



Cybersecurity

ALL DOMAINS - Day 3 Activity Guide

Protect Your Web Application with Azure's Security Features (Azure Free Domain and GoDaddy 99 Cent Domain)

Today, you will protect your web application. Specifically, you will:

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 / Prerequisites

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

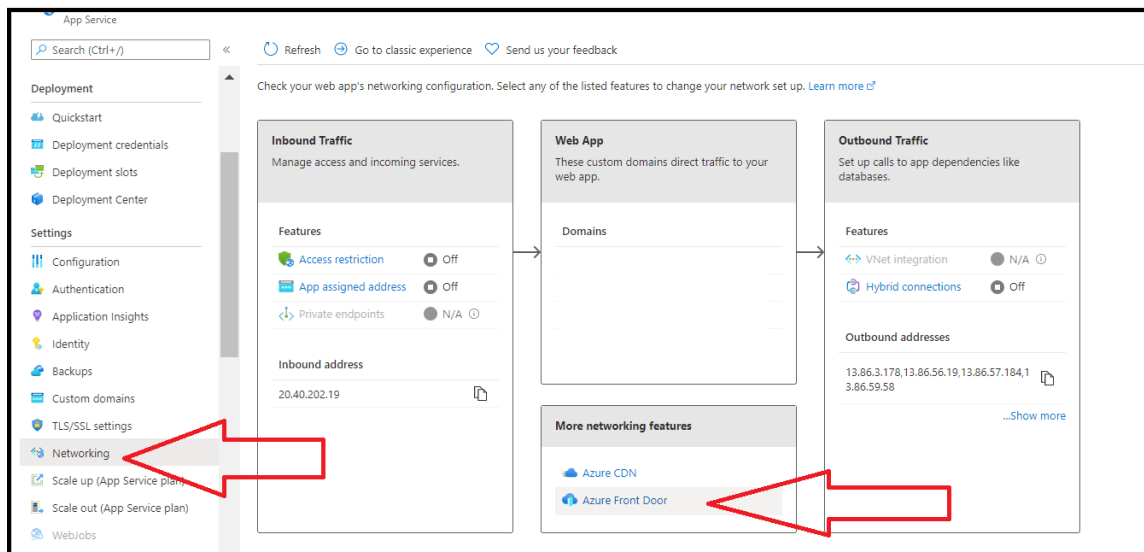
- Created a key vault.
- Created a self-signed certificate.
- Imported and Bound your self-signed certificate to your web app (Paid domains)
- Created and Bound an App Service Managed Certificate (Paid domains)
- Analyzed and compared self-signed certificates and trusted certificates.

Instructions

Part 1: Create a Front Door Instance

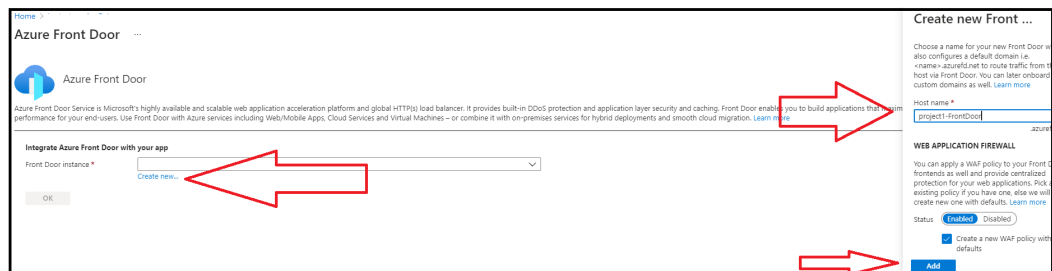
In this first part, you will create an Azure Front Door instance. To do so, complete the following steps:

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 “More networking features,” as the following image shows:



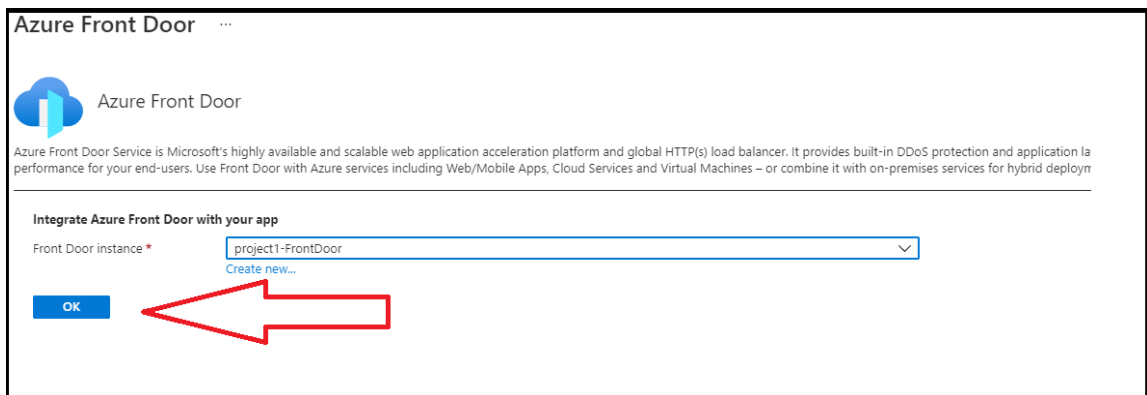
5. On the next page, since you haven't created your Front Door resource yet, select “Create new” under “Front Door instance.”
6. This will open a pane on the right side of your screen.
 - In this pane, name your Front Door “project1-FrontDoor”.

- Leave the default settings to create a default web application firewall (WAF).
- Click the “Add” button at the bottom of the pane, as the following image shows:



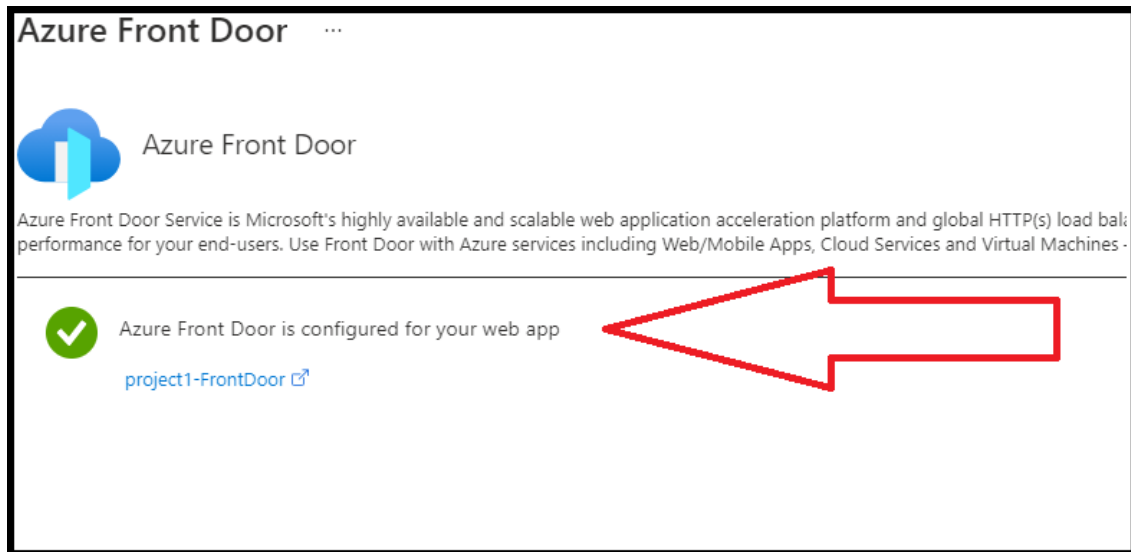
7. This will return you to the Azure Front Door page.

