null – The Open Security Community

Common Cloud Security Issues

Azure Edition

Table of Contents

About null

null - The open security community is one of the most active and vibrant communities of cybersecurity professionals. Started with the simple idea of providing a knowledge-sharing platform to cybersecurity professionals, null has grown many folds. Currently, null has 20+ active chapters and organizes many security events for aspiring cybersecurity professionals. null is about spreading information security awareness. All our activities such as null Monthly Meets, null Humla, null Bachaav, null Puliya, null Job Portal are for the cause of that.

null is now focusing on contributing to enterprise security, by working on many projects to collaborate with the enterprise, such as:

- Defining security frameworks and standards for producing security guidelines in the upcoming IT technology like Cloud, Blockchain/Cryptography, IoT, AI/ML, and many more.
- Develop tools and methodologies in order to secure the products and infrastructure based on the above-mentioned technologies.
- Start many new security projects and publish research papers.

This white paper is a small effort to make a contribution in achieving the above mentioned objectives.

Acknowledgment

On behalf of null - The open security community, we would like to thank the authors of this white paper, who have contributed their precious time and effort to publish this paper.

Authors:

- Raghav Rao : https://www.linkedin.com/in/raghav-rao/
- Sagar Yadwad : https://www.linkedin.com/in/sagar-yadwad-cissp-79711123/
- Mayank Arora : https://www.linkedin.com/in/connect2mayank/
- Deep Shankar Yadav : https://www.linkedin.com/in/deepshankaryadav/
- Vitthal Shinde : https://www.linkedin.com/in/vitthal-shinde-7447699a/

Project Coordinator:

- Murtuja Bharmal : https://www.linkedin.com/in/murtujabharmal/

Abstract

Cloud technologies empower organizations to build and run scalable applications in modern, dynamic environments such as cloud services, containers, cloud functions (serverless), service meshes, microservices, immutable infrastructure, and declarative APIs to exemplify this approach. Cloud-native application is a fundamentally new and exciting approach to designing and building software. However, it also raises an entirely new set of security challenges. For example, when you move to a microservice model, end-to-end visibility, monitoring, and detection becomes more complex and challenging to execute, and security operations and management become hectic.

This white paper aims to create awareness and act as a reference document that highlights the most common Azure security issues.

Overview

The Azure cloud provides a shared responsibility model. Azure manages cloud security for its own infrastructure, while your organization is responsible for securing your own data and workloads. Microsoft provides a range of security services and features, including encryption, key management, and identity and access management (IAM), to help you implement your organization's security policies.

Another important aspect of security is compliance standards and regulations, since a misstep here can be costly for your organization. Microsoft's infrastructure is certified for almost every compliance standard in the world. However, this doesn't mean that the workloads you deploy on Azure will be compliant as well. You must be mindful of your compliance obligations, and use the tools provided by Azure to enforce the required security and privacy controls.

With the help of this whitepaper we have tried to cover most common security issues that may occur in an Azure environment.

List of Issues

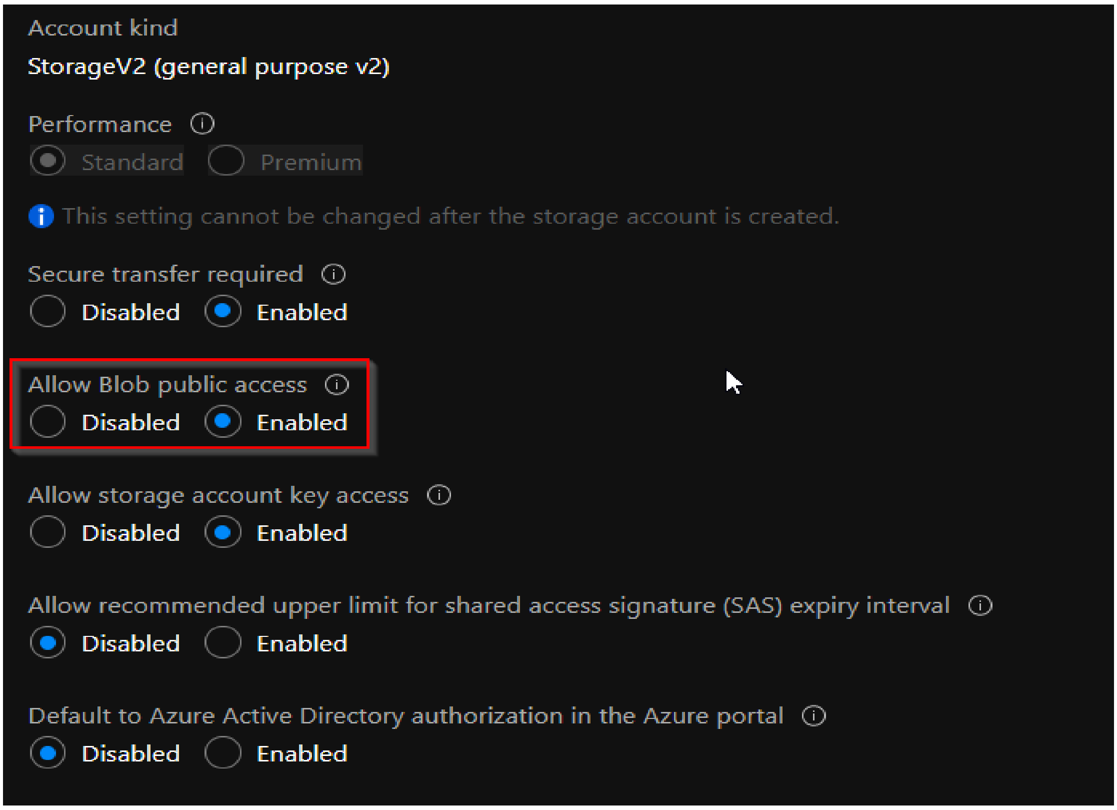
1. Storage accounts accessible from the Internet

Azure blob storage is Microsoft's persistent cloud data storage. A blob can be any type of text or binary data, such as a document, media file, or application installer. By default, a container and any blob within it may be accessed only by the owner of the storage account. If you want to give anonymous users read permissions to a container and its blobs, you can set the container permissions to allow public access. Anonymous users can read blobs within a publicly accessible container without authenticating the request.

Attacker's View:

- Blob Storage is of the format ***<storage-account>.blob.core.windows.net***
- So attackers can hunt for publicly accessible tools like blob-hunter and dumpster diver mentioned in the tools section.

Attack Scenario:



Account kind
StorageV2 (general purpose v2)

Performance ⓘ
● Standard ○ Premium

ⓘ This setting cannot be changed after the storage account is created.

Secure transfer required ⓘ
○ Disabled ● Enabled

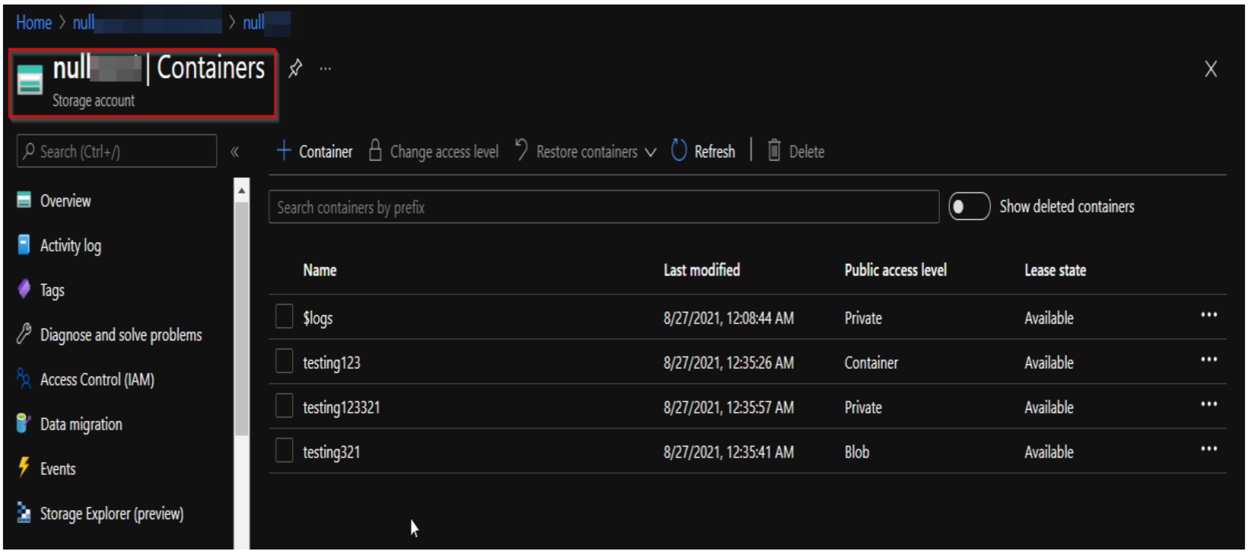
Allow Blob public access ⓘ
○ Disabled ● Enabled

