defender for Cloud continuously monitors the configuration of your app services to identify potential security vulnerabilities and recommends actions to mitigate them.

Description	Severity
Web apps should request an SSL certificate for all incoming requests	 Medium
Managed identity should be used in web apps	 Medium
D diagnostic logs in App Service should be enabled	 Medium

[View additional recommendations in Defender for Cloud >](#)

- When this page opens, expand the remediation steps, as shown in the following screenshot:

Web apps should request an SSL certificate for all incoming requests ...

 Exempt  View policy definition  Open query

Severity

Medium

Freshness interval

 30 Min

Tactics and techniques

 Initial Access

^ Description

Client certificates allow for the app to request a certificate for incoming requests.
Only clients that have a valid certificate will be able to reach the app.

^ Remediation steps

Manual remediation:

To set Client Certificates for your Web App:

1. Navigate to Azure App Service
2. Select Configuration
3. Go to the General Settings tab
4. Set Incoming Client Certificates to Require.

For more information, visit here: <https://aka.ms/auth-tls>

Take action

Trigger logic app

Exempt

Assign owner

Change owner and set ETA

5. Follow the recommended steps to remediate this recommendation.

Part 5: Answer Review Questions

- Open your copy of the [review questions](#), make a copy of the document, and answer the Day 3 review questions.
 - Note that you will submit this document as one of your deliverables at the end of the project.

Part 6: Conclude and Submit Your Project

Congratulations on completing your first project! Complete the following important instructions to submit and conclude your project.

- **Project Deliverables**

- Submit your review questions with all required screen shots through Bootcamp Spot.

- **Disable Any Paid Features**

- As a reminder, you are provided a \$200 credit by Microsoft to use for the resources of Cloud Week and this project.
 - If you are going to maintain your website:
 - After today's activity, you should minimally delete your Azure Front Door instance and WAF and any resources from the previous Cloud Security Unit.
 - If you are not going to maintain your website:
 - After you have submitted your review questions with screen shots, you are welcome to delete your **ALL** of your cloud resources used over the last 2 Units.
 - Use the following [guide](#) to assist with monitoring and stopping your costs.

- **Interview and Resume Guidance**

- When networking and talking to potential employers, you should be able to reference the work done on this project to answer specific interview questions or to demonstrate your skills within a specific domain.
- Reference the following document for guidance on how to add your project to your resume, discuss your project, and answer potential interview questions regarding your project activities: [Interview and Resume Guidance](#).