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



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:

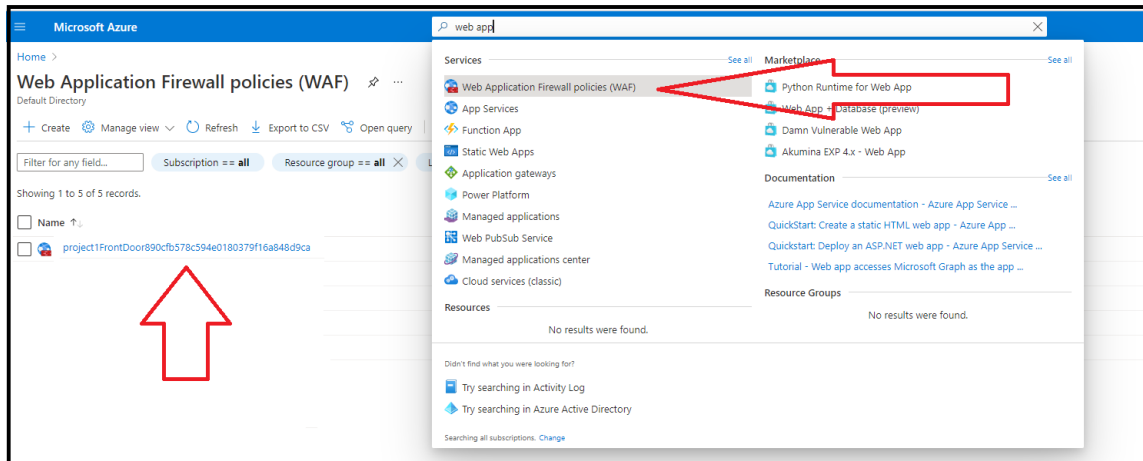


10. Take a screenshot of this confirmation.

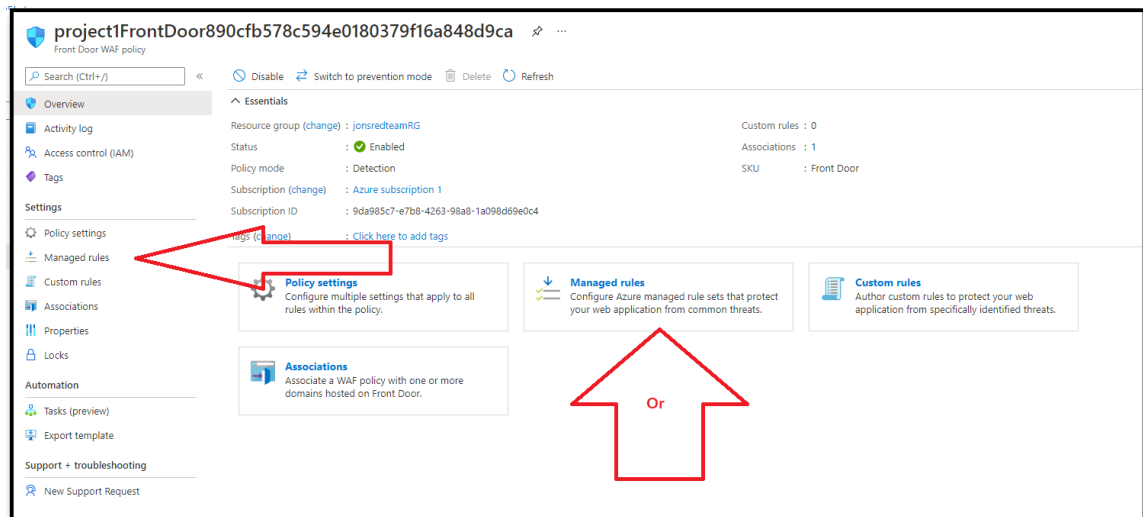
Part 2: Analyze WAF Rule Sets

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:



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



6. When the “Managed rules” page appears, scroll through the page to view the various rules, as shown in the following image:

project1FrontDoor890cfb578c594e0180379f16a848d9ca | Managed rules

Front Door WAF policy

Search (Ctrl+/) 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

112 rules

Rule Id	Description	Action	Status	Exclusions	Rule group	Rule set
DefaultRuleSet_1.0						
921110	HTTP Request Smuggling Attack	Block	Enabled		PROTOCOL-ATTACK	DefaultRuleSet_1.0
921120	HTTP Response Splitting Attack	Block	Enabled		PROTOCOL-ATTACK	DefaultRuleSet_1.0
921130	HTTP Response Splitting Attack	Block	Enabled		PROTOCOL-ATTACK	DefaultRuleSet_1.0
921140	HTTP Header Injection Attack via headers	Block	Enabled		PROTOCOL-ATTACK	DefaultRuleSet_1.0
921150	HTTP Header Injection Attack via payload (...)	Block	Enabled		PROTOCOL-ATTACK	DefaultRuleSet_1.0
921160	HTTP Header Injection Attack via payload (...)	Block	Enabled		PROTOCOL-ATTACK	DefaultRuleSet_1.0
921151	HTTP Header Injection Attack via payload (...)	Block	Enabled		PROTOCOL-ATTACK	DefaultRuleSet_1.0
930100	Path Traversal Attack (/../)	Block	Enabled		LFI	DefaultRuleSet_1.0
930110	Path Traversal Attack (/../)	Block	Enabled		LFI	DefaultRuleSet_1.0
930120	OS File Access Attempt	Block	Enabled		LFI	DefaultRuleSet_1.0
930130	Restricted File Access Attempt	Block	Enabled		LFI	DefaultRuleSet_1.0

- 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 module).
 - 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.