Allow storage account key access ⓘ
○ Disabled ● Enabled

Allow recommended upper limit for shared access signature (SAS) expiry interval ⓘ
● Disabled ○ Enabled

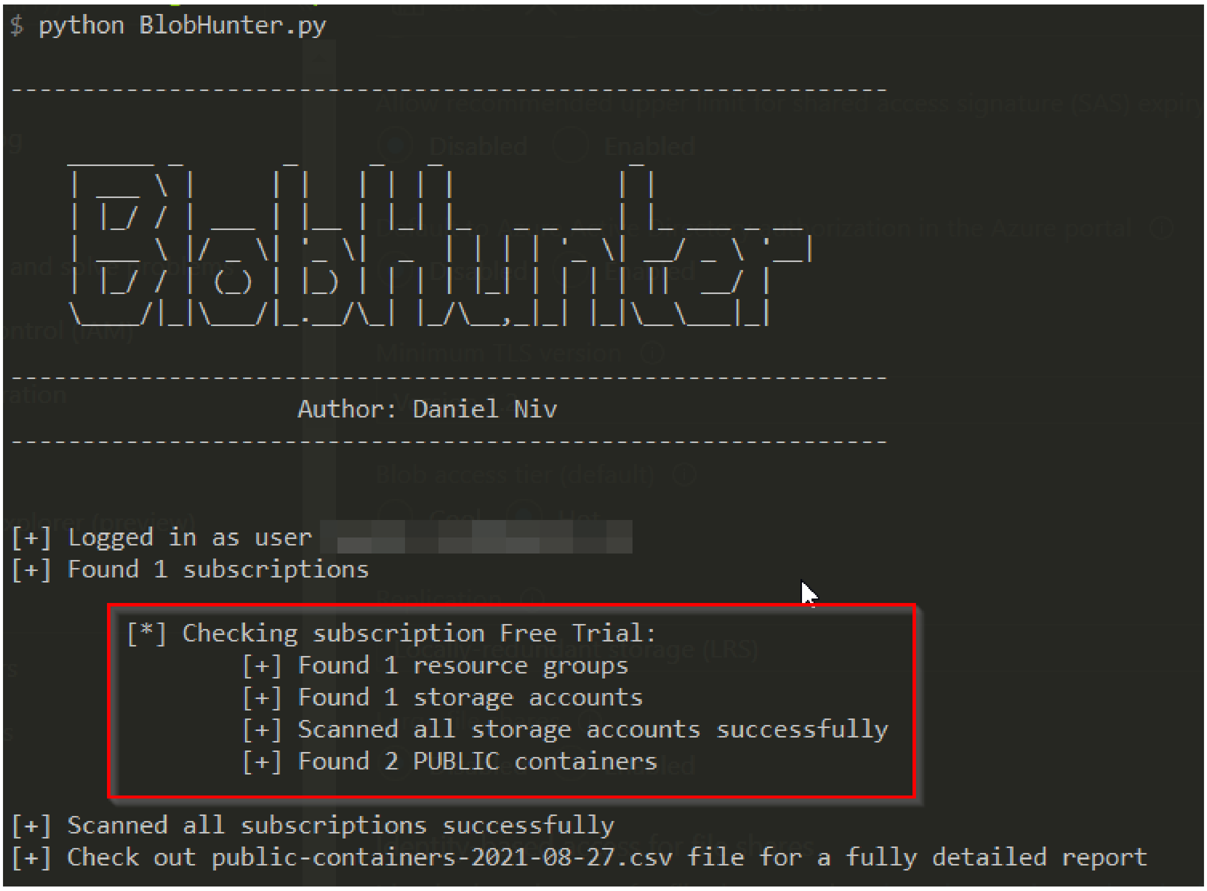
Default to Azure Active Directory authorization in the Azure portal ⓘ
● Disabled ○ Enabled

Figure 1 Blob container public access enabled



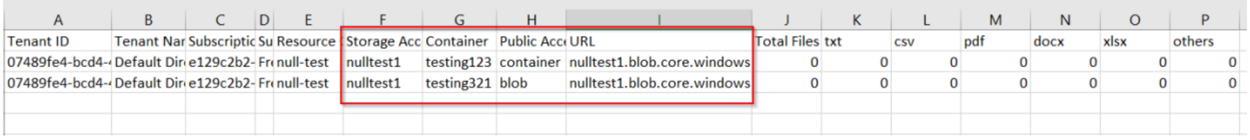
	Name	Last modified	Public access level	Lease state	
□	$logs	8/27/2021, 12:08:44 AM	Private	Available	···
□	testing123	8/27/2021, 12:35:26 AM	Container	Available	···
□	testing123321	8/27/2021, 12:35:57 AM	Private	Available	···
□	testing321	8/27/2021, 12:35:41 AM	Blob	Available	···

Figure 2 Public access level configured for containers



```
$ python BlobHunter.py

--------------------------------------------------------------
 ______ _       _     _   _             _
 | ___ \ |     | |   | | | |           | |
 | |_/ / | ___ | |__ | |_| |_   _ _ __ | |_ ___ _ __
 | ___ \ |/ _ \| '_ \|  _  | | | | '_ \| __/ _ \ '__|
 | |_/ / | (_) | |_) | | | | |_| | | | | ||  __/ |
 \____/|_|\___/|_.__/\_| |_/\__,_|_| |_|\__\___|_|

--------------------------------------------------------------
                    Author: Daniel Niv
--------------------------------------------------------------


[+] Logged in as user [redacted]
[+] Found 1 subscriptions

        [*] Checking subscription Free Trial:
                [+] Found 1 resource groups
                [+] Found 1 storage accounts
                [+] Scanned all storage accounts successfully
                [+] Found 2 PUBLIC containers

[+] Scanned all subscriptions successfully
[+] Check out public-containers-2021-08-27.csv file for a fully detailed report
```

Figure 3 Using blob hunter tool to find public containers



A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
Tenant ID	Tenant Nar	Subscriptic	Su	Resource	Storage Acc	Container	Public Acc	URL	Total Files	txt	csv	pdf	docx	xlsx	others
07489fe4-bcd4-4	Default Dir	e129c2b2-	Fr	null-test	nulltest1	testing123	container	nulltest1.blob.core.windows	0	0	0	0	0	0	0
07489fe4-bcd4-4	Default Dir	e129c2b2-	Fr	null-test	nulltest1	testing321	blob	nulltest1.blob.core.windows	0	0	0	0	0	0	0

Figure 4 Blob hunter tool results

Defender's View:

- Enable the Security centre to detect all the storage accounts which are publicly accessible.
- Enable Azure defender for all your storage accounts
- Store business-critical data in immutable blobs
- Use storage access policies in a secured way
- Use of private end points to restrict access to specific subnets rather than keeping it public
- Use of storage access signatures pertaining to time limits and also giving RBAC (role based access) to specific user accounts only to operate storages like File storage/Blob storage especially when the storages contain sensitive information.
- Use of storage firewalls (Resource Firewalls) to restrict access to specific subnets.

