

# CIS Microsoft Azure Foundations Benchmark

v2.0.0 - 01-31-2023

# Terms of Use

Please see the below link for our current terms of use:

<https://www.cisecurity.org/cis-securesuite/cis-securesuite-membership-terms-of-use/>

DRAFT

# Table of Contents

<b>Terms of Use</b> .....	<b>1</b>
<b>Table of Contents</b> .....	<b>2</b>
<b>Overview</b> .....	<b>7</b>
<b>Intended Audience</b> .....	<b>9</b>
<b>Consensus Guidance</b> .....	<b>10</b>
<b>Typographical Conventions</b> .....	<b>11</b>
<b>Recommendation Definitions</b> .....	<b>12</b>
<b>Title</b> .....	<b>12</b>
<b>Assessment Status</b> .....	<b>12</b>
Automated .....	<b>12</b>
Manual.....	<b>12</b>
<b>Profile</b> .....	<b>12</b>
<b>Description</b> .....	<b>12</b>
<b>Rationale Statement</b> .....	<b>12</b>
<b>Impact Statement</b> .....	<b>13</b>
<b>Audit Procedure</b> .....	<b>13</b>
<b>Remediation Procedure</b> .....	<b>13</b>
<b>Default Value</b> .....	<b>13</b>
<b>References</b> .....	<b>13</b>
<b>CIS Critical Security Controls® (CIS Controls®)</b> .....	<b>13</b>
<b>Additional Information</b> .....	<b>13</b>
<b>Profile Definitions</b> .....	<b>14</b>
<b>Acknowledgements</b> .....	<b>15</b>
<b>Recommendations</b> .....	<b>18</b>
<b>1 Identity and Access Management</b> .....	<b>18</b>
<b>1.1 Security Defaults</b> .....	<b>19</b>
1.1.1 Ensure Security Defaults is enabled on Azure Active Directory (Manual) .....	20
1.1.2 Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Privileged Users (Manual) .....	22
1.1.3 Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users (Manual) .....	26
1.1.4 Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is Disabled (Manual).....	29
<b>1.2 Conditional Access</b> .....	<b>31</b>
1.2.1 Ensure Trusted Locations Are Defined (Manual) .....	32
1.2.2 Ensure that an exclusionary Geographic Access Policy is considered (Manual) .....	35
1.2.3 Ensure that A Multi-factor Authentication Policy Exists for Administrative Groups (Manual).....	40
1.2.4 Ensure that A Multi-factor Authentication Policy Exists for All Users (Manual) .....	43
1.2.5 Ensure Multi-factor Authentication is Required for Risky Sign-ins (Manual) .....	46

1.2.6 Ensure Multi-factor Authentication is Required for Azure Management (Manual).....	49
1.3 Ensure that 'Users can create Azure AD Tenants' is set to 'No' (Automated) .....	52
1.4 Ensure Access Review is Set Up for External Users in Azure AD Privileged Identity Management (Manual).....	54
1.5 Ensure Guest Users Are Reviewed on a Regular Basis (Manual) .....	57
1.6 Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is 'Disabled' (Manual).....	61
1.7 Ensure That 'Number of methods required to reset' is set to '2' (Manual) .....	63
1.8 Ensure that a Custom Bad Password List is set to 'Enforce' for your Organization (Manual) .....	65
1.9 Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0' (Manual).....	68
1.10 Ensure that 'Notify users on password resets?' is set to 'Yes' (Manual).....	70
1.11 Ensure That 'Notify all admins when other admins reset their password?' is set to 'Yes' (Manual).....	72
1.12 Ensure that 'Users can consent to apps accessing company data on their behalf' is set to 'No' (Manual).....	74
1.13 Ensure That 'Users Can Consent to Apps Accessing Company Data on Their Behalf' Is Set To 'Allow for Verified Publishers' (Manual).....	76
1.14 Ensure that 'Users can add gallery apps to My Apps' is set to 'No' (Manual) .....	79
1.15 Ensure That 'Users Can Register Applications' Is Set to 'No' (Manual) .....	81
1.16 Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects' (Manual) .....	84
1.17 Ensure that 'Guest invite restrictions' is set to "Only users assigned to specific admin roles can invite guest users" (Manual) .....	87
1.18 Ensure That 'Restrict access to Azure AD administration portal' is Set to 'Yes' (Manual) .....	90
1.19 Ensure that 'Restrict user ability to access groups features in the Access Pane' is Set to 'Yes' (Manual).....	92
1.20 Ensure that 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No' (Manual).....	94
1.21 Ensure that 'Owners can manage group membership requests in the Access Panel' is set to 'No' (Manual).....	96
1.22 Ensure that 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No' (Manual).....	98
1.23 Ensure that 'Require Multi-Factor Authentication to register or join devices with Azure AD' is set to 'Yes' (Manual) .....	100
1.24 Ensure That No Custom Subscription Administrator Roles Exist (Automated) .....	102
1.25 Ensure a Custom Role is Assigned Permissions for Administering Resource Locks (Manual).....	105
1.26 Ensure That 'Subscription Entering AAD Directory' and 'Subscription Leaving AAD Directory' Is Set To 'Permit No One' (Manual) .....	108
<b>2 Microsoft Defender .....</b>	<b>110</b>
<b>2.1 Microsoft Defender for Cloud .....</b>	<b>111</b>
2.1.1 Ensure That Microsoft Defender for Servers Is Set to 'On' (Manual).....	112
2.1.2 Ensure That Microsoft Defender for App Services Is Set To 'On' (Manual).....	115
2.1.3 Ensure That Microsoft Defender for Databases Is Set To 'On' (Manual).....	118
2.1.4 Ensure That Microsoft Defender for Azure SQL Databases Is Set To 'On' (Manual) .....	121
2.1.5 Ensure That Microsoft Defender for SQL Servers on Machines Is Set To 'On' (Manual) .....	124
2.1.6 Ensure That Microsoft Defender for Open-Source Relational Databases Is Set To 'On' (Manual) ..	127
2.1.7 Ensure That Microsoft Defender for Storage Is Set To 'On' (Manual) .....	130
2.1.8 Ensure That Microsoft Defender for Containers Is Set To 'On' (Manual) .....	132
2.1.9 Ensure That Microsoft Defender for Azure Cosmos DB Is Set To 'On' (Manual) .....	135
2.1.10 Ensure That Microsoft Defender for Key Vault Is Set To 'On' (Manual) .....	138
2.1.11 Ensure That Microsoft Defender for DNS Is Set To 'On' (Manual) .....	140
2.1.12 Ensure That Microsoft Defender for Resource Manager Is Set To 'On' (Manual) .....	143
2.1.13 Ensure that Microsoft Defender Recommendation for 'Apply system updates' status is 'Completed' (Manual).....	146

2.1.14 Ensure Any of the ASC Default Policy Settings are Not Set to 'Disabled' (Manual) .....	148
2.1.15 Ensure that Auto provisioning of 'Log Analytics agent for Azure VMs' is Set to 'On' (Automated) ..	151
2.1.16 Ensure that Auto provisioning of 'Vulnerability assessment for machines' is Set to 'On' (Manual) ..	154
2.1.17 Ensure that Auto provisioning of 'Microsoft Defender for Containers components' is Set to 'On' (Manual).....	156
2.1.18 Ensure That 'All users with the following roles' is set to 'Owner' (Automated).....	158
2.1.19 Ensure 'Additional email addresses' is Configured with a Security Contact Email (Automated) ....	161
2.1.20 Ensure That 'Notify about alerts with the following severity' is Set to 'High' (Automated).....	164
2.1.21 Ensure that Microsoft Defender for Cloud Apps integration with Microsoft Defender for Cloud is Selected (Manual).....	167
2.1.22 Ensure that Microsoft Defender for Endpoint integration with Microsoft Defender for Cloud is selected (Manual) .....	171
<b>2.2 Microsoft Defender for IoT .....</b>	<b>175</b>
2.2.1 Ensure That Microsoft Defender for IoT Hub Is Set To 'On' (Manual).....	176
<b>2.3 Microsoft Defender for External Attack Surface Monitoring .....</b>	<b>178</b>
<b>3 Storage Accounts .....</b>	<b>179</b>
3.1 Ensure that 'Secure transfer required' is set to 'Enabled' (Automated) .....	180
3.2 Ensure that 'Enable Infrastructure Encryption' for Each Storage Account in Azure Storage is Set to 'enabled' (Manual) .....	182
3.3 Ensure that 'Enable key rotation reminders' is enabled for each Storage Account (Manual) .....	185
3.4 Ensure that Storage Account Access Keys are Periodically Regenerated (Manual).....	188
3.5 Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' requests (Automated) .....	191
3.6 Ensure that Shared Access Signature Tokens Expire Within an Hour (Manual).....	194
3.7 Ensure that 'Public access level' is disabled for storage accounts with blob containers (Automated) ..	196
3.8 Ensure Default Network Access Rule for Storage Accounts is Set to Deny (Automated) .....	199
3.9 Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access (Automated) .....	202
3.10 Ensure Private Endpoints are used to access Storage Accounts (Automated).....	205
3.11 Ensure Soft Delete is Enabled for Azure Containers and Blob Storage (Automated) .....	209
3.12 Ensure Storage for Critical Data are Encrypted with Customer Managed Keys (Manual).....	212
3.13 Ensure Storage logging is Enabled for Blob Service for 'Read', 'Write', and 'Delete' requests (Automated) .....	214
3.14 Ensure Storage Logging is Enabled for Table Service for 'Read', 'Write', and 'Delete' Requests (Automated) .....	217
3.15 Ensure the "Minimum TLS version" for storage accounts is set to "Version 1.2" (Automated).....	220
<b>4 Database Services .....</b>	<b>223</b>
<b>4.1 SQL Server - Auditing.....</b>	<b>224</b>
4.1.1 Ensure that 'Auditing' is set to 'On' (Automated) .....	225
4.1.2 Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP) (Automated).....	228
4.1.3 Ensure SQL server's Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key (Automated).....	232
4.1.4 Ensure that Azure Active Directory Admin is Configured for SQL Servers (Automated) .....	236
4.1.5 Ensure that 'Data encryption' is set to 'On' on a SQL Database (Automated).....	239
4.1.6 Ensure that 'Auditing' Retention is 'greater than 90 days' (Automated).....	242
<b>4.2 SQL Server - Microsoft Defender for SQL .....</b>	<b>245</b>
4.2.1 Ensure that Microsoft Defender for SQL is set to 'On' for critical SQL Servers (Automated) .....	246
4.2.2 Ensure that Vulnerability Assessment (VA) is enabled on a SQL server by setting a Storage Account (Automated) .....	249
4.2.3 Ensure that Vulnerability Assessment (VA) setting 'Periodic recurring scans' is set to 'on' for each SQL server (Automated) .....	253
4.2.4 Ensure that Vulnerability Assessment (VA) setting 'Send scan reports to' is configured for a SQL server (Automated) .....	256

4.2.5 Ensure that Vulnerability Assessment (VA) setting 'Also send email notifications to admins and subscription owners' is set for each SQL Server (Automated) .....	259
<b>4.3 PostgreSQL Database Server .....</b>	<b>262</b>
4.3.1 Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database Server (Automated) .....	263
4.3.2 Ensure Server Parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server (Automated) .....	265
4.3.3 Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server (Automated) .....	267
4.3.4 Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server (Automated) .....	269
4.3.5 Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server (Automated) .....	272
4.3.6 Ensure Server Parameter 'log_retention_days' is greater than 3 days for PostgreSQL Database Server (Automated) .....	274
4.3.7 Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled (Manual) ....	277
4.3.8 Ensure 'Infrastructure double encryption' for PostgreSQL Database Server is 'Enabled' (Automated) .....	279
<b>4.4 MySQL Database .....</b>	<b>282</b>
4.4.1 Ensure 'Enforce SSL connection' is set to 'Enabled' for Standard MySQL Database Server (Automated) .....	283
4.4.2 Ensure 'TLS Version' is set to 'TLSV1.2' for MySQL flexible Database Server (Automated) .....	285
4.4.3 Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL Database Server (Manual) .....	288
4.4.4 Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL Database Server (Manual) .....	290
<b>4.5 Cosmos DB .....</b>	<b>292</b>
4.5.1 Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks (Manual) .....	293
4.5.2 Ensure That Private Endpoints Are Used Where Possible (Manual) .....	296
4.5.3 Use Azure Active Directory (AAD) Client Authentication and Azure RBAC where possible. (Manual) .....	298
<b>5 Logging and Monitoring .....</b>	<b>299</b>
<b>5.1 Configuring Diagnostic Settings .....</b>	<b>300</b>
5.1.1 Ensure that a 'Diagnostic Setting' exists (Manual) .....	301
5.1.2 Ensure Diagnostic Setting captures appropriate categories (Automated) .....	305
5.1.3 Ensure the Storage Container Storing the Activity Logs is not Publicly Accessible (Automated) .....	308
5.1.4 Ensure the storage account containing the container with activity logs is encrypted with Customer Managed Key (Automated) .....	311
5.1.5 Ensure that logging for Azure Key Vault is 'Enabled' (Automated) .....	314
5.1.6 Ensure that Network Security Group Flow logs are captured and sent to Log Analytics (Manual) .....	318
5.1.7 Ensure that logging for Azure AppService 'HTTP logs' is enabled (Manual) .....	320
<b>5.2 Monitoring using Activity Log Alerts .....</b>	<b>322</b>
5.2.1 Ensure that Activity Log Alert exists for Create Policy Assignment (Automated) .....	323
5.2.2 Ensure that Activity Log Alert exists for Delete Policy Assignment (Automated) .....	327
5.2.3 Ensure that Activity Log Alert exists for Create or Update Network Security Group (Automated) .....	331
5.2.4 Ensure that Activity Log Alert exists for Delete Network Security Group (Automated) .....	335
5.2.5 Ensure that Activity Log Alert exists for Create or Update Security Solution (Automated) .....	339
5.2.6 Ensure that Activity Log Alert exists for Delete Security Solution (Automated) .....	343
5.2.7 Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule (Automated) .....	347
5.2.8 Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule (Automated) .....	351
5.2.9 Ensure that Activity Log Alert exists for Create or Update Public IP Address rule (Automated) .....	355
5.2.10 Ensure that Activity Log Alert exists for Delete Public IP Address rule (Automated) .....	359
<b>5.3 Configuring Application Insights .....</b>	<b>363</b>

5.3.1 Ensure Application Insights are Configured (Automated).....	364
5.4 Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it (Manual)....	367
5.5 Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads) (Automated) .....	371
<b>6 Networking .....</b>	<b>373</b>
6.1 Ensure that RDP access from the Internet is evaluated and restricted (Automated) .....	374
6.2 Ensure that SSH access from the Internet is evaluated and restricted (Automated).....	376
6.3 Ensure that UDP access from the Internet is evaluated and restricted (Automated) .....	378
6.4 Ensure that HTTP(S) access from the Internet is evaluated and restricted (Automated).....	381
6.5 Ensure that Network Security Group Flow Log retention period is 'greater than 90 days' (Automated) .....	383
6.6 Ensure that Network Watcher is 'Enabled' (Automated).....	385
6.7 Ensure that Public IP addresses are Evaluated on a Periodic Basis (Manual) .....	387
<b>7 Virtual Machines .....</b>	<b>389</b>
7.1 Ensure Virtual Machines are utilizing Managed Disks (Automated).....	390
7.2 Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK) (Automated) ....	393
7.3 Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK) (Automated) ....	396
7.4 Ensure that Only Approved Extensions Are Installed (Manual).....	399
7.5 Ensure that Endpoint Protection for all Virtual Machines is installed (Manual).....	402
7.6 [Legacy] Ensure that VHDs are Encrypted (Manual) .....	404
7.7 Ensure an Azure Bastion Host Exists (Automated).....	407
<b>8 Key Vault .....</b>	<b>411</b>
8.1 Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults (Automated) .....	412
8.2 Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults. (Automated) .....	415
8.3 Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults (Automated).....	418
8.4 Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults (Automated).....	421
8.5 Ensure the Key Vault is Recoverable (Automated) .....	424
8.6 Enable Role Based Access Control for Azure Key Vault (Manual) .....	428
8.7 Ensure that Private Endpoints are Used for Azure Key Vault (Manual) .....	430
8.8 Ensure Automatic Key Rotation is Enabled Within Azure Key Vault for the Supported Services (Manual).....	434
<b>9 AppService.....</b>	<b>439</b>
9.1 Ensure App Service Authentication is set up for apps in Azure App Service (Automated) .....	440
9.2 Ensure Web App Redirects All HTTP traffic to HTTPS in Azure App Service (Automated) .....	443
9.3 Ensure Web App is using the latest version of TLS encryption (Automated) .....	445
9.4 Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On' (Automated) ....	447
9.5 Ensure that Register with Azure Active Directory is enabled on App Service (Automated) .....	449
9.6 Ensure That 'PHP version' is the Latest, If Used to Run the Web App (Manual) .....	451
9.7 Ensure that 'Python version' is the Latest Stable Version, if Used to Run the Web App (Manual) ....	454
9.8 Ensure that 'Java version' is the latest, if used to run the Web App (Manual).....	457
9.9 Ensure that 'HTTP Version' is the Latest, if Used to Run the Web App (Automated).....	461
9.10 Ensure FTP deployments are Disabled (Automated).....	464
9.11 Ensure Azure Key Vaults are Used to Store Secrets (Manual) .....	467
<b>10 Miscellaneous .....</b>	<b>472</b>
10.1 Ensure that Resource Locks are set for Mission-Critical Azure Resources (Manual) .....	473
<b>Appendix: Summary Table .....</b>	<b>476</b>

# Overview

All CIS Benchmarks focus on technical configuration settings used to maintain and/or increase the security of the addressed technology, and they should be used in **conjunction** with other essential cyber hygiene tasks like:

- Monitoring the base operating system for vulnerabilities and quickly updating with the latest security patches
- Monitoring applications and libraries for vulnerabilities and quickly updating with the latest security patches

In the end, the CIS Benchmarks are designed as a key **component** of a comprehensive cybersecurity program.

This document, CIS Microsoft Azure Foundations Benchmark, provides prescriptive guidance for establishing a secure baseline configuration for Microsoft Azure. The scope of this benchmark is to establish the foundation level of security for anyone adopting Microsoft Azure Cloud. The benchmark is, however, not an exhaustive list of all possible security configurations and architecture. The benchmark should be understood as a starting point. Site-specific tailoring will almost certainly be required. The CIS Azure Foundations Benchmark provides recommendations for the following Azure Services:

- App Service
- Application Gateway
- Azure Active Directory
- Azure Advisor
- Azure Cosmos DB
- Azure Disk Storage
- Azure Files
- Azure Monitor
- Azure Policy
- Azure Private Link
- Azure Resource Manager
- Azure Service Health
- Azure SQL
- Azure SQL Database
- Key Vault
- Microsoft Azure portal
- Microsoft Defender for Cloud
- Static Web Apps
- Storage Accounts
- Virtual Machines
- Virtual Network



## Multiple Methods of Audit and Remediation

Throughout the Benchmark, Audit and Remediation procedures are prescribed using up to four different methods. These multiple methods are presented for the convenience of readers who will be coming from different technical and experiential backgrounds. To perform any given Audit or Remediation, only one method needs to be performed. Not every method is available for every recommendation, and many that are available are not yet written for every recommendation. The methods presented in the Benchmark are formatted and titled as follows:

- **"From Azure Portal"** - This is the administrative GUI accessed at <https://portal.azure.com>.
- **"From Azure CLI"** - See additional detail in the next section.
- **"From PowerShell"** - See additional detail in the next section.
- **"From REST API"** - An Application Programming Interface (API) for HTTP operations on service endpoints.

## Setting Up PowerShell and Azure CLI

In order to use the Azure Command Line Interface (CLI) and the Azure PowerShell methods for audit and remediation procedures, the following permissions are required for the account running the procedures:

1. Global Reader
2. Security Reader
3. Subscription Contributor
4. Key Vault Get/List privileges on Keys, Secrets, Certificates, and Certificate Authorities
5. Network allow listing for any source IP address performing the audit activities
6. Permissions to use PowerShell and Azure CLI

These permissions can be directly assigned or assigned via Privileged Identity Management.

The Azure CLI tool can be installed from the following location:

<https://docs.microsoft.com/en-us/cli/azure/install-azure-cli-windows?tabs=azure-cli>

For PowerShell, the following cmdlets are required:

1. Azure PowerShell: <https://docs.microsoft.com/en-us/powershell/azure/install-az-ps-msi?view=azps-8.2.0>
2. Azure AD PowerShell for Graph: <https://docs.microsoft.com/en-us/powershell/azure/active-directory/overview?view=azureadps-2.0>
3. MS Online PowerShell: <https://docs.microsoft.com/en-us/powershell/module/msonline/?view=azureadps-1.0>

## Authenticating with Azure CLI

Run the following command from either PowerShell or command prompt:

```
az login --tenant <tenant id> --subscription <subscription ID>
```

## Authenticating with PowerShell

Login to the Azure tenant and subscription using the following command:

```
Connect-AzAccount -Subscription <subscription ID> -Tenant <Tenant ID>  
Connect-MsolService  
Connect-AzureAD
```

*NOTE:* This will store session information within the PowerShell environment and may persist after closing PowerShell. Please take all necessary precautions to shorten the lifespan of this session and protect it from unauthorized access.

### Latest Version

To obtain the latest version of this guide, please visit <https://www.cisecurity.org/cis-benchmarks/>.

### Feedback

If you have questions, comments, or have identified ways to improve this guide, please write us at [benchmarkinfo@cisecurity.org](mailto:benchmarkinfo@cisecurity.org).

## Intended Audience

This document is intended for system and application administrators, security specialists, auditors, help desk, and platform deployment personnel who plan to develop, deploy, assess, or secure solutions that incorporate Microsoft Azure.

## Consensus Guidance

This CIS Benchmark was created using a consensus review process comprised of a global community of subject matter experts. The process combines real world experience with data-based information to create technology specific guidance to assist users to secure their environments. Consensus participants provide perspective from a diverse set of backgrounds including consulting, software development, audit and compliance, security research, operations, government, and legal.

Each CIS Benchmark undergoes two phases of consensus review. The first phase occurs during initial Benchmark development. During this phase, subject matter experts convene to discuss, create, and test working drafts of the Benchmark. This discussion occurs until consensus has been reached on Benchmark recommendations. The second phase begins after the Benchmark has been published. During this phase, all feedback provided by the Internet community is reviewed by the consensus team for incorporation in the Benchmark. If you are interested in participating in the consensus process, please visit <https://workbench.cisecurity.org/>.

DRAFT

## Typographical Conventions

The following typographical conventions are used throughout this guide:

Convention	Meaning
<code>Stylized Monospace font</code>	Used for blocks of code, command, and script examples. Text should be interpreted exactly as presented.
Monospace font	Used for inline code, commands, or examples. Text should be interpreted exactly as presented.
< <i>italic font in brackets</i> >	Italic texts set in angle brackets denote a variable requiring substitution for a real value.
<i>Italic font</i>	Used to denote the title of a book, article, or other publication.
<b>Note</b>	Additional information or caveats

# Recommendation Definitions

The following defines the various components included in a CIS recommendation as applicable. If any of the components are not applicable it will be noted or the component will not be included in the recommendation.

## Title

Concise description for the recommendation's intended configuration.

## Assessment Status

An assessment status is included for every recommendation. The assessment status indicates whether the given recommendation can be automated or requires manual steps to implement. Both statuses are equally important and are determined and supported as defined below:

### Automated

Represents recommendations for which assessment of a technical control can be fully automated and validated to a pass/fail state. Recommendations will include the necessary information to implement automation.

### Manual

Represents recommendations for which assessment of a technical control cannot be fully automated and requires all or some manual steps to validate that the configured state is set as expected. The expected state can vary depending on the environment.

## Profile

A collection of recommendations for securing a technology or a supporting platform. Most benchmarks include at least a Level 1 and Level 2 Profile. Level 2 extends Level 1 recommendations and is not a standalone profile. The Profile Definitions section in the benchmark provides the definitions as they pertain to the recommendations included for the technology.

## Description

Detailed information pertaining to the setting with which the recommendation is concerned. In some cases, the description will include the recommended value.

## Rationale Statement

Detailed reasoning for the recommendation to provide the user a clear and concise understanding on the importance of the recommendation.

## **Impact Statement**

Any security, functionality, or operational consequences that can result from following the recommendation.

## **Audit Procedure**

Systematic instructions for determining if the target system complies with the recommendation

## **Remediation Procedure**

Systematic instructions for applying recommendations to the target system to bring it into compliance according to the recommendation.

## **Default Value**

Default value for the given setting in this recommendation, if known. If not known, either not configured or not defined will be applied.

## **References**

Additional documentation relative to the recommendation.

## **CIS Critical Security Controls® (CIS Controls®)**

The mapping between a recommendation and the CIS Controls is organized by CIS Controls version, Safeguard, and Implementation Group (IG). The Benchmark in its entirety addresses the CIS Controls safeguards of (v7) "5.1 - Establish Secure Configurations" and (v8) "4.1 - Establish and Maintain a Secure Configuration Process" so individual recommendations will not be mapped to these safeguards.

## **Additional Information**

Supplementary information that does not correspond to any other field but may be useful to the user.

## Profile Definitions

The following configuration profiles are defined by this Benchmark:

- **Level 1**

Items in this profile intend to:

- be practical and prudent;
- provide security focused best practice hardening of a technology; and
- limit impact to the utility of the technology beyond acceptable means.

- **Level 2**

This profile extends the "Level 1" profile. Items in this profile exhibit one or more of the following characteristics:

- are intended for environments or use cases where security is more critical than manageability and usability
- acts as defense in depth measure
- may impact the utility or performance of the technology
- may include additional licensing, cost, or addition of third party software

## Acknowledgements

This Benchmark exemplifies the great things a community of users, vendors, and subject matter experts can accomplish through consensus collaboration. The CIS community thanks the entire consensus team with special recognition to the following individuals who contributed greatly to the creation of this guide:

DRAFT



**Contributor**

Zeeshan Mustafa  
Nathan Young  
Mark Weaver  
Marc Garcia  
Robert Burton  
Jim Cheng  
Stephen Keller  
Gururaj Pandurangi  
Felix Simmons  
Pravin Goyal  
Pradeep R B  
Robin Drake  
Shobha H D  
Rahul Khengare  
Jesse Mrasek  
Kesten Broughton  
Himalay Kondekar  
JR Aquino  
Jeremie Kass  
Sujit Singh  
Clément Bonnet  
Lewis Matlock  
Clifford Moten  
Sean Decker  
Phil White  
Mike Wicks  
Ronit Reger  
Lewis Hardy  
Gareth Boyes  
Ellie Goggin  
Luke Schultheis  
Sagar Chhatrala  
Jeffrey Lemmermann  
Apostolos Gioulis  
Richard Rives  
Nirbhay Kumar  
Ben Layer  
Jonathan Trull  
Parag Patil  
Prabhu Angadi

**Editor**

Rachel Rice

Michael Born

Zan Liffick

Ian McRee

Logan McMillan

Iben Rodriguez

DRAFT

# Recommendations

## 1 Identity and Access Management

This section covers security recommendations to set identity and access management policies on an Azure Subscription. Identity and Access Management policies are the first step towards a defense-in-depth approach to securing an Azure Cloud Platform environment.

Many of the recommendations from this section are marked as "Manual" while Azure CLI and PowerShell are being improved to support and perform the respective audits and remediation. From a security posture standpoint, these recommendations are still very important and should not be discounted because they are "Manual." As automation capability using Rest API is developed for this Benchmark, the related recommendations will be updated with the respective audit and remediation steps and changed to an "automated" assessment status.

If any problems are encountered running Azure CLI or PowerShell methodologies, please refer to the Overview for this benchmark where you will find additional detail on permission and required cmdlets.

DRAFT

## 1.1 Security Defaults

**IMPORTANT:** The Azure "Security Defaults" recommendations represent an entry-level set of recommendations which will be relevant to organizations and tenants that are either just starting to use Azure as an IaaS solution, or are only utilizing a bare minimum feature set such as the freely licensed tier of Azure Active Directory. Security Defaults recommendations are intended to ensure that these entry-level use cases are still capable of establishing a strong baseline of secure configuration.

**If your subscription is licensed to use Azure AD Premium P1 or P2, it is strongly recommended that the "Security Defaults" section (this section and the recommendations therein) be bypassed in favor of the use of "Conditional Access."**

DRAFT

## 1.1.1 Ensure Security Defaults is enabled on Azure Active Directory (Manual)

### Profile Applicability:

- Level 1

### Description:

Security defaults in Azure Active Directory (Azure AD) make it easier to be secure and help protect your organization. Security defaults contain preconfigured security settings for common attacks.

Microsoft is making security defaults available to everyone. The goal is to ensure that all organizations have a basic level of security enabled at no extra cost. You may turn on security defaults in the Azure portal.

### Rationale:

Security defaults provide secure default settings that we manage on behalf of organizations to keep customers safe until they are ready to manage their own identity security settings.

For example, doing the following:

- Requiring all users and admins to register for MFA.
- Challenging users with MFA - mostly when they show up on a new device or app, but more often for critical roles and tasks.
- Disabling authentication from legacy authentication clients, which can't do MFA.

### Impact:

Enabling security defaults may negatively impact the functionality of other Microsoft services, such as MS365. This recommendation should be implemented initially and then may be overridden by other service/product specific CIS Benchmarks.

### Audit:

#### From Azure Portal

To ensure security defaults is enabled in your directory:

1. From Azure Home select the Portal Menu.
2. Browse to `Azure Active Directory > Properties`.
3. Select `Manage security defaults`.
4. Verify the `Enable security defaults` toggle is `Yes`.

## Remediation:

### From Azure Portal

To enable security defaults in your directory:

1. From Azure Home select the Portal Menu.
2. Browse to Azure Active Directory > Properties
3. Select Manage security defaults
4. Set the Enable security defaults toggle to Yes
5. Select Save

### Default Value:

If your tenant was created on or after October 22, 2019, security defaults may already be enabled in your tenant.







### References:

1. <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/concept-fundamentals-security-defaults>
2. <https://techcommunity.microsoft.com/t5/azure-active-directory-identity/introducing-security-defaults/ba-p/1061414>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-2-protect-identity-and-authentication-systems>

### Additional Information:

This recommendation differs from the [Microsoft 365 Benchmark](#). This is because the potential impact associated with disabling Security Defaults is dependent upon the security settings implemented in the environment. It is recommended that organizations disabling Security Defaults implement appropriate security settings to replace the settings configured by Security Defaults.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 Establish and Maintain a Secure Configuration Process</b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b>5.1 Establish Secure Configurations</b> Maintain documented, standard security configuration standards for all authorized operating systems and software.			

## 1.1.2 Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Privileged Users (Manual)

### Profile Applicability:

- Level 1

### Description:

Enable multi-factor authentication for all roles, groups, and users that have write access or permissions to Azure resources. These include custom created objects or built-in roles such as;

- Service Co-Administrators
- Subscription Owners
- Contributors

### Rationale:

Multi-factor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted. Multi-factor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multi-factor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.

### Impact:

Users would require two forms of authentication before any access is granted. Additional administrative time will be required for managing dual forms of authentication when enabling multi-factor authentication.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select the Azure Active Directory blade
3. Select Users
4. Take note of all users with the role Service Co-Administrators, Owners or Contributors
5. Click on the Per-User MFA button in the top row menu
6. Ensure that MULTI-FACTOR AUTH STATUS is Enabled for all noted users

## From REST API

For Every Subscription, For Every Tenant

### Step 1: Identify Users with Administrative Access

1. List All Users Using Microsoft Graph API:

```
GET https://graph.microsoft.com/v1.0/users
```

Capture `id` and corresponding `userPrincipalName` (`'$uid'`, `'$userPrincipalName'`)

2. List all Role Definitions Using Azure management API:

```
https://management.azure.com/subscriptions/:subscriptionId/providers/Microsoft.Authorization/roleDefinitions?api-version=2017-05-01
```

Capture Role Definition IDs/Name (`'$name'`) and role names (`'$properties/roleName'`) where `"properties/roleName"` contains (`Owner` or `*contributor` or `admin`)

3. List All Role Assignments (Mappings `$A.uid` to `$B.name`) Using Azure Management API:

```
GET https://management.azure.com/subscriptions/:subscriptionId/providers/Microsoft.Authorization/roleassignments?api-version=2017-10-01-preview
```

Find all administrative roles (`$B.name`) in `"Properties/roleDefinitionId"` mapped with user ids (`$A.id`) in `"Properties/principalId"` where `"Properties/principalType" == "User"`

4. Now Match (`$CProperties/principalId`) with `$A.uid` and get `$A.userPrincipalName` save this as `D.userPrincipalName`

### Step 2: Run MSOL PowerShell command:

```
Get-MsolUser -All | where {$_.StrongAuthenticationMethods.Count -eq 0} |  
Select-Object -Property UserPrincipalName
```

If the output contains any of the `$D.userPrincipalName`, then this recommendation is non-compliant.



## Remediation:

### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory blade
3. Select Users
4. Take note of all users with the role Service Co-Administrators, Owners OR Contributors
5. Click on the Per-User MFA button in the top row menu
6. Check the box next to each noted user
7. Click Enable under quick steps in the right-hand panel
8. Click enable multi-factor auth
9. Click close

### Other Options within Azure Portal

Follow Microsoft Azure documentation and enable multi-factor authentication in your environment.

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa>

Enabling and configuring MFA with conditional access policy is a multi-step process. Here are some additional resources on the process within Azure AD to enable multi-factor authentication for users within your subscriptions with conditional access policy.

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa>

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted#enable-multi-factor-authentication-with-conditional-access>

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings>

### Default Value:

By default, multi-factor authentication is disabled for all users.

### References:

1. <https://docs.microsoft.com/en-us/azure/multi-factor-authentication/multi-factor-authentication>
2. <https://stackoverflow.com/questions/41156206/azure-active-directory-premium-mfa-attributes-via-graph-api>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-4-use-strong-authentication-controls-for-all-azure-active-directory-based-access>

### Additional Information:

Please note that at the time of writing, there is no API, Azure CLI or Powershell mechanism available to programmatically conduct security assessment or remediation for this recommendation. The only option is MSOL.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.3 <u>Require MFA for Externally-Exposed Applications</u></b> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	<b>6.4 <u>Require MFA for Remote Network Access</u></b> Require MFA for remote network access.	●	●	●
v8	<b>6.5 <u>Require MFA for Administrative Access</u></b> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v7	<b>4.5 <u>Use Multifactor Authentication For All Administrative Access</u></b> Use multi-factor authentication and encrypted channels for all administrative account access.		●	●
v7	<b>16.3 <u>Require Multi-factor Authentication</u></b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

### 1.1.3 Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users (Manual)

#### Profile Applicability:

- Level 2

#### Description:

Enable multi-factor authentication for all non-privileged users.

#### Rationale:

Multi-factor authentication requires an individual to present a minimum of two separate forms of authentication before access is granted. Multi-factor authentication provides additional assurance that the individual attempting to gain access is who they claim to be. With multi-factor authentication, an attacker would need to compromise at least two different authentication mechanisms, increasing the difficulty of compromise and thus reducing the risk.

#### Impact:

Users would require two forms of authentication before any access is granted. Also, this requires an overhead for managing dual forms of authentication.

#### Audit:

##### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select the Azure Active Directory blade
3. Then Users
4. Select All Users
5. Click on Per-User MFA button on the top bar
6. Ensure that for all users MULTI-FACTOR AUTH STATUS is Enabled

##### From REST API

For Every Subscription, For Every Tenant

##### Step 1: Identify Users with non-administrative Access

1. List All Users Using Microsoft Graph API:

```
GET https://graph.microsoft.com/v1.0/users
```

Capture `id` and corresponding `userPrincipalName` (`$uid`, `$userPrincipalName`)

## 2. List all Role Definitions Using Azure management API:

```
https://management.azure.com/subscriptions/<subscriptionId>/providers/Microsoft.Authorization/roleDefinitions?api-version=2017-05-01
```

Capture Role Definition IDs/Name (\$name) and role names (\$properties/roleName) where "properties/roleName" does NOT contain (Owner or \*contributor or admin )

## 3. List All Role Assignments (Mappings \$A.uid to \$B.name) Using Azure Management API:

```
GET
https://management.azure.com/subscriptions/<subscriptionId>/providers/Microsoft.Authorization/roleassignments?api-version=2017-10-01-preview
```

Find all non-administrative roles (\$B.name) in "Properties/roleDefinitionId" mapped with user ids (\$A.id) in "Properties/principalId" where "Properties/principalType" == "User"

D> Now Match (\$CProperties/principalId) with \$A.uid and get \$A.userPrincipalName save this as D.userPrincipleName

**Step 2:** Run MSOL PowerShell command:

```
Get-MsolUser -All | where {$_.StrongAuthenticationMethods.Count -eq 0} |
Select-Object -Property UserPrincipalName
```

If the output contains any of the \$D.userPrincipleName, then this recommendation is non-compliant.