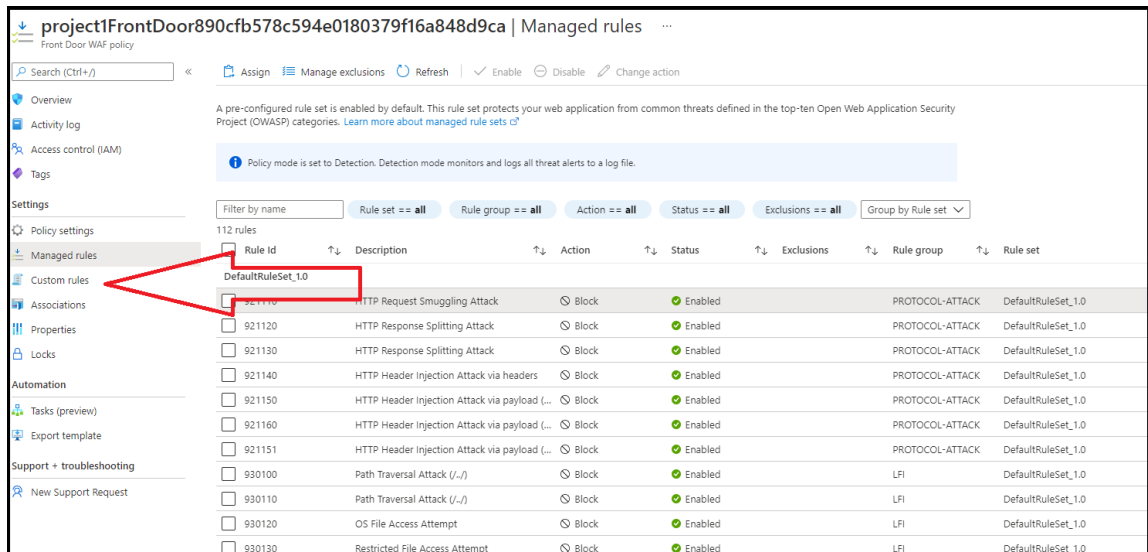
Part 3: Configure Custom WAF Rules

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

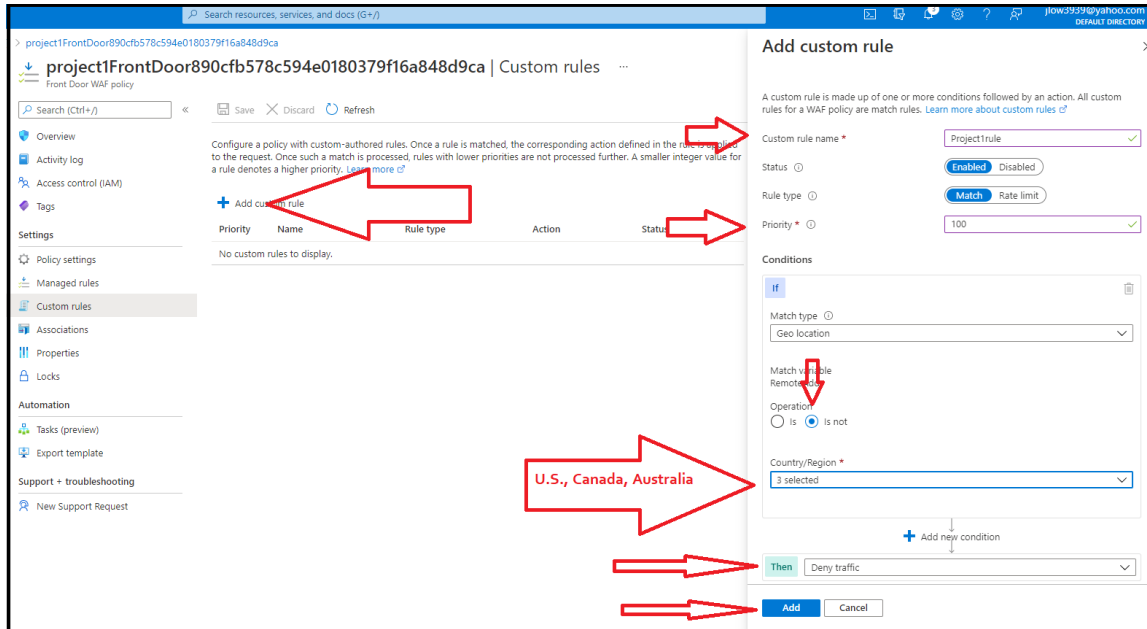
Let's assume for this project that you have been experiencing a variety of attacks from international IP addresses, and you need to only accept traffic from the locations where your business partners reside: the United States, Canada, and Australia.

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:

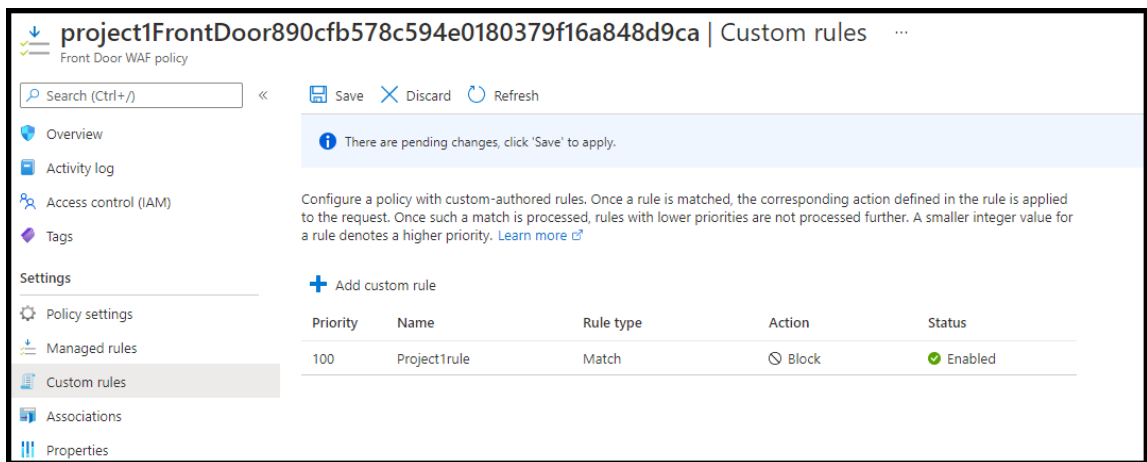
1. Select “Custom rules” from the toolbar on the left-hand side of the screen, as the following image shows:



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:



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



4. Take a screenshot of your custom rule. Press “Save.”

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

⚠ Checkpoint ⚠

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

✓ Created your Azure Front Door instance.

✓ Created a WAF and analyzed your rule sets.

✓ Created a custom WAF rule to protect against international traffic.