Tools:

- https://github.com/cyberark/blobhunter
- https://github.com/securing/DumpsterDiver

Reference:

- https://docs.microsoft.com/en-us/azure/storage/blobs/security-recommendations
- https://www.cyberark.com/resources/threat-research-blog/hunting-azure-blobs-exposes-millions-of-sensitive-files

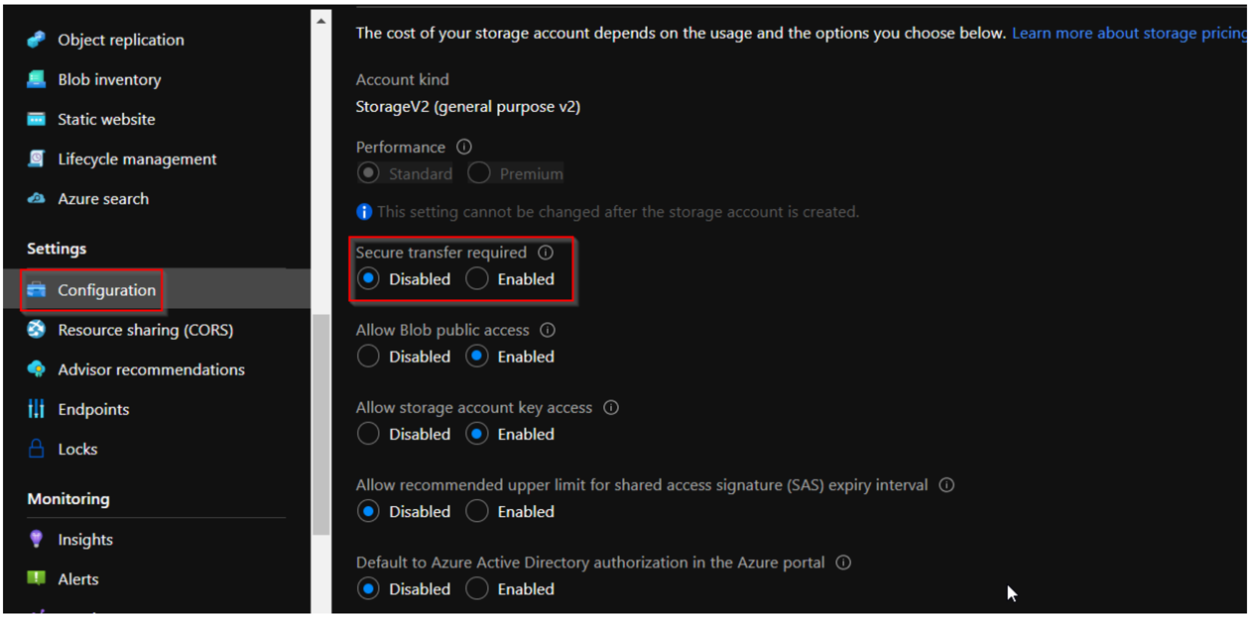
2. Storage account with insecure transfer allowed

The secure transfer option enhances the security of your storage account by only allowing requests to the storage account by a secure connection. For example, when calling REST APIs to access your storage accounts, you must connect using HTTPS. Any requests using HTTP will be rejected when 'secure transfer required' is enabled. When you are using the Azure files service, connection without encryption will fail, including scenarios using SMB 2.1, SMB 3.0 without encryption, and some flavours of the Linux SMB client. Because Azure storage doesn't support HTTPS for custom domain names, this option is not applied when using a custom domain name.

Defender's View

- Recommended solution to enable secure transfer for Azure Storage Accounts.
- Ensure that secure transfer is enabled for Azure Storage Accounts. Please make sure the template has "enable_https_traffic_only" set as "true".

Command " ***az storage account update --ids ${resourceId} --https-only true***"



The cost of your storage account depends on the usage and the options you choose below. Learn more about storage pricing

Account kind
StorageV2 (general purpose v2)

Performance ⓘ
● Standard ○ Premium

ⓘ This setting cannot be changed after the storage account is created.

Secure transfer required ⓘ
● Disabled ○ Enabled

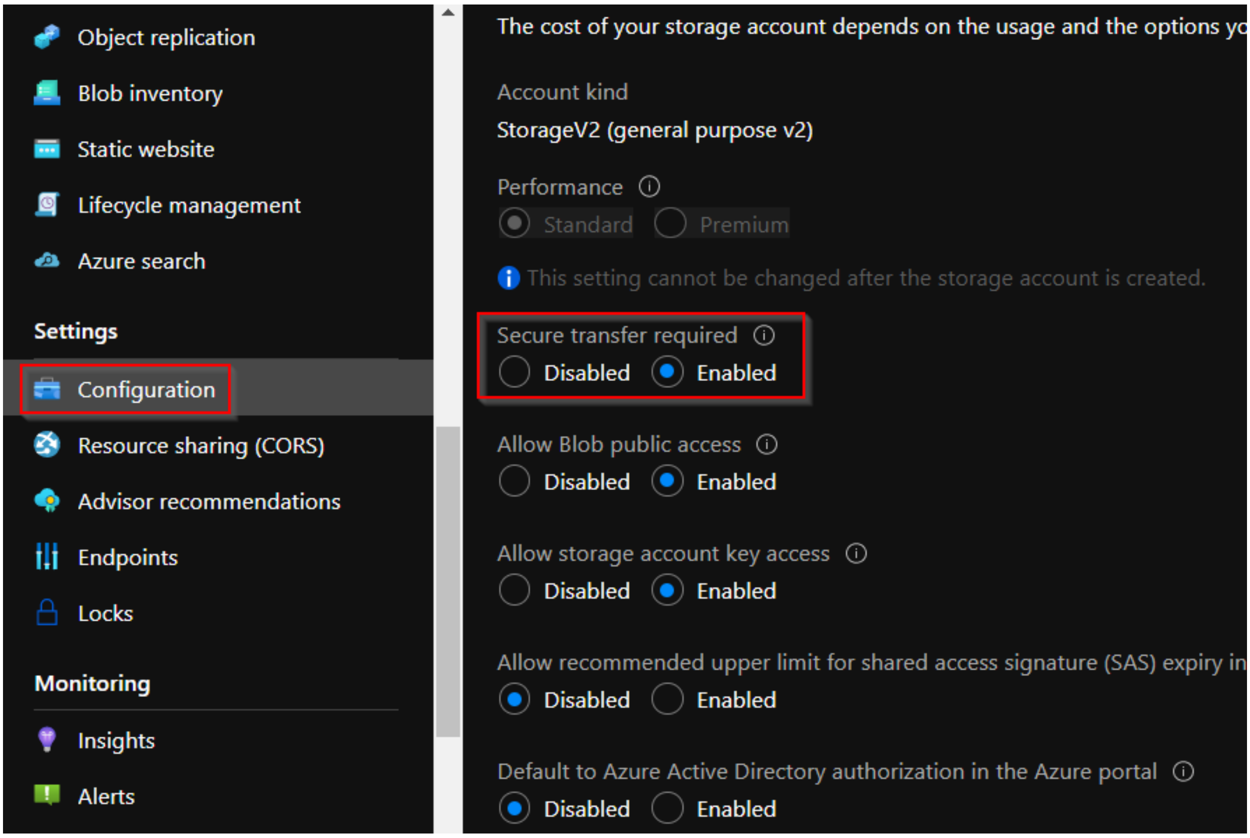
Allow Blob public access ⓘ
○ Disabled ● Enabled

Allow storage account key access ⓘ
○ Disabled ● Enabled

Allow recommended upper limit for shared access signature (SAS) expiry interval ⓘ
● Disabled ○ Enabled

Default to Azure Active Directory authorization in the Azure portal ⓘ
● Disabled ○ Enabled

Figure 5 Secure Transfer Disabled



The cost of your storage account depends on the usage and the options yo

Account kind

StorageV2 (general purpose v2)

Performance ⓘ

● Standard ○ Premium

ⓘ This setting cannot be changed after the storage account is created.