### Remediation:

Follow Microsoft Azure documentation and enable multi-factor authentication in your environment.

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-azure-mfa>

Enabling and configuring MFA is a multi-step process. Here are some additional resources on the process within Azure AD:

<https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa>

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-getstarted#enable-multi-factor-authentication-with-conditional-access>

<https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings>

### Default Value:

By default, multi-factor authentication is disabled for all users.

## References:

1. <https://docs.microsoft.com/en-us/azure/multi-factor-authentication/multi-factor-authentication>
2. <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-userstates>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-4-use-strong-authentication-controls-for-all-azure-active-directory-based-access>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.3 Require MFA for Externally-Exposed Applications</b> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	<b>6.4 Require MFA for Remote Network Access</b> Require MFA for remote network access.	●	●	●
v7	<b>16.3 Require Multi-factor Authentication</b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

## 1.1.4 Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is Disabled (Manual)

### Profile Applicability:

- Level 1

### Description:

Do not allow users to remember multi-factor authentication on devices.

### Rationale:

Remembering Multi-Factor Authentication (MFA) for devices and browsers allows users to have the option to bypass MFA for a set number of days after performing a successful sign-in using MFA. This can enhance usability by minimizing the number of times a user may need to perform two-step verification on the same device. However, if an account or device is compromised, remembering MFA for trusted devices may affect security. Hence, it is recommended that users not be allowed to bypass MFA.

### Impact:

For every login attempt, the user will be required to perform multi-factor authentication.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Select Users
4. Click the Per-user MFA button on the top bar
5. Click on service settings
6. Ensure that Allow users to remember multi-factor authentication on devices they trust is not enabled

### Remediation:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Select Users
4. Click the Per-user MFA button on the top bar
5. Click on service settings
6. Uncheck the box next to Allow users to remember multi-factor authentication on devices they trust

## Default Value:

By default, Allow users to remember multi-factor authentication on devices they trust is disabled.

## References:

1. <https://learn.microsoft.com/en-us/azure/active-directory/authentication/howto-mfa-mfasettings#remember-multi-factor-authentication-for-devices-that-users-trust>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-4-use-strong-authentication-controls-for-all-azure-active-directory-based-access>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-6-use-strong-authentication-controls>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.3 <u>Require MFA for Externally-Exposed Applications</u></b> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	<b>6.4 <u>Require MFA for Remote Network Access</u></b> Require MFA for remote network access.	●	●	●
v7	<b>16.3 <u>Require Multi-factor Authentication</u></b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

## 1.2 Conditional Access

For most Azure tenants, and certainly for organizations with a significant use of Azure Active Directory, Conditional Access policies are recommended and preferred. To use conditional access policies, a licensing plan is required, and **Security Defaults must be disabled**.

Conditional Access requires one of the following plans:

- Azure Active Directory Premium P1 or P2
- Microsoft 365 Business Premium
- Microsoft 365 E3 or E5
- Enterprise Mobility & Security E3 or E5

DRAFT



## 1.2.1 Ensure Trusted Locations Are Defined (Manual)

### Profile Applicability:

- Level 1

### Description:

Azure Active Directory Conditional Access allows an organization to configure `Named locations` and configure whether those locations are trusted or untrusted. These settings provide organizations the means to specify Geographical locations for use in conditional access policies, or define actual IP addresses and IP ranges and whether or not those IP addresses and/or ranges are trusted by the organization.

### Rationale:

Defining trusted source IP addresses or ranges helps organizations create and enforce Conditional Access policies around those trusted or untrusted IP addresses and ranges. Users authenticating from trusted IP addresses and/or ranges may have less access restrictions or access requirements when compared to users that try to authenticate to Azure Active Directory from untrusted locations or untrusted source IP addresses/ranges.

### Impact:

When configuring `Named locations`, the organization can create locations using Geographical location data or by defining source IP addresses or ranges. Configuring `Named locations` using a Country location does not provide the organization the ability to mark those locations as trusted, and any Conditional Access policy relying on those `Countries location` setting will not be able to use the `All trusted locations` setting within the Conditional Access policy. They instead will have to rely on the `Select locations` setting. This may add additional resource requirements when configuring, and will require thorough organizational testing.

In general, Conditional Access policies may completely prevent users from authenticating to Azure Active Directory, and thorough testing is recommended. To avoid complete lockout, a 'Break Glass' account with full Global Administrator rights is recommended in the event all other administrators are locked out of authenticating to Azure Active Directory. This 'Break Glass' account should be excluded from Conditional Access Policies and should be configured with the longest pass phrase feasible. This account should only be used in the event of an emergency and complete administrator lockout.

## Audit:

### From Azure Portal

1. In the Azure Portal, navigate to Azure AD Conditional Access
2. Click on Named locations

Ensure there are IP ranges location settings configured and marked as Trusted

### From PowerShell

```
Get-AzureADMSNamedLocationPolicy
```

In the output from the above command, for each Named location group, make sure at least one entry contains the `IsTrusted` parameter with a value of `True`. Otherwise, if there is no output as a result of the above command or all of the entries contain the `IsTrusted` parameter with an empty value, a `NULL` value, or a value of `False`, the results are out of compliance with this check.

## Remediation:

### From Azure Portal

1. Navigate to the Azure AD Conditional Access Blade
2. Click on the Named locations blade
3. Within the Named locations blade, click on IP ranges location
4. Enter a name for this location setting in the Name text box
5. Click on the + sign
6. Add an IP Address Range in CIDR notation inside the text box that appears
7. Click on the Add button
8. Repeat steps 5 through 7 for each IP Range that needs to be added
9. If the information entered are trusted ranges, select the Mark as trusted location check box
10. Once finished, click on Create

### From PowerShell

Create a new trusted IP-based Named location policy

```
[System.Collections.Generic.List`1[Microsoft.Open.MSGraph.Model.IpRange]]$ipRanges = @()
$ipRanges.Add("<first IP range in CIDR notation>")
$ipRanges.Add("<second IP range in CIDR notation>")
$ipRanges.Add("<third IP range in CIDR notation>")
New-AzureADMSNamedLocationPolicy -OdataType
"#microsoft.graph.ipNamedLocation" -DisplayName "<name of IP Named location
policy>" -IsTrusted $true -IpRanges $ipRanges
```

Set an existing IP-based Named location policy to trusted

```
Set-AzureADMSNamedLocationPolicy -PolicyId "<ID of the policy>" -OdataType
"#microsoft.graph.ipNamedLocation" -IsTrusted $true
```

## Default Value:

By default, no locations are configured under the `Named locations` blade within the Azure AD Conditional Access blade.

## References:

1. <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/location-condition>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-7-restrict-resource-access-based-on--conditions>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.7 Centralize Access Control</b> Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v8	<b>12.2 Establish and Maintain a Secure Network Architecture</b> Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	<b>11.1 Maintain Standard Security Configurations for Network Devices</b> Maintain standard, documented security configuration standards for all authorized network devices.		●	●

## 1.2.2 Ensure that an exclusionary Geographic Access Policy is considered (Manual)

### Profile Applicability:

- Level 1

### Description:

**CAUTION:** If these policies are created without first auditing and testing the result, misconfiguration can potentially lock out administrators or create undesired access issues.

Conditional Access Policies can be used to block access from geographic locations that are deemed out-of-scope for your organization or application. The scope and variables for this policy should be carefully examined and defined.

### Rationale:

Conditional Access, when used as a deny list for the tenant or subscription, is able to prevent ingress or egress of traffic to countries that are outside of the scope of interest (e.g.: customers, suppliers) or jurisdiction of an organization. This is an effective way to prevent unnecessary and long-lasting exposure to international threats such as APTs.

### Impact:

Azure AD Premium is required. Limiting access geographically will deny access to users that are traveling or working remotely in a different part of the world. A point-to-site or site to site tunnel such as a VPN is recommended to address exceptions to geographic access policies.

### Audit:

#### From Azure Portal

1. From Azure Home open the Portal menu in the top left, and select `Azure Active Directory`.
2. Scroll down in the menu on the left, and select `Security`.
3. Select on the left side `Conditional Access`.
4. Select the policy you wish to audit, then:
  - Under `Assignments`, Review the `Users and Groups` for the personnel the policy will apply to
  - Under `Assignments`, Review the `Cloud apps or actions` for the systems the policy will apply to
  - Under `Conditions`, Review the `Include locations` for those that should be **blocked**

- Under `Conditions`, Review the `Exclude` locations for those that should be allowed (Note: locations set up in the previous recommendation for `Trusted Location` should be in the `Exclude` list.)
- Under `Access Controls > Grant - Confirm` that `Block Access` is selected.

## From Azure CLI

As of this writing there are no subcommands for Conditional Access Policies within the Azure CLI

## From PowerShell

```
$conditionalAccessPolicies = Get-AzureADMSConditionalAccessPolicy

foreach($policy in $conditionalAccessPolicies) {$policy | Select-Object
@{N='Policy ID'; E={$policy.id}}, @{N="Included Locations";
E={$policy.Conditions.Locations.IncludeLocations}}, @{N="Excluded Locations";
E={$policy.Conditions.Locations.ExcludeLocations}}, @{N="BuiltIn
GrantControls"; E={$policy.GrantControls.BuiltInControls}}}
```

Make sure there is at least 1 row in the output of the above PowerShell command that contains `Block` under the `BuiltIn GrantControls` column and location IDs under the `Included Locations` and `Excluded Locations` columns. If not, a policy containing these options has not been created and is considered a finding.

## Remediation:

### From Azure Portal

Part 1 of 2 - Create the policy and enable it in `Report-only` mode.

1. From Azure Home open the portal menu in the top left, and select `Azure Active Directory`.
2. Scroll down in the menu on the left, and select `Security`.
3. Select on the left side `Conditional Access`.
4. Click the `+ New policy` button, then:
5. Provide a name for the policy.
6. Under `Assignments`, select `Users` or workload identities then:
  - Under `Include`, select `All users`
  - Under `Exclude`, check `Users and groups` and only select emergency access accounts and service accounts (**NOTE:** Service accounts are excluded here because service accounts are non-interactive and cannot complete MFA)
7. Under `Assignments`, select `Cloud apps or actions` then:
  - Under `Include`, select `All cloud apps`
  - Leave `Exclude` blank unless you have a well defined exception
8. Under `Conditions`, select `Locations` then:
  - Select `Include`, then add entries for locations for those that should be **blocked**
  - Select `Exclude`, then add entries for those that should be allowed (**IMPORTANT:** Ensure that all `Trusted Locations` are in the `Exclude` list.)

9. Under `Access Controls`, select `Grant and Confirm` that `Block Access` is selected.
10. Set `Enable policy` to `Report-only`.
11. Click `Create`.

**NOTE:** The policy is not yet 'live,' since `Report-only` is being used to audit the effect of the policy.

Part 2 of 2 - Confirm that the policy is not blocking access that should be granted, then toggle to `On`.

1. With your policy now in report-only mode, return to the Azure Active Directory blade and click on `Sign-in logs`.
2. Review the recent sign-in events - click an event then review the event details (specifically the `Report-only` tab) to ensure:
  - o The sign-in event you're reviewing occurred **after** turning on the policy in report-only mode
  - o The policy name from step 5 above is listed in the `Policy Name` column
  - o The `Result` column for the new policy shows that the policy was `Not applied` (indicating the location origin was not blocked)
3. If the above conditions are present, navigate back to the policy name in `Conditional Access` and open it.
4. Toggle the policy from `Report-only` to `On`.
5. Click `Save`.

### From PowerShell

First, set up the conditions objects values before updating an existing conditional access policy or before creating a new one. You may need to use additional PowerShell cmdlets to retrieve specific IDs such as the `Get-AzureADMSNamedLocationPolicy` which outputs the `Location IDs` for use with conditional access policies.

```

$conditions = New-Object -TypeName
Microsoft.Open.MSGraph.Model.ConditionalAccessConditionSet

$conditions.Applications = New-Object -TypeName
Microsoft.Open.MSGraph.Model.ConditionalAccessApplicationCondition
$conditions.Applications.IncludeApplications = <"All" | "Office365" | "app
ID" | @("app ID 1", "app ID 2", etc...)>
$conditions.Applications.ExcludeApplications = <"Office365" | "app ID" |
@("app ID 1", "app ID 2", etc...)>

$conditions.Users = New-Object -TypeName
Microsoft.Open.MSGraph.Model.ConditionalAccessUserCondition
$conditions.Users.IncludeUsers = <"All" | "None" | "GuestsOrExternalUsers" |
"Specific User ID" | @("User ID 1", "User ID 2", etc.)>
$conditions.Users.ExcludeUsers = <"GuestsOrExternalUsers" | "Specific User
ID" | @("User ID 1", "User ID 2", etc.)>
$conditions.Users.IncludeGroups = <"group ID" | "All" | @("Group ID 1",
"Group ID 2", etc...)>
$conditions.Users.ExcludeGroups = <"group ID" | @("Group ID 1", "Group ID 2",
etc...)>
$conditions.Users.IncludeRoles = <"Role ID" | "All" | @("Role ID 1", "Role ID
2", etc...)>
$conditions.Users.ExcludeRoles = <"Role ID" | @("Role ID 1", "Role ID 2",
etc...)>

$conditions.Locations = New-Object -TypeName
Microsoft.Open.MSGraph.Model.ConditionalAccessLocationCondition
$conditions.Locations.IncludeLocations = <"Location ID" | @("Location ID 1",
"Location ID 2", etc...) >
$conditions.Locations.ExcludeLocations = <"AllTrusted" | "Location ID" |
@("Location ID 1", "Location ID 2", etc...)>

$controls = New-Object -TypeName
Microsoft.Open.MSGraph.Model.ConditionalAccessGrantControls
$controls._Operator = "OR"
$controls.BuiltInControls = "block"

```

Next, update the existing conditional access policy with the condition set options configured with the previous commands.

```

Set-AzureADMSConditionalAccessPolicy -PolicyId <policy ID> -Conditions
$conditions -GrantControls $controls

```

To create a new conditional access policy that complies with this best practice, run the following commands after creating the condition set above

```

New-AzureADMSConditionalAccessPolicy -Name "Policy Name" -State
<enabled|disabled> -Conditions $conditions -GrantControls $controls

```

### Default Value:

This policy does not exist by default.

## References:

1. <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-location>
2. <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-report-only>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-7-restrict-resource-access-based-on--conditions>

## Additional Information:

These policies should be tested by using the What If tool in the References. Setting these can and will create issues with logging in for users until they use an MFA device linked to their accounts. Further testing can also be done via the insights and reporting resource in References which monitors Azure sign ins.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.7 Centralize Access Control</b> Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	<b>12.1 Maintain an Inventory of Network Boundaries</b> Maintain an up-to-date inventory of all of the organization's network boundaries.	●	●	●



## 1.2.3 Ensure that A Multi-factor Authentication Policy Exists for Administrative Groups (Manual)

### Profile Applicability:

- Level 1

### Description:

For designated users, they will be prompted to use their multi-factor authentication (MFA) process on login.

### Rationale:

Enabling multi-factor authentication is a recommended setting to limit the use of Administrative accounts to authenticated personnel.

### Impact:

There is an increased cost, as Conditional Access policies require Azure AD Premium. Similarly, MFA may require additional overhead to maintain. There is also a potential scenario in which the multi-factor authentication method can be lost, and administrative users are no longer able to log in. For this scenario, there should be an emergency access account. Please see References for creating this.

### Audit:

#### From Azure Portal

1. From Azure Home open the Portal Menu in the top left, and select `Azure Active Directory`.
2. Select `Security`.
3. Select `Conditional Access`.
4. Select the policy you wish to audit.
5. View under `Users and Groups` the corresponding users and groups to whom the policy is applied. Be certain the emergency access account is not in the list.
6. View under `Exclude` to determine which Users and groups to whom the policy is not applied.

### Remediation:

#### From Azure Portal

1. From Azure Home open the Portal Menu in top left, and select `Azure Active Directory`.
2. Select `Security`.
3. Select `Conditional Access`.
4. Click + `New policy`.

5. Enter a name for the policy.
6. Select `Users` or workload identities.
7. Check `Users` and groups.
8. Select administrative groups this policy should apply to and click `Select`.
9. Under `Exclude`, check `Users` and groups.
10. Select users this policy not should apply to and click `Select`.
11. Select `Cloud apps` or actions.
12. Select `All cloud apps`.
13. Select `Grant`.
14. Under `Grant access`, check `Require multifactor authentication` and click `Select`.
15. Set `Enable policy` to `Report-only`.
16. Click `Create`.

After testing the policy in report-only mode, update the `Enable policy` setting from `Report-only` to `On`.

### **Default Value:**

By default, MFA is not enabled for any administrative accounts.

### **References:**

1. <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-admin-mfa>
2. <https://docs.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access>
3. <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/troubleshoot-conditional-access-what-if>
4. <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-insights-reporting>
5. <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/plan-conditional-access>
6. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-7-restrict-resource-access-based-on--conditions>

### **Additional Information:**

These policies should be tested by using the What If tool in the References. Setting these can and will create issues with logging in for users until they use an MFA device linked to their accounts. Further testing can also be done via the insights and reporting resource in References which monitors Azure sign ins.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.3 <u>Require MFA for Externally-Exposed Applications</u></b> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	<b>6.4 <u>Require MFA for Remote Network Access</u></b> Require MFA for remote network access.	●	●	●
v8	<b>6.5 <u>Require MFA for Administrative Access</u></b> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v8	<b>6.7 <u>Centralize Access Control</u></b> Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	<b>4.5 <u>Use Multifactor Authentication For All Administrative Access</u></b> Use multi-factor authentication and encrypted channels for all administrative account access.		●	●
v7	<b>16.3 <u>Require Multi-factor Authentication</u></b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

## 1.2.4 Ensure that A Multi-factor Authentication Policy Exists for All Users (Manual)

### Profile Applicability:

- Level 1

### Description:

For designated users, they will be prompted to use their multi-factor authentication (MFA) process on logins.

### Rationale:

Enabling multi-factor authentication is a recommended setting to limit the potential of accounts being compromised and limiting access to authenticated personnel.

### Impact:

There is an increased cost, as Conditional Access policies require Azure AD Premium. Similarly, this may require additional overhead to maintain if users lose access to their MFA.

### Audit:

#### From Azure Portal

1. From Azure Home open the Portal Menu in the top left, and select `Azure Active Directory`.
2. Scroll down in the menu on the left, and select `Security`.
3. Select on the left side `Conditional Access`.
4. Select the policy you wish to audit.
5. View under `Users and Groups` the corresponding users and groups to whom the policy is applied.
6. View under `Exclude` to determine which users and groups to whom the policy is not applied.

### Remediation:

#### From Azure Portal

1. From Azure Home open Portal menu in the top left, and select `Azure Active Directory`.
2. Select `Security`.
3. Select `Conditional Access`.
4. Click `+ New policy`.
5. Enter a name for the policy.
6. Select `Users or workload identities`.

7. Under `Include`, select `All users`.
8. Under `Exclude`, check `Users and groups`.
9. Select users this policy should not apply to and click `Select`.
10. Select `Cloud apps or actions`.
11. Select `All cloud apps`.
12. Select `Grant`.
13. Under `Grant access`, check `Require multifactor authentication` and click `Select`.
14. Set `Enable policy to` `Report-only`.
15. Click `Create`.

After testing the policy in report-only mode, update the `Enable policy` setting from `Report-only` to `On`.

### Default Value:

MFA is not enabled by default.

### References:

1. <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-all-users-mfa>
2. <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/troubleshoot-conditional-access-what-if>
3. <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-insights-reporting>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-7-restrict-resource-access-based-on--conditions>

### Additional Information:

These policies should be tested by using the What If tool in the References. Setting these can and will create issues with logging in for users until they use an MFA device linked to their accounts. Further testing can also be done via the insights and reporting resource the in References which monitors Azure sign ins.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.3 Require MFA for Externally-Exposed Applications</b> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	<b>6.4 Require MFA for Remote Network Access</b> Require MFA for remote network access.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.7 Centralize Access Control</b> Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	<b>16.3 Require Multi-factor Authentication</b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

DRAFT

## 1.2.5 Ensure Multi-factor Authentication is Required for Risky Sign-ins (Manual)

### Profile Applicability:

- Level 1

### Description:

For designated users, they will be prompted to use their multi-factor authentication (MFA) process on login.

### Rationale:

Enabling multi-factor authentication is a recommended setting to limit the potential of accounts being compromised and limiting access to authenticated personnel.

### Impact:

There is an increased cost, as Conditional Access policies require Azure AD Premium. Similarly, they may require additional overhead to maintain if users lose access to their MFA.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu and select `Security`.
2. Select on the left side `Conditional Access`.
3. Select the policy you wish to audit.
4. View under `Users and Groups` the corresponding users and groups to whom the policy is applied.
5. View under `Exclude` to determine which users and groups to whom the policy is not applied.

### Remediation:

#### From Azure Portal

1. From Azure Home select the Portal Menu in the top left, and select `Azure Active Directory`.
2. Select `Security`
3. Select `Conditional Access`.
4. Click `+ New policy`.
5. Enter a name for the policy.
6. Select `Users or workload identities`.
7. Under `Include`, select `All users`.
8. Under `Exclude`, check `Users and groups`.

9. Select users this policy should not apply to and click `Select`.
10. Select `Cloud apps or actions`.
11. Select `All cloud apps`.
12. Select `Conditions`.
13. Select `Sign-in risk`.
14. Update the `Configure` toggle to `Yes`.
15. Check the sign-in risk level this policy should apply to, e.g. `High` and `Medium`.
16. Select `Done`.
17. Select `Grant`.
18. Under `Grant access`, check `Require multifactor authentication` and click `Select`.
19. Set `Enable policy` to `Report-only`.
20. Click `Create`.

After testing the policy in report-only mode, update the `Enable policy` setting from `Report-only` to `On`.

#### **Default Value:**

MFA is not enabled by default.

#### **References:**

1. <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-policy-risk>
2. <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/troubleshoot-conditional-access-what-if>
3. <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/howto-conditional-access-insights-reporting>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-7-restrict-resource-access-based-on--conditions>

#### **Additional Information:**

These policies should be tested by using the What If tool in the References. Setting these can and will create issues with logging in for users until they use an MFA device linked to their accounts. Further testing can also be done via the insights and reporting resource the in References which monitors Azure sign ins.



**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.3 <u>Require MFA for Externally-Exposed Applications</u></b> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	<b>6.4 <u>Require MFA for Remote Network Access</u></b> Require MFA for remote network access.	●	●	●
v8	<b>6.7 <u>Centralize Access Control</u></b> Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	<b>16.3 <u>Require Multi-factor Authentication</u></b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

DRAFT

## 1.2.6 Ensure Multi-factor Authentication is Required for Azure Management (Manual)

### Profile Applicability:

- Level 1

### Description:

For designated users, they will be prompted to use their multi-factor authentication (MFA) process on logins.

### Rationale:

Enabling multi-factor authentication is a recommended setting to limit the use of Administrative actions and to prevent intruders from changing settings.

### Impact:

There is an increased cost, as Conditional Access policies require Azure AD Premium. Similarly, they may require additional overhead to maintain if users lose access to their MFA.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu and select `Azure Active Directory`.
2. Scroll down in the menu on the left, and select `Security`.
3. Select on the left side `Conditional Access`.
4. Select the policy you wish to audit.
5. View under `Users and Groups` the corresponding users and groups to whom the policy is applied.
6. View under `Exclude` to determine which Users and groups to whom the policy is not applied.

### Remediation:

#### From Azure Portal

1. From Azure Home select the Portal Menu and select `Azure Active Directory`.
2. Select `Security`.
3. Select `Conditional Access`.
4. Click `+ New policy`.
5. Enter a name for the policy.
6. Select `Users or workload identities`.
7. Under `Include`, select `All users`.
8. Under `Exclude`, check `Users and groups`.

9. Select users this policy should not apply to and click `Select`.
10. Select `Cloud apps` or `actions`.
11. Select `Select apps`.
12. Check the box next to `Microsoft Azure Management` and click `Select`.
13. Select `Grant`.
14. Under `Grant access`, check `Require multifactor authentication` and click `Select`.
15. Set `Enable policy` to `Report-only`.
16. Click `Create`.

After testing the policy in report-only mode, update the `Enable policy` setting from `Report-only` to `On`.

### Default Value:

MFA is not enabled by default for administrative actions.

### References:

1. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-7-restrict-resource-access-based-on--conditions>
2. <https://docs.microsoft.com/en-us/azure/active-directory/conditional-access/concept-conditional-access-users-groups>

### Additional Information:

These policies should be tested by using the What If tool in the References. Setting these can and will create issues with administrators changing settings until they use an MFA device linked to their accounts. An emergency access account is recommended for this eventuality if all administrators are locked out. Please see the documentation in the references for further information. Similarly further testing can also be done via the insights and reporting resource in References which monitors Azure sign ins.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.3 <u>Require MFA for Externally-Exposed Applications</u></b> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	<b>6.4 <u>Require MFA for Remote Network Access</u></b> Require MFA for remote network access.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.5 <u>Require MFA for Administrative Access</u></b> Require MFA for all administrative access accounts, where supported, on all enterprise assets, whether managed on-site or through a third-party provider.	●	●	●
v8	<b>6.7 <u>Centralize Access Control</u></b> Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	<b>4.5 <u>Use Multifactor Authentication For All Administrative Access</u></b> Use multi-factor authentication and encrypted channels for all administrative account access.		●	●
v7	<b>16.3 <u>Require Multi-factor Authentication</u></b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

DRAFT

## 1.3 Ensure that 'Users can create Azure AD Tenants' is set to 'No' (Automated)

### Profile Applicability:

- Level 1

### Description:

Require administrators or appropriately delegated users to create new tenants.

### Rationale:

It is recommended to only allow an administrator to create new tenants. This prevent users from creating new Azure AD or Azure AD B2C tenants and ensures that only authorized users are able to do so.

### Impact:

Enforcing this setting will ensure that only authorized users are able to create new tenants.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Select Users
4. Select User settings
5. Ensure that Users can create Azure AD Tenants is set to No

*Please note that at this point of time, there is no Azure CLI or other API commands available to programmatically conduct security assessment for this recommendation.*

### Remediation:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Select Users
4. Select User settings
5. Set Users can create Azure AD Tenants to No

### References:

1. <https://learn.microsoft.com/en-us/azure/active-directory/fundamentals/users-default-permissions>

2. <https://learn.microsoft.com/en-us/azure/active-directory/roles/permissions-reference#tenant-creator>

DRAFT

## 1.4 Ensure Access Review is Set Up for External Users in Azure AD Privileged Identity Management (Manual)

### Profile Applicability:

- Level 2

### Description:

This recommendation extends guest access review by utilizing the Azure AD Privileged Identity Management feature provided in Azure AD Premium P2.

Azure AD is extended to include Azure AD B2B collaboration, allowing you to invite people from outside your organization to be guest users in your cloud account and sign in with their own work, school, or social identities. Guest users allow you to share your company's applications and services with users from any other organization, while maintaining control over your own corporate data.

Work with external partners, large or small, even if they don't have Azure AD or an IT department. A simple invitation and redemption process lets partners use their own credentials to access your company's resources as a guest user.

### Rationale:

Guest users in the Azure AD are generally required for collaboration purposes in Office 365, and may also be required for Azure functions in enterprises with multiple Azure tenants. Guest users should be reviewed on a regular basis, at least annually. Guest users should not be granted administrative roles where possible.

Guest users are typically added outside your employee on-boarding/off-boarding process and could potentially be overlooked indefinitely, leading to a potential vulnerability.

Guest users should be reviewed on a monthly basis to ensure that inactive and unneeded accounts are removed.

### Impact:

Until you have a business need to provide guest access to any user, avoid creating guest users. If guest accounts are being used, they should be removed when no longer required.

### Audit:

#### From Azure Portal

1. From the Azure Portal home page click the portal menu in the top left.
2. Select `Azure Active Directory`
3. Select `Users` in the left column under the `Manage` heading.
4. Next to the search box select the `filter` option.

5. Search for and select `User Type`
6. In the third drop down Value select `Guest`.
7. Review the guest users in your `Active Directory`.

### From Azure CLI

Run the following command:

```
az ad user list --filter "UserType eq 'Guest'"
```

### From PowerShell

Run the following command:

```
Get-AzureADUser -Filter "UserType eq 'Guest'"
```

### Remediation:

#### From Azure Portal

1. From the Azure Portal home page click the portal menu in the top left.
2. Select `Azure Active Directory`
3. Select `Users` in the left column under the `Manage` heading.
4. Next to the search box select the `filter` option.
5. Search for and select `User Type`
6. In the third drop down Value select `Guest`.
7. Review the guest users in your `Active Directory`.
8. For those you wish to delete, select the checkbox on the left then the `Delete` option in the top row.

### From Azure CLI

With the information from the audit procedure, to remove a Guest user run the following command with their User Principal Value.

```
Remove-AzureADUser -ObjectId "<UserPrincipalName@emailaddress.com>"
```

### From PowerShell

With the information from the audit procedure, to remove a Guest user run the following command with their User Principal Value.

```
Remove-AzureADUser -ObjectId "<UserPrincipalName@emailaddress.com>"
```

### Default Value:

By default no guest users are created.

### References:

1. <https://docs.microsoft.com/en-us/azure/active-directory/b2b/user-properties>
2. <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory#delete-a-user>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-3-review-and-reconcile-user-access-regularly>



4. <https://docs.microsoft.com/en-us/azure/active-directory/governance/manage-guest-access-with-access-reviews>
5. <https://www.microsoft.com/en-us/security/business/identity-access-management/azure-ad-pricing>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>5.1 <u>Establish and Maintain an Inventory of Accounts</u></b>            Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.</p>	●	●	●
v8	<p><b>5.3 <u>Disable Dormant Accounts</u></b>            Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.</p>	●	●	●
v8	<p><b>6.2 <u>Establish an Access Revoking Process</u></b>            Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.</p>	●	●	●
v8	<p><b>6.8 <u>Define and Maintain Role-Based Access Control</u></b>            Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.</p>			●
v7	<p><b>16.6 <u>Maintain an Inventory of Accounts</u></b>            Maintain an inventory of all accounts organized by authentication system.</p>		●	●
v7	<p><b>16.8 <u>Disable Any Unassociated Accounts</u></b>            Disable any account that cannot be associated with a business process or business owner.</p>	●	●	●

## 1.5 Ensure Guest Users Are Reviewed on a Regular Basis (Manual)

### Profile Applicability:

- Level 1

### Description:

Azure AD is extended to include Azure AD B2B collaboration, allowing you to invite people from outside your organization to be guest users in your cloud account and sign in with their own work, school, or social identities. Guest users allow you to share your company's applications and services with users from any other organization, while maintaining control over your own corporate data.

Work with external partners, large or small, even if they don't have Azure AD or an IT department. A simple invitation and redemption process lets partners use their own credentials to access your company's resources as a guest user.

Guest users in every subscription should be review on a regular basis to ensure that inactive and unneeded accounts are removed.

### Rationale:

Guest users in the Azure AD are generally required for collaboration purposes in Office 365, and may also be required for Azure functions in enterprises with multiple Azure tenants. Guest users are typically added outside your employee on-boarding/off-boarding process and could potentially be overlooked indefinitely, leading to a potential vulnerability. To prevent this, guest users should be reviewed on a regular basis. During this audit, guest users should also be determined to not have administrative privileges.

### Impact:

Before removing guest users, determine their use and scope. Like removing any user, there may be unforeseen consequences to systems if it is deleted.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Select Users
4. Click on Add filter
5. Select User type
6. Select Guest from the Value dropdown
7. Click Apply
8. Audit the listed guest users

## From Azure CLI

```
az ad user list --query "[?userType=='Guest']"
```

Ensure all users listed are still required and not inactive.

## From Azure PowerShell

```
Get-AzureADUser |Where-Object {$_.UserType -like "Guest"} |Select-Object  
DisplayName, UserPrincipalName, UserType -Unique
```

## Remediation:

### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Select Users
4. Click on Add filter
5. Select User type
6. Select Guest from the Value dropdown
7. Click Apply
8. Delete all Guest users that are no longer required or are inactive

## From Azure CLI

Before deleting the user, set it to inactive using the ID from the Audit Procedure to determine if there are any dependent systems.

```
az ad user update --id <exampleaccountid@domain.com> --account-enabled  
{false}
```

After determining that there are no dependent systems delete the user.

```
Remove-AzureADUser -ObjectId <exampleaccountid@domain.com>
```

## From Azure PowerShell

Before deleting the user, set it to inactive using the ID from the Audit Procedure to determine if there are any dependent systems.

```
Set-AzureADUser -ObjectId "<exampleaccountid@domain.com>" -AccountEnabled  
false
```

After determining that there are no dependent systems delete the user.

```
PS C:\>Remove-AzureADUser -ObjectId <exampleaccountid@domain.com>
```

## Default Value:

By default no guest users are created.

## References:

1. <https://docs.microsoft.com/en-us/azure/active-directory/b2b/user-properties>
2. <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/add-users-azure-active-directory#delete-a-user>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-3-review-and-reconcile-user-access-regularly>
4. <https://www.microsoft.com/en-us/security/business/identity-access-management/azure-ad-pricing>
5. <https://docs.microsoft.com/en-us/azure/active-directory/reports-monitoring/howto-manage-inactive-user-accounts>
6. <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-users-restore>

## Additional Information:

It is good practice to use a dynamic group to manage guest users.

To create the dynamic group:

1. Navigate to the 'Active Directory' blade in the Azure Portal
2. Select the 'Groups' item
3. Create new
4. Type of 'dynamic'
5. Use the following dynamic selection rule. "(user.userType -eq "Guest")"
6. Once the group has been created, select access reviews option and create a new access review with a period of monthly and send to relevant administrators for review.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.1 Establish and Maintain an Inventory of Accounts</b> Establish and maintain an inventory of all accounts managed in the enterprise. The inventory must include both user and administrator accounts. The inventory, at a minimum, should contain the person's name, username, start/stop dates, and department. Validate that all active accounts are authorized, on a recurring schedule at a minimum quarterly, or more frequently.	●	●	●
v8	<b>5.3 Disable Dormant Accounts</b> Delete or disable any dormant accounts after a period of 45 days of inactivity, where supported.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>6.2 <u>Establish an Access Revoking Process</u></b>            Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.</p>	●	●	●
v8	<p><b>6.8 <u>Define and Maintain Role-Based Access Control</u></b>            Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.</p>			●
v7	<p><b>16.6 <u>Maintain an Inventory of Accounts</u></b>            Maintain an inventory of all accounts organized by authentication system.</p>		●	●
v7	<p><b>16.8 <u>Disable Any Unassociated Accounts</u></b>            Disable any account that cannot be associated with a business process or business owner.</p>	●	●	●

DRAFT

## *1.6 Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is 'Disabled' (Manual)*

### **Profile Applicability:**

- Level 1

### **Description:**

Do not allow users to remember multi-factor authentication on devices.

### **Rationale:**

Remembering Multi-Factor Authentication (MFA) for devices and browsers allows users to have the option to bypass MFA for a set number of days after performing a successful sign-in using MFA. This can enhance usability by minimizing the number of times a user may need to perform two-step verification on the same device. However, if an account or device is compromised, remembering MFA for trusted devices may affect security. Hence, it is recommended that users not be allowed to bypass MFA.

### **Impact:**

For every login attempt, the user will be required to perform multi-factor authentication.

