

Experiment no. 8

Aim: To study and Implement Security as a Service on AWS/Azure

Requirements: Azure account

Theory:

We know that security is job one in the cloud and how important it is that you find accurate and timely information about Azure security. One of the best reasons to use Azure for your applications and services is to take advantage of its wide array of security tools and capabilities. These tools and capabilities help make it possible to create secure solutions on the secure Azure platform. Microsoft Azure provides confidentiality, integrity, and availability of customer data, while also enabling transparent accountability.

General Azure security

Microsoft Defender for Cloud A cloud workload protection solution that provides security management and advanced threat protection across hybrid cloud workloads.

Azure Key Vault A secure secrets store for the passwords, connection strings, and other information you need to keep your apps working.

Azure Monitor logs A monitoring service that collects telemetry and other data, and provides a query language and analytics engine to deliver operational insights for your apps and resources. Can be used alone or with other services such as Defender for Cloud.

Azure Dev/Test Labs A service that helps developers and testers quickly create environments in Azure while minimizing waste and controlling cost.

Storage security

Azure Storage Service Encryption A security feature that automatically encrypts your data in Azure storage.

StorSimple Encrypted Hybrid Storage An integrated storage solution that manages storage tasks between on-premises devices and Azure cloud storage.

Azure Client-Side Encryption A client-side encryption solution that encrypts data inside client applications before uploading to Azure Storage; also decrypts the data while downloading.

Azure Storage Shared Access Signatures A shared access signature provides delegated access to resources in your storage account.

Azure Storage Account Keys An access control method for Azure storage that is used for authentication when the storage account is accessed.

Azure File shares with SMB 3.0 Encryption A network security technology that enables automatic network encryption for the Server Message Block (SMB) file sharing protocol.

Azure Storage Analytics A logging and metrics-generating technology for data in your storage account.

Database security

Azure SQL Firewall A network access control feature that protects against network-based attacks to database.

Azure SQL Cell Level Encryption A database security technology that provides encryption at a granular level.

Azure SQL Connection Encryption To provide security, SQL Database controls access with firewall rules limiting connectivity by IP address, authentication mechanisms requiring users

to prove their identity, and authorization mechanisms limiting users to specific actions and data.

Azure SQL Always Encryption Protects sensitive data, such as credit card numbers or national identification numbers (for example, U.S. social security numbers), stored in Azure SQL Database or SQL Server databases.

Azure SQL Transparent Data Encryption A database security feature that encrypts the storage of an entire database.

Azure SQL Database Auditing A database auditing feature that tracks database events and writes them to an audit log in your Azure storage account.

Identity and access management

Azure role-based access control An access control feature designed to allow users to access only the resources they are required to access based on their roles within the organization.

Azure Active Directory A cloud-based authentication repository that supports a multi-tenant, cloud-based directory and multiple identity management services within Azure.

Azure Active Directory B2C An identity management service that enables control over how customers sign-up, sign-in, and manage their profiles when using Azure-based applications.

Azure Active Directory Domain Services A cloud-based and managed version of Active Directory Domain Services.

Azure AD Multi-Factor Authentication A security provision that employs several different forms of authentication and verification before allowing access to secured information.

Backup and disaster recovery

Azure Backup An Azure-based service used to back up and restore data in the Azure cloud.

Azure Site Recovery An online service that replicates workloads running on physical and virtual machines (VMs) from a primary site to a secondary location to enable recovery of services after a failure.

Networking

Network Security Groups A network-based access control feature using a 5-tuple to make allow or deny decisions.

Azure VPN Gateway A network device used as a VPN endpoint to allow cross-premises access to Azure Virtual Networks.

Azure Application Gateway An advanced web application load balancer that can route based on URL and perform SSL-offloading.

Web application firewall (WAF) A feature of Application Gateway that provides centralized protection of your web applications from common exploits and vulnerabilities

Azure Load Balancer A TCP/UDP application network load balancer.

Azure ExpressRoute A dedicated WAN link between on-premises networks and Azure Virtual Networks.

Azure Traffic Manager A global DNS load balancer.

Azure Application Proxy An authenticating front-end used to secure remote access for web applications hosted on-premises.

Azure Firewall A managed, cloud-based network security service that protects your Azure Virtual Network resources.

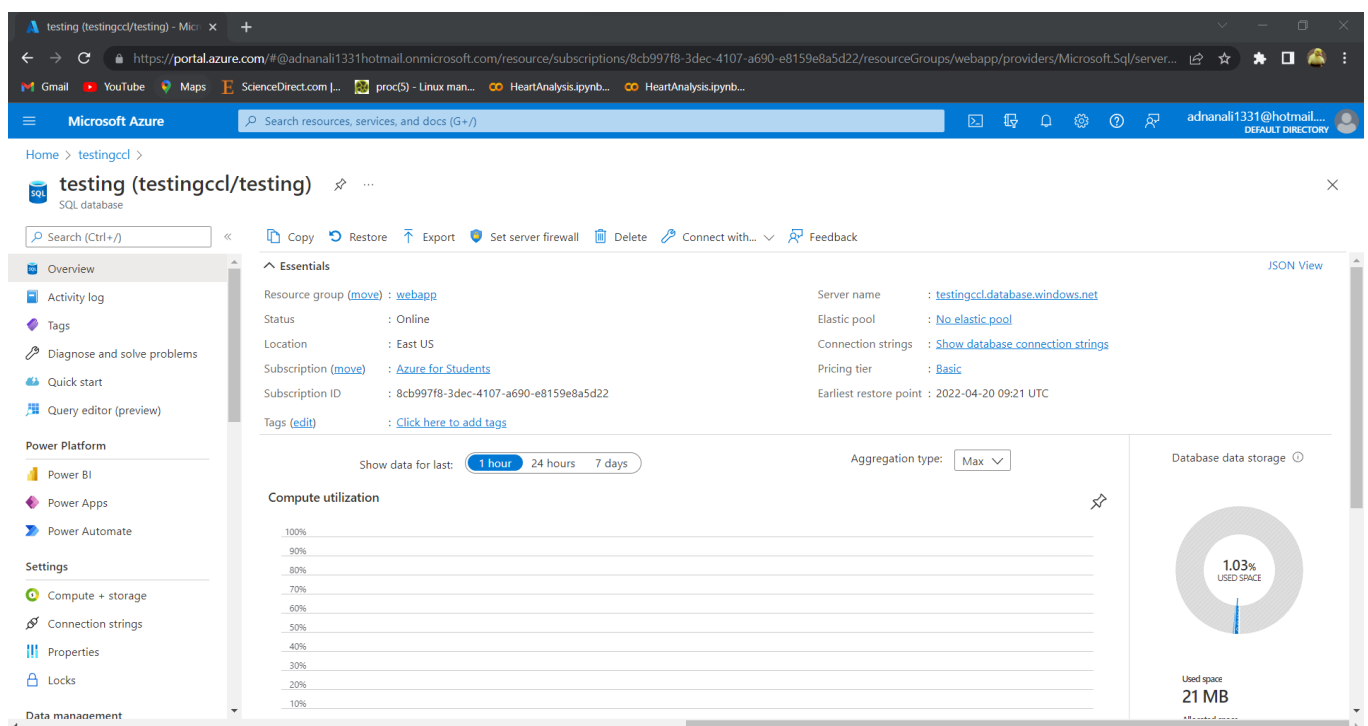
Azure DDoS protection Combined with application design best practices, provides defense against DDoS attacks.