Secure transfer required ⓘ

○ Disabled ● Enabled

Allow Blob public access ⓘ

○ Disabled ● Enabled

Allow storage account key access ⓘ

○ Disabled ● Enabled

Allow recommended upper limit for shared access signature (SAS) expiry in

● Disabled ○ Enabled

Default to Azure Active Directory authorization in the Azure portal ⓘ

● Disabled ○ Enabled

Figure 6 Secure Transfer Enabled

Reference:

- https://www.cloudconformity.com/knowledge-base/azure/StorageAccounts/secure-transfer-required.html
- https://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-policy-reference/configuration-policies/configuration-policies-build-phase/microsoft-azure-configuration-policies/policy_bc4e467f-10fa-471e-aa9b-28981dc73e93.htmlhttps://docs.paloaltonetworks.com/prisma/prisma-cloud/prisma-cloud-policy-reference/configuration-policies/configuration-policies-build-phase/microsoft-azure-configuration-policies/policy_bc4e467f-10fa-471e-aa9b-28981dc73e93.html

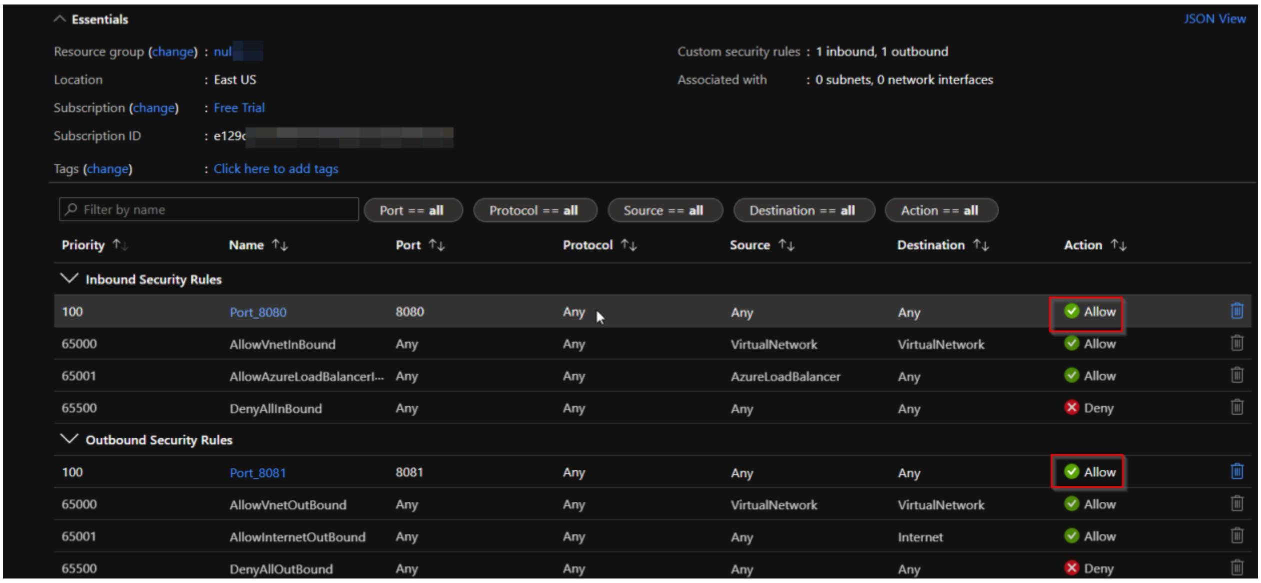
3. Azure NSG inbound rules configured with ANY

Common misconfiguration when defining firewall rules in the NSG (Network Security Groups) is to use the protocol “ANY”, source “ANY” or the destination “ANY”.

Such practice can lead to a risk of allowing more traffic in than what is intended. For attackers, these little seemingly benign details oftentimes play an important role in allowing them to breach the premises.

Attacker's View:

Attackers can take RDP/ Remote access to the application using brute force attack where proper conditional access policies are not applied, or using tools like Hydra can guess the password of the user and can get the cloud access.



Resource group (change) : nul[redacted]
Location : East US
Subscription (change) : Free Trial
Subscription ID : e129c[redacted]
Tags (change) : Click here to add tags

Custom security rules : 1 inbound, 1 outbound
Associated with : 0 subnets, 0 network interfaces

Priority ↑↓	Name ↑↓	Port ↑↓	Protocol ↑↓	Source ↑↓	Destination ↑↓	Action ↑↓
Inbound Security Rules						
100	Port_8080	8080	Any	Any	Any	✓ Allow
65000	AllowVnetInBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowAzureLoadBalancerI...	Any	Any	AzureLoadBalancer	Any	✓ Allow
65500	DenyAllInBound	Any	Any	Any	Any	✗ Deny
Outbound Security Rules						
100	Port_8081	8081	Any	Any	Any	✓ Allow
65000	AllowVnetOutBound	Any	Any	VirtualNetwork	VirtualNetwork	✓ Allow
65001	AllowInternetOutBound	Any	Any	Any	Internet	✓ Allow
65500	DenyAllOutBound	Any	Any	Any	Any	✗ Deny

Figure 7 NSG any-to-any rule allow

Defender's View:

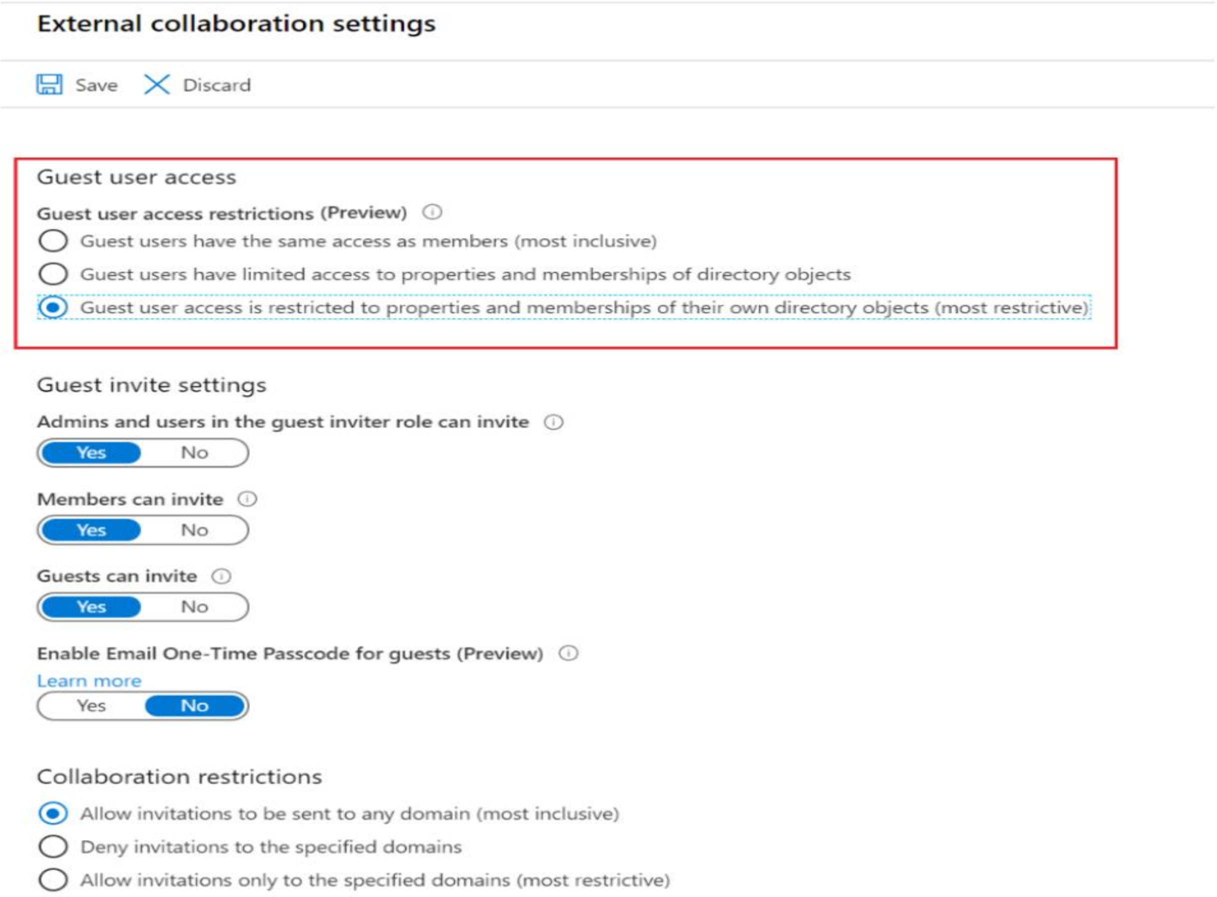
- Login to azure portal and navigate to Network security group and audit if there are "ANY-ANY" rules set.
- Disable all the "Any-Any" rules and use only appropriate ports and protocols.
- Configure CSPM to alert on misconfiguration in your cloud environment.