### **Audit:**

#### **From Azure Portal**

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Select Users
4. Click the Per-user MFA button on the top bar
5. Click on service settings
6. Ensure that Allow users to remember multi-factor authentication on devices they trust is not enabled

### **Remediation:**

#### **From Azure Portal**

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Select Users
4. Click the Per-user MFA button on the top bar
5. Click on service settings
6. Uncheck the box next to Allow users to remember multi-factor authentication on devices they trust

## Default Value:

By default, Allow users to remember multi-factor authentication on devices they trust is disabled.

## References:

1. <https://docs.microsoft.com/en-us/azure/multi-factor-authentication/multi-factor-authentication-whats-next#remember-multi-factor-authentication-for-devices-that-users-trust>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-6-use-strong-authentication-controls>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.3 Require MFA for Externally-Exposed Applications</b> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	<b>6.4 Require MFA for Remote Network Access</b> Require MFA for remote network access.	●	●	●
v7	<b>16.3 Require Multi-factor Authentication</b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

## 1.7 Ensure That 'Number of methods required to reset' is set to '2' (Manual)

### Profile Applicability:

- Level 1

### Description:

Ensures that two alternate forms of identification are provided before allowing a password reset.

### Rationale:

A Self-service Password Reset (SSPR) through Azure Multi-factor Authentication (MFA) ensures the user's identity is confirmed using two separate methods of identification. With multiple methods set, an attacker would have to compromise both methods before they could maliciously reset a user's password.

### Impact:

There may be administrative overhead, as users who lose access to their secondary authentication methods will need an administrator with permissions to remove it. There will also need to be organization-wide security policies and training to teach administrators to verify the identity of the requesting user so that social engineering can not render this setting useless.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Then Users
4. Select Password reset
5. Then Authentication methods
6. Ensure that Number of methods required to reset is set to 2

### Remediation:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Then Users
4. Select Password reset
5. Then Authentication methods
6. Set the Number of methods required to reset to 2



## Default Value:

By default, the `Number of methods required to reset` is set to "2".

## References:

1. <https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr>
2. <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-registration-mfa-sspr-combined>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-4-use-strong-authentication-controls-for-all-azure-active-directory-based-access>
4. <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-passwords-faq#password-reset-registration>
5. <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment>
6. <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.3 <u>Require MFA for Externally-Exposed Applications</u></b> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	<b>6.4 <u>Require MFA for Remote Network Access</u></b> Require MFA for remote network access.	●	●	●
v7	<b>16.3 <u>Require Multi-factor Authentication</u></b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

## 1.8 Ensure that a Custom Bad Password List is set to 'Enforce' for your Organization (Manual)

### Profile Applicability:

- Level 1

### Description:

Microsoft Azure creates a default bad password policy that is already applied to Azure administrative and normal user accounts. This is not applied to user accounts that are synced from an on-premise Active Directory unless Azure AD Connect is used and you enable `EnforceCloudPasswordPolicyForPasswordSyncedUsers`. Please see the list in default values on the specifics of this policy.

### Rationale:

Enabling this gives your organization further customization on what secure passwords are allowed. Setting a bad password list enables your organization to fine-tune its password policy further, depending on your needs. Removing easy-to-guess passwords increases the security of access to your Azure resources.

### Impact:

Increasing needed password complexity might increase overhead on administration of user accounts.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Azure Active directory`.
3. Select 'Security'.
4. Under `Manage`, select `Authentication Methods`.
5. Select `Password Protection`.
6. Ensure `Enforce custom list` is set to `Yes`.
7. Scroll through the list to view the enforced passwords.

### Remediation:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Azure Active Directory`
3. Select `Security`.
4. Under `Manage`, select `Authentication Methods`.
5. Select `Password Protection`.

6. Set the `Enforce custom list` option to `Yes`.
7. Double click the custom banned password list to add a string.

### Default Value:

By default the custom bad password list is not 'Enabled'. Organizational-specific terms can be added to the custom banned password list, such as the following examples:

- Brand names
- Product names
- Locations, such as company headquarters
- Company-specific internal terms
- Abbreviations that have specific company meaning
- Months and weekdays with your company's local languages

The default Azure bad password policy is already applied to your resources which applies the following basic requirements:

### Characters allowed:

- Uppercase characters (A - Z)
- Lowercase characters (a - z)
- Numbers (0 - 9)
- Symbols:  
@ # \$ % ^ & \* - \_ ! + = [ ] { } | \ : ' , . ? / ` ~ " ( ) ; < >
- blank space

### Characters not allowed:

- Unicode characters
- Password length Passwords require
- A minimum of eight characters
- A maximum of 256 characters

**Password complexity:** Passwords require three out of four of the following categories:

- Uppercase characters
- Lowercase characters
- Numbers
- Symbols Note: Password complexity check isn't required for Education tenants.

### Password not recently used:

- When a user changes or resets their password, the new password can't be the same as the current or recently used passwords.
- Password isn't banned by Azure AD Password Protection.

- The password can't be on the global list of banned passwords for Azure AD Password Protection, or on the customizable list of banned passwords specific to your organization.

**References:**

1. <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad-combined-policy>
2. <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-password-ban-bad>
3. <https://docs.microsoft.com/en-us/powershell/module/Azuread/>
4. <https://www.microsoft.com/en-us/research/publication/password-guidance/>
5. <https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-configure-custom-password-protection>
6. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-6-use-strong-authentication-controls>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.2 Use Unique Passwords</b> Use unique passwords for all enterprise assets. Best practice implementation includes, at a minimum, an 8-character password for accounts using MFA and a 14-character password for accounts not using MFA.	●	●	●
v8	<b>6.7 Centralize Access Control</b> Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	<b>4.4 Use Unique Passwords</b> Where multi-factor authentication is not supported (such as local administrator, root, or service accounts), accounts will use passwords that are unique to that system.		●	●

## *1.9 Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0' (Manual)*

### **Profile Applicability:**

- Level 1

### **Description:**

Ensure that the number of days before users are asked to re-confirm their authentication information is not set to 0.

### **Rationale:**

This setting is necessary if you have setup 'Require users to register when signing in option'. If authentication re-confirmation is disabled, registered users will never be prompted to re-confirm their existing authentication information. If the authentication information for a user changes, such as a phone number or email, then the password reset information for that user reverts to the previously registered authentication information.

### **Impact:**

Users will be prompted for their multifactor authentication at the duration set here.

### **Audit:**

#### **From Azure Portal**

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Then Users
4. Select Password reset
5. Then Registration
6. Ensure that Number of days before users are asked to re-confirm their authentication information is not set to 0

### **Remediation:**

#### **From Azure Portal**

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Then Users
4. Select Password reset
5. Then Registration
6. Set the Number of days before users are asked to re-confirm their authentication information to your organization-defined frequency.






## Default Value:

By default, the Number of days before users are asked to re-confirm their authentication information is set to "180 days".

## References:

1. <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-passwords-how-it-works#registration>
2. <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-6-define-identity-and-privileged-access-strategy>
4. <https://docs.microsoft.com/en-us/azure/active-directory/authentication/concept-authentication-methods>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.2 <u>Establish an Access Revoking Process</u></b> Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v7	<b>16.10 <u>Ensure All Accounts Have An Expiration Date</u></b> Ensure that all accounts have an expiration date that is monitored and enforced.			

## 1.10 Ensure that 'Notify users on password resets?' is set to 'Yes' (Manual)

### Profile Applicability:

- Level 1

### Description:

Ensure that users are notified on their primary and secondary emails on password resets.

### Rationale:

User notification on password reset is a passive way of confirming password reset activity. It helps the user to recognize unauthorized password reset activities.

### Impact:

Users will receive emails alerting them to password changes to both their primary and secondary emails.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Select Users
4. Go to Password reset
5. Under Manage, select Notifications
6. Ensure that Notify users on password resets? is set to Yes

### Remediation:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Select Users
4. Select Password reset
5. Under Manage, select Notifications
6. Set Notify users on password resets? to Yes

### Default Value:

By default, Notify users on password resets? is set to "Yes".

## References:

1. <https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr#set-up-notifications-and-customizations>
2. <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-passwords-how-it-works#notifications>
3. <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-6-define-identity-and-privileged-access-strategy>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.7 Centralize Access Control</b> Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.		●	●
v7	<b>16.2 Configure Centralized Point of Authentication</b> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●



## 1.11 Ensure That 'Notify all admins when other admins reset their password?' is set to 'Yes' (Manual)

### Profile Applicability:

- Level 1

### Description:

Ensure that all administrators are notified if any other administrator resets their password.

### Rationale:

Administrator accounts are sensitive. Any password reset activity notification, when sent to all administrators, ensures that all administrators can passively confirm if such a reset is a common pattern within their group. For example, if all administrators change their password every 30 days, any password reset activity before that may require administrator(s) to evaluate any unusual activity and confirm its origin.

### Impact:

All other Admins will receive a notification from Azure every time a password is reset. This is useful for auditing procedures to confirm that there are no out of the ordinary password resets for Admins. There is additional overhead, however, in the time required for Admins to audit the notifications. This setting is only useful if all Admins pay attention to the notifications, and audit each one.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Select Users
4. Select Password reset
5. Under Manage, select Notifications
6. Ensure that notify all admins when other admins reset their password? is set to Yes

### Remediation:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Select Users
4. Select Password reset

5. Under Manage, select `Notifications`
6. Set `Notify all admins when other admins reset their password?` to `Yes`

**Default Value:**

By default, `Notify all admins when other admins reset their password?` is set to "No".

**References:**

1. <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-passwords-how-it-works#notifications>
2. <https://docs.microsoft.com/en-us/azure/active-directory/authentication/howto-sspr-deployment>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-6-define-identity-and-privileged-access-strategy>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-1-protect-and-limit-highly-privileged-users>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems>
6. <https://docs.microsoft.com/en-us/azure/active-directory/authentication/tutorial-enable-sspr#set-up-notifications-and-customizations>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u></b>            Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.</p>	●	●	●
v8	<p><b>6.7 <u>Centralize Access Control</u></b>            Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.</p>		●	●
v7	<p><b>4.8 <u>Log and Alert on Changes to Administrative Group Membership</u></b>            Configure systems to issue a log entry and alert when an account is added to or removed from any group assigned administrative privileges.</p>		●	●

## 1.12 Ensure that 'Users can consent to apps accessing company data on their behalf' is set to 'No' (Manual)

### Profile Applicability:

- Level 1

### Description:

Require administrators to provide consent for the apps before use.

### Rationale:

Unless Azure Active Directory is running as an identity provider for third-party applications, do not allow users to use their identity outside of the cloud environment. User profiles contain private information such as phone numbers and email addresses which could then be sold off to other third parties without requiring any further consent from the user.

### Impact:

Enforcing this setting may create additional requests that administrators need to fulfill quite often.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Then Users
4. Select User settings
5. Then on Manage how end users launch and view their applications
6. Under the Enterprise applications heading ensure that Users can consent to apps accessing company data on their behalf is set to No

#### From PowerShell

```
Connect-MsolService  
Get-MsolCompanyInformation | Select-Object  
UsersPermissionToUserConsentToAppEnabled
```

Command should return UsersPermissionToUserConsentToAppEnabled with the value of False

### Remediation:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory

3. Then Users
4. Select User settings
5. Then Manage how end users launch and view their applications
6. Under the Enterprise applications heading, set Users can consent to apps accessing company data on their behalf to No

**Default Value:**

By default, Users can consent to apps accessing company data on their behalf is set to Yes.

**References:**

1. <https://nicksnettravels.builttoroam.com/post/2017/01/24/Admin-Consent-for-Permissions-in-Azure-Active-Directory.aspx>
2. <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent#configure-user-consent-to-applications>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-1-protect-and-limit-highly-privileged-users>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-2-define-enterprise-segmentation-strategy>
6. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-6-define-identity-and-privileged-access-strategy>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>2.3 Address Unauthorized Software</b> Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v8	<b>6.1 Establish an Access Granting Process</b> Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.			
v8	<b>6.7 Centralize Access Control</b> Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.			
v7	<b>2.6 Address unapproved software</b> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			

## 1.13 Ensure That 'Users Can Consent to Apps Accessing Company Data on Their Behalf' Is Set To 'Allow for Verified Publishers' (Manual)

### Profile Applicability:

- Level 2

### Description:

Allow users to provide consent for selected permissions when a request is coming from a verified publisher.

### Rationale:

Unless Azure Active Directory is running as an identity provider for third-party applications, do not allow users to use their identity outside of the cloud environment. User profiles contain private information such as phone numbers and email addresses which could then be sold off to other third parties without requiring any further consent from the user.

### Impact:

Enforcing this setting may create additional requests that administrators need to fulfill quite often.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Select Users
4. Select User settings
5. Select Manage how end users launch and view their applications
6. Select Consent and permissions
7. Under User consent for applications, **ensure** Allow user consent for apps from verified publishers, for selected permissions **is selected**

#### From PowerShell

```
Connect-MsolService
Get-MsolCompanyInformation | Select-Object
UsersPermissionToUserConsentToAppEnabled
```

Command should return `UsersPermissionToUserConsentToAppEnabled` with the value of `False`

## Remediation:

### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Select Users
4. Select User settings
5. Select Manage how end users launch and view their applications
6. Select Consent and permissions
7. Under User consent for applications, select Allow user consent for apps from verified publishers, for selected permissions
8. Select Save

### From PowerShell

```
Connect-MsolService  
Set-MsolCompanyInformation --UsersPermissionToUserConsentToAppEnabled $False
```

### Default Value:

By default, Users can consent to apps accessing company data on their behalf is set to Yes.

### References:

1. <https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-user-consent#configure-user-consent-to-applications>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-1-protect-and-limit-highly-privileged-users>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-2-define-enterprise-segmentation-strategy>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-6-define-identity-and-privileged-access-strategy>
6. <https://docs.microsoft.com/en-us/powershell/module/msonline/set-msolcompanysettings?view=azureadps-1.0>
7. <https://docs.microsoft.com/en-us/powershell/module/msonline/get-msolcompanyinformation?view=azureadps-1.0>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>2.3 <u>Address Unauthorized Software</u></b>            Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.</p>	●	●	●
v8	<p><b>2.5 <u>Allowlist Authorized Software</u></b>            Use technical controls, such as application allowlisting, to ensure that only authorized software can execute or be accessed. Reassess bi-annually, or more frequently.</p>		●	●
v8	<p><b>6.1 <u>Establish an Access Granting Process</u></b>            Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.</p>	●	●	●
v8	<p><b>6.7 <u>Centralize Access Control</u></b>            Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.</p>		●	●
v7	<p><b>2.6 <u>Address unapproved software</u></b>            Ensure that unauthorized software is either removed or the inventory is updated in a timely manner</p>	●	●	●
v7	<p><b>2.7 <u>Utilize Application Whitelisting</u></b>            Utilize application whitelisting technology on all assets to ensure that only authorized software executes and all unauthorized software is blocked from executing on assets.</p>			●

## 1.14 Ensure that 'Users can add gallery apps to My Apps' is set to 'No' (Manual)

### Profile Applicability:

- Level 1

### Description:

Require administrators to provide consent for the apps before use.

### Rationale:

Unless Azure Active Directory is running as an identity provider for third-party applications, do not allow users to use their identity outside of your cloud environment. User profiles contain private information such as phone numbers and email addresses which could then be sold off to other third parties without requiring any further consent from the user.

### Impact:

Can cause additional requests to administrators that need to be fulfilled quite often.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Then Users
4. Select User settings
5. Then Manage how end users launch and view their applications, and ensure that Users can add gallery apps to My Apps is set to No

### Remediation:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Then Users
4. Select User settings
5. Then Manage how end users launch and view their applications
6. Set Users can add gallery apps to My Apps to No

### Default Value:











By default, Users can add gallery apps to My Apps is set to No.



## References:

1. <https://blogs.msdn.microsoft.com/exchangedev/2014/06/05/managing-user-consent-for-applications-using-office-365-apis/>
2. <https://nicksnettravels.builttoroam.com/post/2017/01/24/Admin-Consent-for-Permissions-in-Azure-Active-Directory.aspx>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-1-define-asset-management-and-data-protection-strategy>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-1-protect-and-limit-highly-privileged-users>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>2.3 Address Unauthorized Software</b> Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.			
v8	<b>2.4 Utilize Automated Software Inventory Tools</b> Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.			
v7	<b>2.3 Utilize Software Inventory Tools</b> Utilize software inventory tools throughout the organization to automate the documentation of all software on business systems.			
v7	<b>2.6 Address unapproved software</b> Ensure that unauthorized software is either removed or the inventory is updated in a timely manner			

## 1.15 Ensure That 'Users Can Register Applications' Is Set to 'No' (Manual)

### Profile Applicability:

- Level 1

### Description:

Require administrators or appropriately delegated users to register third-party applications.

### Rationale:

It is recommended to only allow an administrator to register custom-developed applications. This ensures that the application undergoes a formal security review and approval process prior to exposing Azure Active Directory data. Certain users like developers or other high-request users may also be delegated permissions to prevent them from waiting on an administrative user. Your organization should review your policies and decide your needs.

### Impact:

Enforcing this setting will create additional requests for approval that will need to be addressed by an administrator. If permissions are delegated, a user may approve a malevolent third party application, potentially giving it access to your data.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Select Users
4. Select User settings
5. Ensure that Users can register applications is set to No

#### From PowerShell

```
Connect-MsolService  
Get-MsolCompanyInformation | Select-Object  
UsersPermissionToCreateLOBAppsEnabled
```

Command should return UsersPermissionToCreateLOBAppsEnabled with the value of False

## Remediation:

### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Select Users
4. Select User settings
5. Set Users can register applications to No

### From PowerShell

```
Connect-MsolService  
Set-MsolCompanyInformation -UsersPermissionToCreateLOBAppsEnabled $False
```

### Default Value:

By default, Users can register applications is set to "Yes".

### References:

1. <https://docs.microsoft.com/en-us/azure/active-directory/roles/delegate-app-roles#restrict-who-can-create-applications>
2. <https://docs.microsoft.com/en-us/azure/active-directory/develop/active-directory-how-applications-are-added#who-has-permission-to-add-applications-to-my-azure-ad-instance>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-1-define-asset-management-and-data-protection-strategy>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-1-protect-and-limit-highly-privileged-users>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems>
6. <https://blogs.msdn.microsoft.com/exchangedev/2014/06/05/managing-user-consent-for-applications-using-office-365-apis/>
7. <https://nicksnettravels.builttoroam.com/post/2017/01/24/Admin-Consent-for-Permissions-in-Azure-Active-Directory.aspx>
8. <https://docs.microsoft.com/en-us/powershell/module/msonline/get-msolcompanyinformation?view=azureadps-1.0>
9. <https://docs.microsoft.com/en-us/powershell/module/msonline/set-msolcompanysettings?view=azureadps-1.0>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>2.3 <u>Address Unauthorized Software</u></b>            Ensure that unauthorized software is either removed from use on enterprise assets or receives a documented exception. Review monthly, or more frequently.</p>	●	●	●
v8	<p><b>2.4 <u>Utilize Automated Software Inventory Tools</u></b>            Utilize software inventory tools, when possible, throughout the enterprise to automate the discovery and documentation of installed software.</p>		●	●
v8	<p><b>6.7 <u>Centralize Access Control</u></b>            Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.</p>		●	●
v7	<p><b>2.6 <u>Address unapproved software</u></b>            Ensure that unauthorized software is either removed or the inventory is updated in a timely manner</p>	●	●	●

DRAFT

## *1.16 Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects' (Manual)*

### **Profile Applicability:**

- Level 1

### **Description:**

Limit guest user permissions.

### **Rationale:**

Limiting guest access ensures that guest accounts do not have permission for certain directory tasks, such as enumerating users, groups or other directory resources, and cannot be assigned to administrative roles in your directory. Guest access has three levels of restriction.

1. Guest users have the same access as members (most inclusive),
2. Guest users have limited access to properties and memberships of directory objects (default value),
3. Guest user access is restricted to properties and memberships of their own directory objects (most restrictive).

The recommended option is the 3rd, most restrictive: "Guest user access is restricted to their own directory object".

### **Impact:**

This may create additional requests for permissions to access resources that administrators will need to approve.

### **Audit:**

#### **From Azure Portal**

1. From Azure Home select the Portal Menu
2. **Select** Azure Active Directory
3. **Then** External Identities
4. **Select** External collaboration settings
5. **Under** Guest user access, **ensure that** Guest user access restrictions **is set to** Guest user access is restricted to properties and memberships of their own directory objects

## From PowerShell

1. Enter the following `Get-AzureADMSAuthorizationPolicy`  
Which will give a result like:

```
Id : authorizationPolicy
OdataType :
Description : Used to manage
authorization related settings across the company.
DisplayName : Authorization Policy
EnabledPreviewFeatures : {}
GuestUserRoleId : 10dae51f-b6af-4016-8d66-
8c2a99b929b3
PermissionGrantPolicyIdsAssignedToDefaultUserRole : {user-default-legacy}
```

If the `GuestUserRoleID` property does not equal `2af84b1e-32c8-42b7-82bc-daa82404023b` then it is not set to most restrictive.

### Remediation:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Then External Identities
4. Select External collaboration settings
5. Under Guest user access, change Guest user access restrictions to be Guest user access is restricted to properties and memberships of their own directory objects

#### From PowerShell

1. From a PowerShell session enter `Set-AzureADMSAuthorizationPolicy -GuestUserRoleId '2af84b1e-32c8-42b7-82bc-daa82404023b'`
2. Check that the setting was applied by entering `Get-AzureADMSAuthorizationPolicy`
3. Make certain that the `GuestUserRoleId` is equal to the earlier entered value of `2af84b1e-32c8-42b7-82bc-daa82404023b`.

### Default Value:

By default, Guest user access restrictions is set to Guest user access is restricted to properties and memberships of their own directory objects.

## References:

1. <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/users-default-permissions#member-and-guest-users>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-5-automate-entitlement-management>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-2-define-enterprise-segmentation-strategy>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-6-define-identity-and-privileged-access-strategy>
5. <https://docs.microsoft.com/en-us/azure/active-directory/enterprise-users/users-restrict-guest-permissions>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 Configure Data Access Control Lists</b>            Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.</p>			
v8	<p><b>3.7 Establish and Maintain a Data Classification Scheme</b>            Establish and maintain an overall data classification scheme for the enterprise. Enterprises may use labels, such as "Sensitive," "Confidential," and "Public," and classify their data according to those labels. Review and update the classification scheme annually, or when significant enterprise changes occur that could impact this Safeguard.</p>			
v8	<p><b>6.7 Centralize Access Control</b>            Centralize access control for all enterprise assets through a directory service or SSO provider, where supported.</p>			
v8	<p><b>6.8 Define and Maintain Role-Based Access Control</b>            Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.</p>			
v7	<p><b>14.6 Protect Information through Access Control Lists</b>            Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.</p>			

## 1.17 Ensure that 'Guest invite restrictions' is set to "Only users assigned to specific admin roles can invite guest users" (Manual)

### Profile Applicability:

- Level 2

### Description:

Restrict invitations to users with specific administrative roles only.

### Rationale:

Restricting invitations to users with specific administrator roles ensures that only authorized accounts have access to cloud resources. This helps to maintain "Need to Know" permissions and prevents inadvertent access to data.

By default the setting `Guest invite restrictions` is set to `Anyone` in the organization can invite guest users including guests and non-admins. This would allow anyone within the organization to invite guests and non-admins to the tenant, posing a security risk.

### Impact:

With the option of `Only users assigned to specific admin roles can invite guest users` selected, users with specific admin roles will be in charge of sending invitations to the Azure Workspace, requiring additional overhead by them to manage user accounts. This will mean coordinating with other departments as they are onboarding new users, and manually removing access from users who no longer need it.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Azure Active Directory`
3. Then `External Identities`
4. `External collaboration settings`
5. Under `Guest invite settings`, for `Guest invite restrictions`, ensure that that `Only users assigned to specific admin roles can invite guest users` is selected

Note: This setting has 4 levels of restriction, which include:

- Anyone in the organization can invite guest users including guests and non-admins (most inclusive),



- Member users and users assigned to specific admin roles can invite guest users including guests with member permissions,
- Only users assigned to specific admin roles can invite guest users,
- No one in the organization can invite guest users including admins (most restrictive).

**Remediation:**

**From Azure Portal**

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Then External Identities
4. Select External collaboration settings
5. Under Guest invite settings, for Guest invite restrictions, ensure that Only users assigned to specific admin roles can invite guest users is selected

**Default Value:**

By default, Guest invite restrictions is set to Anyone in the organization can invite guest users including guests and non-admins

**References:**

1. <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-b2b-delegate-invitations>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-6-define-identity-and-privileged-access-strategy>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-2-define-enterprise-segmentation-strategy>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-5-automate-entitlement-management>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.1 Establish an Access Granting Process</b> Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.	●	●	●
v8	<b>6.8 Define and Maintain Role-Based Access Control</b> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●

Controls Version	Control	IG 1	IG 2	IG 3
v7	<b>16.2 Configure Centralized Point of Authentication</b> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

DRAFT

## 1.18 Ensure That 'Restrict access to Azure AD administration portal' is Set to 'Yes' (Manual)

### Profile Applicability:

- Level 1

### Description:

Restrict access to the Azure AD administration portal to administrators only.

**NOTE:** This only affects access to the Azure AD administrator's web portal. This setting does not prohibit privileged users from using other methods such as Rest API or Powershell to obtain sensitive information from Azure AD.

### Rationale:

The Azure AD administrative portal has sensitive data and permission settings. All non-administrators should be prohibited from accessing any Azure AD data in the administration portal to avoid exposure.

### Impact:

All administrative tasks will need to be done by Administrators, causing additional overhead in management of users and resources.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Then Users
4. Select User settings
5. Ensure that Restrict access to Azure AD administration portal is set to Yes

### Remediation:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Then Users
4. Select User settings
5. Set Restrict access to Azure AD administration portal to Yes








### Default Value:

By default, Restrict access to Azure AD administration portal is set to No

## References:

1. <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-assign-admin-roles-azure-portal>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-2-define-enterprise-segmentation-strategy>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-6-define-identity-and-privileged-access-strategy>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-1-protect-and-limit-highly-privileged-users>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u></b></p> <p>Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.</p>			
v8	<p><b><u>6.8 Define and Maintain Role-Based Access Control</u></b></p> <p>Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.</p>			
v7	<p><b><u>4.3 Ensure the Use of Dedicated Administrative Accounts</u></b></p> <p>Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.</p>			

## 1.19 Ensure that 'Restrict user ability to access groups features in the Access Pane' is Set to 'Yes' (Manual)

### Profile Applicability:

- Level 2

### Description:

Restricts group creation to administrators with permissions only.

### Rationale:

Self-service group management enables users to create and manage security groups or Office 365 groups in Azure Active Directory (Azure AD). Unless a business requires this day-to-day delegation for some users, self-service group management should be disabled.

### Impact:

Setting to `Yes` could create administrative overhead by customers seeking certain group memberships that will have to be manually managed by administrators with appropriate permissions.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Azure Active Directory`
3. Select `Groups`
4. Select `General` under `Settings`
5. Ensure that `Restrict user ability to access groups features in the Access Panel` is set to `Yes`

### Remediation:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Azure Active Directory`
3. Select `Groups`
4. Select `General` under `Settings`
5. Ensure that `Restrict user ability to access groups features in the Access Panel` is set to `Yes`

## Default Value:

By default, Restrict user ability to access groups features in the Access Pane is set to No

## References:

1. <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-accessmanagement-self-service-group-management>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-1-protect-and-limit-highly-privileged-users>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-5-automate-entitlement-management>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-2-define-enterprise-segmentation-strategy>
6. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-6-define-identity-and-privileged-access-strategy>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.8 Define and Maintain Role-Based Access Control</b> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	<b>14.6 Protect Information through Access Control Lists</b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

## *1.20 Ensure that 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No' (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

Restrict security group creation to administrators only.

### **Rationale:**

When creating security groups is enabled, all users in the directory are allowed to create new security groups and add members to those groups. Unless a business requires this day-to-day delegation, security group creation should be restricted to administrators only.

### **Impact:**

Enabling this setting could create a number of requests that would need to be managed by an administrator.

### **Audit:**

#### **From Azure Portal**

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Select Groups
4. Select General under Settings
5. Ensure that Users can create security groups in Azure portals, API or PowerShell is set to No

### **Remediation:**

#### **From Azure Portal**

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Select Groups
4. Select General under Settings
5. Set Users can create security groups in Azure portals, API or PowerShell to No

## Default Value:

By default, Users can create security groups in Azure portals, API or PowerShell is set to Yes

## References:

1. <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-accessmanagement-self-service-group-management#making-a-group-available-for-end-user-self-service>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-6-define-identity-and-privileged-access-strategy>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-2-define-enterprise-segmentation-strategy>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-1-protect-and-limit-highly-privileged-users>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-5-automate-entitlement-management>
6. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.8 <u>Define and Maintain Role-Based Access Control</u></b> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●



## 1.21 Ensure that 'Owners can manage group membership requests in the Access Panel' is set to 'No' (Manual)

### Profile Applicability:

- Level 2

### Description:

Restrict security group management to administrators only.

### Rationale:

Restricting security group management to administrators only prohibits users from making changes to security groups. This ensures that security groups are appropriately managed and their management is not delegated to non-administrators.

### Impact:

Group Membership for user accounts will need to be handled by Admins and cause administrative overhead.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Then Groups
4. Select General in settings
5. Ensure that Owners can manage group membership requests in the Access Panel is set to No

### Remediation:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Then Groups
4. Select General in settings
5. Set Owners can manage group membership requests in the Access Panel to No

### Default Value:

By default, Owners can manage group membership requests in the Access Panel is set to No.

**References:**

1. <https://docs.microsoft.com/en-us/azure/active-directory/active-directory-accessmanagement-self-service-group-management#making-a-group-available-for-end-user-self-service>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-1-protect-and-limit-highly-privileged-users>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-5-automate-entitlement-management>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-8-choose-approval-process-for-microsoft-support>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-2-define-enterprise-segmentation-strategy>
6. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-6-define-identity-and-privileged-access-strategy>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>6.8 Define and Maintain Role-Based Access Control</b>            Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.</p>			●
v7	<p><b>14.6 Protect Information through Access Control Lists</b>            Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.</p>	●	●	●

## *1.22 Ensure that 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No' (Manual)*

### **Profile Applicability:**

- Level 2

### **Description:**

Restrict Microsoft 365 group creation to administrators only.

### **Rationale:**

Restricting Microsoft 365 group creation to administrators only ensures that creation of Microsoft 365 groups is controlled by the administrator. Appropriate groups should be created and managed by the administrator and group creation rights should not be delegated to any other user.

### **Impact:**

Enabling this setting could create a number of requests that would need to be managed by an administrator.

### **Audit:**

#### **From Azure Portal**

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Then Groups
4. Select General in setting
5. Ensure that Users can create Microsoft 365 groups in Azure portals, API or PowerShell is set to No

### **Remediation:**

#### **From Azure Portal**

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Then Groups
4. Select General in settings
5. Set Users can create Microsoft 365 groups in Azure portals, API or PowerShell to No

## Default Value:

By default, Users can create Microsoft 365 groups in Azure portals, API or PowerShell is set to Yes.

## References:

1. <https://whitepages.unlimitedviz.com/2017/01/disable-office-365-groups-2/>
2. <https://support.office.com/en-us/article/Control-who-can-create-Office-365-Groups-4c46c8cb-17d0-44b5-9776-005fcd8e618>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-6-define-identity-and-privileged-access-strategy>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-2-define-enterprise-segmentation-strategy>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-1-protect-and-limit-highly-privileged-users>
6. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-5-automate-entitlement-management>
7. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.8 <u>Define and Maintain Role-Based Access Control</u></b> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

## 1.23 Ensure that 'Require Multi-Factor Authentication to register or join devices with Azure AD' is set to 'Yes' (Manual)

### Profile Applicability:

- Level 1

### Description:

Joining or registering devices to the active directory should require Multi-factor authentication.

### Rationale:

Multi-factor authentication is recommended when adding devices to Azure AD. When set to `Yes`, users who are adding devices from the internet must first use the second method of authentication before their device is successfully added to the directory. This ensures that rogue devices are not added to the domain using a compromised user account. *Note:* Some Microsoft documentation suggests to use conditional access policies for joining a domain from certain whitelisted networks or devices. Even with these in place, using Multi-Factor Authentication is still recommended, as it creates a process for review before joining the domain.

### Impact:

A slight impact of additional overhead, as Administrators will now have to approve every access to the domain.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Select Devices
4. Select Device settings
5. Ensure that `Require Multi-Factor Authentication to register or join devices with Azure AD` is set to `Yes`

## Remediation:

### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Azure Active Directory
3. Select Devices
4. Select Device settings
5. Set Require Multi-Factor Authentication to register or join devices with Azure AD to Yes

### Default Value:

By default, Require Multi-Factor Authentication to register or join devices with Azure AD is set to No.

### References:

1. <https://blogs.technet.microsoft.com/janketil/2016/02/29/azure-mfa-for-enrollment-in-intune-and-azure-ad-device-registration-explained/>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-4-use-strong-authentication-controls-for-all-azure-active-directory-based-access>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>6.3 Require MFA for Externally-Exposed Applications</b> Require all externally-exposed enterprise or third-party applications to enforce MFA, where supported. Enforcing MFA through a directory service or SSO provider is a satisfactory implementation of this Safeguard.		●	●
v8	<b>6.4 Require MFA for Remote Network Access</b> Require MFA for remote network access.	●	●	●
v7	<b>16.3 Require Multi-factor Authentication</b> Require multi-factor authentication for all user accounts, on all systems, whether managed onsite or by a third-party provider.		●	●

## 1.24 Ensure That No Custom Subscription Administrator Roles Exist (Automated)

### Profile Applicability:

- Level 1

### Description:

The principle of least privilege should be followed and only necessary privileges should be assigned instead of allowing full administrative access.

### Rationale:

Classic subscription admin roles offer basic access management and include Account Administrator, Service Administrator, and Co-Administrators. It is recommended the least necessary permissions be given initially. Permissions can be added as needed by the account holder. This ensures the account holder cannot perform actions which were not intended.

### Impact:

Subscriptions will need to be handled by Administrators with permissions.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu.
2. Select Subscriptions.
3. Select Access control (IAM).
4. Select Roles.
5. Click Type and select CustomRole from the drop down menu.
6. Select View next to a role.
7. Select JSON.
8. Check for assignableScopes set to / or the subscription, and actions set to \*.
9. Repeat steps 6-8 for each custom role.

#### From Azure CLI

List custom roles:

```
az role definition list --custom-role-only True
```

Check for entries with assignableScope of / or the subscription, and an action of \*

#### From PowerShell

```
Connect-AzAccount  
Get-AzRoleDefinition |Where-Object {($_.IsCustom -eq $true) -and  
($_.Actions.contains('*'))}
```

Check the output for AssignableScopes value set to '/' or the subscription.

## Remediation:

### From Azure Portal

1. From Azure Home select the Portal Menu.
2. Select Subscriptions.
3. Select Access control (IAM).
4. Select Roles.
5. Click Type and select CustomRole from the drop down menu.
6. Check the box next to each role which grants subscription administrator privileges.
7. Select Remove.
8. Select Yes.

### From Azure CLI

List custom roles:

```
az role definition list --custom-role-only True
```

Check for entries with assignableScope of / or the subscription, and an action of \*.  
To remove a violating role:

```
az role definition delete --name <role name>
```

Note that any role assignments must be removed before a custom role can be deleted. Ensure impact is assessed before deleting a custom role granting subscription administrator privileges.

### Default Value:

By default, no custom owner roles are created.

### References:

1. <https://docs.microsoft.com/en-us/azure/billing/billing-add-change-azure-subscription-administrator>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-2-define-enterprise-segmentation-strategy>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-6-define-identity-and-privileged-access-strategy>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-1-protect-and-limit-highly-privileged-users>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-5-automate-entitlement-management>
6. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems>
7. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-2-define-enterprise-segmentation-strategy>



8. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-6-define-identity-and-privileged-access-strategy>
9. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-7-follow-just-enough-administration-least-privilege-principle>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u></b>            Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.</p>	●	●	●
v8	<p><b>6.8 <u>Define and Maintain Role-Based Access Control</u></b>            Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.</p>			●
v7	<p><b>4.1 <u>Maintain Inventory of Administrative Accounts</u></b>            Use automated tools to inventory all administrative accounts, including domain and local accounts, to ensure that only authorized individuals have elevated privileges.</p>		●	●

## 1.25 Ensure a Custom Role is Assigned Permissions for Administering Resource Locks (Manual)

### Profile Applicability:

- Level 2

### Description:

Resource locking is a powerful protection mechanism that can prevent inadvertent modification/deletion of resources within Azure subscriptions/Resource Groups and is a recommended NIST configuration.