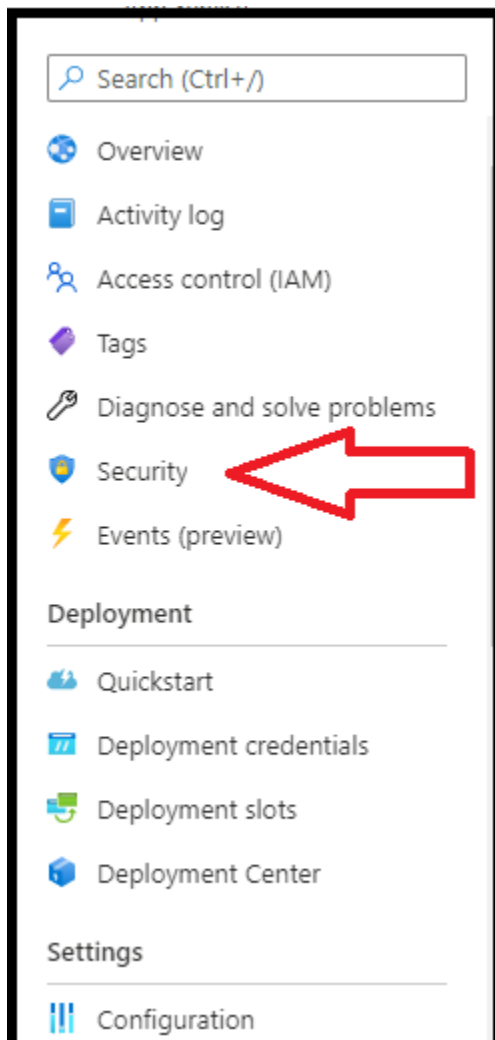
Part 4: Analyze and Fix a Security Center Recommendation

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 Azure Security Center to analyze and fix a recommendation from the Security Center dashboard. To do so, complete the following steps:

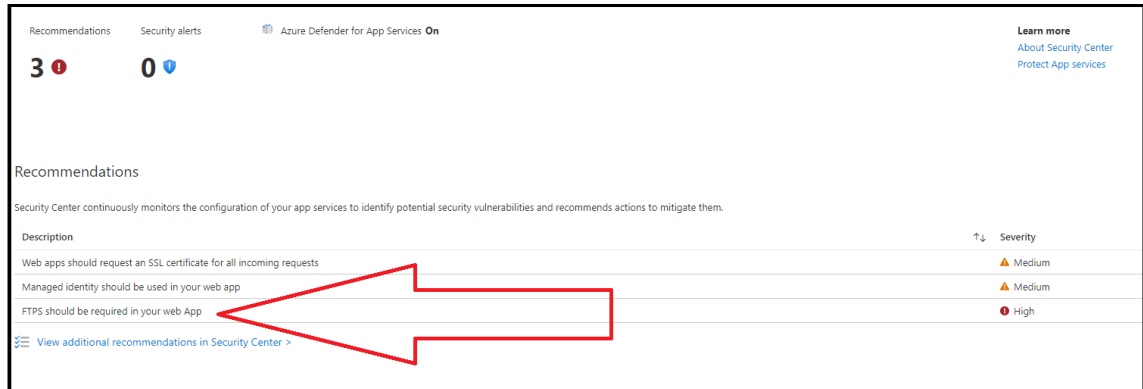
1. To access Azure Security Center, from your web app, select “Security” from the toolbar, as the following image shows:



2. When the Security Center 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: “Security Center 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 “FTPS should be required in your web App,” as shown in the following image:



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


FTPS should be required in your web App ...

 Exempt  View policy definition  Open query

Severity

High

Freshness interval

 30 Min

^ Description

Enable FTPS enforcement for enhanced security

^ Remediation steps

Manual remediation:

To ensure enforcement of FTPS only for your web app:

1. Go to the App Service for your API app

2. Select Configuration, and go to the General Settings tab

3. In FTP state, select FTPS only.

For more information, visit here: <https://aka.ms/deploy-ftp>

5. Follow the recommended steps to remediate this recommendation.

Part 5: Answer Review Questions

- Open your copy of the [Project 1 Technical Brief](#) review questions, and answer the Day 3 review questions.
 - Note that you will submit this document as your deliverable 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
 - Make sure that your website is still accessible, and submit your review questions through Canvas.
- 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.
 - After today's activity, once your screenshots have been submitted with your review questions, you should minimally delete your Azure Front Door instance and WAF.
 - You are welcome to delete your web application once it has been graded, but we strongly recommend keeping it up and maintaining your cyber blog.
 - 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.
 - Refer to 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](#).