4. Insecure guest user settings in Azure AD

Microsoft Azure has a tenant-level feature that allows all Azure Active Directory (AAD) members to create and invite guest users. The official name for this feature is Azure Active Directory B2B.control over another domain.

Attacker's View:

- Log in to the Azure Portal with the guest account, and try to access AAD.
- Through osint get email and employee names
- Figure out the principal name for each user, which is usually their corporate email address or a variation of the same with the format of <companyname>.onmicrosoft.com.
- By default, every AAD member in your tenant can create and invite guest users. This option is set under the "User Settings" section of your Azure Active Directory, under "External collaboration settings:"
- Check if you can add users with higher privileges.



External collaboration settings

Guest user access

Guest user access restrictions (Preview)

○ Guest users have the same access as members (most inclusive)
○ Guest users have limited access to properties and memberships of directory objects
● Guest user access is restricted to properties and memberships of their own directory objects (most restrictive)

Guest invite settings

Admins and users in the guest inviter role can invite: [✓ Yes] No

Members can invite: [✓ Yes] No

Guests can invite: [✓ Yes] No

Enable Email One-Time Passcode for guests (Preview)
Learn more
Yes [✓ No]

Collaboration restrictions

● Allow invitations to be sent to any domain (most inclusive)
○ Deny invitations to the specified domains
○ Allow invitations only to the specified domains (most restrictive)

Figure 8 Insecure guest settings in Azure

Defender's View:

- By default, every AAD member in your tenant can create and invite guest users. This option is set under the “User Settings” section of your Azure Active Directory, under “External collaboration settings:”
- Limit the guest user permissions.
- Disable the feature guest can invite users in ““External collaboration settings:”

5. Data leakage using over permissive role

Microsoft Azure has various types of roles that are assigned to users using RBAC. This scenario takes into consideration access abuse using over permissive roles with which a user / malicious insider can gain access to sensitive information

Attacker's View:

Let's say a user has restricted access on the storage account that contains very sensitive information. However, the user has contributor access to a Virtual machine. Virtual machines in turn are connected to a storage using storage endpoint and thus, a user which doesn't contain direct access now can access the sensitive information by accessing a Virtual machine as the user has a contributor level of access.

Defender's View:

Access Review needs to be done for all the users.

Any storage that has sensitive information, needs to be restricted to specific resources and careful role-based access controls need to be provisioned on the resources as the resources that access storage now are equally critical resources that process sensitive information.

6. Unencrypted OS and Data disks

As the cloud environment is a multitenancy environment, for the security and compliance requirements, it is always secured and considered a best practice to encrypt the OS and data disks that are attached to azure virtual machines.

Without disk encryption of OS and data disks, these are the attack scenarios that are possible:

- As the cloud is multi-tenant environment, provisioning of disks, and infrastructure happens to be on the same physical server and this server is shared amongst all other entities.
    - Because of sharing of the same physical server, there is a risk of leakage of sensitive data to other competitors who are using the same physical server.
- As the data is unencrypted, communication of data between different virtual machines goes unencrypted, so there is a risk of confidentiality of sensitive information to a malicious insider.
- Compliance requirements related to confidentiality can be achieved by encrypting the data at rest, in this case encrypting the OS and data disks attached to virtual machines.

Attacker's View:

- Malicious insider that has the access of a virtual machine can take an undue advantage of the data disks that are unencrypted and can detach disks from the virtual machines and then attach them to their own virtual machine and access sensitive information that the disk contains.
- A skilled hacker can use tools like Wireshark, TCP dump and can access the net flow logs between virtual machines, if the data is not encrypted, he can access the sensitive information

Defender's View:

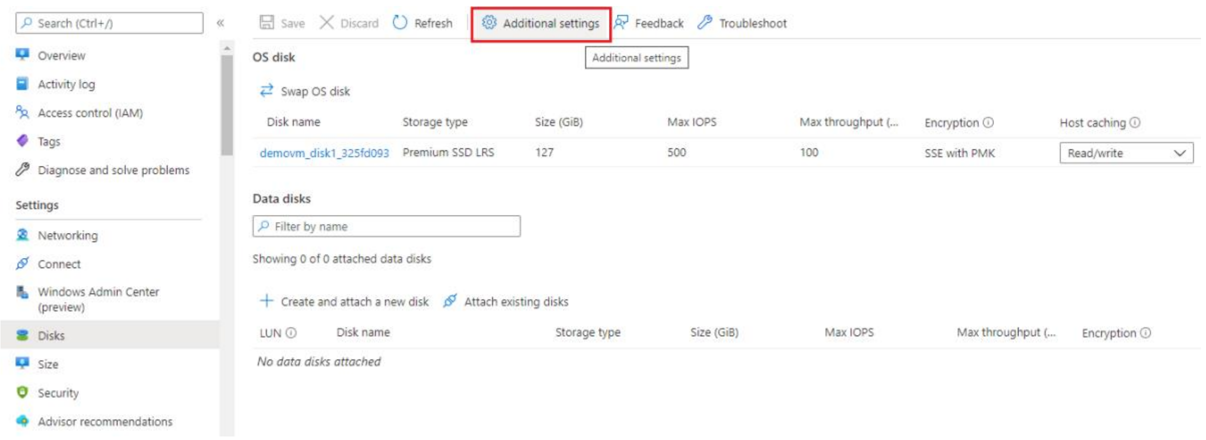
There are 2 approaches to encrypt the data at rest (encrypt OS and data disk):

1. Using Disk encryption using the Azure portal:

   Step 1: Select the Virtual machine for which disk needs to be encrypted.

   Step 2: Go to Additional settings and select the disk to be encrypted.

   Step 3: Create a key in azure key vault and select it to encrypt the data disk.