### Rationale:

Given the resource lock functionality is outside of standard Role Based Access Control (RBAC), it would be prudent to create a resource lock administrator role to prevent inadvertent unlocking of resources.

### Impact:

By adding this role, specific permissions may be granted for managing just resource locks rather than needing to provide the wide owner or contributor role, reducing the risk of the user being able to do unintentional damage.

### Audit:

#### From Azure Portal

1. In the Azure portal, open a subscription or resource group where you want to view assigned roles.
2. Select `Access control (IAM)`
3. Select `Roles`
4. Search for the custom role named `<role_name>` Ex. `from remediation Resource Lock Administrator`
5. Ensure that the role is assigned to the appropriate users.

## Remediation:

### From Azure Portal

1. In the Azure portal, open a subscription or resource group where you want the custom role to be assigned.
2. Select Access control (IAM).
3. Click Add.
4. Select Add custom role.
5. In the Custom Role Name field enter Resource Lock Administrator.
6. In the Description field enter Can Administer Resource Locks.
7. For Baseline permissions select Start from scratch
8. Select next.
9. In the Permissions tab select Add permissions.
10. In the Search for a permission box, type in Microsoft.Authorization/locks to search for permissions.
11. Select the check box next to the permission Microsoft.Authorization/locks.
12. Select Add.
13. Select Review + create.
14. Select Create.
15. Assign the newly created role to the appropriate user.

### From PowerShell:

Below is a power shell definition for a resource lock administrator role created at an Azure Management group level

```
Import-Module Az.Accounts
Connect-AzAccount

$role = Get-AzRoleDefinition "User Access Administrator"
$role.Id = $null
$role.Name = "Resource Lock Administrator"
$role.Description = "Can Administer Resource Locks"
$role.Actions.Clear()
$role.Actions.Add("Microsoft.Authorization/locks/*")
$role.AssignableScopes.Clear()

* Scope at the Management group level Management group

$role.AssignableScopes.Add("/providers/Microsoft.Management/managementGroups/
MG-Name")

New-AzRoleDefinition -Role $role
Get-AzureRmRoleDefinition "Resource Lock Administrator"
```

## References:

1. <https://docs.microsoft.com/en-us/azure/role-based-access-control/custom-roles>
2. <https://docs.microsoft.com/en-us/azure/role-based-access-control/check-access>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-1-protect-and-limit-highly-privileged-users>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-7-follow-just-enough-administration-least-privilege-principle>
6. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-5-automate-entitlement-management>
7. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-2-define-enterprise-segmentation-strategy>
8. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-6-define-identity-and-privileged-access-strategy>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	<b>6.8 <u>Define and Maintain Role-Based Access Control</u></b> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

## 1.26 Ensure That 'Subscription Entering AAD Directory' and 'Subscription Leaving AAD Directory' Is Set To 'Permit No One' (Manual)

### Profile Applicability:

- Level 2

### Description:

Users who are set as subscription owners are able to make administrative changes to the subscriptions and move them into and out of Azure Active Directories.

### Rationale:

Permissions to move subscriptions in and out of Azure Active Directory must only be given to appropriate administrative personnel. A subscription that is moved into an Azure Active Directory may be within a folder to which other users have elevated permissions. This prevents loss of data or unapproved changes of the objects within by potential bad actors.

### Impact:

Subscriptions will need to have these settings turned off to be moved.

### Audit:

#### From Azure Portal

1. From the Azure Portal Home select the portal menu
2. Select Subscriptions
3. Select Manage Policies
4. Ensure Subscription leaving AAD directory **and** Subscription entering AAD directory **are set to** Permit no one

### Remediation:

#### From Azure Portal

1. From the Azure Portal Home select the portal menu
2. Select Subscriptions
3. Select Manage Policies
4. Under Subscription leaving AAD directory **and** Subscription entering AAD directory **select** Permit no one













## Default Value:

By default Subscription leaving AAD directory and Subscription entering AAD are set to Allow everyone (default)

## References:

1. <https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/manage-azure-subscription-policy>
2. <https://docs.microsoft.com/en-us/azure/active-directory/fundamentals/active-directory-how-subscriptions-associated-directory>
3. <https://docs.microsoft.com/en-us/azure/cost-management-billing/manage/manage-azure-subscription-policy>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-2-protect-identity-and-authentication-systems>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.4 <u>Restrict Administrator Privileges to Dedicated Administrator Accounts</u></b> Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.			
v8	<b>6.1 <u>Establish an Access Granting Process</u></b> Establish and follow a process, preferably automated, for granting access to enterprise assets upon new hire, rights grant, or role change of a user.			
v8	<b>6.2 <u>Establish an Access Revoking Process</u></b> Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.			
v7	<b>4.3 <u>Ensure the Use of Dedicated Administrative Accounts</u></b> Ensure that all users with administrative account access use a dedicated or secondary account for elevated activities. This account should only be used for administrative activities and not internet browsing, email, or similar activities.			

## 2 Microsoft Defender

This section covers recommendations to consider for tenant-wide security policies and plans related to Microsoft Defender. Please note that because Microsoft Defender products require additional licensing, all Microsoft Defender plan recommendations in subsection 2.1 are assigned as “Level 2.”

Microsoft Defender products addressed in this section include:

- Microsoft Defender for Cloud
- Microsoft Defender for IoT
- Microsoft Defender External Attack Surface Management

DRAFT

## 2.1 Microsoft Defender for Cloud

This subsection is dedicated to providing guidance on Microsoft Defender for Cloud product plans. This guidance is intended to ensure that - at a minimum - the protective measures offered by these plans are being considered. Organizations may find that they have existing products or services that provide the same utility as some Microsoft Defender for Cloud products. Security and Administrative personnel need to make the determination on their organization's behalf regarding which - if any - of these recommendations are relevant to their organization's needs. In consideration of the above, and because of the potential for increased cost and complexity, please be aware that all Defender Plan recommendations are profiled as "Level 2" recommendations.

DRAFT



## 2.1.1 Ensure That Microsoft Defender for Servers Is Set to 'On' (Manual)

### Profile Applicability:

- Level 2

### Description:

Turning on Microsoft Defender for Servers enables threat detection for Servers, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.

### Rationale:

Enabling Microsoft Defender for Servers allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

### Impact:

Turning on Microsoft Defender for Servers in Microsoft Defender for Cloud incurs an additional cost per resource.

### Audit:

#### From Azure Portal

1. Go to Microsoft Defender for Cloud
2. Select Environment Settings
3. Click on the subscription name
4. Select Defender plans
5. Ensure Servers Status is set to On.

#### From Azure CLI

Run the following command:

```
az security pricing show -n VirtualMachines --query pricingTier
```

If the tenant is licensed and enabled, the output should indicate Standard

#### From PowerShell

Run the following command:

```
Get-AzSecurityPricing -Name 'VirtualMachines' |Select-Object Name, PricingTier
```

If the tenant is licensed and enabled, the -PricingTier parameter will indicate Standard

## Remediation:

### From Azure Portal

1. Go to Microsoft Defender for Cloud
2. Select Environment Settings
3. Click on the subscription name
4. Select Defender plans
5. Set Server Status to On
6. Select Save

### From Azure CLI

Run the following command:

```
az security pricing create -n VirtualMachines --tier 'standard'
```

### From PowerShell

Run the following command:

```
Set-AzSecurityPricing -Name 'VirtualMachines' -PricingTier 'Standard'
```

### Default Value:

By default, Microsoft Defender plan is off.

### References:

1. <https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities>
2. <https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/list>
3. <https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update>
4. <https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security#es-1-use-endpoint-detection-and-response-edr>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</b> Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	<b>10.1 Deploy and Maintain Anti-Malware Software</b> Deploy and maintain anti-malware software on all enterprise assets.	●	●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	<b>3.1 <u>Run Automated Vulnerability Scanning Tools</u></b> Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●
v7	<b>8.1 <u>Utilize Centrally Managed Anti-malware Software</u></b> Utilize centrally managed anti-malware software to continuously monitor and defend each of the organization's workstations and servers.		●	●

DRAFT

## 2.1.2 Ensure That Microsoft Defender for App Services Is Set To 'On' (Manual)

### Profile Applicability:

- Level 2

### Description:

Turning on Microsoft Defender for App Service enables threat detection for App Service, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.

### Rationale:

Enabling Microsoft Defender for App Service allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

### Impact:

Turning on Microsoft Defender for App Service incurs an additional cost per resource.

### Audit:

#### From Azure Portal

1. Go to Microsoft Defender for Cloud
2. Select Environment Settings
3. Click on the subscription name
4. Select Defender plans
5. Ensure Status is On for App Service

#### From Azure CLI

Run the following command:

```
az security pricing show -n AppServices
```

Ensure `-PricingTier` is set to Standard

#### From PowerShell

Run the following command:

```
Get-AzSecurityPricing -Name 'AppServices' |Select-Object Name,PricingTier
```

Ensure the `-PricingTier` is set to Standard

## Remediation:

### From Azure Portal

1. Go to Microsoft Defender for Cloud
2. Select Environment Settings
3. Click on the subscription name
4. Select Defender plans
5. Set App Service Status to On
6. Select Save

### From Azure CLI

Run the following command:

```
az security pricing create -n Appservices --tier 'standard'
```

### From PowerShell

Run the following command:

```
Set-AzSecurityPricing -Name "AppServices" -PricingTier "Standard"
```

### Default Value:

By default, Microsoft Defender plan is off.

### References:

1. <https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities>
2. <https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/list>
3. <https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update>
4. <https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-1-enable-threat-detection-capabilities>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</b> Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>7.6 <u>Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets</u></b></p> <p>Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.</p>		●	●
v8	<p><b>16.11 <u>Leverage Vetted Modules or Services for Application Security Components</u></b></p> <p>Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.</p>		●	●
v7	<p><b>3.1 <u>Run Automated Vulnerability Scanning Tools</u></b></p> <p>Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.</p>		●	●

DRAFT

## 2.1.3 Ensure That Microsoft Defender for Databases Is Set To 'On' (Manual)

### Profile Applicability:

- Level 2

### Description:

Turning on Microsoft Defender for Databases enables threat detection for the instances running your database software. This provides threat intelligence, anomaly detection, and behavior analytics in the Azure Microsoft Defender for Cloud. Instead of being enabled on services like Platform as a Service (PaaS), this implementation will run within your instances as Infrastructure as a Service (IaaS) on the Operating Systems hosting your databases.

### Rationale:

Enabling Microsoft Defender for Azure SQL Databases allows your organization more granular control of the infrastructure running your database software. Instead of waiting on Microsoft release updates or other similar processes, you can manage them yourself. Threat detection is provided by the Microsoft Security Response Center (MSRC).

### Impact:

Running Defender on Infrastructure as a service (IaaS) may incur increased costs associated with running the service and the instance it is on. Similarly, you will need qualified personnel to maintain the operating system and software updates. If it is not maintained, security patches will not be applied and it may be open to vulnerabilities.

### Audit:

#### From Azure Portal

1. Go to Microsoft Defender for Cloud
2. Select Environment Settings
3. Click on the subscription name
4. Select Defender plans
5. Ensure Databases Status is set to On
6. Review the chosen pricing tier

## From Azure CLI

Ensure the output of the below commands is Standard

```
az security pricing show -n 'SqlServers'  
az security pricing show -n 'SqlServerVirtualMachines'  
az security pricing show -n 'OpenSourceRelationalDatabases'  
az security pricing show -n 'CosmosDbs'
```

If the output of any of the above commands shows `pricingTier` with a value of `Free`, the setting is out of compliance.

## From PowerShell

```
Connect-AzAccount  
Get-AzSecurityPricing |select-object Name, PricingTier |where-object {$_.Name  
-match 'Sql' -or $_.Name -match 'Cosmos' -or $_.Name -match 'OpenSource'}
```

Ensure the output shows **Standard** for each database type under the **PricingTier** column. Any that show **Free** are considered out of compliance.

## Remediation:

### From Azure Portal

1. Go to Microsoft Defender for Cloud
2. Select Environment Settings
3. Click on the subscription name
4. Select Defender plans
5. Set Databases Status to On
6. Select Save

Review the chosen pricing tier. For the Azure Databases resource review the different plan information and choose one that fits the needs of your organization.

## From Azure CLI

Run the following commands:

```
az security pricing create -n 'SqlServers' --tier 'Standard'  
az security pricing create -n 'SqlServerVirtualMachines' --tier 'Standard'  
az security pricing create -n 'OpenSourceRelationalDatabases' --tier  
'Standard'  
az security pricing create -n 'CosmosDbs' --tier 'Standard'
```

## From Azure PowerShell

Run the following commands:

```
Set-AzSecurityPricing -Name 'SqlServers' -PricingTier 'Standard'  
Set-AzSecurityPricing -Name 'SqlServerVirtualMachines' -PricingTier  
'Standard'  
Set-AzSecurityPricing -Name 'OpenSourceRelationalDatabases' -PricingTier  
'Standard'  
Set-AzSecurityPricing -Name 'CosmosDbs' -PricingTier 'Standard'
```

## Default Value:

By default, Microsoft Defender Plans are off.



**References:**

1. <https://docs.microsoft.com/en-us/azure/azure-sql/database/azure-defender-for-sql?view=azuresql>
2. <https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-enable-database-protections>
3. <https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-databases-usage>
4. <https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities>
5. <https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/list>
6. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-1-enable-threat-detection-capabilities>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</u></b>            Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.</p>		●	●
v8	<p><b><u>16.11 Leverage Vetted Modules or Services for Application Security Components</u></b>            Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.</p>		●	●
v7	<p><b><u>3.1 Run Automated Vulnerability Scanning Tools</u></b>            Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.</p>		●	●

## 2.1.4 Ensure That Microsoft Defender for Azure SQL Databases Is Set To 'On' (Manual)

### Profile Applicability:

- Level 2

### Description:

Turning on Microsoft Defender for Azure SQL Databases enables threat detection for Azure SQL database servers, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.

### Rationale:

Enabling Microsoft Defender for Azure SQL Databases allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

### Impact:

Turning on Microsoft Defender for Azure SQL Databases incurs an additional cost per resource.

### Audit:

#### From Azure Portal

1. Go to Microsoft Defender for Cloud.
2. Select Environment Settings blade.
3. Click on the subscription name.
4. Select the Defender plans blade.
5. Click Select types > in the row for Databases.
6. Ensure the radio button next to Azure SQL Databases is set to On.

#### From Azure CLI

Run the following command:

```
az security pricing show -n SqlServers
```

Ensure `-PricingTier` is set to Standard

#### From PowerShell

Run the following command:

```
Get-AzSecurityPricing -Name 'SqlServers' | Select-Object Name,PricingTier
```

Ensure the `-PricingTier` is set to Standard

## Remediation:

### From Azure Portal

1. Go to Microsoft Defender for Cloud.
2. Select Environment Settings blade.
3. Click on the subscription name.
4. Select the Defender plans blade.
5. Click Select types > in the row for Databases.
6. Set the radio button next to Azure SQL Databases to On.
7. Select Continue.
8. Select Save.

### From Azure CLI

Run the following command:

```
az security pricing create -n SqlServers --tier 'standard'
```

### From PowerShell

Run the following command:

```
Set-AzSecurityPricing -Name 'SqlServers' -PricingTier 'Standard'
```

### Default Value:

By default, Microsoft Defender plan is off.

### References:

1. <https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities>
2. <https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/list>
3. <https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update>
4. <https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-2-monitor-anomalies-and-threats-targeting-sensitive-data>
6. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-1-enable-threat-detection-capabilities>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</u></b>            Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.</p>		●	●
v8	<p><b><u>16.11 Leverage Vetted Modules or Services for Application Security Components</u></b>            Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.</p>		●	●
v7	<p><b><u>3.1 Run Automated Vulnerability Scanning Tools</u></b>            Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.</p>		●	●

DRAFT

## 2.1.5 Ensure That Microsoft Defender for SQL Servers on Machines Is Set To 'On' (Manual)

### Profile Applicability:

- Level 2

### Description:

Turning on Microsoft Defender for SQL servers on machines enables threat detection for SQL servers on machines, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.

### Rationale:

Enabling Microsoft Defender for SQL servers on machines allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

### Impact:

Turning on Microsoft Defender for SQL servers on machines incurs an additional cost per resource.

### Audit:

#### From Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Select `Environment Settings` blade.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Click `Select types >` in the row for `Databases`.
6. Ensure the radio button next to `SQL servers on machines` is set to `On`.

#### From Azure CLI

Run the following command:

```
az security pricing show -n SqlServerVirtualMachines
```

Ensure the 'PricingTier' is set to 'Standard'

#### From PowerShell

Run the following command:

```
Get-AzSecurityPricing -Name 'SqlServerVirtualMachines' | Select-Object Name,PricingTier
```

## Remediation:

### From Azure Portal

1. Go to Microsoft Defender for Cloud.
2. Select Environment Settings blade.
3. Click on the subscription name.
4. Select the Defender plans blade.
5. Click Select types > in the row for Databases.
6. Set the radio button next to SQL servers on machines to On.
7. Select Continue.
8. Select Save.

### From Azure CLI

Run the following command:

```
az security pricing create -n SqlServerVirtualMachines --tier 'standard'
```

### From PowerShell

Run the following command:

```
Set-AzSecurityPricing -Name 'SqlServerVirtualMachines' -PricingTier 'Standard'
```

### Default Value:

By default, Microsoft Defender plan is off.

### References:

1. <https://docs.microsoft.com/en-us/azure/security-center/defender-for-sql-usage>
2. <https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities>
3. <https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update>
4. <https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-3-monitor-for-unauthorized-transfer-of-sensitive-data>
6. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-1-enable-threat-detection-capabilities>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</u></b>            Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.</p>		●	●
v8	<p><b><u>16.11 Leverage Vetted Modules or Services for Application Security Components</u></b>            Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.</p>		●	●
v7	<p><b><u>3.1 Run Automated Vulnerability Scanning Tools</u></b>            Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.</p>		●	●

DRAFT

## 2.1.6 Ensure That Microsoft Defender for Open-Source Relational Databases Is Set To 'On' (Manual)

### Profile Applicability:

- Level 2

### Description:

Turning on Microsoft Defender for Open-source relational databases enables threat detection for Open-source relational databases, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.

### Rationale:

Enabling Microsoft Defender for Open-source relational databases allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

### Impact:

Turning on Microsoft Defender for Open-source relational databases incurs an additional cost per resource.

### Audit:

#### From Azure Portal

1. Go to `Microsoft Defender for Cloud`.
2. Select `Environment Settings` blade.
3. Click on the subscription name.
4. Select the `Defender plans` blade.
5. Click `Select types >` in the row for `Databases`.
6. Ensure the radio button next to `Open-source relational databases` is set to `On`.

#### From Azure CLI

Run the following command:

```
az security pricing show -n OpenSourceRelationalDatabases --query pricingTier
```

#### From PowerShell

```
Get-AzSecurityPricing | Where-Object {$_.Name -eq 'OpenSourceRelationalDatabases'} | Select-Object Name, PricingTier
```

Ensure output for `Name PricingTier` is `OpenSourceRelationalDatabases Standard`



## Remediation:

### From Azure Portal

1. Go to Microsoft Defender for Cloud.
2. Select Environment Settings blade.
3. Click on the subscription name.
4. Select the Defender plans blade.
5. Click Select types > in the row for Databases.
6. Set the radio button next to Open-source relational databases to On.
7. Select Continue.
8. Select Save.

### From Azure CLI

Run the following command:

```
az security pricing create -n 'OpenSourceRelationalDatabases' --tier 'standard'
```

### From PowerShell

Use the below command to enable Standard pricing tier for Open-source relational databases

```
set-azsecuritypricing -name "OpenSourceRelationalDatabases" -pricingtier "Standard"
```

### Default Value:

By default, Microsoft Defender plan is off.

### References:

1. <https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities>
2. <https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update>
3. <https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-2-monitor-anomalies-and-threats-targeting-sensitive-data>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-1-enable-threat-detection-capabilities>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</u></b>            Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.</p>		●	●
v8	<p><b><u>16.11 Leverage Vetted Modules or Services for Application Security Components</u></b>            Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.</p>		●	●
v7	<p><b><u>3.1 Run Automated Vulnerability Scanning Tools</u></b>            Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.</p>		●	●

DRAFT

## 2.1.7 Ensure That Microsoft Defender for Storage Is Set To 'On' (Manual)

### Profile Applicability:

- Level 2

### Description:

Turning on Microsoft Defender for Storage enables threat detection for Storage, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.

### Rationale:

Enabling Microsoft Defender for Storage allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

### Impact:

Turning on Microsoft Defender for Storage incurs an additional cost per resource.

### Audit:

#### From Azure Portal

1. Go to Microsoft Defender for Cloud.
2. Select Environment Settings blade.
3. Click on the subscription name.
4. Select the Defender plans blade.
5. Ensure Status is set to On for Storage.

#### From Azure CLI

Ensure the output of the below command is Standard

```
az security pricing show -n StorageAccounts
```

#### From PowerShell

```
Get-AzSecurityPricing -Name 'StorageAccounts' | Select-Object  
Name, PricingTier
```

Ensure output for Name PricingTier is StorageAccounts Standard

## Remediation:

### From Azure Portal

1. Go to Microsoft Defender for Cloud.
2. Select Environment Settings blade.
3. Click on the subscription name.
4. Select the Defender plans blade.
5. Set Status to On for Storage.
6. Select Save.

### From Azure CLI

Ensure the output of the below command is Standard

```
az security pricing create -n StorageAccounts --tier 'standard'
```

### From PowerShell

```
Set-AzSecurityPricing -Name 'StorageAccounts' -PricingTier 'Standard'
```





### Default Value:

By default, Microsoft Defender plan is off.

### References:

1. <https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities>
2. <https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/list>
3. <https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update>
4. <https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-1-enable-threat-detection-capabilities>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</b> Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.			
v7	<b>3.1 Run Automated Vulnerability Scanning Tools</b> Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.			

## 2.1.8 Ensure That Microsoft Defender for Containers Is Set To 'On' (Manual)

### Profile Applicability:

- Level 2

### Description:

Turning on Microsoft Defender for Containers enables threat detection for Container Registries including Kubernetes, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.

### Rationale:

Enabling Microsoft Defender for Container Registries allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

### Impact:

Turning on Microsoft Defender for Containers incurs an additional cost per resource.

### Audit:

#### From Azure Portal

1. Go to Microsoft Defender for Cloud.
2. Select Environment Settings.
3. Click on the subscription name.
4. Select Defender plans.
5. Ensure On is set under Status for Containers.

#### From Azure CLI

Ensure the output of the commands below indicates Standard pricing.

For legacy Defender for Container Registries instances:

```
az security pricing show --name "ContainerRegistry" --query pricingTier
```

For new Defender for Containers instances:

```
az security pricing show --name "Containers" --query pricingTier
```

#### From PowerShell

Ensure the output of the commands below indicates Standard pricing.

For legacy Defender for Container Registries instances:

```
Get-AzSecurityPricing -Name 'ContainerRegistry' | Select-Object Name, PricingTier
```

For new Defender for Containers instances:

```
Get-AzSecurityPricing -Name 'Containers' | Select-Object Name, PricingTier
```

## Remediation:

### From Azure Portal

1. Go to Microsoft Defender for Cloud.
2. Select Environment Settings.
3. Click on the subscription name.
4. Select Defender plans.
5. Set Status to On for Containers.
6. Click Save.

### From Azure CLI

(Note: 'ContainerRegistry' has been deprecated and is replaced by 'Containers')  
Use the below command to enable Standard pricing tier for Containers.

```
az security pricing create -n 'Containers' --tier 'standard'
```

### From PowerShell

(Note: 'ContainerRegistry' has been deprecated and is replaced by 'Containers')  
Use the below command to enable Standard pricing tier for Containers.

```
Set-AzSecurityPricing -Name 'Containers' -PricingTier 'Standard'
```

### Default Value:

By default, Microsoft Defender for Containers is off.

### References:

1. <https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities>
2. <https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/list>
3. <https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update>
4. <https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-1-enable-threat-detection-capabilities>
6. <https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction?tabs=defender-for-container-arch-aks>

### Additional Information:

**Deprecation of previous product plans** 'Container registries' and 'Kubernetes' plans for Microsoft Defender are being deprecated and replaced with 'Containers' or Microsoft Defender for Containers.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</u></b>            Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.</p>		●	●
v7	<p><b><u>3.1 Run Automated Vulnerability Scanning Tools</u></b>            Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.</p>		●	●

DRAFT

## 2.1.9 Ensure That Microsoft Defender for Azure Cosmos DB Is Set To 'On' (Manual)

### Profile Applicability:

- Level 2

### Description:

Microsoft Defender for Azure Cosmos DB scans all incoming network requests for threats to your Azure Cosmos DB resources.

### Rationale:

In scanning Azure Cosmos DB requests within a subscription, requests are compared to a heuristic list of potential security threats. These threats could be a result of a security breach within your services, thus scanning for them could prevent a potential security threat from being introduced.

### Impact:

Enabling Microsoft Defender for Azure Cosmos DB requires enabling Microsoft Defender for your subscription. Both will incur additional charges.

### Audit:

#### From Azure Portal

1. Go to `Microsoft Defender for Cloud`
2. Select `Environment Settings` blade
3. Click on the subscription name
4. Select the `Defender plans` blade
5. On the `Database` row click on `Select types >`
6. Ensure the radio button next to `Azure Cosmos DB` is set to `On`.

#### From Azure CLI

Ensure the output of the below command is `Standard`

```
az security pricing show -n CosmosDbs --query pricingTier
```

#### From PowerShell

```
Get-AzSecurityPricing -Name 'CosmosDbs' | Select-Object Name, PricingTier
```

Ensure output of `-PricingTier` is `Standard`



## Remediation:

### From Azure Portal

1. Go to Microsoft Defender for Cloud.
2. Select Environment Settings blade.
3. Click on the subscription name.
4. Select the Defender plans blade.
5. On the Database row click on Select types >.
6. Set the radio button next to Azure Cosmos DB to On.
7. Click Continue.
8. Click Save.

### From Azure CLI

Run the following command:

```
az security pricing create -n 'CosmosDbs' --tier 'standard'
```

### From PowerShell

Use the below command to enable Standard pricing tier for Azure Cosmos DB

```
Set-AzSecurityPricing -Name 'CosmosDbs' -PricingTier 'Standard'
```

### Default Value:

By default, Microsoft Defender for Azure Cosmos DB is not enabled.

### References:

1. <https://azure.microsoft.com/en-us/pricing/details/defender-for-cloud/>
2. <https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-enhanced-security>
3. <https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/cosmos-db-security-baseline>
5. <https://docs.microsoft.com/en-us/azure/defender-for-cloud/quickstart-enable-database-protections>
6. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-1-enable-threat-detection-capabilities>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</u></b>            Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.</p>		●	●
v8	<p><b><u>16.11 Leverage Vetted Modules or Services for Application Security Components</u></b>            Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.</p>		●	●
v7	<p><b><u>3.1 Run Automated Vulnerability Scanning Tools</u></b>            Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.</p>		●	●

DRAFT

## 2.1.10 Ensure That Microsoft Defender for Key Vault Is Set To 'On' (Manual)

### Profile Applicability:

- Level 2

### Description:

Turning on Microsoft Defender for Key Vault enables threat detection for Key Vault, providing threat intelligence, anomaly detection, and behavior analytics in the Microsoft Defender for Cloud.

### Rationale:

Enabling Microsoft Defender for Key Vault allows for greater defense-in-depth, with threat detection provided by the Microsoft Security Response Center (MSRC).

### Impact:

Turning on Microsoft Defender for Key Vault incurs an additional cost per resource.

### Audit:

#### From Azure Portal

1. Go to Microsoft Defender for Cloud
2. Select Environment Settings blade
3. Click on the subscription name
4. Select the Defender plans blade
5. Ensure Status is set to On for Key Vault.

#### From Azure CLI

Ensure the output of the below command is Standard

```
az security pricing show -n 'KeyVaults' --query 'PricingTier'
```

#### From PowerShell

```
Get-AzSecurityPricing -Name 'KeyVaults' | Select-Object Name,PricingTier
```

Ensure output for PricingTier is Standard

### Remediation:

#### From Azure Portal

1. Go to Microsoft Defender for Cloud
2. Select Environment Settings blade
3. Click on the subscription name
4. Select the Defender plans blade

5. Select **On** under **Status** for **Key Vault**.
6. Select **Save**.

### From Azure CLI

Enable Standard pricing tier for Key Vault:

```
az security pricing create -n 'KeyVaults' --tier 'Standard'
```

### From PowerShell

Enable Standard pricing tier for Key Vault:

```
Set-AzSecurityPricing -Name 'KeyVaults' -PricingTier 'Standard'
```

### Default Value:

By default, Microsoft Defender plan is off.

### References:

1. <https://docs.microsoft.com/en-us/azure/security-center/security-center-detection-capabilities>
2. <https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/list>
3. <https://docs.microsoft.com/en-us/rest/api/securitycenter/pricings/update>
4. <https://docs.microsoft.com/en-us/powershell/module/az.security/get-azsecuritypricing>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-1-enable-threat-detection-capabilities>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</b> Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v7	<b>3.1 Run Automated Vulnerability Scanning Tools</b> Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

## 2.1.11 Ensure That Microsoft Defender for DNS Is Set To 'On' (Manual)

### Profile Applicability:

- Level 2

### Description:

Microsoft Defender for DNS scans all network traffic exiting from within a subscription.

### Rationale:

DNS lookups within a subscription are scanned and compared to a dynamic list of websites that might be potential security threats. These threats could be a result of a security breach within your services, thus scanning for them could prevent a potential security threat from being introduced.

### Impact:

Enabling Microsoft Defender for DNS requires enabling Microsoft Defender for your subscription. Both will incur additional charges, with Defender for DNS being a small amount per million queries.

### Audit:

#### From Azure Portal

1. Go to Microsoft Defender for Cloud
2. Select Environment Settings blade
3. Click on the subscription name
4. Select the Defender plans blade
5. Ensure Status is set to On for DNS.

#### From Azure CLI

Ensure the output of the below command is Standard

```
az security pricing show -n 'DNS' --query 'PricingTier'
```

#### From PowerShell

```
Get-AzSecurityPricing --Name 'DNS' | Select-Object Name,PricingTier
```

Ensure output of PricingTier is Standard

## Remediation:

### From Azure Portal

1. Go to Microsoft Defender for Cloud.
2. Select Environment Settings blade.
3. Click on the subscription name.
4. Select the Defender plans blade.
5. Select On under Status for DNS.
6. Select Save.

### From Powershell

Enable Standard pricing tier for DNS:

```
az security pricing create -n 'DNS' --tier 'Standard'
```

### From PowerShell

Enable Standard pricing tier for DNS:

```
Set-AzSecurityPricing -Name 'DNS' -PricingTier 'Standard'
```

### Default Value:

By default, Microsoft Defender for DNS is not enabled.

### References:

1. <https://azure.microsoft.com/en-us/pricing/details/defender-for-cloud/>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/dns-security-baseline>
3. <https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-dns-alerts>
4. <https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-enhanced-security>
5. <https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview>
6. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-10-ensure-domain-name-system-dns-security>
7. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-1-enable-threat-detection-capabilities>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.9 <u>Configure Trusted DNS Servers on Enterprise Assets</u></b>            Configure trusted DNS servers on enterprise assets. Example implementations include: configuring assets to use enterprise-controlled DNS servers and/or reputable externally accessible DNS servers.</p>		●	●
v8	<p><b>7.5 <u>Perform Automated Vulnerability Scans of Internal Enterprise Assets</u></b>            Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.</p>		●	●
v8	<p><b>13.6 <u>Collect Network Traffic Flow Logs</u></b>            Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.</p>		●	●
v7	<p><b>3.1 <u>Run Automated Vulnerability Scanning Tools</u></b>            Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.</p>		●	●
v7	<p><b>7.6 <u>Log all URL requests</u></b>            Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.</p>		●	●

## 2.1.12 Ensure That Microsoft Defender for Resource Manager Is Set To 'On' (Manual)

### Profile Applicability:

- Level 2

### Description:

Microsoft Defender for Resource Manager scans incoming administrative requests to change your infrastructure from both CLI and the Azure portal.

### Rationale:

Scanning resource requests lets you be alerted every time there is suspicious activity in order to prevent a security threat from being introduced.

### Impact:

Enabling Microsoft Defender for Resource Manager requires enabling Microsoft Defender for your subscription. Both will incur additional charges.

### Audit:

#### From Azure Portal

1. Go to Microsoft Defender for Cloud
2. Select Environment Settings blade
3. Click on the subscription name
4. Select the Defender plans blade
5. Ensure Status is set to On for Resource Manager.

#### From Azure CLI

Ensure the output of the below command is Standard

```
az security pricing show -n 'Arm' --query 'PricingTier'
```

#### From Azure PowerShell

```
Get-AzSecurityPricing -Name 'Arm' | Select-Object Name,PricingTier
```

Ensure the output of PricingTier is Standard



## Remediation:

### From Azure Portal

1. Go to Microsoft Defender for Cloud.
2. Select Environment Settings blade.
3. Click on the subscription name.
4. Select the Defender plans blade.
5. Select On under Status for Resource Manager.
6. Select `Save`.

### From Azure CLI

Use the below command to enable Standard pricing tier for Defender for Resource Manager

```
az security pricing create -n 'Arm' --tier 'Standard'
```

### From PowerShell

Use the below command to enable Standard pricing tier for Defender for Resource Manager

```
Set-AzSecurityPricing -Name 'Arm' -PricingTier 'Standard'
```

### Default Value:

By default, Microsoft Defender for Resource Manager is not enabled.

### References:

1. <https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-enhanced-security>
2. <https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-resource-manager-introduction>
3. <https://azure.microsoft.com/en-us/pricing/details/defender-for-cloud/>
4. <https://docs.microsoft.com/en-us/azure/defender-for-cloud/alerts-overview>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-1-enable-threat-detection-capabilities>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>5.4 Restrict Administrator Privileges to Dedicated Administrator Accounts</u></b>            Restrict administrator privileges to dedicated administrator accounts on enterprise assets. Conduct general computing activities, such as internet browsing, email, and productivity suite use, from the user's primary, non-privileged account.</p>	●	●	●
v8	<p><b><u>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</u></b>            Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.</p>		●	●
v7	<p><b><u>3.1 Run Automated Vulnerability Scanning Tools</u></b>            Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.</p>		●	●

DRAFT

## 2.1.13 Ensure that Microsoft Defender Recommendation for 'Apply system updates' status is 'Completed' (Manual)

### Profile Applicability:

- Level 1

### Description:

Ensure that the latest OS patches for all virtual machines are applied.

### Rationale:

Windows and Linux virtual machines should be kept updated to:

- Address a specific bug or flaw
- Improve an OS or application's general stability
- Fix a security vulnerability

The Azure Security Center retrieves a list of available security and critical updates from Windows Update or Windows Server Update Services (WSUS), depending on which service is configured on a Windows VM. The security center also checks for the latest updates in Linux systems. If a VM is missing a system update, the security center will recommend system updates be applied.

### Impact:

Running Microsoft Defender for Cloud incurs additional charges for each resource monitored. Please see attached reference for exact charges per hour.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Defender for Cloud`
3. Then the `Recommendations` blade
4. Ensure that there are no recommendations for `Apply system updates`

Alternatively, you can employ your own patch assessment and management tool to periodically assess, report and install the required security patches for your OS.

### Remediation:

Follow Microsoft Azure documentation to apply security patches from the security center. Alternatively, you can employ your own patch assessment and management tool to periodically assess, report, and install the required security patches for your OS.







**Default Value:**

By default, patches are not automatically deployed.