Virtual Network service endpoints Extends your virtual network private address space and the identity of your VNet to the Azure services, over a direct connection.

Output:

Database Firewall protection

Database:



Adding Firewall security:

The screenshot shows the 'Firewall settings' page for a resource named 'testingcd (SQL server)'. The page includes options to 'Save', 'Discard', or 'Add client IP'. Key settings include:

- Deny public network access:** ☐
- Minimum TLS Version:** 1.0, 1.1, 1.2 (1.2 is selected)
- Connection Policy:** Default, Proxy, Redirect (Default is selected)
- Allow Azure services and resources to access this server:** Yes, No (Yes is selected)
- Client IP address:** 45.115.187.209
- Rule name, Start IP, End IP table:**

Rule name	Start IP	End IP
ClientIPAddress_2022-4...	45.115.187.209	45.115.187.209

Below the table, there is a section for 'Virtual networks' with a table showing 'Rule name', 'Virtual network', 'Subnet', 'Address Range', and 'Endpoint status'. A message states 'No vnet rules for this server.' The 'Outbound networking' section is partially visible at the bottom.

Access Control (IAM)

The screenshot shows the 'Access control (IAM)' page for a resource group named 'webapp'. The page includes a search bar and a list of actions: 'Add', 'Download role assignments', 'Edit columns', 'Refresh', 'Remove', and 'Got feedback?'. The 'Check access' tab is selected, showing options to 'View my access', 'Check access', and 'Grant access to this resource'. The 'Grant access to this resource' section includes a button to 'Add role assignment' and a 'Learn more' link. The 'View access to this resource' section includes a 'View' button and a 'Learn more' link. The 'View deny assignments' section includes a 'View' button and a 'Learn more' link.

76_Adnan Shaikh

1. Getting started — Deploying — X Add role assignment - Microsoft Azure Computer_TE_Syllabus_R2019.1 X +

https://portal.azure.com/#@adnanali1331@hotmail.onmicrosoft.com/resource/subscriptions/8cb997fb-3dec-4107-a690-e8159e8a5d22/resourceGroups/webapp/users

Microsoft Azure Search resources, services, and docs (G+)

adnanali1331@hotmail.com DEFAULT DIRECTORY

Home > webapp >

Add role assignment

Got feedback?

Role **Members** Review + assign

Selected role Contributor

Assign access to ☒ User, group, or service principal ☐ Managed identity

Members + Select members

Name	Object ID	Type
No members selected		

Description Optional

Review + assign Previous Next

Select members

Select safwanali78642@hotmail.com

This user will be sent an email that enables them to collaborate with Default Directory.

safwanali78642@hotmail.com (Guest)

Selected members: No members selected. Search for and add one or more members you want to assign to the role for this resource.

Learn more about RBAC

Select Close

1. Getting started — Deploying — X Add role assignment - Microsoft Azure Computer_TE_Syllabus_R2019.1 X +

https://portal.azure.com/#@adnanali1331@hotmail.onmicrosoft.com/resource/subscriptions/8cb997fb-3dec-4107-a690-e8159e8a5d22/resourceGroups/webapp/users

Microsoft Azure Search resources, services, and docs (G+)

adnanali1331@hotmail.com DEFAULT DIRECTORY

Home > webapp >

Add role assignment

Got feedback?

Role **Members** **Review + assign**

Role Contributor

Scope /subscriptions/8cb997fb-3dec-4107-a690-e8159e8a5d22/resourceGroups/webapp

Members

Name	Object ID	Type
safwanali78642@hotmail.com		User

Description No description

Review + assign Previous

Invited user

safwanali78642@hotmail.com was added to the Default Directory directory as a guest.
safwanali78642@hotmail.com was also sent an invitation link they must accept.
To manually invite:

1. Right-click and copy this [invitation link](#). (Do not click the link because it starts the invitation process.)
2. Send the invitation link to the invited user.

Home > webapp

webapp | Access control (IAM)

Search (Ctrl+/) « + Add Download role assignments Edit columns Refresh Remove Got feedback?

Overview Activity log Access control (IAM) Tags Resource visualizer Events

Settings Deployments Security Policies Properties Locks Cost Management Cost analysis Cost alerts (preview) Budgets

Check access **Role assignments** Roles Deny assignments Classic administrators

Number of role assignments for this subscription 1 2000

Search by name or email Type: All Role: All Scope: All scopes Group by: Role

1 items (1 Users)

Name	Type	Role	Scope	Condition
Contributor				
<input type="checkbox"/> safwanali78642 (Guest) safwanali78642@hotmail.com	User	Contributor	This resource	None

DDOS

Creating DDOS plan:

DDoS protection plans - Microsoft

What is Azure Active Directory | WhatsApp

https://portal.azure.com/#blade/HubsExtension/BrowseResource/resourceType/Microsoft.Network%2FddosProtectionPlans

Microsoft Azure Search resources, services, and docs (G+)

Home >

DDoS protection plans

Default Directory

+ Create Manage view Refresh Export to CSV Open query Assign tags Feedback

Filter for any field... Subscription == all Resource group == all Location == all Add filter

No grouping List view

Name ↑↓ Type ↑↓ Resource group ↑↓ Location ↑↓ Subscription ↑↓

No DDoS protection plans to display

DDoS Protection leverages the scale and elasticity of Microsoft's global network to bring massive DDoS mitigation capacity in every Azure region. Microsoft's DDoS Protection service protects your Azure applications by scrubbing traffic at the Azure network edge before it can impact your service's availability.