OS disk

Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (...	Encryption ⓘ	Host caching ⓘ
demovm_disk1_325fd093	Premium SSD LRS	127	500	100	SSE with PMK	Read/write

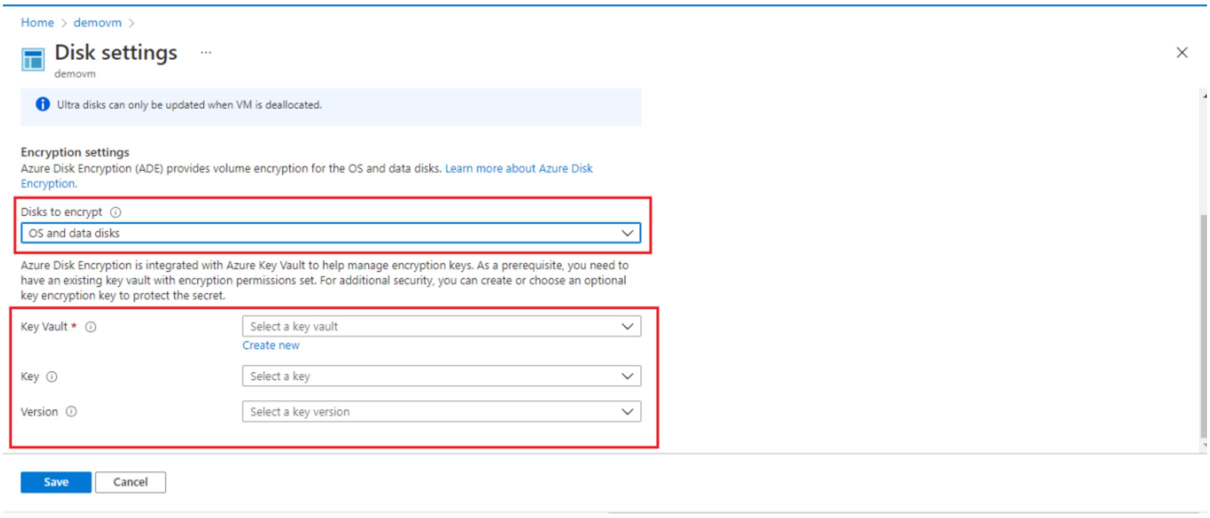
Data disks

Showing 0 of 0 attached data disks

LUN ⓘ	Disk name	Storage type	Size (GiB)	Max IOPS	Max throughput (...	Encryption ⓘ

No data disks attached

Figure 9 OS Disk settings



Disk settings

demovm

Ultra disks can only be updated when VM is deallocated.

Encryption settings

Azure Disk Encryption (ADE) provides volume encryption for the OS and data disks. Learn more about Azure Disk Encryption.

Disks to encrypt ⓘ: OS and data disks

Azure Disk Encryption is integrated with Azure Key Vault to help manage encryption keys. As a prerequisite, you need to have an existing key vault with encryption permissions set. For additional security, you can create or choose an optional key encryption key to protect the secret.

Key Vault * ⓘ: Select a key vault

Create new

Key ⓘ: Select a key

Version ⓘ: Select a key version

Figure 10 Encrypting OS and Disk

2. Using Powershell script

Use below PowerShell command to encrypt the Operating system of the virtual machine. Azure uses BitLocker to encrypt the windows OS and data disk.

Set-AzVMDiskEncryptionExtension -ResourceGroupName ResourceGroupName -VMName VMName -DiskEncryptionKeyVaultUrl $KeyVault.VaultUri -DiskEncryptionKeyVaultId $KeyVault.ResourceId

Prerequisites: This requires key vault to be created and a key needs to be present in the key vault.

Reference:

- https://docs.datadoghq.com/security_platform/default_rules/cis-azure-1.3.0-7.2/

7. Webapps don’t have authentication enabled

Web applications that don’t have authentication enabled can be accessed by anyone on the internet and can take undue advantage of fuzzing and exploiting vulnerabilities if any.

Attacker's view:

- Access the unauthenticated web application that doesn’t require any authentication.
- Get the API or information exposed by web application using any API scanning tool such as postman.
- Access the sensitive information processed by web application or modify the data using exposed api

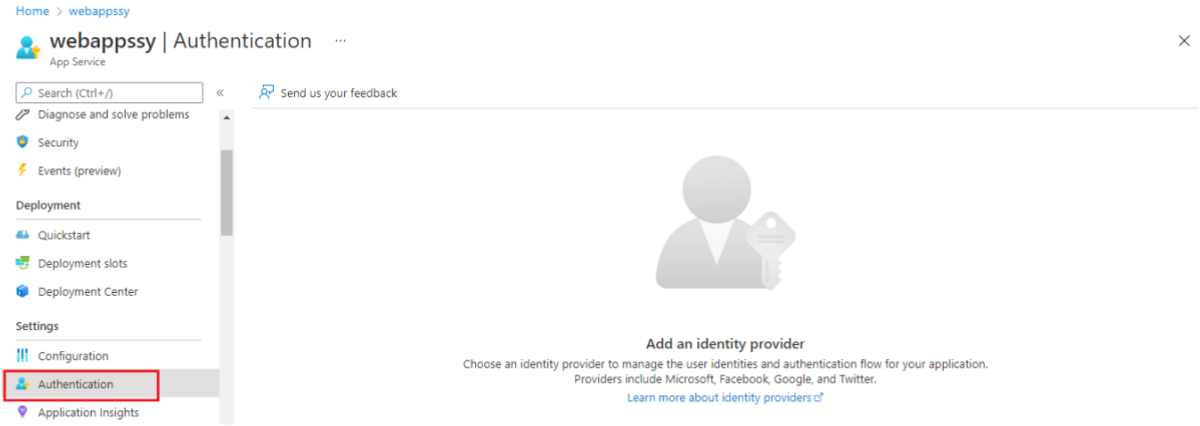
Defender's view:

Authentication needs to be enabled at the web app level. It can be done by enabling the ‘Require Authentication’ option.

Authentication can be done by providing the identity provider with a custom choice. It can be Microsoft, Google, Facebook, Twitter or any other Open ID account that is configured on the Identity Provider.

After adding the Identity provider, complete app registration, it will create an entry in the azure AD as the service principal for the corresponding application, and grants the permission to access the Web app for which authentication is enabled.

For unauthenticated requests, there needs to be a custom error page for 302 redirection or 401 unauthorized access or 403 Forbidden access that needs to be configured.

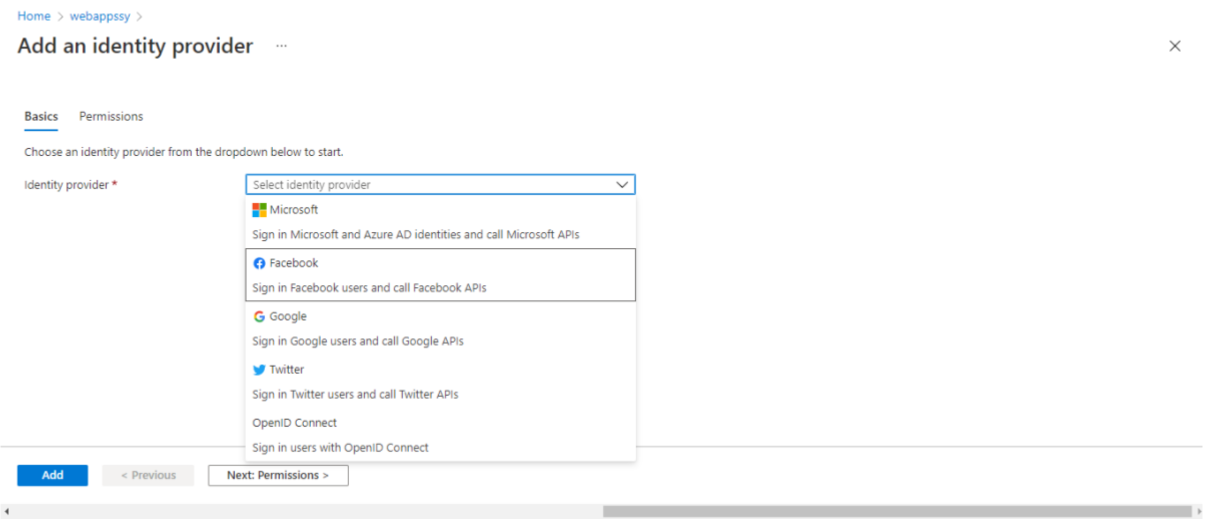


Add an identity provider

Choose an identity provider to manage the user identities and authentication flow for your application. Providers include Microsoft, Facebook, Google, and Twitter.