**References:**

1. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities>
2. <https://azure.microsoft.com/en-us/pricing/details/defender-for-cloud/>
3. <https://docs.microsoft.com/en-us/azure/defender-for-cloud/deploy-vulnerability-assessment-vm>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>7.3 <u>Perform Automated Operating System Patch Management</u></b> Perform operating system updates on enterprise assets through automated patch management on a monthly, or more frequent, basis.			
v7	<b>3.4 <u>Deploy Automated Operating System Patch Management Tools</u></b> Deploy automated software update tools in order to ensure that the operating systems are running the most recent security updates provided by the software vendor.			

## 2.1.14 Ensure Any of the ASC Default Policy Settings are Not Set to 'Disabled' (Manual)

### Profile Applicability:

- Level 1

### Description:

None of the settings offered by ASC Default policy should be set to effect Disabled.

### Rationale:

A security policy defines the desired configuration of your workloads and helps ensure compliance with company or regulatory security requirements. ASC Default policy is associated with every subscription by default. ASC default policy assignment is a set of security recommendations based on best practices. Enabling recommendations in ASC default policy ensures that Azure security center provides the ability to monitor all of the supported recommendations and optionally allow automated action for a few of the supported recommendations.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Microsoft Defender for Cloud
3. Then Environment Settings
4. Select subscription
5. Then on Security Policy in the left column.
6. Followed by on ASC Default under Default initiative
7. Scroll down to Policy Enforcement and ensure it is set to Enabled
8. Click on the Parameters tab and uncheck Only show parameters that need input or review
9. Review the Parameters to ensure none of the items are set to Disabled.

The View effective Policy button can be used to see all effects of policies even if they have not been modified.

## From Azure CLI

Ensure the `properties.enforcementMode` in the output of the below command is set to Default. If `properties.enforcementMode` is set to `DoNotEnforce`, the default policies are disabled and therefore out of compliance.

```
az account get-access-token --query
"{<subscription:subscription>,<accessToken:accessToken>}" --out tsv | xargs -
L1 bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/<subscriptionID>/providers/Microso
ft.Authorization/policyAssignments/SecurityCenterBuiltIn?api-version=2021-06-
01'
```

**Note** policies that have not been modified will not be listed in this output

## From PowerShell

```
Get-AzPolicyAssignment | Where-Object {$_.Name -eq 'SecurityCenterBuiltIn' |
Select-Object -ExpandProperty Properties
```

If the `EnforcementMode` value equals `Default` the ASC Default Policies are enabled. Because several of the policies are in the `Disabled` state by default, check to see if the `Parameters` attribute in the output of the above command contains policies with the value of `Disabled` or if it's empty altogether. If so, these settings are out of compliance. If none of the values in the `Parameters` attribute show `Disabled`, these settings are in compliance. If the `EnforcementMode` parameter equals `DoNotEnforce` the ASC Default Policies are all disabled and thus out of compliance.

## Remediation:

### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Microsoft Defender for Cloud
3. Select Environment Settings
4. Click on a subscription
5. Select Security Policy in the left column.
6. Click on ASC Default under Default initiative
7. Ensure Policy Enforcement is Enabled
8. Click on the Parameters tab and uncheck Only show parameters that need input or review
9. For any parameters set to `Disabled` or empty, update to a valid value for the organization
10. Click Save

## References:

1. <https://docs.microsoft.com/en-us/azure/security-center/security-center-policies>
2. <https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-transparent-data-encryption>
3. <https://msdn.microsoft.com/en-us/library/mt704062.aspx>
4. <https://msdn.microsoft.com/en-us/library/mt704063.aspx>
5. <https://docs.microsoft.com/en-us/rest/api/policy/policy-assignments/get>
6. <https://docs.microsoft.com/en-us/rest/api/policy/policy-assignments/create>
7. <https://docs.microsoft.com/en-in/azure/security-center/tutorial-security-policy>
8. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-7-define-and-implement-logging-threat-detection-and-incident-response-strategy>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.1 Establish and Maintain a Secure Configuration Process</b>            Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>	●	●	●
v8	<p><b>4.2 Establish and Maintain a Secure Configuration Process for Network Infrastructure</b>            Establish and maintain a secure configuration process for network devices. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>	●	●	●
v8	<p><b>13.11 Tune Security Event Alerting Thresholds</b>            Tune security event alerting thresholds monthly, or more frequently.</p>			●
v7	<p><b>5.1 Establish Secure Configurations</b>            Maintain documented, standard security configuration standards for all authorized operating systems and software.</p>	●	●	●
v7	<p><b>5.5 Implement Automated Configuration Monitoring Systems</b>            Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.</p>		●	●

## 2.1.15 Ensure that Auto provisioning of 'Log Analytics agent for Azure VMs' is Set to 'On' (Automated)

### Profile Applicability:

- Level 1

### Description:

Enable automatic provisioning of the monitoring agent to collect security data.

### Rationale:

When Log Analytics agent for Azure VMs is turned on, Microsoft Defender for Cloud provisions the Microsoft Monitoring Agent on all existing supported Azure virtual machines and any new ones that are created. The Microsoft Monitoring Agent scans for various security-related configurations and events such as system updates, OS vulnerabilities, endpoint protection, and provides alerts.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Microsoft Defender for Cloud
3. Then Environment Settings
4. Select a subscription
5. Then Auto Provisioning in the left column.
6. Ensure that Log Analytics agent for Azure VMs is set to On

Repeat the above for any additional subscriptions.

#### From Azure CLI

Ensure the output of the below command is On

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/<subscriptionID>/providers/Microso
ft.Security/autoProvisioningSettings?api-version=2017-08-01-preview' | jq
'.|.value[] | select(.name=="default")'|jq '.properties.autoProvision'
```

#### Using PowerShell

```
Connect-AzAccount
Get-AzSecurityAutoProvisioningSetting
```

Ensure output for Id Name AutoProvision is

```
/subscriptions//providers/Microsoft.Security/autoProvisioningSettings/default
default On
```



## Remediation:

### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Microsoft Defender for Cloud
3. Select Environment Settings
4. Select a subscription
5. Select Auto Provisioning in the left column.
6. Ensure that Log Analytics agent for Azure VMs is set to On

Repeat the above for any additional subscriptions.

### From Azure CLI

Use the below command to set Automatic provisioning of monitoring agent to On.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/subscriptionID/providers/Microsoft
.Security/autoProvisioningSettings/default?api-version=2017-08-01-preview -
d@"input.json"'
```

Where `input.json` contains the Request body json data as mentioned below.

```
{
  "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/autoProvi
sioningSettings/default",
  "name": "default",
  "type": "Microsoft.Security/autoProvisioningSettings",
  "properties": {
    "autoProvision": "On"
  }
}
```

### Default Value:

By default, Automatic provisioning of monitoring agent is set to On.

## References:

1. <https://docs.microsoft.com/en-us/azure/security-center/security-center-data-security>
2. <https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-data-collection>
3. <https://msdn.microsoft.com/en-us/library/mt704062.aspx>
4. <https://msdn.microsoft.com/en-us/library/mt704063.aspx>
5. <https://docs.microsoft.com/en-us/rest/api/securitycenter/autoprovisioningsettings/list>
6. <https://docs.microsoft.com/en-us/rest/api/securitycenter/autoprovisioningsettings/create>
7. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-5-centralize-security-log-management-and-analysis>
8. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-3-enable-logging-for-security-investigation>
9. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-incident-response#ir-2-preparation--setup-incident-notification>

## Additional Information:

- Excluding any of the entries in `input.json` may disable the specific setting by default
- Microsoft has recently changed APIs to get and Update Automatic Provisioning Setting. This recommendation is updated accordingly.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</u></b> Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	<b><u>7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets</u></b> Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		●	●
v7	<b><u>3.1 Run Automated Vulnerability Scanning Tools</u></b> Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

## 2.1.16 Ensure that Auto provisioning of 'Vulnerability assessment for machines' is Set to 'On' (Manual)

### Profile Applicability:

- Level 2

### Description:

Enable automatic provisioning of vulnerability assessment for machines on both Azure and hybrid (Arc enabled) machines.

### Rationale:

Vulnerability assessment for machines scans for various security-related configurations and events such as system updates, OS vulnerabilities, and endpoint protection, then produces alerts on threat and vulnerability findings.

### Impact:

Additional licensing is required and configuration of Azure Arc introduces complexity beyond this recommendation.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Microsoft Defender for Cloud
3. Then Environment Settings
4. Select a subscription
5. Click on Settings & Monitoring
6. Ensure that Vulnerability assessment for machines is set to On

Repeat the above for any additional subscriptions.

### Remediation:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Microsoft Defender for Cloud
3. Then Environment Settings
4. Select a subscription
5. Click on Settings & Monitoring
6. Ensure that Vulnerability assessment for machines is set to On

Repeat the above for any additional subscriptions.

## Default Value:

By default, Automatic provisioning of monitoring agent is set to Off.

## References:

1. <https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection?tabs=autoprovision-va>
2. <https://msdn.microsoft.com/en-us/library/mt704062.aspx>
3. <https://msdn.microsoft.com/en-us/library/mt704063.aspx>
4. <https://docs.microsoft.com/en-us/rest/api/securitycenter/autoprovisioningsettings/list>
5. <https://docs.microsoft.com/en-us/rest/api/securitycenter/autoprovisioningsettings/create>
6. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-5-perform-vulnerability-assessments>

## Additional Information:

While this feature is generally available as of publication, it is not yet available for Azure Government tenants.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b><u>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</u></b> Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	<b><u>7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets</u></b> Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		●	●
v7	<b><u>3.1 Run Automated Vulnerability Scanning Tools</u></b> Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

## 2.1.17 Ensure that Auto provisioning of 'Microsoft Defender for Containers components' is Set to 'On' (Manual)

### Profile Applicability:

- Level 2

### Description:

Enable automatic provisioning of the Microsoft Defender for Containers components.

### Rationale:

As with any compute resource, Container environments require hardening and run-time protection to ensure safe operations and detection of threats and vulnerabilities.

### Impact:

Microsoft Defender for Containers will require additional licensing.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Microsoft Defender for Cloud
3. Then Environment Settings
4. Select a subscription
5. Then Auto Provisioning in the left column.
6. Ensure that Microsoft Defender for Containers components is set to On

Repeat the above for any additional subscriptions.

### Remediation:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Microsoft Defender for Cloud
3. Then Environment Settings
4. Select a subscription
5. Then Auto Provisioning in the left column.
6. Set Microsoft Defender for Containers components to On

### Default Value:

By default, Microsoft Defender for Containers is disabled. If Defender for Containers is enabled from the Microsoft Defender for Cloud portal, auto provisioning will be enabled.

## References:

1. <https://docs.microsoft.com/en-us/azure/defender-for-cloud/defender-for-containers-introduction>
2. <https://docs.microsoft.com/en-us/azure/defender-for-cloud/enable-data-collection?tabs=autoprovision-containers>
3. <https://msdn.microsoft.com/en-us/library/mt704062.aspx>
4. <https://msdn.microsoft.com/en-us/library/mt704063.aspx>
5. <https://docs.microsoft.com/en-us/rest/api/securitycenter/autoprovisioningsettings/list>
6. <https://docs.microsoft.com/en-us/rest/api/securitycenter/autoprovisioningsettings/create>
7. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-incident-response#ir-2-preparation--setup-incident-notification>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</u></b>            Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.</p>		●	●
v8	<p><b><u>7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets</u></b>            Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.</p>		●	●
v7	<p><b><u>3.1 Run Automated Vulnerability Scanning Tools</u></b>            Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.</p>		●	●

## 2.1.18 Ensure That 'All users with the following roles' is set to 'Owner' (Automated)

### Profile Applicability:

- Level 1

### Description:

Enable security alert emails to subscription owners.

### Rationale:

Enabling security alert emails to subscription owners ensures that they receive security alert emails from Microsoft. This ensures that they are aware of any potential security issues and can mitigate the risk in a timely fashion.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Microsoft Defender for Cloud
3. Then Environment Settings
4. Click on the appropriate Management Group, Subscription, or Workspace
5. Click on Email notifications
6. Ensure that All users with the following roles is set to Owner

#### From Azure CLI

Ensure the output of below command is set to true.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts?api-version=2020-01-01-preview' | jq '!.value[] |
select(.name=="default")'|jq '.properties.notificationsByRole'
```

### Remediation:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Microsoft Defender for Cloud
3. Click on Environment Settings
4. Click on the appropriate Management Group, Subscription, or Workspace
5. Click on Email notifications
6. In the drop down of the All users with the following roles field select Owner
7. Click Save

## From Azure CLI

Use the below command to set Send email also to subscription owners to On.

```
az account get-access-token --query  
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1  
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:  
application/json"  
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se  
curityContacts/default1?api-version=2017-08-01-preview -d"input.json"'
```

Where `input.json` contains the data below, replacing `validEmailAddress` with a single email address or multiple comma-separated email addresses:

```
{  
  "id":  
  "/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/securityC  
ontacts/default1",  
  "name": "default1",  
  "type": "Microsoft.Security/securityContacts",  
  "properties": {  
    "email": "<validEmailAddress>",  
    "alertNotifications": "On",  
    "alertsToAdmins": "On",  
    "notificationsByRole": "Owner"  
  }  
}
```

### Default Value:

By default, `Owner` is selected

### References:

1. <https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details>
2. <https://docs.microsoft.com/en-us/rest/api/securitycenter/securitycontacts/list>
3. <https://docs.microsoft.com/en-us/rest/api/securitycenter/security-contacts>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-incident-response#ir-2-preparation--setup-incident-notification>

### Additional Information:

Excluding any entries in the `input.json` properties block disables the specific setting by default.



**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>17.2 Establish and Maintain Contact Information for Reporting Security Incidents</u></b>                      Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.</p>	●	●	●
v7	<p><b><u>19.5 Maintain Contact Information For Reporting Security Incidents</u></b>                      Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and ISAC partners.</p>	●	●	●

DRAFT

## 2.1.19 Ensure 'Additional email addresses' is Configured with a Security Contact Email (Automated)

### Profile Applicability:

- Level 1

### Description:

Microsoft Defender for Cloud emails the subscription owners whenever a high-severity alert is triggered for their subscription. You should provide a security contact email address as an additional email address.

### Rationale:

Microsoft Defender for Cloud emails the Subscription Owner to notify them about security alerts. Adding your Security Contact's email address to the 'Additional email addresses' field ensures that your organization's Security Team is included in these alerts. This ensures that the proper people are aware of any potential compromise in order to mitigate the risk in a timely fashion.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu.
2. Select Microsoft Defender for Cloud
3. Click on Environment Settings
4. Click on the appropriate Management Group, Subscription, or Workspace
5. Click on Email notifications
6. Ensure that a valid security contact email address is listed in the Additional email addresses field

#### From Azure CLI

Ensure the output of the below command is set not empty and is set with appropriate email ids.

```
az account get-access-token --query  
"{subscription:subscription,accessToken}" --out tsv | xargs -L1  
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:  
application/json"  
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se  
curityContacts?api-version=2020-01-01-preview' | jq '.|.[] |  
select(.name=="default")'|jq '.properties.emails'
```

## Remediation:

### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Microsoft Defender for Cloud
3. Click on Environment Settings
4. Click on the appropriate Management Group, Subscription, or Workspace
5. Click on Email notifications
6. Enter a valid security contact email address (or multiple addresses separated by commas) in the Additional email addresses field
7. Click Save

### From Azure CLI

Use the below command to set Security contact emails to On.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts/default?api-version=2020-01-01-preview -d@input.json'
```

Where `input.json` contains the data below, replacing `validEmailAddress` with a single email address or multiple comma-separated email addresses:

```
{
  "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/securityC
ontacts/default",
  "name": "default",
  "type": "Microsoft.Security/securityContacts",
  "properties": {
    "email": "<validEmailAddress>",
    "alertNotifications": "On",
    "alertsToAdmins": "On"
  }
}
```

### Default Value:

By default, there are no additional email addresses entered.







### References:

1. <https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details>
2. <https://docs.microsoft.com/en-us/rest/api/securitycenter/securitycontacts/list>
3. <https://docs.microsoft.com/en-us/rest/api/securitycenter/security-contacts>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-incident-response#ir-2-preparation--setup-incident-notification>

**Additional Information:**

Excluding any entries in the input.json properties block disables the specific setting by default.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>17.2 Establish and Maintain Contact Information for Reporting Security Incidents</u></b> Establish and maintain contact information for parties that need to be informed of security incidents. Contacts may include internal staff, third-party vendors, law enforcement, cyber insurance providers, relevant government agencies, Information Sharing and Analysis Center (ISAC) partners, or other stakeholders. Verify contacts annually to ensure that information is up-to-date.</p>			
v7	<p><b><u>19.5 Maintain Contact Information For Reporting Security Incidents</u></b> Assemble and maintain information on third-party contact information to be used to report a security incident, such as Law Enforcement, relevant government departments, vendors, and ISAC partners.</p>			

DRAFT

## 2.1.20 Ensure That 'Notify about alerts with the following severity' is Set to 'High' (Automated)

### Profile Applicability:

- Level 1

### Description:

Enables emailing security alerts to the subscription owner or other designated security contact.

### Rationale:

Enabling security alert emails ensures that security alert emails are received from Microsoft. This ensures that the right people are aware of any potential security issues and are able to mitigate the risk.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Microsoft Defender for Cloud
3. Click on Environment Settings
4. Click on the appropriate Management Group, Subscription, or Workspace
5. Click on Email notifications
6. Ensure that the Notify about alerts with the following severity (or higher) setting is checked and set to High

#### From Azure CLI

Ensure the output of below command is set to `true`, enter your Subscription ID at the `$0` between `/subscriptions/<$0>/providers`.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/providers/Microsoft.Security/se
curityContacts?api-version=2020-01-01-preview' | jq '.|.[] |
select(.name=="default")'|jq '.properties.alertNotifications'
```

### Remediation:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select Microsoft Defender for Cloud
3. Click on Environment Settings
4. Click on the appropriate Management Group, Subscription, or Workspace

5. Click on Email notifications
6. Under Notification types, check the check box next to Notify about alerts with the following severity (or higher): and select High from the drop down menu
7. Click Save

### From Azure CLI

Use the below command to set Send email notification for high severity alerts to On.

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/<$0>/providers/Microsoft.Security/
securityContacts/default1?api-version=2017-08-01-preview -d@input.json'
```

Where input.json contains the data below, replacing validEmailAddress with a single email address or multiple comma-separated email addresses:

```
{
  "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/securityC
ontacts/default1",
  "name": "default1",
  "type": "Microsoft.Security/securityContacts",
  "properties": {
    "email": "<validEmailAddress>",
    "alertNotifications": "On",
    "alertsToAdmins": "On"
  }
}
```

### Default Value:

By default, Send email notification for high severity alerts is not set.

### References:

1. <https://docs.microsoft.com/en-us/azure/security-center/security-center-provide-security-contact-details>
2. <https://docs.microsoft.com/en-us/rest/api/securitycenter/securitycontacts/list>
3. <https://docs.microsoft.com/en-us/rest/api/securitycenter/security-contacts>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-incident-response#ir-2-preparation--setup-incident-notification>

### Additional Information:

Excluding any entries in the input.json properties block disables the specific setting by default. This recommendation has been updated to reflect recent changes to Microsoft REST APIs for getting and updating security contact information.

**CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>13.11 <u>Tune Security Event Alerting Thresholds</u></b> Tune security event alerting thresholds monthly, or more frequently.			●
v7	<b>6.8 <u>Regularly Tune SIEM</u></b> On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.			●

DRAFT

## 2.1.21 Ensure that Microsoft Defender for Cloud Apps integration with Microsoft Defender for Cloud is Selected (Manual)

### Profile Applicability:

- Level 2

### Description:

This integration setting enables Microsoft Defender for Cloud Apps (formerly 'Microsoft Cloud App Security' or 'MCAS' - see additional info) to communicate with Microsoft Defender for Cloud.

### Rationale:

Microsoft Defender for Cloud offers an additional layer of protection by using Azure Resource Manager events, which is considered to be the control plane for Azure. By analyzing the Azure Resource Manager records, Microsoft Defender for Cloud detects unusual or potentially harmful operations in the Azure subscription environment. Several of the preceding analytics are powered by Microsoft Defender for Cloud Apps. To benefit from these analytics, subscription must have a Cloud App Security license.

Microsoft Defender for Cloud Apps works only with Standard Tier subscriptions.

### Impact:

Microsoft Defender for Cloud Apps works with Standard pricing tier Subscription. Choosing the Standard pricing tier of Microsoft Defender for Cloud incurs an additional cost per resource.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Defender for Cloud`
3. Select `Environment Settings` blade
4. Click on the subscription name
5. Select the `Integrations` blade
6. Ensure setting `Allow Microsoft Defender for Cloud Apps to access my data` is selected.



## From Azure CLI

Ensure the output of the below command is `True`

```
az account get-access-token --query  
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1  
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:  
application/json"  
https://management.azure.com/subscriptions/<subscription_ID>/providers/Micros  
oft.Security/settings?api-version=2021-06-01' | jq '.|.value[] |  
select(.name=="MCAS")'|jq '.properties.enabled'
```

## From PowerShell

Run the following series of commands to audit this configuration

```
Get-AzAccount  
Set-AzContext -Subscription <subscription ID>  
Get-AzSecuritySetting | Select-Object name,enabled |where-object {$_.name -eq  
"MCAS"}
```

## PowerShell Output - Non-Compliant

```
Name Enabled  
-----  
MCAS      False
```

## PowerShell Output - Compliant

```
Name Enabled  
-----  
MCAS      True
```

## Remediation:

### From Azure Portal

1. From Azure Home select the Portal Menu.
2. Select Microsoft Defender for Cloud.
3. Select Environment Settings blade.
4. Select the subscription.
5. Select Integrations.
6. Check Allow Microsoft Defender for Cloud Apps to access my data.
7. Select Save.

## From Azure CLI

Use the below command to enable Standard pricing tier for Storage Accounts

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/<subscription_ID>/providers/Micros
oft.Security/settings/MCAS?api-version=2021-06-01 -d@input.json'
```

Where input.json contains the Request body json data as mentioned below.

```
{
  "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/settings/
MCAS",
  "kind": "DataExportSetting",
  "type": "Microsoft.Security/settings",
  "properties": {
    "enabled": true
  }
}
```

### Default Value:

With Cloud App Security license, these alerts are enabled by default.

### References:

1. <https://docs.microsoft.com/en-in/azure/security-center/security-center-alerts-service-layer#azure-management-layer-azure-resource-manager-preview>
2. <https://docs.microsoft.com/en-us/rest/api/securitycenter/settings/list>
3. <https://docs.microsoft.com/en-us/rest/api/securitycenter/settings/update>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-9-secure-user-access-to-existing-applications>

### Additional Information:

NOTE: "Microsoft Defender for Cloud Apps" ("MDCA") is formerly known as "Microsoft Cloud App Security" ("MCAS"). There are a number of places (e.g. Azure CLI) where the "MCAS" acronym is still used within Azure.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</u></b>            Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.</p>		●	●
v8	<p><b><u>7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets</u></b>            Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.</p>		●	●
v8	<p><b><u>13.10 Perform Application Layer Filtering</u></b>            Perform application layer filtering. Example implementations include a filtering proxy, application layer firewall, or gateway.</p>			●
v8	<p><b><u>16.11 Leverage Vetted Modules or Services for Application Security Components</u></b>            Leverage vetted modules or services for application security components, such as identity management, encryption, and auditing and logging. Using platform features in critical security functions will reduce developers' workload and minimize the likelihood of design or implementation errors. Modern operating systems provide effective mechanisms for identification, authentication, and authorization and make those mechanisms available to applications. Use only standardized, currently accepted, and extensively reviewed encryption algorithms. Operating systems also provide mechanisms to create and maintain secure audit logs.</p>		●	●
v7	<p><b><u>3.1 Run Automated Vulnerability Scanning Tools</u></b>            Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.</p>		●	●

## 2.1.22 Ensure that Microsoft Defender for Endpoint integration with Microsoft Defender for Cloud is selected (Manual)

### Profile Applicability:

- Level 2

### Description:

This integration setting enables Microsoft Defender for Endpoint (formerly 'Advanced Threat Protection' or 'ATP' or 'WDATP' - see additional info) to communicate with Microsoft Defender for Cloud.

**IMPORTANT:** When enabling integration between DfE & DfC it needs to be taken into account that this will have some side effects that may be undesirable.

1. For server 2019 & above if defender is installed (default for these server SKU's) this will trigger a deployment of the new unified agent and link to any of the extended configuration in the Defender portal.
2. If the new unified agent is required for server SKU's of Win 2016 or Linux and lower there is additional integration that needs to be switched on and agents need to be aligned.

### Rationale:

Microsoft Defender for Endpoint integration brings comprehensive Endpoint Detection and Response (EDR) capabilities within Microsoft Defender for Cloud. This integration helps to spot abnormalities, as well as detect and respond to advanced attacks on endpoints monitored by Microsoft Defender for Cloud.

MDE works only with Standard Tier subscriptions.

### Impact:

Microsoft Defender for Endpoint works with Standard pricing tier Subscription. Choosing the Standard pricing tier of Microsoft Defender for Cloud incurs an additional cost per resource.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Microsoft Defender for Cloud`
3. Select `Environment Settings` blade
4. Click on the subscription name
5. Select the `Integrations` blade

6. Ensure setting Allow Microsoft Defender for Endpoint to access my data is selected.

### From Azure CLI

Ensure the output of the below command is True

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/<subscriptionID>/providers/Microso
ft.Security/settings?api-version=2021-06-01' | jq '.|.value[] |
select(.name=="WDATP")'|jq '.properties.enabled'
```

### From PowerShell

Run the following commands to login and audit this check

```
Connect-AzAccount
Set-AzContext -Subscription <subscriptionID>
Get-AzSecuritySetting | Select-Object name,enabled |where-object {$_.name -eq
"WDATP"}
```

### PowerShell Output - Non-Compliant

```
Name    Enabled
----    -
WDATP   False
```

### PowerShell Output - Compliant

```
Name    Enabled
----    -
WDATP   True
```

### Remediation:

#### From Azure Console

1. From Azure Home select the Portal Menu.
2. Go to Microsoft Defender for Cloud.
3. Select Environment Settings blade.
4. Select the subscription.
5. Select Integrations.
6. Check Allow Microsoft Defender for Endpoint to access my data.
7. Select Save.

## From Azure CLI

Use the below command to enable Standard pricing tier for Storage Accounts

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X PUT -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/<subscriptionID>/providers/Microso
ft.Security/settings/WDATP?api-version=2021-06-01 -d@input.json'
```

Where input.json contains the Request body json data as mentioned below.

```
{
  "id":
"/subscriptions/<Your_Subscription_Id>/providers/Microsoft.Security/settings/
WDATP",
  "kind": "DataExportSettings",
  "type": "Microsoft.Security/settings",
  "properties": {
    "enabled": true
  }
}
```

## References:

1. <https://docs.microsoft.com/en-in/azure/defender-for-cloud/integration-defender-for-endpoint?tabs=windows>
2. <https://docs.microsoft.com/en-us/rest/api/securitycenter/settings/list>
3. <https://docs.microsoft.com/en-us/rest/api/securitycenter/settings/update>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security#es-1-use-endpoint-detection-and-response-edr>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security#es-2-use-modern-anti-malware-software>

## Additional Information:

**IMPORTANT:** When enabling integration between DfE & DfC it needs to be taken into account that this will have some side effects that may be undesirable.

1. For server 2019 & above if defender is installed (default for these server SKU's) this will trigger a deployment of the new unified agent and link to any of the extended configuration in the Defender portal.
2. If the new unified agent is required for server SKU's of Win 2016 or Linux and lower there is additional integration that needs to be switched on and agents need to be aligned.

NOTE: "Microsoft Defender for Endpoint (MDE)" was formerly known as "Windows Defender Advanced Threat Protection (WDATP)." There are a number of places (e.g. Azure CLI) where the "WDATP" acronym is still used within Azure.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</u></b>            Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.</p>		●	●
v8	<p><b><u>10.1 Deploy and Maintain Anti-Malware Software</u></b>            Deploy and maintain anti-malware software on all enterprise assets.</p>	●	●	●
v8	<p><b><u>10.6 Centrally Manage Anti-Malware Software</u></b>            Centrally manage anti-malware software.</p>		●	●
v8	<p><b><u>13.2 Deploy a Host-Based Intrusion Detection Solution</u></b>            Deploy a host-based intrusion detection solution on enterprise assets, where appropriate and/or supported.</p>		●	●
v7	<p><b><u>3.1 Run Automated Vulnerability Scanning Tools</u></b>            Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.</p>		●	●

DRAFT

## 2.2 Microsoft Defender for IoT

DRAFT



## 2.2.1 Ensure That Microsoft Defender for IoT Hub Is Set To 'On' (Manual)

### Profile Applicability:

- Level 2

### Description:

Microsoft Defender for IoT acts as a central security hub for IoT devices within your organization.

### Rationale:

IoT devices are very rarely patched and can be potential attack vectors for enterprise networks. Updating their network configuration to use a central security hub allows for detection of these breaches.

### Impact:

Enabling Microsoft Defender for IoT will incur additional charges dependent on the level of usage.

### Audit:

#### From Azure Portal

1. Go to `IoT Hub`.
2. Select a `IoT Hub` to validate.
3. Select `Overview` in `Defender for IoT`.
4. The `Threat prevention` and `Threat detection` screen will appear, if `Defender for IoT` is Enabled.

### Remediation:

#### From Azure Portal

1. Go to `IoT Hub`.
2. Select a `IoT Hub` to validate.
3. Select `Overview` in `Defender for IoT`.
4. Click on `Secure your IoT solution`, and complete the onboarding.

### Default Value:

By default, Microsoft Defender for IoT is not enabled.

### References:

1. <https://azure.microsoft.com/en-us/services/iot-defender/#overview>

2. <https://docs.microsoft.com/en-us/azure/defender-for-iot/>
3. <https://azure.microsoft.com/en-us/pricing/details/iot-defender/>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/baselines/defender-for-iot-security-baseline>
5. <https://docs.microsoft.com/en-us/cli/azure/iot?view=azure-cli-latest>
6. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-1-enable-threat-detection-capabilities>
7. <https://learn.microsoft.com/en-us/azure/defender-for-iot/device-builders/quickstart-onboard-iot-hub>

**Additional Information:**

There are additional configurations for Microsoft Defender for IoT that allow for types of deployments called hybrid or local. Both run on your physical infrastructure. These are complicated setups and are primarily outside of the scope of a purely Azure benchmark. Please see the references to consider these options for your organization.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</b> Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	<b>13.6 Collect Network Traffic Flow Logs</b> Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.		●	●
v7	<b>3.1 Run Automated Vulnerability Scanning Tools</b> Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.		●	●

## 2.3 Microsoft Defender for External Attack Surface Monitoring

As more services are exposed to the public internet it is important to be able to monitor the externally exposed surface of your Azure Tenant, to this end it is recommended that tools that monitor this surface are implemented.

Microsoft have a new tool to do this in their Defender Suite of products. Defender EASM, this tool is configured very simply to scan specified domains and report on them, specific domains and addresses can be excluded from the scan.

Typically these tools will report on any vulnerability that is identified (CVE) and will also identify ports and protocols that are open on devices.

Results are classified Critical/High/Medium & Low with proposed mitigations.

DRAFT

### 3 Storage Accounts

This section covers security recommendations to follow to set storage account policies on an Azure Subscription. An Azure storage account provides a unique namespace to store and access Azure Storage data objects.

DRAFT

### 3.1 Ensure that 'Secure transfer required' is set to 'Enabled' (Automated)

#### Profile Applicability:

- Level 1

#### Description:

Enable data encryption in transit.

#### Rationale:

The secure transfer option enhances the security of a storage account by only allowing requests to the storage account by a secure connection. For example, when calling REST APIs to access storage accounts, the connection must use HTTPS. Any requests using HTTP will be rejected when 'secure transfer required' is enabled. When using the Azure files service, connection without encryption will fail, including scenarios using SMB 2.1, SMB 3.0 without encryption, and some flavors 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.

#### Audit:

##### From Azure Portal

1. Go to `Storage Accounts`
2. For each storage account, go to `Configuration`
3. Ensure that `Secure transfer required` is set to `Enabled`

##### From Azure CLI

Use the below command to ensure the `Secure transfer required` is enabled for all the `Storage Accounts` by ensuring the output contains `true` for each of the `Storage Accounts`.