[Create DDoS protection plan](#)

[Learn more about DDoS protection plan](#)

76_Adnan Shaikh

Create a DDoS protection plan

Home > Resource groups > appsvc_linux_centralus > Create a resource > DDoS protection plan >

Create a DDoS protection plan

Basics Tags Review + create

Azure DDoS protection can help defend against DDoS (distributed denial of service) attacks directed at your resources. Your resources automatically receive a basic level of protection at no additional charge. Create a DDoS protection plan to enable DDoS standard protection for an advanced level of protection. [Learn more about DDoS protection plans](#)

Project details

Subscription * Azure for Students

Resource group * appsvc_linux_centralus

Create new

Instance details

Name * testing

Region * Central US

You can create a single DDoS protection plan and apply it to resources in all of your subscriptions.

Review + create Previous Next: Tags > Download a template for automation

Create a DDoS protection plan

Home > Resource groups > appsvc_linux_centralus > Create a resource > DDoS protection plan >

Create a DDoS protection plan

Validation passed

Basics Tags Review + create

Basics

Subscription Azure for Students

Resource group appsvc_linux_centralus

Name testing

Region Central US

Tags

None

Terms

By clicking create, you agree that you are aware of the cost and pricing structure of a DDoS protection plan and are willing to accept the charges. [Read more about DDoS protection plan pricing](#)

Create Previous Next > Download a template for automation

Deleted resource group webapp
Deleted resource group webapp

testing - Microsoft Azure

Home > Microsoft.DdosProtectionPlan-20220420185532 >

testing

DDoS protection plan

Search (Ctrl+J)

Move Delete Refresh Lock

Overview

- Activity log
- Access control (IAM)
- Tags
- Diagnose and solve problems

Settings

- Protected resources
- Properties
- Locks

Monitoring

- Alerts
- Metrics

Automation

- Tasks (preview)
- Export template

Essentials

Resource group (move) : appsvc_linux_centralus

Location : Central US

Subscription (move) : Azure for Students

Subscription ID : 8cb997fb-3dec-4107-a690-e8159e8a5d22

Tags (edit) : [Click here to add tags](#)

Configure and manage a protection plan for your organization

Make changes to your plan or link virtual networks from multiple subscriptions to the same plan. [Learn more](#)

Manage protected resources

Enable your DDoS protection plan on a virtual network to automatically mitigate DDoS attacks on your networks. [Learn more](#)

[Add protected resource](#)

Telemetry and reporting

View real-time DDoS mitigation metrics via Azure Monitor when the resource is under attack or review post-attack mitigation reports.

[View metrics](#)

Configure alerts & export diagnostic logs

DDoS protection planning

Preparation is crucial for minimizing an actual DDoS attack. View best practices and reference architectures to set up your protection plan.

[View best practices](#)

Creating Network with DDOS plan:

The screenshot shows the 'Create virtual network' page in the Azure portal, specifically the 'Basics' tab. The page is titled 'Create virtual network' and includes a breadcrumb trail: Home > Virtual networks >. Below the title, there are tabs for 'Basics', 'IP Addresses', 'Security', 'Tags', and 'Review + create'. The 'Basics' tab is active, showing a description of Azure Virtual Network (VNet) and its benefits. The form fields are as follows:

- Project details:**
 - Subscription: Azure for Students
 - Resource group: appsvc_linux_centralus (with a 'Create new' link below it)
- Instance details:**
 - Name: testing
 - Region: Central US

At the bottom, there are navigation buttons: 'Review + create' (in blue), '< Previous', 'Next : IP Addresses >', and a link to 'Download a template for automation'.

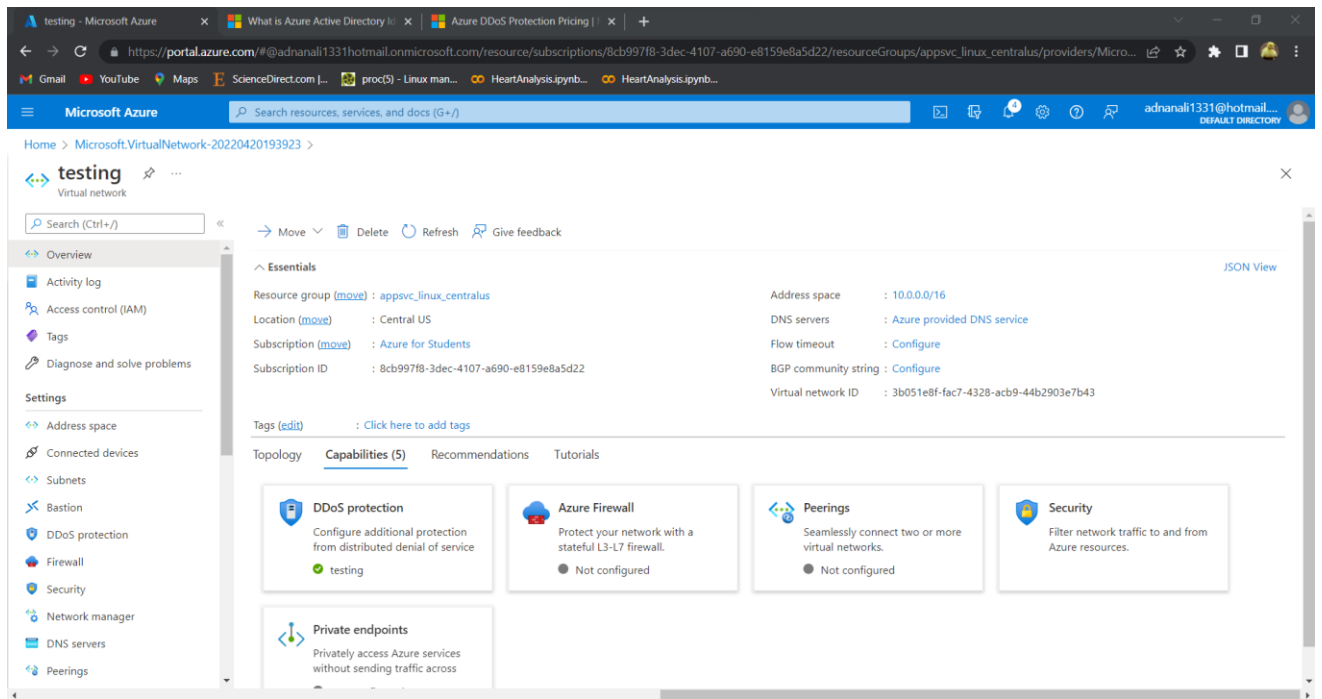
Adding DDOS plan as security:

The screenshot shows the 'Create virtual network' page in the Azure portal, specifically the 'Security' tab. The page is titled 'Create virtual network' and includes a breadcrumb trail: Home > Virtual networks >. Below the title, there are tabs for 'Basics', 'IP Addresses', 'Security', 'Tags', and 'Review + create'. The 'Security' tab is active, showing options for enabling security features. The form fields are as follows:

- BastionHost:** ☒ Disable, ☐ Enable
- DDoS Protection Standard:** ☐ Disable, ☒ Enable
- I know my resource ID:** ☐
- DDoS protection plan:** testing (selected from a dropdown menu)
- Firewall:** ☒ Disable, ☐ Enable

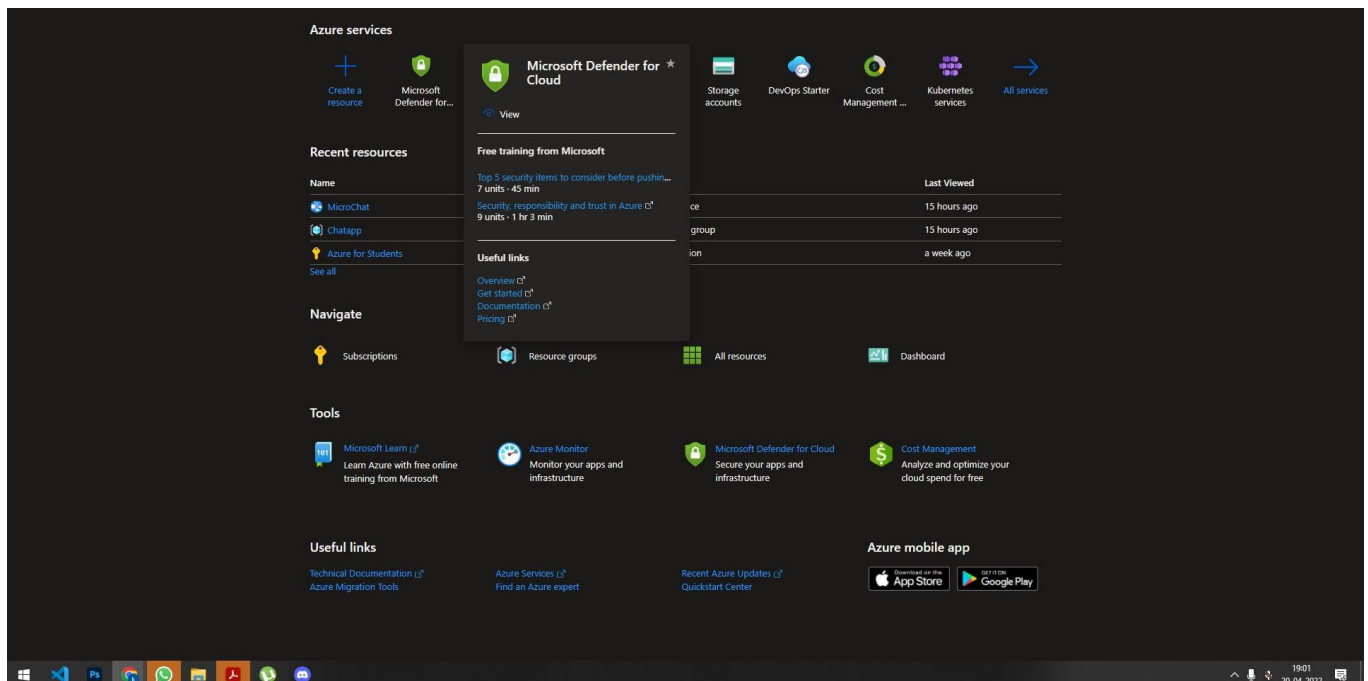
At the bottom, there are navigation buttons: 'Review + create' (in blue), '< Previous', 'Next : Tags >', and a link to 'Download a template for automation'.

Network with active DDOS plan:

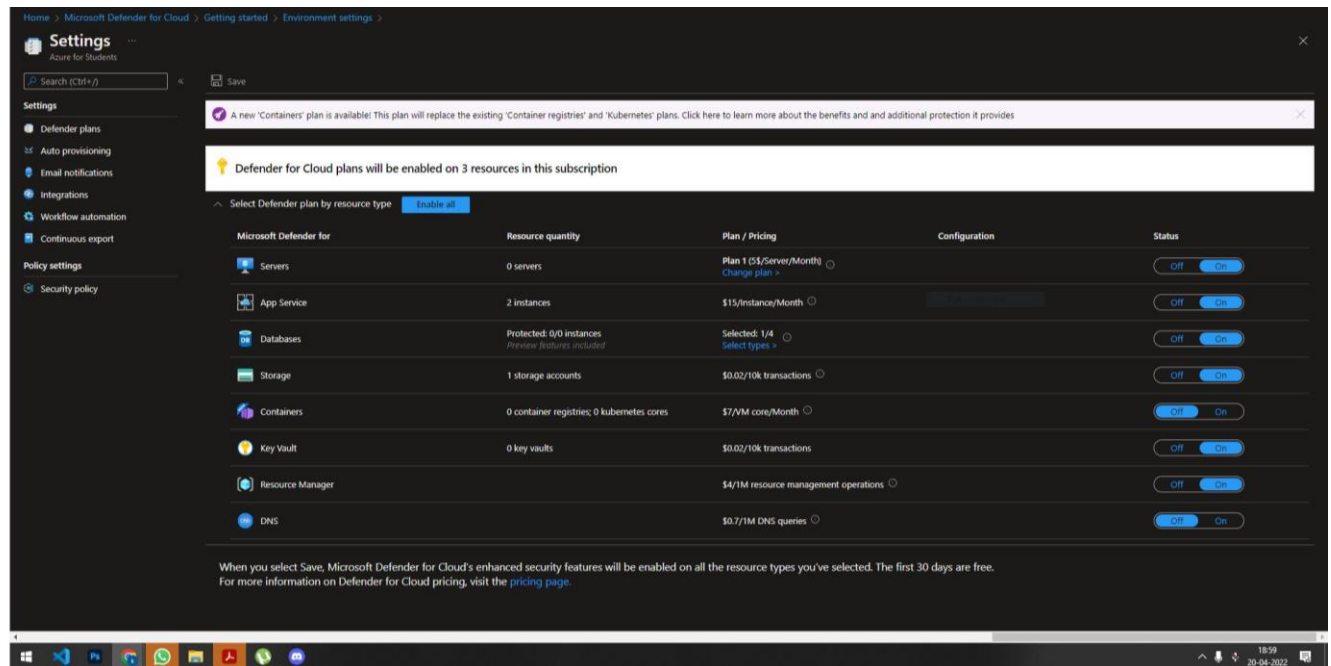


Microsoft Defender Security

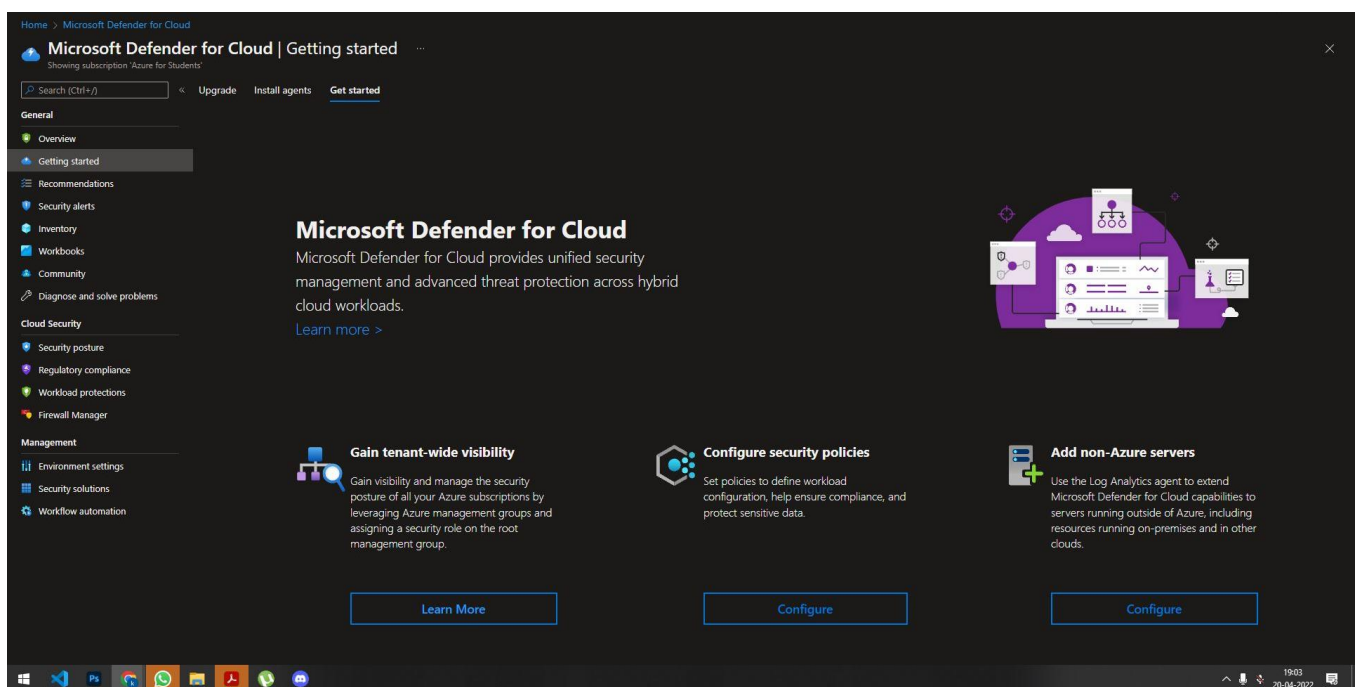
Creating Microsoft defender resource:

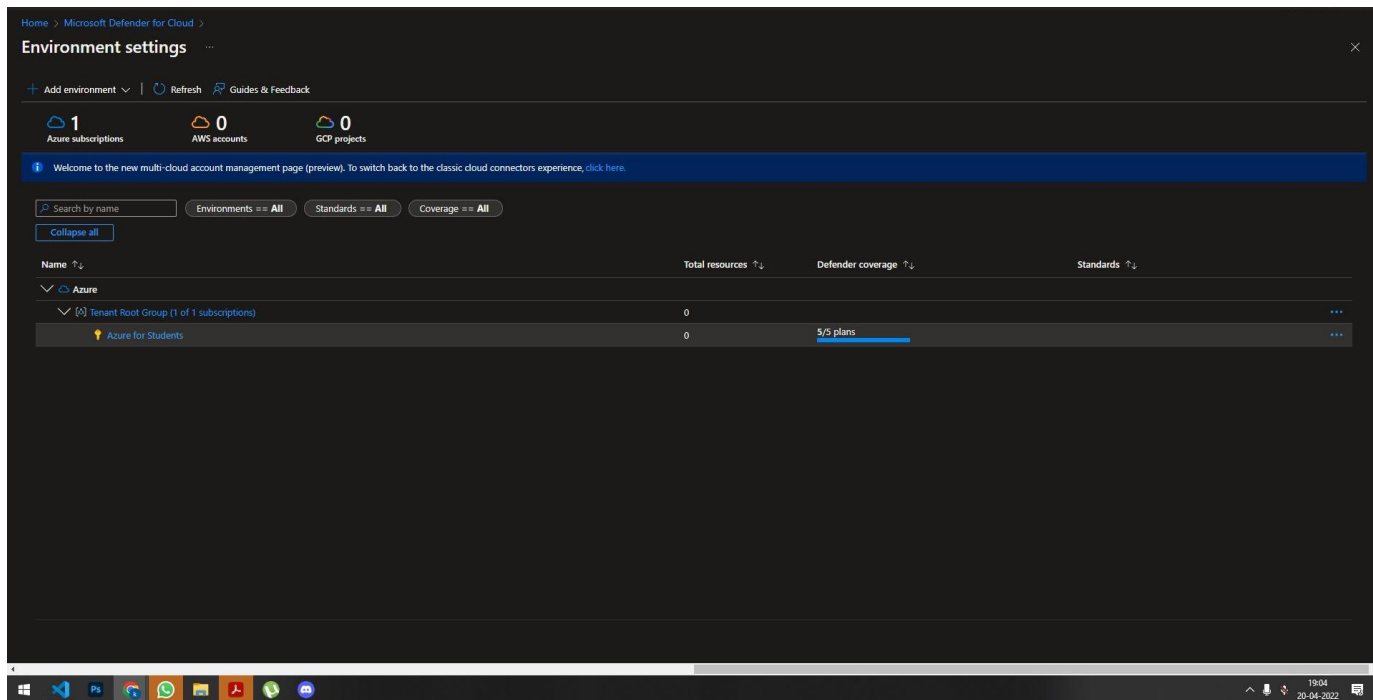


Adding resources:

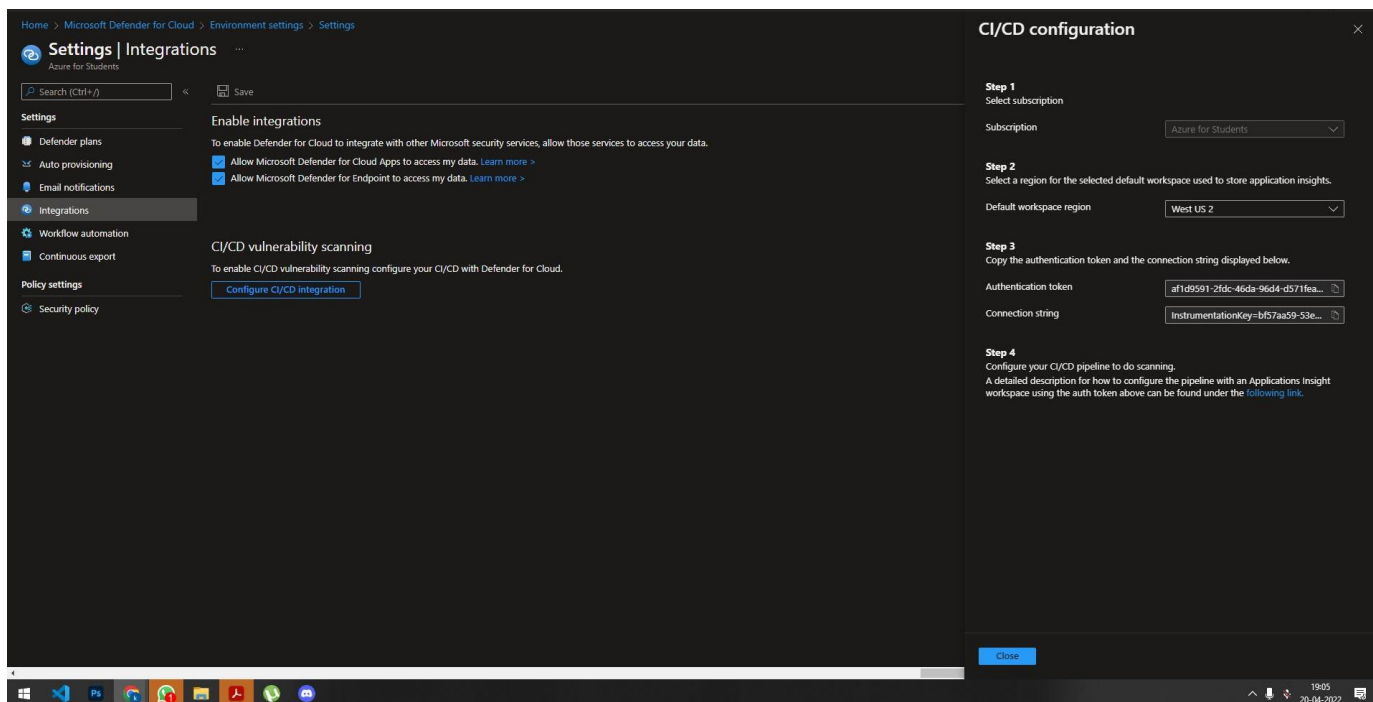


Checking active plan:

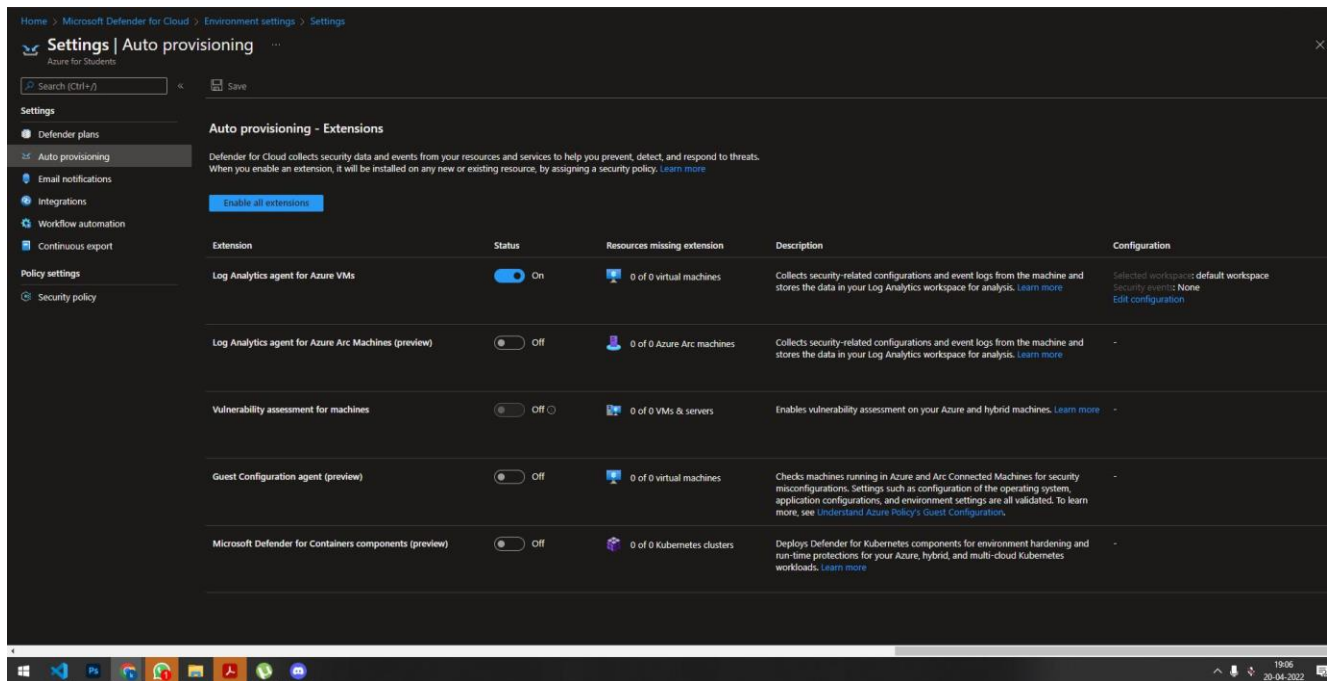




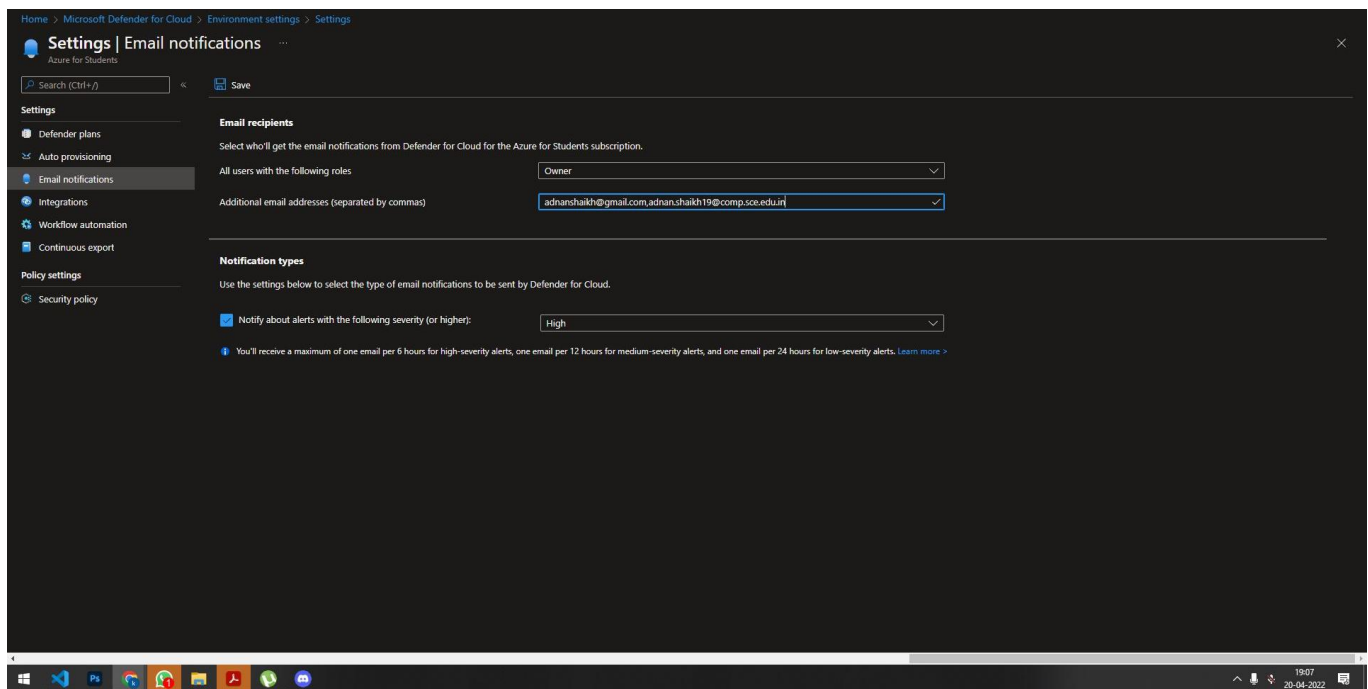
Enabling Integration:



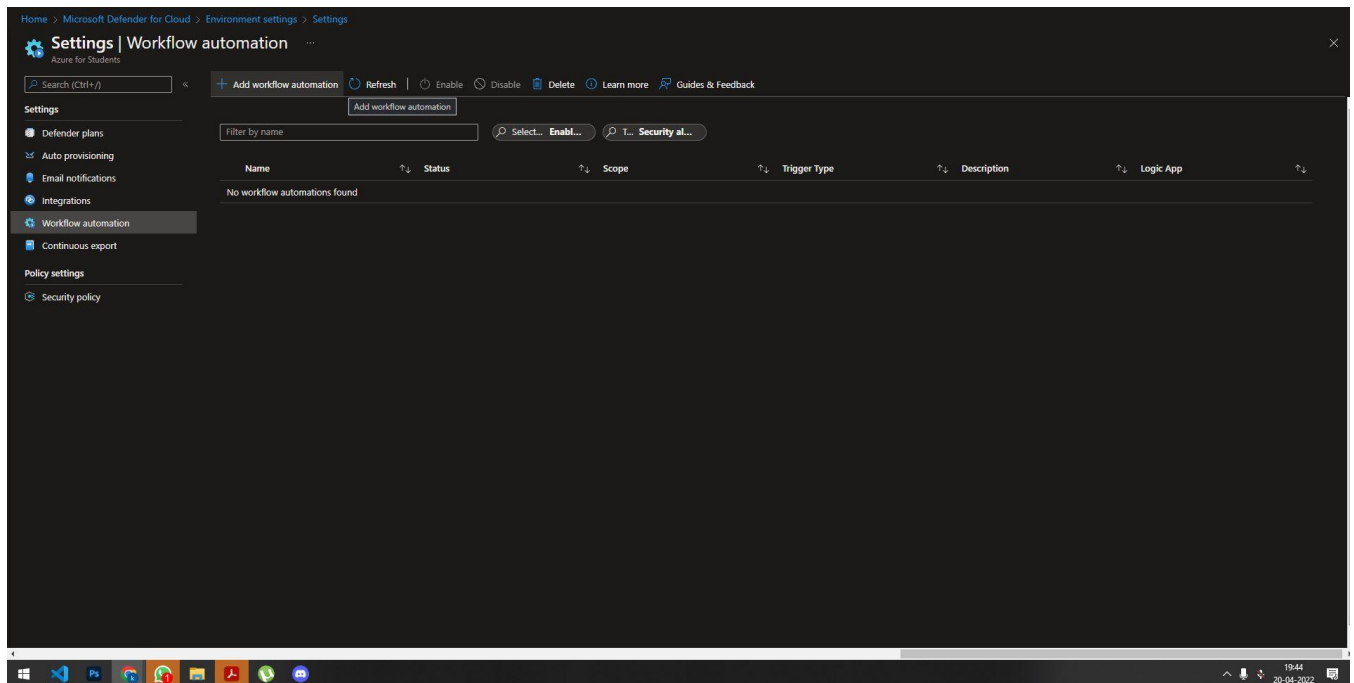
Enable Logging:



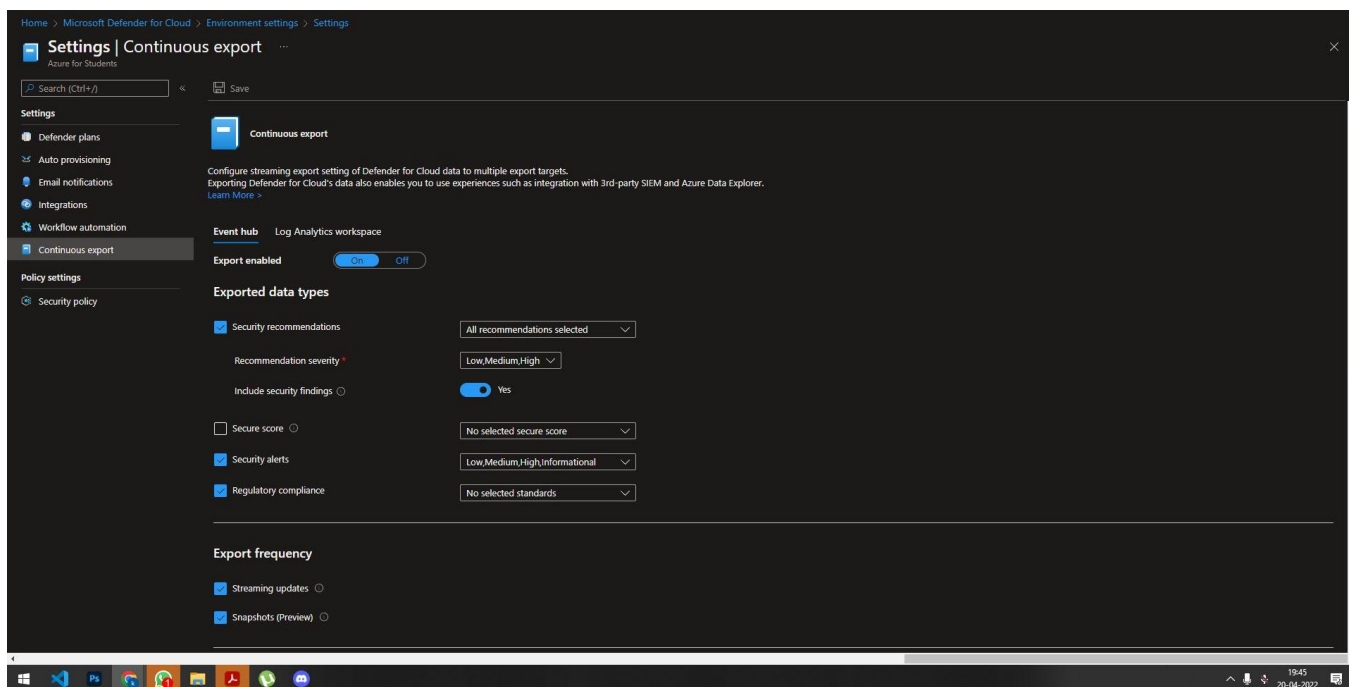
Setting Email for notification:



Work flow automation:



Continuous export:



Security Policy:

The screenshot shows the 'Settings | Security policy' page in the Microsoft Defender for Cloud console. The left sidebar contains navigation options: Settings, Defender plans, Auto provisioning, Email notifications, Integrations, Workflow automation, Continuous export, Policy settings, and Security policy (selected). The main content area is titled 'Security policy on: Azure for Students' and shows 'initiatives enabled on this subscription'. It lists two initiatives: 'Default initiative' and 'Industry & regulatory standards'. The 'Default initiative' section includes a table with columns: Assignment, Assigned On, Audit policies, Deny policies, Disabled policies, and Exempted policies. The 'Industry & regulatory standards' section lists four standards: Azure Security Benchmark, PCI DSS 3.2.1, ISO 27001, and SOC TSP, each with a description and a status button (Disable, Enable, or Deprecated).

Home > Microsoft Defender for Cloud > Environment settings > Settings

Settings | Security policy

Search (Ctrl+/)

Settings

- Defender plans
- Auto provisioning
- Email notifications
- Integrations
- Workflow automation
- Continuous export
- Policy settings
- Security policy

Security policy on: Azure for Students

initiatives enabled on this subscription

Default initiative

The default initiative enabled on your subscription generates the security recommendations in the **Recommendations** page.

Assignment	Assigned On	Audit policies	Deny policies	Disabled policies	Exempted policies
ASC Default (subscription: af1d9591-28dc-46da-96d...	Subscription	191	0	15	0

Industry & regulatory standards

Compliance initiatives shown in the **Regulatory compliance dashboard**.

Standard	Description	Status	Action
Azure Security Benchmark	Track Azure Security Benchmark controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	<button>Disable</button>
PCI DSS 3.2.1	Track PCI-DSS v3.2.1:2018 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	<button>Enable</button>
ISO 27001	Track ISO 27001:2013 controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	<button>Deprecated</button>
SOC TSP	Track SOC TSP controls in the Compliance Dashboard, based on a recommended set of policies and assessments.	Out of the box	<button>Enable</button>

Add more standards

Your custom initiatives

Conclusion: We have successfully implemented Security as a service on Azure