Learn more about identity providers

Figure 11 Authentication setting



Home > webappssy >

Add an identity provider

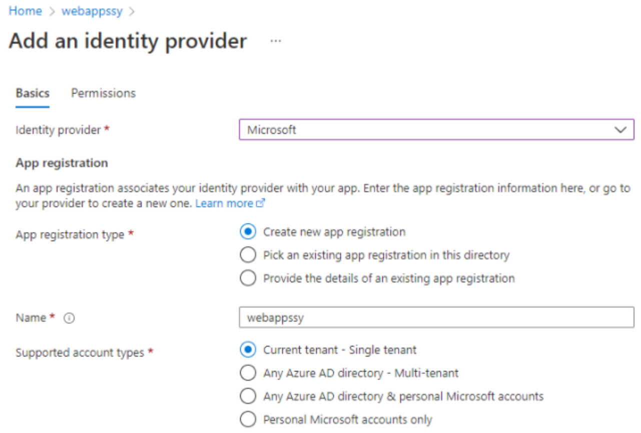
Basics | Permissions

Choose an identity provider from the dropdown below to start.

Identity provider * : Select identity provider

- Microsoft – Sign in Microsoft and Azure AD identities and call Microsoft APIs
- Facebook – Sign in Facebook users and call Facebook APIs
- Google – Sign in Google users and call Google APIs
- Twitter – Sign in Twitter users and call Twitter APIs
- OpenID Connect – Sign in users with OpenID Connect

Figure 12 Adding an identity provider for web application



Home > webappssy >

Add an identity provider

Basics | Permissions

Identity provider * : Microsoft

App registration

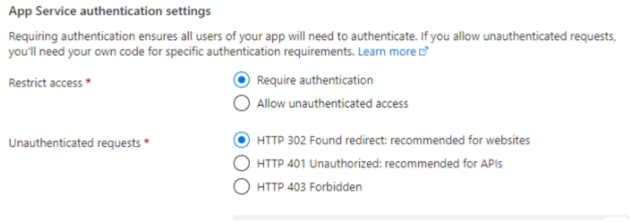
An app registration associates your identity provider with your app. Enter the app registration information here, or go to your provider to create a new one. Learn more

App registration type *
● Create new app registration
○ Pick an existing app registration in this directory
○ Provide the details of an existing app registration

Name * : webappssy

Supported account types *
● Current tenant - Single tenant
○ Any Azure AD directory - Multi-tenant
○ Any Azure AD directory & personal Microsoft accounts
○ Personal Microsoft accounts only

Figure 13 Adding Microsoft identity provider



App Service authentication settings

Requiring authentication ensures all users of your app will need to authenticate. If you allow unauthenticated requests, you'll need your own code for specific authentication requirements. Learn more

Restrict access *
● Require authentication
○ Allow unauthenticated access

Unauthenticated requests *
● HTTP 302 Found redirect: recommended for websites
○ HTTP 401 Unauthorized: recommended for APIs
○ HTTP 403 Forbidden

Figure 14 Adding re-directs to the web application

Reference:

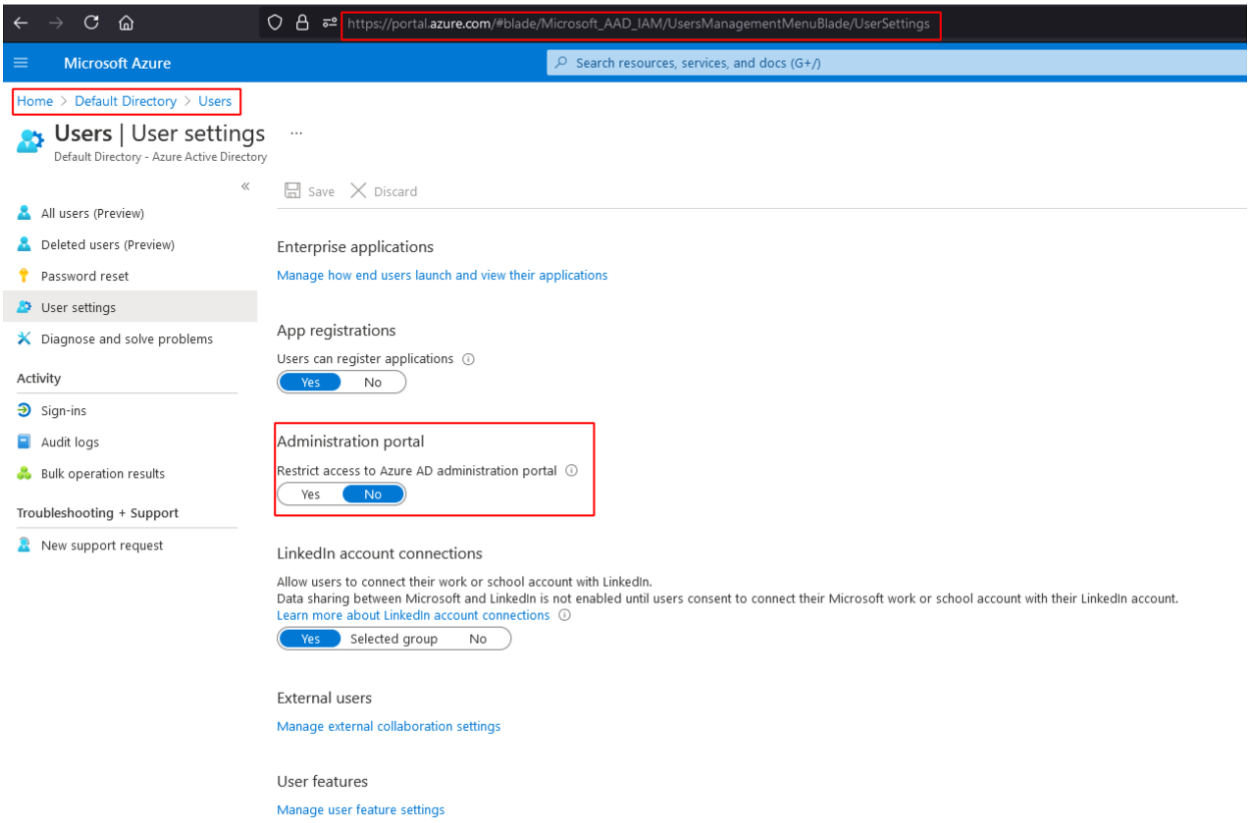
- https://docs.microsoft.com/en-us/azure/app-service/overview-authentication-authorization
- Tutorial - Add authentication to a web app on Azure App Service - Azure App Service | Microsoft Docs

8. Unrestricted access to Azure AD administration portal

The Azure Active Directory administrative portal provides access to sensitive or private information, therefore all non-admin users should be prohibited from accessing any Azure AD resource or information available on the administration portal in order to avoid data exposure. Setting this option to ‘No’ lets non-administrators use the Azure AD administration portal to read and manage Azure AD resources. ‘Yes’ restricts all non-administrators from accessing any Azure AD data in the administration portal.

Defender's view:

Change setting to "Yes" to Restrict access in Azure AD administration portal setting to disable non-administrator users' ability to access Azure Active Directory administration portal.


https://portal.azure.com/#blade/Microsoft_AAD_IAM/UsersManagementMenuBlade/UserSettings
Microsoft Azure
Search resources, services, and docs (G+/)
Home > Default Directory > Users
Users | User settings
Default Directory - Azure Active Directory
All users (Preview)
Deleted users (Preview)
Password reset
User settings
Diagnose and solve problems
Activity
Sign-ins
Audit logs
Bulk operation results
Troubleshooting + Support
New support request
Save
Discard

Enterprise applications

Manage how end users launch and view their applications

App registrations

Users can register applications: [✓ Yes] No

Administration portal

Restrict access to Azure AD administration portal: Yes [✓ No]

LinkedIn account connections

Allow users to connect their work or school account with LinkedIn.
Data sharing between Microsoft and LinkedIn is not enabled until users consent to connect their Microsoft work or school account with their LinkedIn account.
Learn more about LinkedIn account connections