```
az storage account list --query "[*].[name,enableHttpsTrafficOnly]"
```

#### Remediation:

##### From Azure Portal

1. Go to `Storage Accounts`
2. For each storage account, go to `Configuration`
3. Set `Secure transfer required` to `Enabled`

## From Azure CLI

Use the below command to enable Secure transfer required for a Storage Account

```
az storage account update --name <storageAccountName> --resource-group <resourceGroupName> --https-only true
```

### Default Value:

By default, Secure transfer required is set to Disabled.

### References:

1. <https://docs.microsoft.com/en-us/azure/storage/blobs/security-recommendations#encryption-in-transit>
2. [https://docs.microsoft.com/en-us/cli/azure/storage/account?view=azure-cli-latest#az\\_storage\\_account\\_list](https://docs.microsoft.com/en-us/cli/azure/storage/account?view=azure-cli-latest#az_storage_account_list)
3. [https://docs.microsoft.com/en-us/cli/azure/storage/account?view=azure-cli-latest#az\\_storage\\_account\\_update](https://docs.microsoft.com/en-us/cli/azure/storage/account?view=azure-cli-latest#az_storage_account_update)
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-4-encrypt-sensitive-information-in-transit>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 <u>Encrypt Sensitive Data in Transit</u></b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	<b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b> Encrypt all sensitive information in transit.		●	●

## 3.2 Ensure that 'Enable Infrastructure Encryption' for Each Storage Account in Azure Storage is Set to 'enabled' (Manual)

### Profile Applicability:

- Level 2

### Description:

Enabling encryption at the hardware level on top of the default software encryption for Storage Accounts accessing Azure storage solutions.

### Rationale:

Azure Storage automatically encrypts all data in a storage account at the network level using 256-bit AES encryption, which is one of the strongest, FIPS 140-2-compliant block ciphers available. Customers who require higher levels of assurance that their data is secure can also enable 256-bit AES encryption at the Azure Storage infrastructure level for double encryption. Double encryption of Azure Storage data protects against a scenario where one of the encryption algorithms or keys may be compromised. Similarly, data is encrypted even before network transmission and in all backups. In this scenario, the additional layer of encryption continues to protect your data. For the most secure implementation of key based encryption, it is recommended to use a Customer Managed asymmetric RSA 2048 Key in Azure Key Vault.

### Impact:

The read and write speeds to the storage will be impacted if both default encryption and Infrastructure Encryption are checked, as a secondary form of encryption requires more resource overhead for the cryptography of information. This performance impact should be considered in an analysis for justifying use of the feature in your environment. Customer-managed keys are recommended for the most secure implementation, leading to overhead of key management. The key will also need to be backed up in a secure location, as loss of the key will mean loss of the information in the storage.

### Audit:

#### From Azure Portal

1. From Azure Portal select the portal menu in the top left.
2. Select `Storage Accounts`.
3. Click on each storage account within each resource group you wish to audit.
4. In the overview, under `Security`, ensure `Infrastructure encryption` is set to `Enabled`.

## From Azure CLI

```
az storage blob show \  
  --account-name <storage-account> \  
  --container-name <container> \  
  --name <blob> \  
  --query "properties.serverEncrypted"
```

## From PowerShell

```
$account = Get-AzStorageAccount -ResourceGroupName <resource-group> \  
  -Name <storage-account> \  
$blob = Get-AzStorageBlob -Context $account.Context \  
  -Container <container> \  
  -Blob <blob> \  
$blob.ICloudBlob.Properties.IsServerEncrypted
```

## Remediation:

### From Azure Portal

1. During Storage Account creation, in the `Encryption` tab, check the box next to `Enable infrastructure encryption`.

## From Azure CLI

Replace the information within `<>` with appropriate values:

```
az storage account create \  
  --name <storage-account> \  
  --resource-group <resource-group> \  
  --location <location> \  
  --sku Standard_RAGRS \  
  --kind StorageV2 \  
  --require-infrastructure-encryption
```

## From PowerShell

Replace the information within `<>` with appropriate values:

```
New-AzStorageAccount -ResourceGroupName <resource_group> \  
  -AccountName <storage-account> \  
  -Location <location> \  
  -SkuName "Standard_RAGRS" \  
  -Kind StorageV2 \  
  -RequireInfrastructureEncryption
```

## Enabling Infrastructure Encryption after Storage Account Creation

If infrastructure encryption was not enabled on blob storage creation, there is no **official** way to enable it. Please see the additional information section.

## Default Value:

By default, Infrastructure Encryption is disabled in blob creation.



## References:

1. <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-encryption-status>
2. <https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption>
3. <https://docs.microsoft.com/en-us/azure/storage/common/infrastructure-encryption-enable>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-4-enable-data-at-rest-encryption-by-default>

## Additional Information:

The default service side encryption for Azure Storage is enabled on every block blob, append blob, or page blob that was written to Azure Storage after October 20, 2017. Hardware encryption, however, cannot be enabled on a blob storage after its creation. There are ways to copy all data from a blob storage into another or download and reupload into another blob storage. This could result in data loss and is not recommended.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 <u>Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	<b>14.8 <u>Encrypt Sensitive Information at Rest</u></b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

### 3.3 Ensure that 'Enable key rotation reminders' is enabled for each Storage Account (Manual)

#### Profile Applicability:

- Level 1

#### Description:

Access Keys authenticate application access requests to data contained in Storage Accounts. A periodic rotation of these keys is recommended to ensure that potentially compromised keys cannot result in a long-term exploitable credential. The "Rotation Reminder" is an automatic reminder feature for a manual procedure.

#### Rationale:

Reminders such as those generated by this recommendation will help maintain a regular and healthy cadence for activities which improve the overall efficacy of a security program.

Cryptographic key rotation periods will vary depending on your organization's security requirements and the type of data which is being stored in the Storage Account. For example, PCI DSS mandates that cryptographic keys be replaced or rotated 'regularly,' and advises that keys for static data stores be rotated every 'few months.'

For the purposes of this recommendation, 90 days will be prescribed for the reminder. Review and adjustment of the 90 day period is recommended, and may even be necessary. Your organization's security requirements should dictate the appropriate setting.

#### Impact:

This recommendation only creates a periodic reminder to regenerate access keys. Regenerating access keys can affect services in Azure as well as the organization's applications that are dependent on the storage account. All clients that use the access key to access the storage account must be updated to use the new key.

#### Audit:

##### From Azure Portal

1. Go to `Storage Accounts`
2. For each `Storage Account`, go to `Access keys`
3. Click `Set rotation reminder`

If the checkbox for `Enable key rotation reminders` is already checked, that Storage Account is compliant. Review the `Remind me every` field for a desirable periodic setting that fits your security program's needs.

## Remediation:

### From Azure Portal

1. Go to `Storage Accounts`
2. For each `Storage Account` that is not compliant, go to `Access keys`
3. Click `Set rotation reminder`
4. Check `Enable key rotation reminders`
5. In the `Send reminders` field select `Custom`, then set the `Remind me every` field to `90` and the period drop down to `Days`.
6. Click `Save`




### Default Value:

By default, Key rotation reminders is not configured.

### References:

1. <https://docs.microsoft.com/en-us/azure/storage/common/storage-create-storage-account#regenerate-storage-access-keys>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-1-protect-and-limit-highly-privileged-users>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-2-manage-application-identities-securely-and-automatically>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-6-define-identity-and-privileged-access-strategy>
6. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-8-restrict-the-exposure-of-credential-and-secrets>
7. <https://www.pcidssguide.com/pci-dss-key-rotation-requirements/>
8. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.1 Establish and Maintain a Secure Configuration Process</b> Establish and maintain a secure configuration process for enterprise assets (end-user devices, including portable and mobile, non-computing/IoT devices, and servers) and software (operating systems and applications). Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>13.11 <u>Tune Security Event Alerting Thresholds</u></b> Tune security event alerting thresholds monthly, or more frequently.</p>			●
v7	<p><b>6.8 <u>Regularly Tune SIEM</u></b> On a regular basis, tune your SIEM system to better identify actionable events and decrease event noise.</p>			●
v7	<p><b>11.3 <u>Use Automated Tools to Verify Standard Device Configurations and Detect Changes</u></b> Compare all network device configuration against approved security configurations defined for each network device in use and alert when any deviations are discovered.</p>		●	●

DRAFT

### 3.4 Ensure that Storage Account Access Keys are Periodically Regenerated (Manual)

#### Profile Applicability:

- Level 1

#### Description:

For increased security, regenerate storage account access keys periodically.

#### Rationale:

When a storage account is created, Azure generates two 512-bit storage access keys which are used for authentication when the storage account is accessed. Rotating these keys periodically ensures that any inadvertent access or exposure does not result from the compromise of these keys.

Cryptographic key rotation periods will vary depending on your organization's security requirements and the type of data which is being stored in the Storage Account. For example, PCI DSS mandates that cryptographic keys be replaced or rotated 'regularly,' and advises that keys for static data stores be rotated every 'few months.'

For the purposes of this recommendation, 90 days will be prescribed for the reminder. Review and adjustment of the 90 day period is recommended, and may even be necessary. Your organization's security requirements should dictate the appropriate setting.

#### Impact:

Regenerating access keys can affect services in Azure as well as the organization's applications that are dependent on the storage account. All clients who use the access key to access the storage account must be updated to use the new key.

#### Audit:

##### From Azure Portal

1. Go to `Storage Accounts`
2. For each `Storage Account`, go to `Access keys`
3. Review the date in the `Last rotated` field for **each** key.

If the `Last rotated` field indicates a value greater than 90 days [or greater than your organization's period of validity], the key should be rotated.

## From Azure CLI

1. Get a list of storage accounts

```
az storage account list --subscription <subscription-id>
```

Make a note of `id`, `name` and `resourceGroup`.

2. For every storage account make sure that key is regenerated in past 90 days.

```
az monitor activity-log list --namespace Microsoft.Storage --offset 90d --query "[?contains(authorization.action, 'regenerateKey')]" --resource-id <resource id>
```

The output should contain

```
"authorization"/"scope": <your_storage_account> AND "authorization"/"action": "Microsoft.Storage/storageAccounts/regeneratekey/action" AND "status"/"localizedValue": "Succeeded" "status"/"Value": "Succeeded"
```

## Remediation:

### From Azure Portal

1. Go to `Storage Accounts`
2. For each `Storage Account` with outdated keys, go to `Access keys`
3. Click `Rotate key` next to the outdated key, then click `Yes` to the prompt confirming that you want to regenerate the access key.

After Azure regenerates the `Access Key`, you can confirm that `Access keys` reflects a `Last rotated date of` (0 days ago).

### Default Value:

By default, access keys are not regenerated periodically.

**References:**

1. <https://docs.microsoft.com/en-us/azure/storage/common/storage-create-storage-account#regenerate-storage-access-keys>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-1-protect-and-limit-highly-privileged-users>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-2-restrict-administrative-access-to-business-critical-systems>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-2-manage-application-identities-securely-and-automatically>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-6-define-identity-and-privileged-access-strategy>
6. <https://www.pcidssguide.com/pci-dss-key-rotation-requirements/>
7. <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.6 Securely Manage Enterprise Assets and Software</b>                      Securely manage enterprise assets and software. Example implementations include managing configuration through version-controlled-infrastructure-as-code and accessing administrative interfaces over secure network protocols, such as Secure Shell (SSH) and Hypertext Transfer Protocol Secure (HTTPS). Do not use insecure management protocols, such as Telnet (Teletype Network) and HTTP, unless operationally essential.</p>	●	●	●
v8	<p><b>6.2 Establish an Access Revoking Process</b>                      Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.</p>	●	●	●
v7	<p><b>16.7 Establish Process for Revoking Access</b>                      Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.</p>		●	●

## 3.5 Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' requests (Automated)

### Profile Applicability:

- Level 2

### Description:

The Storage Queue service stores messages that may be read by any client who has access to the storage account. A queue can contain an unlimited number of messages, each of which can be up to 64KB in size using version 2011-08-18 or newer. Storage Logging happens server-side and allows details for both successful and failed requests to be recorded in the storage account. These logs allow users to see the details of read, write, and delete operations against the queues. Storage Logging log entries contain the following information about individual requests: Timing information such as start time, end-to-end latency, and server latency, authentication details, concurrency information, and the sizes of the request and response messages.

### Rationale:

Storage Analytics logs contain detailed information about successful and failed requests to a storage service. This information can be used to monitor individual requests and to diagnose issues with a storage service. Requests are logged on a best-effort basis.

Storage Analytics logging is not enabled by default for your storage account.

### Impact:

Enabling this setting can have a high impact on the cost of the log analytics service and data storage used by logging more data per each request. Do not enable this without determining your need for this level of logging, and do not forget to check in on data usage and projected cost. Some users have seen their logging costs increase from \$10 per month to \$10,000 per month.

### Audit:

#### From Azure Portal:

1. Go to `Storage Accounts`.
2. Select the specific `Storage Account`.
3. Click the `Diagnostics settings (classic)` blade from `Monitoring (classic)` section.
4. Ensure the `Status` is set to `On`, if set to `Off`.
5. Select `Queue properties`.
6. Ensure `Read Write Delete` options are selected under the `Logging` section.



## From Azure CLI

Ensure the below command's output contains properties `delete`, `read` and `write` set to `true`.

```
az storage logging show --services q --account-name <storageAccountName>
```

## Remediation:

### From Azure Portal

1. Go to Storage Accounts.
2. Select the specific Storage Account.
3. Click the Diagnostics settings (classic) blade from Monitoring (classic) section.
4. Set the Status to On, if set to Off.
5. Select Queue properties.
6. Select Read, Write and Delete options under the Logging section to enable Storage Logging for Queue service.

## From Azure CLI

Use the below command to enable the Storage Logging for Queue service.

```
az storage logging update --account-name <storageAccountName> --account-key <storageAccountKey> --services q --log rwd --retention 90
```

## Default Value:

By default storage account queue services are not logged.

## References:

1. <https://docs.microsoft.com/en-us/rest/api/storageservices/about-storage-analytics-logging>
2. <https://docs.microsoft.com/en-us/cli/azure/storage/logging?view=azure-cli-latest>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-4-enable-logging-for-azure-resources>
4. <https://docs.microsoft.com/en-us/azure/storage/queues/monitor-queue-storage?tabs=azure-portal>

## Additional Information:

We cannot practically generalize detailed audit log requirements for every queue due to their nature and intent. This recommendation may be applicable to storage account queue services where the security is paramount.

**CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

DRAFT

## 3.6 Ensure that Shared Access Signature Tokens Expire Within an Hour (Manual)

### Profile Applicability:

- Level 1

### Description:

Expire shared access signature tokens within an hour.

### Rationale:

A shared access signature (SAS) is a URI that grants restricted access rights to Azure Storage resources. A shared access signature can be provided to clients who should not be trusted with the storage account key but for whom it may be necessary to delegate access to certain storage account resources. Providing a shared access signature URI to these clients allows them access to a resource for a specified period of time. This time should be set as low as possible and preferably no longer than an hour.

### Audit:

Currently, SAS token expiration times cannot be audited. Until Microsoft makes token expiration time a setting rather than a token creation parameter, this recommendation would require a manual verification.

### Remediation:

When generating shared access signature tokens, use start and end time such that it falls within an hour.

#### From Azure Portal

1. Go to Storage Accounts
2. For each storage account, go to Shared access signature
3. Set Start and expiry date/time within an hour

### Default Value:

By default, expiration for shared access signature is set to 8 hours.

### References:

1. <https://docs.microsoft.com/en-us/rest/api/storageservices/delegating-access-with-a-shared-access-signature>
2. <https://docs.microsoft.com/en-us/azure/storage/common/storage-sas-overview>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>6.2 <u>Establish an Access Revoking Process</u></b>            Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.</p>	●	●	●
v7	<p><b>16.7 <u>Establish Process for Revoking Access</u></b>            Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.</p>		●	●

DRAFT

### 3.7 Ensure that 'Public access level' is disabled for storage accounts with blob containers (Automated)

#### Profile Applicability:

- Level 1

#### Description:

Disallowing public access for a storage account overrides the public access settings for individual containers in that storage account.

#### Rationale:

The default configuration for a storage account permits a user with appropriate permissions to configure public (anonymous) access to containers and blobs in a storage account. Keep in mind that public access to a container is always turned off by default and must be explicitly configured to permit anonymous requests. It grants read-only access to these resources without sharing the account key, and without requiring a shared access signature. It is recommended not to provide anonymous access to blob containers until, and unless, it is strongly desired. A shared access signature token or Azure AD RBAC should be used for providing controlled and timed access to blob containers. If no anonymous access is needed on any container in the storage account, it's recommended to set `allowBlobPublicAccess` false at the account level, which forbids any container to accept anonymous access in the future.

#### Impact:

Access will have to be managed using shared access signatures or via Azure AD RBAC.

#### Audit:

##### From Azure Portal

1. Go to `Storage Accounts`
2. For each storage account, go to the `Networking` setting under `Security + networking`
3. Ensure the `Public Network Access` setting is set to `Disabled`.

##### From Azure CLI

Ensure `publicNetworkAccess` is `Disabled`

```
az storage account show --name <storage-account> --resource-group <resource-group> --query "{publicNetworkAccess:publicNetworkAccess}"
```

## From PowerShell

For each Storage Account, ensure `PublicNetworkAccess` is Disabled

```
Get-AzStorageAccount -Name <storage account name> -ResourceGroupName  
<resource group name> |select PublicNetworkAccess
```

## Remediation:

### From Azure Portal

First, follow Microsoft documentation and create shared access signature tokens for your blob containers. Then,

1. Go to Storage Accounts
2. For each storage account, go to Networking in Security + networking
3. Set Public Network Access to Disabled if no anonymous access is needed on the storage account

### From Azure CLI

Set 'Public Network Access' to Disabled on the storage account

```
az storage account update --name <storage-account> --resource-group  
<resource-group> --public-network-access Disabled
```

### From PowerShell

For each Storage Account, run the following to set the `PublicNetworkAccess` setting to Disabled

```
Set-AzStorageAccount -ResourceGroupName <resource group name> -Name <storage  
account name> -PublicNetworkAccess Disabled
```







## Default Value:

By default, Public Network Access is set to Enabled from all networks for the Storage Account.

## References:

1. <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-manage-access-to-resources>
2. <https://docs.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-prevent>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-2-secure-cloud-services-with-network-controls>
5. <https://docs.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-configure>
6. <https://docs.microsoft.com/en-us/azure/storage/blobs/assign-azure-role-data-access>

**CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

DRAFT

## 3.8 Ensure Default Network Access Rule for Storage Accounts is Set to Deny (Automated)

### Profile Applicability:

- Level 1

### Description:

Restricting default network access helps to provide a new layer of security, since storage accounts accept connections from clients on any network. To limit access to selected networks, the default action must be changed.

### Rationale:

Storage accounts should be configured to deny access to traffic from all networks (including internet traffic). Access can be granted to traffic from specific Azure Virtual networks, allowing a secure network boundary for specific applications to be built. Access can also be granted to public internet IP address ranges to enable connections from specific internet or on-premises clients. When network rules are configured, only applications from allowed networks can access a storage account. When calling from an allowed network, applications continue to require proper authorization (a valid access key or SAS token) to access the storage account.

### Impact:

All allowed networks will need to be whitelisted on each specific network, creating administrative overhead. This may result in loss of network connectivity, so do not turn on for critical resources during business hours.

### Audit:

#### From Azure Console

1. Go to Storage Accounts
2. For each storage account, Click on the `Networking` blade.
3. Click the `Firewalls and virtual networks` heading.
4. Ensure that `Allow access from All networks` is not selected.

#### From Azure CLI

Ensure `defaultAction` is not set to `Allow`.

```
az storage account list --query '[*].networkRuleSet'
```



## From PowerShell

```
Connect-AzAccount
Set-AzContext -Subscription <subscription ID>
Get-AzStorageAccountNetworkRuleset -ResourceGroupName <resource group> -Name
<storage account name> |Select-Object DefaultAction
```

### PowerShell Result - Non-Compliant

```
DefaultAction      : Allow
```

### PowerShell Result - Compliant

```
DefaultAction      : Deny
```

## Remediation:

### From Azure Console

1. Go to Storage Accounts
2. For each storage account, Click on the Networking blade
3. Click the Firewalls and virtual networks heading.
4. Ensure that you have elected to allow access from Selected networks
5. Add rules to allow traffic from specific network.
6. Click Save to apply your changes.

### From Azure CLI

Use the below command to update default-action to Deny.

```
az storage account update --name <StorageAccountName> --resource-group
<resourceGroupName> --default-action Deny
```

## Default Value:

By default, Storage Accounts will accept connections from clients on any network.

## References:

1. <https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-2-define-and-implement-enterprise-segmentationseparation-of-duties-strategy>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-2-secure-cloud-services-with-network-controls>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>12.2 <u>Establish and Maintain a Secure Network Architecture</u></b> Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	<b>13.3 <u>Monitor and Block Unauthorized Network Traffic</u></b> Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.			●

DRAFT

### 3.9 Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access (Automated)

#### Profile Applicability:

- Level 2

#### Description:

Some Azure services that interact with storage accounts operate from networks that can't be granted access through network rules. To help this type of service work as intended, allow the set of trusted Azure services to bypass the network rules. These services will then use strong authentication to access the storage account. If the Allow trusted Azure services exception is enabled, the following services are granted access to the storage account: Azure Backup, Azure Site Recovery, Azure DevTest Labs, Azure Event Grid, Azure Event Hubs, Azure Networking, Azure Monitor, and Azure SQL Data Warehouse (when registered in the subscription).

#### Rationale:

Turning on firewall rules for storage account will block access to incoming requests for data, including from other Azure services. We can re-enable this functionality by enabling "Trusted Azure Services" through networking exceptions.

#### Impact:

This creates authentication credentials for services that need access to storage resources so that services will no longer need to communicate via network request. There may be a temporary loss of communication as you set each Storage Account. It is recommended to not do this on mission-critical resources during business hours.

#### Audit:

##### From Azure Portal

1. Go to `Storage Accounts`
2. For each storage account, Click on the `Networking` blade
3. Click on the `Firewalls and virtual networks` heading.
4. Ensure that `Enabled from selected virtual networks and IP addresses` is selected.
5. Ensure that `Allow Azure services on the trusted services list to access this storage account` is checked in `Exceptions`.

## From Azure CLI

Ensure `bypass` contains `AzureServices`

```
az storage account list --query '[*].networkRuleSet'
```

## From PowerShell

```
Connect-AzAccount  
Set-AzContext -Subscription <subscription ID>  
Get-AzStorageAccountNetworkRuleset -ResourceGroupName <resource group> -Name  
<storage account name> |Select-Object Bypass
```

If the resultant output from the above command shows 'NULL', that storage account configuration is out of compliance with this check. If the result of the above command shows 'AzureServices', that storage account configuration is in compliance with this check.

## Remediation:

### From Azure Portal

1. Go to `Storage Accounts`
2. For each storage account, Click on the `Networking` blade
3. Click on the `Firewalls and virtual networks` heading.
4. Ensure that `Enabled from selected virtual networks and IP addresses` is selected.
5. Under the 'Exceptions' label, enable check box for `Allow Azure services on the trusted services list to access this storage account`.
6. Click `Save` to apply your changes.

## From Azure CLI

Use the below command to update `Azure services`.

```
az storage account update --name <StorageAccountName> --resource-group  
<resourceGroupName> --bypass AzureServices
```

## Default Value:

By default, Storage Accounts will accept connections from clients on any network.

## References:

1. <https://docs.microsoft.com/en-us/azure/storage/common/storage-network-security>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-2-secure-cloud-services-with-network-controls>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.3 <u>Configure Data Access Control Lists</u></b>            Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.</p>	●	●	●
v8	<p><b>13.5 <u>Manage Access Control for Remote Assets</u></b>            Manage access control for assets remotely connecting to enterprise resources. Determine amount of access to enterprise resources based on: up-to-date anti-malware software installed, configuration compliance with the enterprise's secure configuration process, and ensuring the operating system and applications are up-to-date.</p>		●	●
v7	<p><b>13.3 <u>Monitor and Block Unauthorized Network Traffic</u></b>            Deploy an automated tool on network perimeters that monitors for unauthorized transfer of sensitive information and blocks such transfers while alerting information security professionals.</p>			●

DRAFT

### 3.10 Ensure Private Endpoints are used to access Storage Accounts (Automated)

#### Profile Applicability:

- Level 1

#### Description:

Use private endpoints for your Azure Storage accounts to allow clients and services to securely access data located over a network via an encrypted Private Link. To do this, the private endpoint uses an IP address from the VNet for each service. Network traffic between disparate services securely traverses encrypted over the VNet. This VNet can also link addressing space, extending your network and accessing resources on it. Similarly, it can be a tunnel through public networks to connect remote infrastructures together. This creates further security through segmenting network traffic and preventing outside sources from accessing it.

#### Rationale:

Securing traffic between services through encryption protects the data from easy interception and reading.

#### Impact:

There is no cost in deploying VNets between Azure resources. If improperly implemented, it may result in loss of critical network traffic.

#### Audit:

##### From Azure Portal

1. Open the `Storage Accounts` blade.
2. For each listed `Storage Account`, perform the following check:
3. Under the `Security + networking` heading, click on `Networking`.
4. Click on the `Private Endpoint Connections` tab at the top of the networking window.
5. Ensure that for each VNet that the `Storage Account` must be accessed from, a unique `Private Endpoint` is deployed and the `Connection State` for each `Private Endpoint` is `Approved`

Repeat the procedure for each `Storage Account`.

## From PowerShell

```
$storageAccount = Get-AzStorageAccount -ResourceGroup '<ResourceGroupName>' -
Name '<storageaccountname>'

Get-AzPrivateEndpoint -ResourceGroup '<ResourceGroupName>' |Where-Object
{$_PrivateLinkServiceConnectionsText -match $storageAccount.id}
```

If the results of the second command returns information, the Storage Account is using a Private Endpoint and complies with this Benchmark, otherwise if the results of the second command are empty, the Storage Account generates a finding.

## From Azure CLI

```
az storage account show --name '<storage account name>' --query
"privateEndpointConnections[0].id"
```

If the above command returns data, the Storage Account complies with this Benchmark, otherwise if the results are empty, the Storage Account generates a finding.

## Remediation:

### From Azure Portal

1. Open the `Storage Accounts` blade
2. For each listed `Storage Account`, perform the following:
3. Under the `Security + networking` heading, click on `Networking`
4. Click on the `Private Endpoint Connections` tab at the top of the networking window
5. Click the `+Private endpoint` button
6. In the `1 - Basics` tab/step:
  - o Enter a name that will be easily recognizable as associated with the `Storage Account` (*Note: The "Network Interface Name" will be automatically completed, but you can customize it if needed.*)
  - o Ensure that the `Region` matches the region of the `Storage Account`
  - o Click `Next`
7. In the `2 - Resource` tab/step:
  - o Select the `target sub-resource` based on what type of storage resource is being made available
  - o Click `Next`
8. In the `3 - Virtual Network` tab/step:
  - o Select the `Virtual network` that your `Storage Account` will be connecting to
  - o Select the `Subnet` that your `Storage Account` will be connecting to
  - o (Optional) Select other network settings as appropriate for your environment
  - o Click `Next`
9. In the `4 - DNS` tab/step:

- (Optional) Select other DNS settings as appropriate for your environment
  - Click `Next`
10. In the `5 - Tags` tab/step:
- (Optional) Set any tags that are relevant to your organization
  - Click `Next`
11. In the `6 - Review + create` tab/step:
- A validation attempt will be made and after a few moments it should indicate `Validation Passed` - if it does not pass, double-check your settings before beginning more in depth troubleshooting.
  - If validation has passed, click `Create` then wait for a few minutes for the scripted deployment to complete.

Repeat the above procedure for each Private Endpoint required within every Storage Account.

### From PowerShell

```
$storageAccount = Get-AzStorageAccount -ResourceGroupName
'<ResourceGroupName>' -Name '<storageaccountname>'

$privateEndpointConnection = @{
    Name = 'connectionName'
    PrivateLinkServiceId = $storageAccount.Id
    GroupID =
"blob|blob_secondary|file|file_secondary|table|table_secondary|queue|queue_se
condary|web|web_secondary|dfs|dfs_secondary"
}

$privateLinkServiceConnection = New-AzPrivateLinkServiceConnection
@privateEndpointConnection

$virtualNetDetails = Get-AzVirtualNetwork -ResourceGroupName
'<ResourceGroupName>' -Name '<name>'

$privateEndpoint = @{
    ResourceGroupName = '<ResourceGroupName>'
    Name = '<PrivateEndpointName>'
    Location = '<location>'
    Subnet = $virtualNetDetails.Subnets[0]
    PrivateLinkServiceConnection =
$privateLinkServiceConnection
}

New-AzPrivateEndpoint @privateEndpoint
```



## From Azure CLI

```
az network private-endpoint create --resource-group <ResourceGroupName> --location <location> --name <private endpoint name> --vnet-name <VNET Name> --subnet <subnet name> --private-connection-resource-id <storage account ID> --connection-name <private link service connection name> --group-id <blob|blob_secondary|file|file_secondary|table|table_secondary|queue|queue_secondary|web|web_secondary|dfs|dfs_secondary>
```

### Default Value:

By default, Private Endpoints are not created for Storage Accounts.

### References:

1. <https://docs.microsoft.com/en-us/azure/storage/common/storage-private-endpoints>
2. <https://docs.microsoft.com/en-us/azure/virtual-network/virtual-networks-overview>
3. <https://docs.microsoft.com/en-us/azure/private-link/create-private-endpoint-portal>
4. <https://docs.microsoft.com/en-us/azure/private-link/create-private-endpoint-cli?tabs=dynamic-ip>
5. <https://docs.microsoft.com/en-us/azure/private-link/create-private-endpoint-powershell?tabs=dynamic-ip>
6. <https://docs.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-storage-portal>
7. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-2-secure-cloud-services-with-network-controls>

### Additional Information:

A NAT gateway is the recommended solution for outbound internet access.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>12.2 Establish and Maintain a Secure Network Architecture</b> Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	<b>14.1 Segment the Network Based on Sensitivity</b> Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).		●	●

### 3.11 Ensure Soft Delete is Enabled for Azure Containers and Blob Storage (Automated)

#### Profile Applicability:

- Level 1

#### Description:

The Azure Storage blobs contain data like ePHI or Financial, which can be secret or personal. Data that is erroneously modified or deleted by an application or other storage account user will cause data loss or unavailability.

It is recommended that both Azure Containers with attached Blob Storage and standalone containers with Blob Storage be made recoverable by enabling the **soft delete** configuration. This is to save and recover data when blobs or blob snapshots are deleted.

#### Rationale:

Containers and Blob Storage data can be incorrectly deleted. An attacker/malicious user may do this deliberately in order to cause disruption. Deleting an Azure Storage blob causes immediate data loss. Enabling this configuration for Azure storage ensures that even if blobs/data were deleted from the storage account, Blobs/data objects are recoverable for a particular time which is set in the "Retention policies," ranging from 7 days to 365 days.

#### Impact:

Additional storage costs may be incurred as snapshots are retained.

#### Audit:

#### From Azure Portal:

1. From the Azure home page, open the hamburger menu in the top left or click on the arrow pointing right with 'More services' underneath.
2. Select Storage.
3. Select Storage Accounts.
4. For each Storage Account, navigate to Data protection in the left scroll column.
5. Ensure that soft delete is checked for both blobs and containers. Also check if the retention period is a sufficient length for your organization.

## From Azure CLI Blob Storage

Ensure that the output of the below command contains enabled status as true and days is not empty or null

```
az storage blob service-properties delete-policy show --account-name  
<StorageAccountName> --account-key <accountkey>
```

## Azure Containers

Make certain that the --enable-container-delete-retention is 'true'.

```
az storage account blob-service-properties show  
  --account-name <StorageAccountName>  
  --account-key <accountkey>  
  --resource-group <resource_group>
```

## Remediation:

### From Azure Portal

1. From the Azure home page, open the hamburger menu in the top left or click on the arrow pointing right with 'More services' underneath.
2. Select Storage.
3. Select Storage Accounts.
4. For each Storage Account, navigate to Data protection in the left scroll column.
5. Check soft delete for both blobs and containers. Set the retention period to a sufficient length for your organization.

## From Azure CLI

Update blob storage retention days in below command

```
az storage blob service-properties delete-policy update --days-retained  
<RetentionDaysValue> --account-name <StorageAccountName> --account-key  
<AccountKey> --enable true
```

Update container retention with the below command

```
az storage account blob-service-properties update  
  --enable-container-delete-retention true  
  --container-delete-retention-days <days>  
  --account-name <storage-account>  
  --resource-group <resource_group>  
  --account-key <AccountKey>
```







## Default Value:

When a new storage account is created, soft delete for containers and blob storage is by default **disabled**.

## References:

1. <https://docs.microsoft.com/en-us/azure/storage/blobs/storage-blob-soft-delete>
2. <https://docs.microsoft.com/en-us/azure/storage/blobs/soft-delete-container-overview>
3. <https://docs.microsoft.com/en-us/azure/storage/blobs/soft-delete-container-enable?tabs=azure-portal>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>11.1 <u>Establish and Maintain a Data Recovery Process</u></b> Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.			
v7	<b>10.4 <u>Ensure Protection of Backups</u></b> Ensure that backups are properly protected via physical security or encryption when they are stored, as well as when they are moved across the network. This includes remote backups and cloud services.			

## 3.12 Ensure Storage for Critical Data are Encrypted with Customer Managed Keys (Manual)

### Profile Applicability:

- Level 2

### Description:

Enable sensitive data encryption at rest using Customer Managed Keys rather than Microsoft Managed keys.

### Rationale:

By default, data in the storage account is encrypted using Microsoft Managed Keys at rest. All Azure Storage resources are encrypted, including blobs, disks, files, queues, and tables. All object metadata is also encrypted. If you want to control and manage this encryption key yourself, however, you can specify a customer-managed key. That key is used to protect and control access to the key that encrypts your data. You can also choose to automatically update the key version used for Azure Storage encryption whenever a new version is available in the associated Key Vault.

### Impact:

If the key expires by setting the 'activation date' and 'expiration date', the user must rotate the key manually.

Using Customer Managed Keys may also incur additional man-hour requirements to create, store, manage, and protect the keys as needed.

### Audit:

#### From Azure Console:

1. Go to `Storage Accounts`
2. For each storage account, go to `Encryption`
3. Ensure that Encryption type is set to `Customer Managed Keys`

#### From PowerShell

```
Connect-AzAccount
Set-AzContext -Subscription <subscription id>
Get-AzStorageAccount |Select-Object -ExpandProperty Encryption
```

#### PowerShell Results - Non-Compliant

```
...
KeySource           : Microsoft.Storage
...
```

## PowerShell Results - Compliant

```
...  
KeySource : Microsoft.Keyvault  
...
```

### Remediation:

#### From Azure Portal

1. Go to `Storage Accounts`
2. For each storage account, go to `Encryption`
3. Set `Customer Managed Keys`
4. Select the Encryption key and enter the appropriate setting value
5. Click `Save`

### Default Value:

By default, Encryption type is set to Microsoft Managed Keys.

### References:

1. <https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption>
2. <https://docs.microsoft.com/en-us/azure/security/fundamentals/data-encryption-best-practices#protect-data-at-rest>
3. <https://docs.microsoft.com/en-us/azure/storage/common/storage-service-encryption#azure-storage-encryption-versus-disk-encryption>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-5-use-customer-managed-key-option-in-data-at-rest-encryption-when-required>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 <u>Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	<b>14.8 <u>Encrypt Sensitive Information at Rest</u></b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

### 3.13 Ensure Storage logging is Enabled for Blob Service for 'Read', 'Write', and 'Delete' requests (Automated)

#### Profile Applicability:

- Level 2

#### Description:

The Storage Blob service provides scalable, cost-efficient object storage in the cloud. Storage Logging happens server-side and allows details for both successful and failed requests to be recorded in the storage account. These logs allow users to see the details of read, write, and delete operations against the blobs. Storage Logging log entries contain the following information about individual requests: timing information such as start time, end-to-end latency, and server latency; authentication details; concurrency information; and the sizes of the request and response messages.

#### Rationale:

Storage Analytics logs contain detailed information about successful and failed requests to a storage service. This information can be used to monitor each individual request to a storage service for increased security or diagnostics. Requests are logged on a best-effort basis.

Storage Analytics logging is not enabled by default for your storage account.

#### Impact:

Being a level 2, enabling this setting can have a high impact on the cost of data storage used for logging more data per each request. Do not enable this without determining your need for this level of logging or forget to check in on data usage and projected cost.

#### Audit:

##### From Azure Portal

1. From the default portal page select `Storage Accounts`.
2. Select the specific `Storage Account`.
3. Click the `Diagnostics settings` under the `Monitoring` section in the left column.
4. Select the 'blob' tab indented below the storage account. Then select the diagnostic setting listed.
5. Ensure `StorageRead`, `StorageWrite`, and `StorageDelete` options are selected under the `Logging` section and that they are sent to the correct destination.

## From Azure CLI

Ensure the below command's output contains properties delete, read and write set to true.

```
az storage logging show --services b --account-name <storageAccountName>
```

## Remediation:

### From Azure Portal

1. From the default portal page select `Storage Accounts`.
2. Select the specific `Storage Account`.
3. Click the `Diagnostics settings` under the `Monitoring` section in the left column.
4. Select the 'blob' tab indented below the storage account.
5. Click '+ Add diagnostic setting'.
6. Select `StorageRead`, `StorageWrite` and `StorageDelete` options under the `Logging` section to enable `Storage Logging for Blob service`.
7. Select a destination for your logs to be sent to.

## From Azure CLI

Use the below command to enable the `Storage Logging for Blob service`.

```
az storage logging update --account-name <storageAccountName> --account-key <storageAccountKey> --services b --log rwd --retention 90
```

## Default Value:

By default, storage account blob service logging is disabled for read, write, and delete operations.

## References:

1. <https://docs.microsoft.com/en-us/rest/api/storageservices/about-storage-analytics-logging>
2. <https://docs.microsoft.com/en-us/cli/azure/storage/logging?view=azure-cli-latest>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-3-enable-logging-for-security-investigation>

## Additional Information:

We cannot practically generalize detailed audit log requirements for every blob due to their nature and intent. This recommendation may be applicable to storage account blob service where the security is paramount.



**CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

DRAFT

### 3.14 Ensure Storage Logging is Enabled for Table Service for 'Read', 'Write', and 'Delete' Requests (Automated)

#### Profile Applicability:

- Level 2

#### Description:

Azure Table storage is a service that stores structured NoSQL data in the cloud, providing a key/attribute store with a schema-less design. Storage Logging happens server-side and allows details for both successful and failed requests to be recorded in the storage account. These logs allow users to see the details of read, write, and delete operations against the tables. Storage Logging log entries contain the following information about individual requests: timing information such as start time, end-to-end latency, and server latency; authentication details; concurrency information; and the sizes of the request and response messages.

#### Rationale:

Storage Analytics logs contain detailed information about successful and failed requests to a storage service. This information can be used to monitor each individual request to a storage service for increased security or diagnostics. Requests are logged on a best-effort basis.

Storage Analytics logging is not enabled by default for your storage account.

#### Impact:

Being a level 2, enabling this setting can have a high impact on the cost of data storage used for logging more data per each request. Do not enable this without determining your need for this level of logging or forget to check in on data usage and projected cost.

#### Audit:

##### From Azure Portal

1. From the default portal page select `Storage Accounts`.
2. Select the specific `Storage Account`.
3. Click the `Diagnostics settings` under the `Monitoring` section in the left column.
4. Select the 'table' tab indented below the storage account. Then select the diagnostic setting listed.
5. Ensure `StorageRead`, `StorageWrite`, and `StorageDelete` options are selected under the `Logging` section and that they are sent to the correct destination.

## From Azure CLI

Ensure the below command's output contains properties delete, read and write set to true.

```
az storage logging show --services t --account-name <storageAccountName>
```

## Remediation:

### From Azure Portal

1. From the default portal page select `Storage Accounts`.
2. Select the specific `Storage Account`.
3. Click the `Diagnostics settings` under the `Monitoring` section in the left column.
4. Select the 'table' tab indented below the storage account.
5. Click '+ Add diagnostic setting'.
6. Select `StorageRead`, `StorageWrite` and `StorageDelete` options under the `Logging` section to enable `Storage Logging for Table service`.
7. Select a destination for your logs to be sent to.

## From Azure CLI

Use the below command to enable the `Storage Logging for Table service`.