[✓ Yes] Selected group No

External users

Manage external collaboration settings

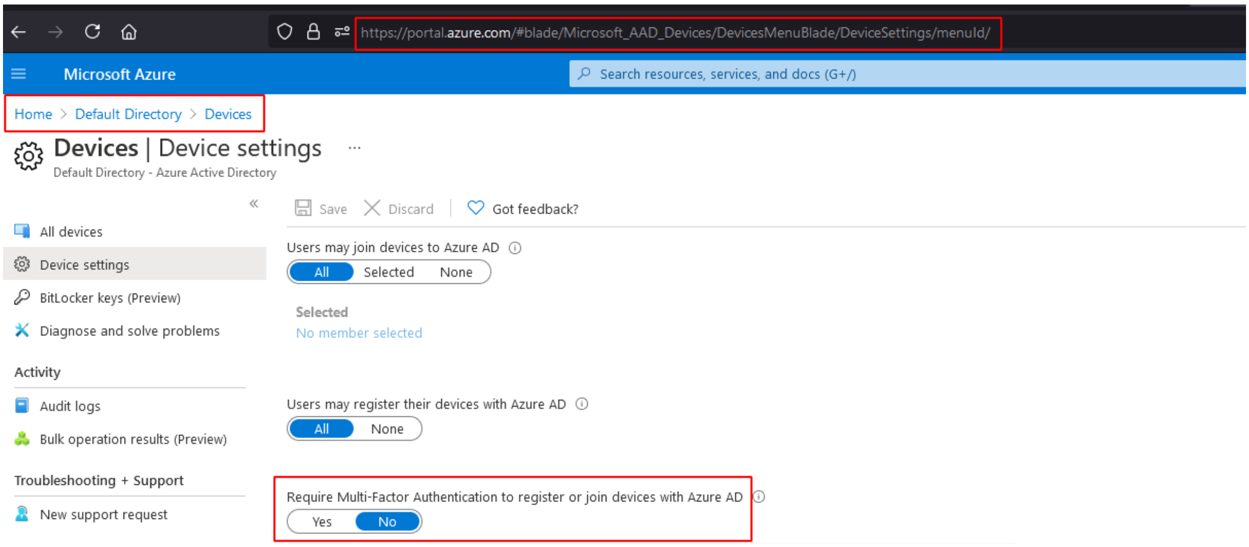
User features

Manage user feature settings

Figure 15 Restricting access to Azure AD admin portal

9. Lack of Multi-factor authentication to add devices

Multi-Factor Authentication should be mandatory when users are adding devices to the Azure Active Directory. This ensures that no rogue devices can be registered to your directory by compromised user accounts. When "Require Multi-Factor Auth to join devices" is set to "Yes", users who are adding devices from the Internet are forced to use the second method of authentication before their devices can be successfully added to your directory.



https://portal.azure.com/#blade/Microsoft_AAD_Devices/DevicesMenuBlade/DeviceSettings/menuId/

Home > Default Directory > Devices

Devices | Device settings

Default Directory - Azure Active Directory

Users may join devices to Azure AD: [✓ All] Selected None

Selected: No member selected

Users may register their devices with Azure AD: [✓ All] None

Require Multi-Factor Authentication to register or join devices with Azure AD: Yes [✓ No]

Microsoft Azure
Search resources, services, and docs (G+/)
Save
Discard
Got feedback?
All devices
Device settings
BitLocker keys (Preview)
Diagnose and solve problems
Activity
Audit logs
Bulk operation results (Preview)
Troubleshooting + Support
New support request

Figure 16 Insecure MFA join devices

Defender's view:

On Device settings page, check the Require Multi-Factor Auth to join devices feature settings. If the feature configuration is set to ‘No’, Multi-Factor Authentication (MFA) is not required when adding devices to the current Azure Active Directory, therefore the configuration is not compliant.

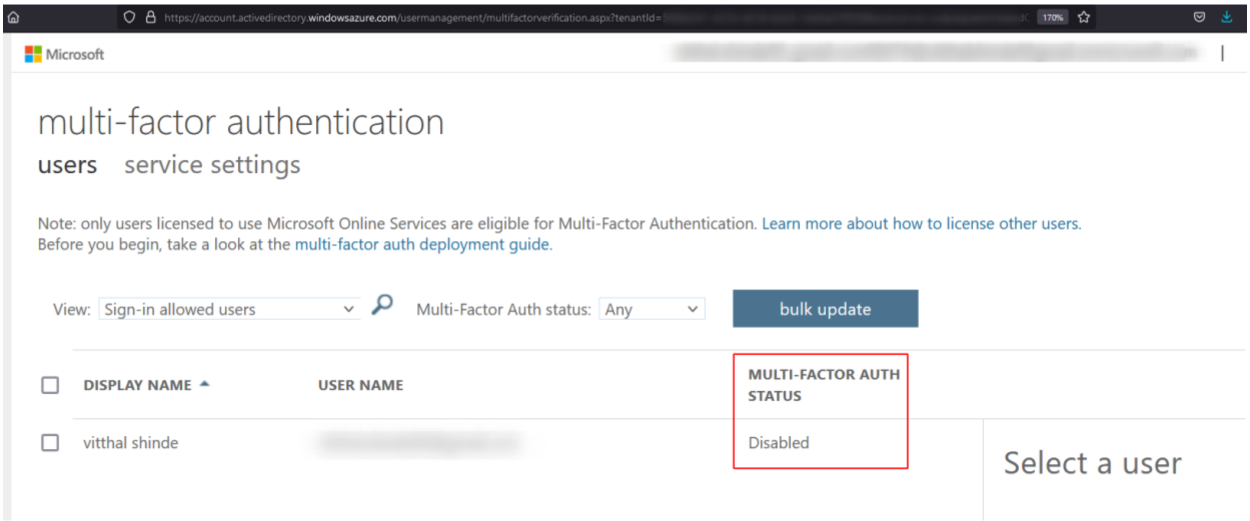
10. Lack of Multi-factor authentication for privileged users

Having an MFA-protected Azure account represents an efficient way to safeguard your cloud resources against malicious users and attackers, as Multi-Factor Authentication adds extra security to the authentication process by requiring privileged users (contributors, subscription owners and service co-administrators) to present a minimum of two separate forms of authorization before their access is granted. With Multi-Factor Authentication (MFA) enabled, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromising access credentials and thus reducing the risk of attack significantly.

If you're only using passwords to authenticate your users, you're leaving an attack vector open. Users often use weak passwords or reuse them for multiple services. With MFA enabled, your accounts are more secure, and users can still authenticate to almost any application with single sign-on (SSO).

Attacker's view:

Attackers can find out the valid usernames in services such as O365, As expected, a 200 indicates a valid username/password, while a 404 indicates the username does not exist.
The O365 brute-force requires a list of email addresses to attack. Attacker can check password dumps (e.g., LinkedIn or Adobe breach) for email addresses. Some sites like hunter.io specialize in providing email addresses for different organizations.
Attacker can use tools like https://github.com/dafthack/MSOLSpray to perform bruteforce.



https://account.activedirectory.windowsazure.com/usermanagement/multifactorverification.aspx?tenantId=[redacted]

Microsoft [redacted]

multi-factor authentication

users service settings

Note: only users licensed to use Microsoft Online Services are eligible for Multi-Factor Authentication. Learn more about how to license other users.
Before you begin, take a look at the multi-factor auth deployment guide.

View: Sign-in allowed users Multi-Factor Auth status: Any

□	DISPLAY NAME	USER NAME	MULTI-FACTOR AUTH STATUS
□	vitthal shinde	[redacted]	Disabled

Select a user

Figure 17 MFA Disabled

Defender's view

1. Enable Multi-factor Authentication
2. Identity Monitoring

When you centralize your identity in Microsoft Azure, your team is given access to different Azure resources. In this case, you need to monitor and manage them. With Azure Active Directory Premium, you take fully advantages of building a risk-based policy to automatically protect identities.

These can include

- Leaked credentials
- Impossible travel to atypical locations
- Sign-ins from infected locations
- Sign-ins from anonymous IP addresses
- Sign-ins from IP addresses with suspicious activity
- Sign-ins from unfamiliar locations

Tools:

- https://bitbucket.org/grimhacker/office365userenum/src/master/
- https://github.com/dafthack/MSOLSpray