```
az storage logging update --account-name <storageAccountName> --account-key <storageAccountKey> --services t --log rwd --retention 90
```

## Default Value:

By default, storage account table service logging is disabled for read, write, and delete operations

## References:

1. <https://docs.microsoft.com/en-us/rest/api/storageservices/about-storage-analytics-logging>
2. <https://docs.microsoft.com/en-us/cli/azure/storage/logging?view=azure-cli-latest>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-4-enable-logging-for-azure-resources>

## Additional Information:

We cannot practically generalize detailed audit log requirements for every table due to their nature and intent. This recommendation may be applicable to storage account table service where the security is paramount.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

DRAFT

### 3.15 Ensure the "Minimum TLS version" for storage accounts is set to "Version 1.2" (Automated)

#### Profile Applicability:

- Level 1

#### Description:

In some cases, Azure Storage sets the minimum TLS version to be version 1.0 by default. TLS 1.0 is a legacy version and has known vulnerabilities. This minimum TLS version can be configured to be later protocols such as TLS 1.2.

#### Rationale:

TLS 1.0 has known vulnerabilities and has been replaced by later versions of the TLS protocol. Continued use of this legacy protocol affects the security of data in transit.

#### Impact:

When set to TLS 1.2 all requests must leverage this version of the protocol. Applications leveraging legacy versions of the protocol will fail.

#### Audit:

##### From Azure Console

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to Storage Accounts
3. Click on each Storage Account
4. Under Setting section, Click on Configuration
5. Ensure that the minimum TLS version is set to be Version 1.2

##### From Azure CLI

Get a list of all storage accounts and their resource groups

```
az storage account list | jq '.[ ] | {name, resourceGroup}'
```

Then query the minimumTLSVersion field

```
az storage account show \
  --name <storage-account> \
  --resource-group <resource-group> \
  --query minimumTlsVersion \
  --output tsv
```

## From Azure PowerShell

To get the minimum TLS version, run the following command:

```
(Get-AzStorageAccount -Name <STORAGEACCOUNTNAME> -ResourceGroupName <RESOURCEGROUPNAME>).MinimumTlsVersion
```

## Remediation:

### From Azure Console

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to Storage Accounts
3. Click on each Storage Account
4. Under Setting section, Click on Configuration
5. Set the minimum TLS version to be Version 1.2

### From Azure CLI

```
az storage account update \  
  --name <storage-account> \  
  --resource-group <resource-group> \  
  --min-tls-version TLS1_2
```

## From Azure PowerShell

To set the minimum TLS version, run the following command:

```
Set-AzStorageAccount -AccountName <STORAGEACCOUNTNAME> \  
  -ResourceGroupName <RESOURCEGROUPNAME> \  
  -MinimumTlsVersion TLS1_2
```

## Default Value:

If a storage account is created through the portal, the MinimumTlsVersion property for that storage account will be set to TLS 1.2.

If a storage account is created through PowerShell or CLI, the MinimumTlsVersion property for that storage account will not be set, and defaults to TLS 1.0.

## References:

1. <https://docs.microsoft.com/en-us/azure/storage/common/transport-layer-security-configure-minimum-version?tabs=portal>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-3-encrypt-sensitive-data-in-transit>

**CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>3.10 <u>Encrypt Sensitive Data in Transit</u></b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	<b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b> Encrypt all sensitive information in transit.		●	●

DRAFT

## 4 Database Services

This section covers security recommendations to follow to set general database services policies on an Azure Subscription. Subsections will address specific database types.

DRAFT



## 4.1 SQL Server - Auditing

Auditing for Azure SQL Servers and SQL Databases tracks database events and writes them to an audit log Azure storage account, Log Analytics workspace or Event Hubs. Auditing helps to maintain regulatory compliance, understand database activity, and gain insight into discrepancies and anomalies that could indicate business concerns or suspected security violations. Auditing enables and facilitates adherence to compliance standards, although it doesn't guarantee compliance.

The Default SQL Server Auditing profile set for SQL server is inherited by all the SQL Databases which are part of the SQL server.

DRAFT

## 4.1.1 Ensure that 'Auditing' is set to 'On' (Automated)

### Profile Applicability:

- Level 1

### Description:

Enable auditing on SQL Servers.

### Rationale:

The Azure platform allows a SQL server to be created as a service. Enabling auditing at the server level ensures that all existing and newly created databases on the SQL server instance are audited. Auditing policy applied on the SQL database does not override auditing policy and settings applied on the particular SQL server where the database is hosted.

Auditing tracks database events and writes them to an audit log in the Azure storage account. It also helps to maintain regulatory compliance, understand database activity, and gain insight into discrepancies and anomalies that could indicate business concerns or suspected security violations.

### Audit:

#### From Azure Portal

1. Go to `SQL servers`
2. For each server instance
3. Click on `Auditing`
4. Ensure that `Enable Azure SQL Auditing` is set to `On`

#### From PowerShell

Get the list of all SQL Servers

```
Get-AzSqlServer
```

For each Server

```
Get-AzSqlServerAudit -ResourceGroupName <ResourceGroupName> -ServerName  
<SQLServerName>
```

Ensure that `BlobStorageTargetState`, `EventHubTargetState`, or `LogAnalyticsTargetState` is set to `Enabled`.

## Remediation:

### From Azure Portal

1. Go to SQL servers
2. Select the SQL server instance
3. Under Security, click Auditing
4. Click the toggle next to Enable Azure SQL Auditing
5. Select an Audit log destination
6. Click Save

### From PowerShell

Get the list of all SQL Servers

```
Get-AzSqlServer
```

For each Server, enable auditing and set the retention for at least 90 days.

#### Log Analytics Example

```
Set-AzSqlServerAudit -ResourceGroupName <resource group name> -ServerName  
<SQL Server name> -RetentionInDays <Number of Days to retain the audit logs,  
should be 90days minimum> -LogAnalyticsTargetState Enabled -  
WorkspaceResourceId "/subscriptions/<subscription  
ID>/resourceGroups/insights-  
integration/providers/Microsoft.OperationalInsights/workspaces/<workspace  
name>
```

#### Event Hub Example

```
Set-AzSqlServerAudit -ResourceGroupName "<resource group name>" -ServerName  
"<SQL Server name>" -EventHubTargetState Enabled -EventHubName  
"<Event Hub name>" -EventHubAuthorizationRuleResourceId "<Event Hub  
Authorization Rule Resource ID>"
```

#### Blob Storage Example\*

```
Set-AzSqlServerAudit -ResourceGroupName "<resource group name>" -ServerName  
"<SQL Server name>" -BlobStorageTargetState Enabled  
-StorageAccountResourceId  
"/subscriptions/<subscription_ID>/resourceGroups/<Resource_Group>/providers/M  
icrosoft.Stora  
ge/storageAccounts/<Storage Account name>"
```

#### Default Value:

By default, Enable Azure SQL Auditing is set to Off.

## References:

1. <https://docs.microsoft.com/en-us/azure/security-center/security-center-enable-auditing-on-sql-servers>
2. <https://docs.microsoft.com/en-us/powershell/module/azurearm.sql/get-azurermsqlserverauditing?view=azurermps-5.2.0>
3. <https://docs.microsoft.com/en-us/powershell/module/azurearm.sql/set-azurermsqlserverauditingpolicy?view=azurermps-5.2.0>
4. <https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-3-enable-logging-for-security-investigation>

## Additional Information:

- A server policy applies to all existing and newly created databases on the server.
- If server blob auditing is enabled, it always applies to the database. The database will be audited, regardless of the database auditing settings. Auditing type table is already deprecated leaving only type blob available.
- Enabling blob auditing on the database, in addition to enabling it on the server, does not override or change any of the settings of the server blob auditing. Both audits will exist side by side. In other words, the database is audited twice in parallel; once by the server policy and once by the database policy.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 Collect Detailed Audit Logs</b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	<b>6.3 Enable Detailed Logging</b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

## 4.1.2 Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP) (Automated)

### Profile Applicability:

- Level 1

### Description:

Ensure that no SQL Databases allow ingress from 0.0.0.0/0 (ANY IP).

### Rationale:

Azure SQL Server includes a firewall to block access to unauthorized connections. More granular IP addresses can be defined by referencing the range of addresses available from specific datacenters.

By default, for a SQL server, a Firewall exists with StartIp of 0.0.0.0 and EndIP of 0.0.0.0 allowing access to all the Azure services.

Additionally, a custom rule can be set up with StartIp of 0.0.0.0 and EndIP of 255.255.255.255 allowing access from ANY IP over the Internet.

In order to reduce the potential attack surface for a SQL server, firewall rules should be defined with more granular IP addresses by referencing the range of addresses available from specific datacenters.

### Impact:

Disabling `Allow Azure services and resources to access this server` will break all connections to SQL server and Hosted Databases unless custom IP specific rules are added in Firewall Policy.

### Audit:

#### From Azure Portal

1. Go to `SQL servers`
2. For each SQL server
3. Click on `Firewall and virtual networks`
4. Ensure that `Allow Azure services and resources to access this server` to set to `No`
5. Ensure that no firewall rule exists with
  - Start IP of `0.0.0.0`
  - or other combinations which allows access to wider public IP ranges

## From Azure CLI

List all SQL servers

```
az sql server list
```

For each SQL server run the following command

```
az sql server firewall-rule list --resource-group <resource group name> --server <sql server name>
```

Ensure the output does not contain any firewall `allow` rules with a source of `0.0.0.0`, or any rules named `AllowAllWindowsAzureIps`

## From PowerShell

Get the list of all SQL Servers

```
Get-AzSqlServer
```

For each Server

```
Get-AzSqlServerFirewallRule -ResourceGroupName <resource group name> -ServerName <server name>
```

Ensure that `StartIpAddress` is not set to `0.0.0.0`, `/0` or other combinations which allows access to wider public IP ranges including Windows Azure IP ranges. Also ensure that `FirewallRuleName` doesn't contain `AllowAllWindowsAzureIps` which is the rule created when the `Allow Azure services and resources to access this server` setting is enabled for that SQL Server.

## Remediation:

### From Azure Portal

1. Go to `SQL servers`
2. For each SQL server
3. Click on `Firewall and virtual networks`
4. Set `Allow Azure services and resources to access this server` to `No`
5. Set firewall rules to limit access to only authorized connections

## From Azure CLI

Disable default firewall rule `Allow access to Azure services`:

```
az sql server firewall-rule delete --resource-group <resource group> --server <sql server name> --name "AllowAllWindowsAzureIps"
```

Remove a custom firewall rule:

```
az sql server firewall-rule delete --resource-group <resource group> --server <sql server name> --name <firewall rule name>
```

Create a firewall rule:

```
az sql server firewall-rule create --resource-group <resource group> --server <sql server name> --name <firewall rule name> --start-ip-address "<IP Address other than 0.0.0.0>" --end-ip-address "<IP Address other than 0.0.0.0 or 255.255.255.255>"
```

## Update a firewall rule:

```
az sql server firewall-rule update --resource-group <resource group> --server <sql server name> --name <firewall rule name> --start-ip-address "<IP Address other than 0.0.0.0>" --end-ip-address "<IP Address other than 0.0.0.0 or 255.255.255.255>"
```

## From PowerShell

Disable Default Firewall Rule Allow access to Azure services :

```
Remove-AzSqlServerFirewallRule -FirewallRuleName "AllowAllWindowsAzureIps" -ResourceGroupName <resource group name> -ServerName <server name>
```

## Remove a custom Firewall rule:

```
Remove-AzSqlServerFirewallRule -FirewallRuleName "<firewall rule name>" -ResourceGroupName <resource group name> -ServerName <server name>
```

## Set the appropriate firewall rules:

```
Set-AzSqlServerFirewallRule -ResourceGroupName <resource group name> -ServerName <server name> -FirewallRuleName "<firewall rule name>" -StartIpAddress "<IP Address other than 0.0.0.0>" -EndIpAddress "<IP Address other than 0.0.0.0 or 255.255.255.255>"
```

## Default Value:

By default, setting Allow access to Azure Services is set to ON allowing access to all Windows Azure IP ranges.







## References:

1. <https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/configure-a-windows-firewall-for-database-engine-access?view=sql-server-2017>
2. <https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/get-azurermssqlserverfirewallrule?view=azurerm-5.2.0>
3. <https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/set-azurermssqlserverfirewallrule?view=azurerm-5.2.0>
4. <https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/remove-azurermssqlserverfirewallrule?view=azurerm-5.2.0>
5. <https://docs.microsoft.com/en-us/azure/sql-database/sql-database-firewall-configure>
6. <https://docs.microsoft.com/en-us/sql/relational-databases/system-stored-procedures/sp-set-database-firewall-rule-azure-sql-database?view=azuresqldb-current>
7. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-2-secure-cloud-services-with-network-controls>

### Additional Information:

Firewall rules configured on individual SQL Database using Transact-sql overrides the rules set on SQL server. Azure does not provide any Powershell, API, CLI, Portal option to check database level firewall rules, and so far Transact-SQL is the only way to check for the same. For comprehensive control over egress traffic on SQL Databases, Firewall rules should be checked using SQL client.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b>14.6 Protect Information through Access Control Lists</b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			



### *4.1.3 Ensure SQL server's Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key (Automated)*

#### **Profile Applicability:**

- Level 2

#### **Description:**

Transparent Data Encryption (TDE) with Customer-managed key support provides increased transparency and control over the TDE Protector, increased security with an HSM-backed external service, and promotion of separation of duties.

With TDE, data is encrypted at rest with a symmetric key (called the database encryption key) stored in the database or data warehouse distribution. To protect this data encryption key (DEK) in the past, only a certificate that the Azure SQL Service managed could be used. Now, with Customer-managed key support for TDE, the DEK can be protected with an asymmetric key that is stored in the Azure Key Vault. The Azure Key Vault is a highly available and scalable cloud-based key store which offers central key management, leverages FIPS 140-2 Level 2 validated hardware security modules (HSMs), and allows separation of management of keys and data for additional security.

Based on business needs or criticality of data/databases hosted on a SQL server, it is recommended that the TDE protector is encrypted by a key that is managed by the data owner (Customer-managed key).

#### **Rationale:**

Customer-managed key support for Transparent Data Encryption (TDE) allows user control of TDE encryption keys and restricts who can access them and when. Azure Key Vault, Azure's cloud-based external key management system, is the first key management service where TDE has integrated support for Customer-managed keys. With Customer-managed key support, the database encryption key is protected by an asymmetric key stored in the Key Vault. The asymmetric key is set at the server level and inherited by all databases under that server.

#### **Impact:**

Once TDE protector is encrypted with a Customer-managed key, it transfers entire responsibility of respective key management on to you, and hence you should be more careful about doing any operations on the particular key in order to keep data from corresponding SQL server and Databases hosted accessible.

When deploying Customer Managed Keys, it is prudent to ensure that you also deploy an automated toolset for managing these keys (this should include discovery and key rotation), and Keys should be stored in an HSM or hardware backed keystore, such as Azure Key Vault.

As far as toolsets go, check with your cryptographic key provider, as they may well provide one as an add-on to their service.

## Audit:

### From Azure Portal

1. Go to `SQL servers`

For the desired server instance

2. Click On `Transparent data encryption`
3. Ensure that `Customer-managed key` is selected
4. Ensure `Make selected key the default TDE protector` is checked

### From Azure CLI

```
az account get-access-token --query
"{subscription:subscription,accessToken:accessToken}" --out tsv | xargs -L1
bash -c 'curl -X GET -H "Authorization: Bearer $1" -H "Content-Type:
application/json"
https://management.azure.com/subscriptions/$0/resourceGroups/{resourceGroupNa
me}/providers/Microsoft.Sql/servers/{serverName}/encryptionProtector?api-
version=2015-05-01-preview'
```

Ensure the output of the command contains properties

```
kind set to azurekeyvault
serverKeyType set to AzureKeyVault
uri is not null
```

### From PowerShell

```
Get-AzSqlServerTransparentDataEncryptionProtector -ServerName <ServerName> -
ResourceGroupName <ResourceGroupName>
```

Ensure the output of the command contains properties

```
Type set to AzureKeyVault
ServerKeyVaultKeyName set to KeyVaultName_KeyName_KeyIdentifierVersion
KeyId set to KeyIdentifier
```

## Remediation:

### From Azure Console

1. Go to `SQL servers`

For the desired server instance

2. Click On `Transparent data encryption`
3. Set `Transparent data encryption` to `Customer-managed key`
4. Browse through your `key vaults` to `Select an existing key or create a new key in the Azure Key Vault.`

5. Check `Make selected key the default TDE protector`

### From Azure CLI

Use the below command to encrypt SQL server's TDE protector with a Customer-managed key

```
az sql server tde-key set --resource-group <resourceName> --server <dbServerName> --server-key-type {AzureKeyVault} --kid <keyIdentifier>
```

### From PowerShell

Use the below command to encrypt SQL server's TDE protector with a Customer-managed Key Vault key

```
Set-AzSqlServerTransparentDataEncryptionProtector -Type AzureKeyVault -KeyId <KeyIdentifier> -ServerName <ServerName> -ResourceGroupName <ResourceGroupName>
```

Select `y` when prompted

### Default Value:

By Default, Microsoft managed TDE protector is enabled for a SQL server.

### References:

1. <https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption-byok-azure-sql>
2. <https://azure.microsoft.com/en-in/blog/preview-sql-transparent-data-encryption-tde-with-bring-your-own-key-support/>
3. <https://winterdom.com/2017/09/07/azure-sql-tde-protector-keyvault>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-5-use-customer-managed-key-option-in-data-at-rest-encryption-when-required>
5. <https://docs.microsoft.com/en-us/azure/key-vault/general/basic-concepts>
6. <https://docs.microsoft.com/en-us/cli/azure/sql/server/tde-key?view=azure-cli-latest>
7. <https://learn.microsoft.com/en-us/powershell/module/az.sql/get-azsqlservertransparentdataencryptionprotector?view=azps-9.2.0>
8. <https://learn.microsoft.com/en-us/powershell/module/az.sql/set-azsqlservertransparentdataencryptionprotector?view=azps-9.2.0>

### Additional Information:

- This configuration is audited or can be done only on SQL server. The same configuration will be in effect on SQL Databases hosted on SQL Server.
- Ensuring TDE is protected by a Customer-managed key on SQL Server does not ensure the encryption of SQL Databases. `Transparent Data Encryption : Data Encryption (ON/OFF)` setting on individual SQL Database decides whether database is encrypted or not.

**CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>3.11 <u>Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	<b>16.4 <u>Encrypt or Hash all Authentication Credentials</u></b> Encrypt or hash with a salt all authentication credentials when stored.		●	●

DRAFT

## 4.1.4 Ensure that Azure Active Directory Admin is Configured for SQL Servers (Automated)

### Profile Applicability:

- Level 1

### Description:

Use Azure Active Directory Authentication for authentication with SQL Database to manage credentials in a single place.

### Rationale:

Azure Active Directory authentication is a mechanism to connect to Microsoft Azure SQL Database and SQL Data Warehouse by using identities in Azure Active Directory (Azure AD). With Azure AD authentication, identities of database users and other Microsoft services can be managed in one central location. Central ID management provides a single place to manage database users and simplifies permission management.

- It provides an alternative to SQL Server authentication.
- Helps stop the proliferation of user identities across database servers.
- Allows password rotation in a single place.
- Customers can manage database permissions using external (AAD) groups.
- It can eliminate storing passwords by enabling integrated Windows authentication and other forms of authentication supported by Azure Active Directory.
- Azure AD authentication uses contained database users to authenticate identities at the database level.
- Azure AD supports token-based authentication for applications connecting to SQL Database.
- Azure AD authentication supports ADFS (domain federation) or native user/password authentication for a local Azure Active Directory without domain synchronization.
- Azure AD supports connections from SQL Server Management Studio that use Active Directory Universal Authentication, which includes Multi-Factor Authentication (MFA). MFA includes strong authentication with a range of easy verification options — phone call, text message, smart cards with pin, or mobile app notification.

### Impact:

This will create administrative overhead with user account and permission management. For further security on these administrative accounts, you may want to consider higher tiers of AAD which support features like Multi Factor Authentication, that will cost more.

## Audit:

### From Azure Portal

1. Go to SQL servers
2. For each SQL server, click on Active Directory admin under the Settings section
3. Ensure that a value has been set for Admin Name under the Azure Active Directory admin section

### From Azure CLI

To list SQL Server Admins on a specific server:

```
az sql server ad-admin list --resource-group <resource-group> --server <server>
```

### From PowerShell

Print a list of all SQL Servers to find which one you want to audit

```
Get-AzSqlServer
```

Audit a list of Administrators on a Specific Server

```
Get-AzSqlServerActiveDirectoryAdministrator -ResourceGroupName <resource group name> -ServerName <server name>
```

Ensure Output shows DisplayName set to AD account.

## Remediation:

### From Azure Portal

1. Go to SQL servers
2. For each SQL server, click on Active Directory admin
3. Click on Set admin
4. Select an admin
5. Click Save

### From Azure CLI

```
az ad user show --id
```

For each Server, set AD Admin

```
az sql server ad-admin create --resource-group <resource group name> --server <server name> --display-name <display name> --object-id <object id of user>
```

### From PowerShell

For each Server, set AD Admin

```
Set-AzSqlServerActiveDirectoryAdministrator -ResourceGroupName <resource group name> -ServerName <server name> -DisplayName "<Display name of AD account to set as DB administrator>"
```

## Default Value:

Azure Active Directory Authentication for SQL Database/Server is not enabled by default

## References:

1. <https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication-configure>
2. <https://docs.microsoft.com/en-us/azure/sql-database/sql-database-aad-authentication>
3. <https://docs.microsoft.com/en-us/powershell/module/azurermsql/get-azurermsqlserveractivedirectoryadministrator?view=azurermps-5.2.0>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-1-use-centralized-identity-and-authentication-system>
5. [https://docs.microsoft.com/en-us/cli/azure/sql/server/ad-admin?view=azure-cli-latest#az\\_sql\\_server\\_ad\\_admin\\_list](https://docs.microsoft.com/en-us/cli/azure/sql/server/ad-admin?view=azure-cli-latest#az_sql_server_ad_admin_list)

## Additional Information:

**NOTE** - Assigning an Administrator in Azure Active Directory (AAD) is just the first step. When using AAD for central authentication there are many other groups and roles that need to be configured base on the needs of your organization. The How-to Guides should be used to determine what roles should be assigned and what groups should be created to manage permissions and access to resources.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.6 Centralize Account Management</b> Centralize account management through a directory or identity service.		●	●
v7	<b>16.2 Configure Centralized Point of Authentication</b> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

## 4.1.5 Ensure that 'Data encryption' is set to 'On' on a SQL Database (Automated)

### Profile Applicability:

- Level 1

### Description:

Enable Transparent Data Encryption on every SQL server.

### Rationale:

Azure SQL Database transparent data encryption helps protect against the threat of malicious activity by performing real-time encryption and decryption of the database, associated backups, and transaction log files at rest without requiring changes to the application.

### Audit:

#### From Azure Portal

1. Go to SQL databases
2. For each DB instance
3. Click on Transparent data encryption
4. Ensure that Data encryption is set to On

#### From Azure CLI

Ensure the output of the below command is Enabled

```
az sql db tde show --resource-group <resourceGroup> --server <dbServerName> -  
-database <dbName> --query status
```

#### From PowerShell

Get a list of SQL Servers.

```
Get-AzSqlServer
```

For each server, list the databases.

```
Get-AzSqlDatabase -ServerName <SQL Server Name> -ResourceGroupName <Resource  
Group Name>
```

For each database not listed as a `Master` database, check for Transparent Data Encryption.

```
Get-AzSqlDatabaseTransparentDataEncryption -ResourceGroupName <Resource Group  
Name> -ServerName <SQL Server Name> -DatabaseName <Database Name>
```

Make sure `DataEncryption` is Enabled for each database except the `Master` database.



## Remediation:

### From Azure Portal

1. Go to SQL databases
2. For each DB instance
3. Click on Transparent data encryption
4. Set Data encryption to On

### From Azure CLI

Use the below command to enable Transparent data encryption for SQL DB instance.

```
az sql db tde set --resource-group <resourceGroup> --server <dbServerName> --database <dbName> --status Enabled
```

### From PowerShell

Use the below command to enable Transparent data encryption for SQL DB instance.

```
Set-AzSqlDatabaseTransparentDataEncryption -ResourceGroupName <Resource Group Name> -ServerName <SQL Server Name> -DatabaseName <Database Name> -State 'Enabled'
```

### Note:

- TDE cannot be used to encrypt the logical master database in SQL Database. The master database contains objects that are needed to perform the TDE operations on the user databases.
- Azure Portal does not show master databases per SQL server. However, CLI/API responses will show master databases.

### Default Value:

By default, Data encryption is set to On.

### References:

1. <https://docs.microsoft.com/en-us/sql/relational-databases/security/encryption/transparent-data-encryption-with-azure-sql-database>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-4-enable-data-at-rest-encryption-by-default>
3. <https://learn.microsoft.com/en-us/powershell/module/az.sql/set-azsqldatabasetransparentdataencryption?view=azps-9.2.0>

### Additional Information:

- Transparent Data Encryption (TDE) can be enabled or disabled on individual `SQL Database` level and not on the `SQL Server` level.
- TDE cannot be used to encrypt the logical master database in SQL Database. The master database contains objects that are needed to perform the TDE operations on the user databases.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 <u>Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	<b>14.8 <u>Encrypt Sensitive Information at Rest</u></b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

## 4.1.6 Ensure that 'Auditing' Retention is 'greater than 90 days' (Automated)

### Profile Applicability:

- Level 1

### Description:

SQL Server Audit Retention should be configured to be greater than 90 days.

### Rationale:

Audit Logs can be used to check for anomalies and give insight into suspected breaches or misuse of information and access.

### Audit:

#### From Azure Portal

1. Go to `SQL servers`
2. For each server instance
3. Click on `Auditing`
4. If storage is selected, expand `Advanced properties`
5. Ensure `Retention (days)` setting is greater than 90 days or 0 for unlimited retention.

#### From PowerShell

Get the list of all SQL Servers

```
Get-AzSqlServer
```

For each Server

```
Get-AzSqlServerAudit -ResourceGroupName <resource group name> -ServerName <server name>
```

Ensure that `RetentionInDays` is set to more than 90

**Note:** If the SQL server is set with `LogAnalyticsTargetState` setting set to `Enabled`, run the following additional command.

```
Get-AzOperationalInsightsWorkspace | Where-Object {$_.ResourceId -eq <SQL Server WorkspaceResourceId>}
```

Ensure that `RetentionInDays` is set to more than 90

## Remediation:

### From Azure Portal

1. Go to `SQL servers`
2. For each server instance
3. Click on `Auditing`
4. If storage is selected, expand `Advanced properties`
5. Set the `Retention (days)` setting greater than 90 days or 0 for unlimited retention.
6. Select `Save`

### From PowerShell

For each Server, set retention policy to more than 90 days

#### Log Analytics Example

```
Set-AzSqlServerAudit -ResourceGroupName <resource group name> -ServerName
<SQL Server name> -RetentionInDays <Number of Days to retain the audit logs,
should be more than 90 days> -LogAnalyticsTargetState Enabled -
WorkspaceResourceId "/subscriptions/<subscription
ID>/resourceGroups/insights-
integration/providers/Microsoft.OperationalInsights/workspaces/<workspace
name>
```

#### Event Hub Example

```
Set-AzSqlServerAudit -ResourceGroupName "<resource group name>" -ServerName
"<SQL Server name>" -EventHubTargetState Enabled -EventHubName
"<Event Hub name>" -EventHubAuthorizationRuleResourceId "<Event Hub
Authorization Rule Resource ID>"
```

#### Blob Storage Example\*

```
Set-AzSqlServerAudit -ResourceGroupName "<resource group name>" -ServerName
"<SQL Server name>" -BlobStorageTargetState Enabled
-StorageAccountResourceId
"/subscriptions/<subscription_ID>/resourceGroups/<Resource_Group>/providers/M
icrosoft.Stora
ge/storageAccounts/<Storage Account name>"
```

#### Default Value:

By default, SQL Server audit storage is disabled.

#### References:

1. <https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing>
2. <https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/get-azurermserverauditing?view=azurerm-5.2.0>
3. <https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/set-azurermserverauditing?view=azurerm-5.2.0>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-6-configure-log-storage-retention>

**CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>8.3 <u>Ensure Adequate Audit Log Storage</u></b> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	<b>6.4 <u>Ensure adequate storage for logs</u></b> Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

DRAFT

## 4.2 SQL Server - Microsoft Defender for SQL

Microsoft Defender for SQL provides a layer of security which enables customers to detect and respond to potential threats as they occur through security alerts on anomalous activities. Users will receive an alert upon suspicious database activities, potential vulnerabilities, and SQL injection attacks, as well as anomalous database access patterns. SQL Server Threat Detection alerts provide details of suspicious activity and recommend action on how to investigate and mitigate the threat.

Microsoft Defender for SQL may incur additional cost per SQL server.

DRAFT

## 4.2.1 Ensure that Microsoft Defender for SQL is set to 'On' for critical SQL Servers (Automated)

### Profile Applicability:

- Level 2

### Description:

Enable "Microsoft Defender for SQL" on critical SQL Servers.

### Rationale:

Microsoft Defender for SQL is a unified package for advanced SQL security capabilities. Microsoft Defender is available for Azure SQL Database, Azure SQL Managed Instance, and Azure Synapse Analytics. It includes functionality for discovering and classifying sensitive data, surfacing and mitigating potential database vulnerabilities, and detecting anomalous activities that could indicate a threat to your database. It provides a single go-to location for enabling and managing these capabilities.

### Impact:

Microsoft Defender for SQL is a paid feature and will incur additional cost for each SQL server.

### Audit:

#### From Azure Portal

1. Go to `SQL servers`
2. For each "critical" server instance (e.g. production SQL servers)
3. Click on the `Security Center` blade
4. Click `configure`, next to `Microsoft Defender for SQL`:
5. Ensure that `Microsoft defender for SQL` is toggled to `On`

#### From PowerShell

Get the list of all SQL Servers

```
Get-AzSqlServer
```

For each Server

```
Get-AzSqlServerAdvancedThreatProtectionSetting -ResourceGroupName <resource group name> -ServerName <server name>
```

Ensure that `ThreatDetectionState` is set to `Enabled`.

## Remediation:

### From Azure Portal

1. Go to `SQL servers`
2. For each "critical" server instance (e.g. production SQL servers)
3. Click on the `Security Center` blade
4. Click configure, next to 'Microsoft Defender for SQL:'
5. Set `Microsoft defender for SQL` is toggled to `On`

### From PowerShell

Enable `Advanced Data Security` for a SQL Server:

```
Set-AzSqlServerThreatDetectionPolicy -ResourceGroupName <resource group name>
-ServerName <server name> -EmailAdmins $True
```

#### Note:

- Enabling 'Microsoft Defender for SQL' from the Azure portal enables `Threat Detection`
- Using Powershell command `Set-AzSqlServerThreatDetectionPolicy` enables `Microsoft Defender for SQL` for a SQL server

### Default Value:

By default, `Microsoft Defender for SQL` is set to `Off`.

### References:

1. <https://docs.microsoft.com/en-us/azure/azure-sql/database/azure-defender-for-sql?view=azuresql>
2. <https://docs.microsoft.com/en-us/powershell/module/azurerm.sql/get-azurermssqlserverthreatdetectionpolicy?view=azurermpps-6.13.0&viewFallbackFrom=azurermpps-5.2.0>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-2-monitor-anomalies-and-threats-targeting-sensitive-data>

### Additional Information:

- The feature 'Microsoft Defender for SQL' can be enabled only on SQL server and the same settings will be inherently applied to the SQL databases hosted on the SQL server.



**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</u></b>            Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.</p>		●	●
v8	<p><b><u>7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets</u></b>            Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.</p>		●	●
v7	<p><b><u>3.1 Run Automated Vulnerability Scanning Tools</u></b>            Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.</p>		●	●

DRAFT

## 4.2.2 Ensure that Vulnerability Assessment (VA) is enabled on a SQL server by setting a Storage Account (Automated)

### Profile Applicability:

- Level 2

### Description:

Enable Vulnerability Assessment (VA) service scans for critical SQL servers and corresponding SQL databases.

### Rationale:

Enabling Microsoft Defender for SQL server does not enable Vulnerability Assessment capability for individual SQL databases unless storage account is set to store the scanning data and reports.

The Vulnerability Assessment service scans databases for known security vulnerabilities and highlights deviations from best practices, such as misconfigurations, excessive permissions, and unprotected sensitive data. Results of the scan include actionable steps to resolve each issue and provide customized remediation scripts where applicable. Additionally, an assessment report can be customized by setting an acceptable baseline for permission configurations, feature configurations, and database settings.

### Impact:

Enabling the Microsoft Defender for SQL features will incur additional costs for each SQL server.

### Audit:

#### From Azure Portal

1. Go to SQL servers
2. Select a server instance
3. Click on Security Center
4. Ensure that Microsoft Defender for SQL is set to Enabled
5. Select Configure next to Enabled at subscription-level
6. In Section Vulnerability Assessment Settings, Ensure Storage Accounts does not read Select Storage account with no storage accounts listed under the Storage account heading.

## From PowerShell

Get the list of all SQL Servers

```
Get-AZSqlServer
```

For each Server

```
Get-AzSqlServerVulnerabilityAssessmentSetting -ResourceGroupName <resource group name> -ServerName <server name>
```

Ensure that value for parameter `StorageAccountName` is not empty (blank).

Sample Output:

```
ResourceGroupName           : ResourceGroup01
ServerName                   : Server01
StorageAccountName          : mystorage
ScanResultsContainerName    : vulnerability-assessment
RecurringScansInterval      : None
EmailSubscriptionAdmins     : False
NotificationEmail           : {}
```

## Remediation:

### From Azure Portal

1. Go to SQL servers
2. Select a server instance
3. Click on Security Center
4. Select **Configure next to** Enabled at subscription-level
5. In Section Vulnerability Assessment Settings, Click Select Storage account
6. Choose Storage Account (Existing or Create New). Click Ok
7. Click Save

## From PowerShell

If not already, Enable Microsoft Defender for a SQL:

```
Set-AZSqlServerThreatDetectionPolicy -ResourceGroupName <resource group name> -ServerName <server name> -EmailAdmins $True
```

## To enable ADS-VA service by setting Storage Account

```
Update-AzSqlServerVulnerabilityAssessmentSetting `
  -ResourceGroupName "<resource group name>" `
  -ServerName "<Server Name>" `
  -StorageAccountName "<Storage Name from same subscription and
same Location" `
  -ScanResultsContainerName "vulnerability-assessment" `
  -RecurringScansInterval Weekly `
  -EmailSubscriptionAdmins $true `
  -NotificationEmail @("mail1@mail.com" , "mail2@mail.com")
```

### Default Value:

By default, Microsoft Defender for SQL is not enabled for a SQL server. Enabling Microsoft Defender for SQL does not enable VA scanning by setting Storage Account automatically.

### References:

1. <https://docs.microsoft.com/en-us/azure/sql-database/sql-vulnerability-assessment>
2. <https://docs.microsoft.com/en-us/rest/api/sql/servervulnerabilityassessments/listbyserver>
3. <https://docs.microsoft.com/en-in/powershell/module/Az.Sql/Update-AzSqlServerVulnerabilityAssessmentSetting?view=azps-2.6.0>
4. <https://docs.microsoft.com/en-in/powershell/module/Az.Sql/Get-AzSqlServerVulnerabilityAssessmentSetting?view=azps-2.6.0>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-6-perform-software-vulnerability-assessments>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</b> Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.		●	●
v8	<b>7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets</b> Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><b>3.1 <u>Run Automated Vulnerability Scanning Tools</u></b>  Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.</p>		●	●

DRAFT

### 4.2.3 Ensure that Vulnerability Assessment (VA) setting 'Periodic recurring scans' is set to 'on' for each SQL server (Automated)

#### Profile Applicability:

- Level 2

#### Description:

Enable Vulnerability Assessment (VA) Periodic recurring scans for critical SQL servers and corresponding SQL databases.

#### Rationale:

VA setting 'Periodic recurring scans' schedules periodic (weekly) vulnerability scanning for the SQL server and corresponding Databases. Periodic and regular vulnerability scanning provides risk visibility based on updated known vulnerability signatures and best practices.

#### Impact:

Enabling the `Azure Defender for SQL` feature will incur additional costs for each SQL server.

#### Audit:

##### From Azure Portal

1. Go to `SQL servers`
2. Select a server instance
3. Click on `Security Center`
4. Ensure that `Microsoft Defender for SQL` is set to `Enabled`
5. In Section `Vulnerability Assessment Settings`, Ensure `Storage Accounts` is configured.
6. In Section `Vulnerability Assessment Settings`, Ensure `Periodic recurring scans` is set to `On`.

##### From PowerShell

Get the list of all SQL Servers

```
Get-AZSqlServer
```

For each Server

```
Get-AzSqlServerVulnerabilityAssessmentSetting -ResourceGroupName <resource group name> -ServerName <server name>
```

Ensure that value for parameter `RecurringScansInterval` is not set to `None`.

Sample Output:

```
ResourceGroupName           : ResourceGroup01
ServerName                  : Server01
StorageAccountName         : mystorage
ScanResultsContainerName   : vulnerability-assessment
RecurringScansInterval     : weekly
EmailSubscriptionAdmins    : False
NotificationEmail          : {}
```

### Remediation:

#### From Azure Portal

1. Go to `SQL servers`
2. For each server instance
3. Click on `Security Center`
4. In Section `Vulnerability Assessment Settings`, set `Storage Account` if not already
5. Toggle `'Periodic recurring scans'` to `ON`.
6. Click `Save`

#### From PowerShell

If not already, Enable `Advanced Data Security` for a `SQL Server`:

```
Set-AZSqlServerThreatDetectionPolicy -ResourceGroupName <resource group name>
-ServerName <server name> -EmailAdmins $True
```

To enable `ADS-VA` service with `'Periodic recurring scans'`

```
Update-AzSqlServerVulnerabilityAssessmentSetting `
  -ResourceGroupName "<resource group name>" `
  -ServerName "<Server Name>" `
  -StorageAccountName "<Storage Name from same subscription and
same Location" `
  -ScanResultsContainerName "vulnerability-assessment" `
  -RecurringScansInterval Weekly `
  -EmailSubscriptionAdmins $true `
  -NotificationEmail @("mail1@mail.com" , "mail2@mail.com")
```

#### Default Value:

Enabling `Microsoft Defender for SQL` enables `'Periodic recurring scans'` by default but does not configure the `Storage account`.

**References:**

1. <https://docs.microsoft.com/en-us/azure/sql-database/sql-vulnerability-assessment>
2. <https://docs.microsoft.com/en-us/rest/api/sql/servervulnerabilityassessments/listbyserver>
3. <https://docs.microsoft.com/en-in/powershell/module/Az.Sql/Update-AzSqlServerVulnerabilityAssessmentSetting?view=azps-2.6.0>
4. <https://docs.microsoft.com/en-in/powershell/module/Az.Sql/Get-AzSqlServerVulnerabilityAssessmentSetting?view=azps-2.6.0>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-6-perform-software-vulnerability-assessments>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</u></b>            Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.</p>		●	●
v8	<p><b><u>7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets</u></b>            Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.</p>		●	●
v7	<p><b><u>3.1 Run Automated Vulnerability Scanning Tools</u></b>            Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.</p>		●	●



## 4.2.4 Ensure that Vulnerability Assessment (VA) setting 'Send scan reports to' is configured for a SQL server (Automated)

### Profile Applicability:

- Level 2

### Description:

Configure 'Send scan reports to' with email addresses of concerned data owners/stakeholders for a critical SQL servers.

### Rationale:

Vulnerability Assessment (VA) scan reports and alerts will be sent to email addresses configured at 'Send scan reports to'. This may help in reducing time required for identifying risks and taking corrective measures.

### Impact:

Enabling the Microsoft Defender for SQL features will incur additional costs for each SQL server.

### Audit:

#### From Azure Portal

1. Go to SQL servers
2. Select a server instance
3. Select Microsoft Defender for Cloud
4. Ensure that Enablement status is set to Enabled
5. Select Configure next to Enablement status
6. Under Vulnerability Assessment Settings, ensure Storage Accounts is configured
7. Under Vulnerability Assessment Settings, ensure Send scan reports to is not empty

#### From PowerShell

Get the list of all SQL Servers

```
Get-AZSqlServer
```

For each Server

```
Get-AzSqlServerVulnerabilityAssessmentSetting -ResourceGroupName <resource group name> -ServerName <server name>
```

Ensure that value for parameter `NotificationEmail` is not blank/empty {}.

Sample Output:

```
ResourceGroupName           : ResourceGroup01
ServerName                  : Server01
StorageAccountName         : mystorage
ScanResultsContainerName   : vulnerability-assessment
RecurringScansInterval     : weekly
EmailSubscriptionAdmins    : False
NotificationEmail          : {}
```

## Remediation:

### From Azure Portal

1. Go to SQL servers
2. Select a server instance
3. Select Microsoft Defender for Cloud
4. Select Configure next to Enablement status
5. Set Microsoft Defender for SQL to On
6. Under Vulnerability Assessment Settings, select a Storage Account
7. Set Periodic recurring scans to On
8. Under Send scan reports to, provide email addresses for data owners and stakeholders
9. Click Save

### From PowerShell

If not already, Enable Advanced Data Security for a SQL Server:

```
Set-AZSqlServerThreatDetectionPolicy -ResourceGroupName <resource group name>
-ServerName <server name> -EmailAdmins $True
```

To enable ADS-VA service and Set 'Send scan reports to'

```
Update-AzSqlServerVulnerabilityAssessmentSetting `
  -ResourceGroupName "<resource group name>" `
  -ServerName "<Server Name>" `
  -StorageAccountName "<Storage Name from same subscription and
same Location" `
  -ScanResultsContainerName "vulnerability-assessment" `
  -RecurringScansInterval Weekly `
  -EmailSubscriptionAdmins $true `
  -NotificationEmail @("mail1@mail.com" , "mail2@mail.com")
```

### Default Value:

By default, 'Send reports to' is blank.

**References:**

1. <https://docs.microsoft.com/en-us/azure/sql-database/sql-vulnerability-assessment>
2. <https://docs.microsoft.com/en-us/rest/api/sql/servervulnerabilityassessments/listbyserver>
3. <https://docs.microsoft.com/en-in/powershell/module/Az.Sql/Update-AzSqlServerVulnerabilityAssessmentSetting?view=azps-2.6.0>
4. <https://docs.microsoft.com/en-in/powershell/module/Az.Sql/Get-AzSqlServerVulnerabilityAssessmentSetting?view=azps-2.6.0>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-6-perform-software-vulnerability-assessments>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</u></b>            Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.</p>		●	●
v8	<p><b><u>7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets</u></b>            Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.</p>		●	●
v7	<p><b><u>3.1 Run Automated Vulnerability Scanning Tools</u></b>            Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.</p>		●	●

## 4.2.5 Ensure that Vulnerability Assessment (VA) setting 'Also send email notifications to admins and subscription owners' is set for each SQL Server (Automated)

### Profile Applicability:

- Level 1

### Description:

Enable Vulnerability Assessment (VA) setting 'Also send email notifications to admins and subscription owners'.

### Rationale:

VA scan reports and alerts will be sent to admins and subscription owners by enabling setting 'Also send email notifications to admins and subscription owners'. This may help in reducing time required for identifying risks and taking corrective measures.

### Impact:

Enabling the Microsoft Defender for SQL features will incur additional costs for each SQL server.

### Audit:

#### From Azure Portal

1. Go to SQL servers
2. Select a server instance
3. Click on Security Center
4. Ensure that Microsoft Defender for SQL is set to Enabled
5. Select Configure next to Enabled at subscription-level
6. In Section Vulnerability Assessment Settings, Ensure Storage Accounts is configured.
7. In Section Vulnerability Assessment Settings, Ensure Also send email notifications to admins and subscription owners is checked/enabled.

#### From PowerShell

Get the list of all SQL Servers

```
Get-AZSqlServer
```

For each Server

```
Get-AzSqlServerVulnerabilityAssessmentSetting -ResourceGroupName <resource group name> -ServerName <server name>
```

Ensure that value for parameter `EmailSubscriptionAdmin` is set to true.

Sample Output:

```
ResourceGroupName           : ResourceGroup01
ServerName                  : Server01
StorageAccountName         : mystorage
ScanResultsContainerName    : vulnerability-assessment
RecurringScansInterval     : weekly
EmailSubscriptionAdmins     : False
NotificationEmail           : {}
```

## Remediation:

### From Azure Portal

1. Go to SQL servers
2. Select a server instance
3. Click on Security Center
4. Select Configure next to Enabled at subscription-level
5. In Section Vulnerability Assessment Settings, configure Storage Accounts if not already
6. Check/enable 'Also send email notifications to admins and subscription owners'
7. Click Save

### From PowerShell

If not already, Enable Advanced Data Security for a SQL Server:

```
Set-AZSqlServerThreatDetectionPolicy -ResourceGroupName <resource group name>
-ServerName <server name> -EmailAdmins $True
```

To enable ADS-VA service and Set 'Also send email notifications to admins and subscription owners'

```
Update-AzSqlServerVulnerabilityAssessmentSetting `
    -ResourceGroupName "<resource group name>" `
    -ServerName "<Server Name>" `
    -StorageAccountName "<Storage Name from same subscription and
same Location" `
    -ScanResultsContainerName "vulnerability-assessment" `
    -RecurringScansInterval Weekly `
    -EmailSubscriptionAdmins $true `
    -NotificationEmail @("mail1@mail.com" , "mail2@mail.com")
```

## Default Value:

By default, 'Also send email notifications to admins and subscription owners' is enabled.

**References:**

1. <https://docs.microsoft.com/en-us/azure/sql-database/sql-vulnerability-assessment>
2. <https://docs.microsoft.com/en-us/rest/api/sql/servervulnerabilityassessments/listbyserver>
3. <https://docs.microsoft.com/en-in/powershell/module/Az.Sql/Update-AzSqlServerVulnerabilityAssessmentSetting?view=azps-2.6.0>
4. <https://docs.microsoft.com/en-in/powershell/module/Az.Sql/Get-AzSqlServerVulnerabilityAssessmentSetting?view=azps-2.6.0>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-6-perform-software-vulnerability-assessments>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b><u>7.5 Perform Automated Vulnerability Scans of Internal Enterprise Assets</u></b>                      Perform automated vulnerability scans of internal enterprise assets on a quarterly, or more frequent, basis. Conduct both authenticated and unauthenticated scans, using a SCAP-compliant vulnerability scanning tool.</p>		●	●
v8	<p><b><u>7.6 Perform Automated Vulnerability Scans of Externally-Exposed Enterprise Assets</u></b>                      Perform automated vulnerability scans of externally-exposed enterprise assets using a SCAP-compliant vulnerability scanning tool. Perform scans on a monthly, or more frequent, basis.</p>		●	●
v7	<p><b><u>3.1 Run Automated Vulnerability Scanning Tools</u></b>                      Utilize an up-to-date SCAP-compliant vulnerability scanning tool to automatically scan all systems on the network on a weekly or more frequent basis to identify all potential vulnerabilities on the organization's systems.</p>		●	●

### 4.3 PostgreSQL Database Server

This section groups security best practices/recommendations for Azure PostgreSQL Database Servers.

DRAFT

### 4.3.1 Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database Server (Automated)

#### Profile Applicability:

- Level 1

#### Description:

Enable SSL connection on PostgreSQL Servers.

#### Rationale:

SSL connectivity helps to provide a new layer of security by connecting database server to client applications using Secure Sockets Layer (SSL). Enforcing SSL connections between database server and client applications helps protect against "man in the middle" attacks by encrypting the data stream between the server and application.

#### Audit:

##### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to Azure Database for PostgreSQL server
3. For each database, click on Connection security
4. In SSL settings, ensure Enforce SSL connection is set to ENABLED.

##### From Azure CLI

Ensure the output of the below command returns Enabled.

```
az postgres server show --resource-group myresourcegroup --name <resourceGroupName> --query sslEnforcement
```

##### From PowerShell

Ensure the output of the below command returns Enabled.

```
Get-AzPostgreSqlServer -ResourceGroupName <ResourceGroupName > -ServerName <ServerName> | Select-Object SslEnforcement
```

#### Remediation:

##### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to Azure Database for PostgreSQL server
3. For each database, click on Connection security
4. In SSL settings, click on ENABLED to enforce SSL connections
5. Click Save



## From Azure CLI

Use the below command to enforce ssl connection for PostgreSQL Database.

```
az postgres server update --resource-group <resourceGroupName> --name  
<serverName> --ssl-enforcement Enabled
```

## From PowerShell

```
Update-AzPostgreSqlServer -ResourceGroupName <ResourceGroupName > -ServerName  
<ServerName> -SslEnforcement Enabled
```





## Default Value:

By default, secure connectivity is enforced, but some application frameworks may not enable it during deployment.

## References:

1. <https://docs.microsoft.com/en-us/azure/postgresql/concepts-ssl-connection-security>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-4-encrypt-sensitive-information-in-transit>
3. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/get-azpostgreSqlServer?view=azps-9.2.0#example-2-get-postgresql-server-by-resource-group-and-server-name>
4. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/update-azpostgreSqlServer?view=azps-9.2.0#example-1-update-postgresql-server-by-resource-group-and-server-name>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 <u>Encrypt Sensitive Data in Transit</u></b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).			
v7	<b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b> Encrypt all sensitive information in transit.			

## 4.3.2 Ensure Server Parameter 'log\_checkpoints' is set to 'ON' for PostgreSQL Database Server (Automated)

### Profile Applicability:

- Level 1

### Description:

Enable `log_checkpoints` ON PostgreSQL Servers.

### Rationale:

Enabling `log_checkpoints` helps the PostgreSQL Database to Log each checkpoint in turn generates query and error logs. However, access to transaction logs is not supported. Query and error logs can be used to identify, troubleshoot, and repair configuration errors and sub-optimal performance.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Go to Azure Database for PostgreSQL server
3. For each database, click on Server parameters
4. Search for `log_checkpoints`.
5. Ensure that value is set to ON.

#### From Azure CLI

Ensure value is set to ON

```
az postgres server configuration show --resource-group <resourceGroupName> -  
-server-name <serverName> --name log_checkpoints
```

#### From PowerShell

Ensure value is set to ON

```
Get-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -  
ServerName <ServerName> -Name log_checkpoints
```

### Remediation:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Go to Azure Database for PostgreSQL server
3. For each database, click on Server parameters
4. Search for `log_checkpoints`.
5. Click ON and save.

## From Azure CLI

Use the below command to update `log_checkpoints` configuration.

```
az postgres server configuration set --resource-group <resourceGroupName> --server-name <serverName> --name log_checkpoints --value on
```

## From PowerShell

```
Update-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -ServerName <ServerName> -Name log_checkpoints -Value on
```







## Default Value:

By default `log_checkpoints` is enabled (set to `on`).

## References:

1. <https://docs.microsoft.com/en-us/rest/api/postgresql/singleserver/configurations/list-by-server>
2. <https://docs.microsoft.com/en-us/azure/postgresql/howto-configure-server-parameters-using-portal>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-4-enable-logging-for-azure-resources>
4. <https://learn.microsoft.com/en-us/azure/postgresql/single-server/concepts-server-logs#configure-logging>
5. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/get-azpostgresqlconfiguration?view=azps-9.2.0#example-2-get-specified-postgresql-configuration-by-name>
6. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/update-azpostgresqlconfiguration?view=azps-9.2.0#example-1-update-postgresql-configuration-by-name>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 <u>Collect Audit Logs</u></b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.			

### 4.3.3 Ensure server parameter 'log\_connections' is set to 'ON' for PostgreSQL Database Server (Automated)

#### Profile Applicability:

- Level 1

#### Description:

Enable `log_connections` ON PostgreSQL Servers.

#### Rationale:

Enabling `log_connections` helps PostgreSQL Database to log attempted connection to the server, as well as successful completion of client authentication. Log data can be used to identify, troubleshoot, and repair configuration errors and suboptimal performance.

#### Audit:

##### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to Azure Database for PostgreSQL server
3. For each database, click on Server parameters
4. Search for `log_connections`.
5. Ensure that value is set to ON.

##### From Azure CLI

Ensure `log_connections` value is set to ON

```
az postgres server configuration show --resource-group <resourceGroupName> --server-name <serverName> --name log_connections
```

##### From PowerShell

Ensure `log_connections` value is set to ON

```
Get-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -ServerName <ServerName> -Name log_connections
```

#### Remediation:

##### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to Azure Database for PostgreSQL server
3. For each database, click on Server parameters
4. Search for `log_connections`.
5. Click ON and save.

## From Azure CLI

Use the below command to update `log_connections` configuration.

```
az postgres server configuration set --resource-group <resourceGroupName> --server-name <serverName> --name log_connections --value on
```

## From PowerShell

Use the below command to update `log_connections` configuration.

```
Update-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -ServerName <ServerName> -Name log_connections -Value on
```

## Default Value:

By default `log_connections` is enabled (set to `on`).

## References:

1. <https://docs.microsoft.com/en-us/rest/api/postgresql/configurations/listbyserver>
2. <https://docs.microsoft.com/en-us/azure/postgresql/howto-configure-server-parameters-using-portal>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-3-enable-logging-for-security-investigation>
4. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/get-azpostgreSqlconfiguration?view=azps-9.2.0#example-2-get-specified-postgresql-configuration-by-name>
5. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/update-azpostgreSqlconfiguration?view=azps-9.2.0#example-1-update-postgresql-configuration-by-name>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 Collect Audit Logs</b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

## 4.3.4 Ensure server parameter 'log\_disconnections' is set to 'ON' for PostgreSQL Database Server (Automated)

### Profile Applicability:

- Level 1

### Description:

Enable `log_disconnections` on PostgreSQL Servers.

### Rationale:

Enabling `log_disconnections` helps PostgreSQL Database to Logs end of a session, including duration, which in turn generates query and error logs. Query and error logs can be used to identify, troubleshoot, and repair configuration errors and sub-optimal performance.

### Impact:

Enabling this setting will enable a log of all disconnections. If this is enabled for a high traffic server, the log may grow exponentially.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Go to Azure Database for PostgreSQL server
3. For each database, click on Server parameters
4. Search for `log_disconnections`.
5. Ensure that value is set to ON.

#### From Azure CLI

Ensure `log_disconnections` value is set to ON

```
az postgres server configuration show --resource-group <resourceGroupName> --server-name <serverName> --name log_disconnections
```

#### From PowerShell

Ensure `log_disconnections` value is set to ON

```
Get-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -ServerName <ServerName> -Name log_disconnections
```

## Remediation:

### From Azure Portal

1. From Azure Home select the Portal Menu
2. Go to Azure Database for PostgreSQL server
3. For each database, click on Server parameters
4. Search for `log_disconnections`.
5. Click ON and save.

### From Azure CLI

Use the below command to update `log_disconnections` configuration.

```
az postgres server configuration set --resource-group <resourceGroupName> --server-name <serverName> --name log_disconnections --value on
```

### From PowerShell

Use the below command to update `log_disconnections` configuration.

```
Update-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -ServerName <ServerName> -Name log_disconnections -Value on
```

### Default Value:

By default `log_disconnections` is disabled (set to `off`).

### References:

1. <https://docs.microsoft.com/en-us/rest/api/postgresql/singleserver/configurations/list-by-server>
2. <https://docs.microsoft.com/en-us/azure/postgresql/howto-configure-server-parameters-using-portal>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-4-enable-logging-for-azure-resources>
4. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/get-azpostgresqlconfiguration?view=azps-9.2.0#example-2-get-specified-postgresql-configuration-by-name>
5. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/update-azpostgresqlconfiguration?view=azps-9.2.0#example-1-update-postgresql-configuration-by-name>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 <u>Collect Audit Logs</u></b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

DRAFT



### 4.3.5 Ensure server parameter 'connection\_throttling' is set to 'ON' for PostgreSQL Database Server (Automated)

#### Profile Applicability:

- Level 1

#### Description:

Enable `connection_throttling` `ON` PostgreSQL Servers.

#### Rationale:

Enabling `connection_throttling` helps the PostgreSQL Database to set the verbosity of logged messages. This in turn generates query and error logs with respect to concurrent connections that could lead to a successful Denial of Service (DoS) attack by exhausting connection resources. A system can also fail or be degraded by an overload of legitimate users. Query and error logs can be used to identify, troubleshoot, and repair configuration errors and sub-optimal performance.

#### Audit:

##### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to Azure Database for PostgreSQL server
3. For each database, click on Server parameters
4. Search for `connection_throttling`.
5. Ensure that value is set to `ON`.

##### From Azure CLI

Ensure `connection_throttling` value is set to `ON`

```
az postgres server configuration show --resource-group <resourceGroupName> --server-name <serverName> --name connection_throttling
```

##### From PowerShell

Ensure `connection_throttling` value is set to `ON`

```
Get-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -ServerName <ServerName> -Name connection_throttling
```

#### Remediation:

##### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to Azure Database for PostgreSQL server
3. For each database, click on Server parameters
4. Search for `connection_throttling`.

5. Click ON and save.

### From Azure CLI

Use the below command to update `connection_throttling` configuration.

```
az postgres server configuration set --resource-group <resourceGroupName> --server-name <serverName> --name connection_throttling --value on
```

### From PowerShell

Use the below command to update `connection_throttling` configuration.

```
Update-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -ServerName <ServerName> -Name connection_throttling -Value on
```







### Default Value:

By default, `connection_throttle` is enabled (set to `on`).

### References:

1. <https://docs.microsoft.com/en-us/rest/api/postgresql/singleserver/configurations/list-by-server>
2. <https://docs.microsoft.com/en-us/azure/postgresql/howto-configure-server-parameters-using-portal>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-4-enable-logging-for-azure-resources>
4. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/get-azpostgresqlconfiguration?view=azps-9.2.0#example-2-get-specified-postgresql-configuration-by-name>
5. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/update-azpostgresqlconfiguration?view=azps-9.2.0#example-1-update-postgresql-configuration-by-name>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 <u>Collect Audit Logs</u></b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.			
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.			

## 4.3.6 Ensure Server Parameter 'log\_retention\_days' is greater than 3 days for PostgreSQL Database Server (Automated)

### Profile Applicability:

- Level 1

### Description:

Enable `log_retention_days` on PostgreSQL Servers.

### Rationale:

Enabling `log_retention_days` helps PostgreSQL Database to Sets number of days a log file is retained which in turn generates query and error logs. Query and error logs can be used to identify, troubleshoot, and repair configuration errors and sub-optimal performance.

### Impact:

Enabling this setting will enable logs to be retained for the number entered. If this is enabled for a high traffic server, the log may grow quickly to occupy a large amount of disk space. In this case you may want to set this to a lower number.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu
2. Go to Azure Database for PostgreSQL server
3. For each database, click on Server parameters
4. Search for `log_retention_days`.
5. Ensure that value greater than 3.

#### From Azure CLI

Ensure `log_retention_days` value is greater than 3.

```
az postgres server configuration show --resource-group <resourceGroupName> --  
server-name <serverName> --name log_retention_days
```

#### From Powershell

Ensure `log_retention_days` value is greater than 3.

```
Get-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -  
ServerName <ServerName> -Name log_retention_days
```

## Remediation:

### From Azure Portal

1. From Azure Home select the Portal Menu
2. Go to Azure Database for PostgreSQL server
3. For each database, click on Server parameters
4. Search for `log_retention_days`.
5. Enter value in range 4-7 (inclusive) and save.

### From Azure CLI

Use the below command to update `log_retention_days` configuration.

```
az postgres server configuration set --resource-group <resourceGroupName> --server-name <serverName> --name log_retention_days --value <4-7>
```

### From Powershell

Use the below command to update `log_retention_days` configuration.

```
Update-AzPostgreSqlConfiguration -ResourceGroupName <ResourceGroupName> -ServerName <ServerName> -Name log_retention_days -Value <4-7>
```

### Default Value:

By default `log_retention_days` is set to 3.

### References:

1. <https://docs.microsoft.com/en-us/azure/postgresql/howto-configure-server-parameters-using-portal>
2. <https://docs.microsoft.com/en-us/rest/api/postgresql/singleserver/configurations/list-by-server>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-6-configure-log-storage-retention>
4. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/get-azpostgresqlconfiguration?view=azps-9.2.0#example-2-get-specified-postgresql-configuration-by-name>
5. <https://learn.microsoft.com/en-us/powershell/module/az.postgresql/update-azpostgresqlconfiguration?view=azps-9.2.0#example-1-update-postgresql-configuration-by-name>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.3 <u>Ensure Adequate Audit Log Storage</u></b> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v7	<b>6.4 <u>Ensure adequate storage for logs</u></b> Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

DRAFT

### 4.3.7 Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled (Manual)

#### Profile Applicability:

- Level 1

#### Description:

Disable access from Azure services to PostgreSQL Database Server

#### Rationale:

If access from Azure services is enabled, the server's firewall will accept connections from all Azure resources, including resources not in your subscription. This is usually not a desired configuration. Instead, set up firewall rules to allow access from specific network ranges or VNET rules to allow access from specific virtual networks.

#### Audit:

##### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>.
2. Go to Azure Database for PostgreSQL server.
3. For each database, click on Connection security.
4. Under Firewall rules, ensure Allow access to Azure services is set to No.

##### From Azure CLI

Ensure the output of the below command does not include a rule with the name AllowAllAzureIps or "startIpAddress": "0.0.0.0" & "endIpAddress": "0.0.0.0",

```
az postgres server firewall-rule list --resource-group <resourceGroupName> -  
-server <serverName>
```

#### Remediation:

##### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>.
2. Go to Azure Database for PostgreSQL server.
3. For each database, click on Connection security.
4. Under Firewall rules, ensure Allow access to Azure services is set to No.
5. Click Save.

## From Azure CLI

Use the below command to delete the AllowAllAzureIps rule for PostgreSQL Database.

```
az postgres server firewall-rule delete --name AllowAllAzureIps --resource-group <resourceGroupName> --server-name <serverName>
```







## Default Value:

The Azure Postgres firewall is set to block all access by default.

## References:

1. <https://docs.microsoft.com/en-us/azure/postgresql/concepts-firewall-rules>
2. <https://docs.microsoft.com/en-us/azure/postgresql/howto-manage-firewall-using-cli>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-1-establish-network-segmentation-boundaries>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-6-deploy-web-application-firewall>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</b> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v7	<b>9.4 Apply Host-based Firewalls or Port Filtering</b> Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			

### 4.3.8 Ensure 'Infrastructure double encryption' for PostgreSQL Database Server is 'Enabled' (Automated)

#### **Profile Applicability:**

- Level 1

#### **Description:**

Enable encryption at rest for PostgreSQL Databases.

#### **Rationale:**

If Double Encryption is enabled, another layer of encryption is implemented at the hardware level before the storage or network level. Information will be encrypted before it is even accessed, preventing both interception of data in motion if the network layer encryption is broken and data at rest in system resources such as memory or processor cache. Encryption will also be in place for any backups taken of the database, so the key will secure access the data in all forms. For the most secure implementation of key based encryption, it is recommended to use a Customer Managed asymmetric RSA 2048 Key in Azure Key Vault.

#### **Impact:**

The read and write speeds to the database will be impacted if both default encryption and Infrastructure Encryption are checked, as a secondary form of encryption requires more resource overhead for the cryptography of information. This cost is justified for information security. Customer managed keys are recommended for the most secure implementation, leading to overhead of key management. The key will also need to be backed up in a secure location, as loss of the key will mean loss of the information in the database.

#### **Audit:**

##### **From Azure Portal**

1. From Azure Home, click on more services.
2. Click on Databases
3. Click on Azure Database for PostgreSQL servers
4. Select the database by clicking on its name.
5. Go to Additional Settings.
6. Ensure that 'Infrastructure encryption enabled' is 'checked'



## From Azure CLI

1. Enter the command

```
az postgres server configuration show --name <servername> --resource-group <resourcegroup> --query 'properties.infrastructureEncryption' -o tsv
```

2. Verify that Infrastructure encryption is enabled.

### Remediation:

#### From Azure Portal

For the creation of a new server;

1. Go through the normal process of database creation.
2. On step 2 titled 'Additional settings' ensure that 'Infrastructure double encryption enabled' is 'checked'
3. Acknowledge that you understand this will impact database performance.
4. Finish database creation as normal.
5. On the final 'Review + create' screen, ensure that at the very bottom of the database properties, that 'Infrastructure (Double) encryption' is 'enabled'.

For existing servers;

1. From Azure Home, click on more services.
2. Click on Databases
3. Click on Azure Database for PostgreSQL servers
4. Select the database by clicking on its name.
5. Select the second from the left option 'Additional settings'.
6. Check the box next to 'Infrastructure double encryption enabled'.

#### From Azure CLI

#### Creating a New Server with Infrastructure Encryption Enabled

Enter the command as follows;

```
az postgres server create --resource-group <resourcegroup> --name <servername> --location <location> --admin-user <adminusername> --admin-password <server_admin_password> --sku-name GP_Gen4_2 --version 11 --infrastructure-encryption 'Enabled'
```

#### Updating a Server's Configuration

```
az postgres server configuration set -g <resourcegroup>-s <servername> --infrastructure-encryption <Enabled>
```

#### Default Value:

By Default, Double Encryption is disabled.

## References:

1. <https://docs.microsoft.com/en-us/azure/postgresql/howto-double-encryption>
2. <https://docs.microsoft.com/en-us/azure/postgresql/concepts-infrastructure-double-encryption>
3. <https://docs.microsoft.com/en-us/azure/postgresql/concepts-data-encryption-postgresql>
4. <https://docs.microsoft.com/en-us/azure/key-vault/keys/byok-specification>
5. <https://docs.microsoft.com/en-us/azure/postgresql/howto-double-encryption>
6. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-4-enable-data-at-rest-encryption-by-default>

## Additional Information:

Flexible PostgreSQL Database Servers are still in preview. A recommendation will be created for Flexible Servers once the service is out of preview.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 <u>Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	<b>14.8 <u>Encrypt Sensitive Information at Rest</u></b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

## 4.4 MySQL Database

This section groups security best practices/recommendations for Azure MySQL Database Servers.

DRAFT

## 4.4.1 Ensure 'Enforce SSL connection' is set to 'Enabled' for Standard MySQL Database Server (Automated)

### Profile Applicability:

- Level 1

### Description:

Enable `SSL connection` on `MYSQL Servers`.

### Rationale:

SSL connectivity helps to provide a new layer of security by connecting database server to client applications using Secure Sockets Layer (SSL). Enforcing SSL connections between database server and client applications helps protect against "man in the middle" attacks by encrypting the data stream between the server and application.

### Audit:

#### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to Azure Database for MySQL servers
3. For each database, click on Connection security
4. In SSL settings, ensure `Enforce SSL connection` is set to `ENABLED`.

#### From Azure CLI

Ensure the output of the below command returns `ENABLED`.

```
az mysql server show --resource-group <resourceGroupName> --name  
<serverName> --query sslEnforcement
```

### Remediation:

#### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to Azure Database for MySQL servers
3. For each database, click on Connection security
4. In SSL settings, click on `ENABLED` to Enforce SSL connections

## From Azure CLI

Use the below command to set MYSQL Databases to Enforce SSL connection.

```
az mysql server update --resource-group <resourceGroupName> --name <serverName> --ssl-enforcement Enabled
```

## Default Value:

Azure Database for MySQL when provisioned through the Azure portal or CLI will require SSL connections by default.

## References:

1. <https://docs.microsoft.com/en-us/azure/mysql/single-server/concepts-ssl-connection-security>
2. <https://docs.microsoft.com/en-us/azure/mysql/single-server/how-to-configure-ssl>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-3-encrypt-sensitive-data-in-transit>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 <u>Encrypt Sensitive Data in Transit</u></b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	<b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b> Encrypt all sensitive information in transit.		●	●

## 4.4.2 Ensure 'TLS Version' is set to 'TLSV1.2' for MySQL flexible Database Server (Automated)

### Profile Applicability:

- Level 1

### Description:

Ensure `tls_version` on MySQL flexible servers is set to the default value.

### Rationale:

TLS connectivity helps to provide a new layer of security by connecting database server to client applications using Transport Layer Security (TLS). Enforcing TLS connections between database server and client applications helps protect against "man in the middle" attacks by encrypting the data stream between the server and application.

### Audit:

#### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to Azure Database for MySQL flexible servers
3. For each database, click on `Server parameters` under `Settings`
4. In the search box, type in `tls_version`
5. Ensure `tls_version` is set to `TLSV1.2`

#### From Azure CLI

Ensure the output of the below command contains the key value pair "values":  
"TLSV1.2".

```
az mysql flexible-server parameter show --name tls_version --resource-group <resourceGroupName> --server-name <serverName>
```

## Example output:

```
{
  "allowedValues": "TLSv1,TLSv1.1,TLSv1.2",
  "dataType": "Set",
  "defaultValue": "TLSv1.2",
  "description": "Which protocols the server permits for encrypted
connections. By default, TLS 1.2 is enforced",
  "id":
"/subscriptions/<subscriptionId>/resourceGroups/<resourceGroupName>/providers
/Microsoft.DBforMySQL/flexibleServers/<serverName>/configurations/tls_version
",
  "isConfigPendingRestart": "False",
  "isDynamicConfig": "False",
  "isReadOnly": "False",
  "name": "tls_version",
  "resourceGroup": "<resourceGroupName>",
  "source": "system-default",
  "systemData": null,
  "type": "Microsoft.DBforMySQL/flexibleServers/configurations",
  "value": "TLSv1.2"
}
```

## Remediation:

### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to Azure Database for MySQL flexible servers
3. For each database, click on Server parameters under Settings
4. In the search box, type in `tls_version`
5. Click on the VALUE dropdown, and ensure only `TLSV1.2` is selected for `tls_version`

### From Azure CLI

Use the below command to set MYSQL flexible databases to used version 1.2 for the `tls_version` parameter.

```
az mysql flexible-server parameter set --name tls_version --resource-
group <resourceGroupName> --server-name <serverName> --value TLSV1.2
```

## Default Value:

By default, TLS is set to v1.2 for MySQL Flexible servers.

## References:

1. <https://docs.microsoft.com/en-us/azure/mysql/concepts-ssl-connection-security>
2. <https://docs.microsoft.com/en-us/azure/mysql/howto-configure-ssl>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-4-enable-data-at-rest-encryption-by-default>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 <u>Encrypt Sensitive Data in Transit</u></b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	<b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b> Encrypt all sensitive information in transit.		●	●

DRAFT



### 4.4.3 Ensure server parameter 'audit\_log\_enabled' is set to 'ON' for MySQL Database Server (Manual)

#### Profile Applicability:

- Level 2

#### Description:

Enable audit\_log\_enabled on MySQL Servers.

#### Rationale:

Enabling audit\_log\_enabled helps MySQL Database to log items such as connection attempts to the server, DDL/DML access, and more. Log data can be used to identify, troubleshoot, and repair configuration errors and suboptimal performance.

#### Impact:

There are further costs incurred for storage of logs. For high traffic databases these logs will be significant. Determine your organization's needs before enabling.

#### Audit:

##### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Select Azure Database for MySQL Servers
3. For each database, under the Settings section in the sidebar, select `Server parameters`
4. Ensure the `audit_log_enabled` parameter is set to ON

#### Remediation:

##### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>.
2. Select Azure Database for MySQL Servers.
3. Select a database.
4. Under Settings, select `Server parameters`.
5. Update `audit_log_enabled` parameter to ON
6. Under Monitoring, select `Diagnostic settings`.
7. Select + Add diagnostic setting.
8. Provide a diagnostic setting name.
9. Under Categories, select `MySQL Audit Logs`.
10. Specify destination details.
11. Click `Save`.

It may take up to 10 minutes for the logs to appear in the configured destination.

**Default Value:**

audit\_log\_enabled is set to OFF by default

**References:**

1. <https://docs.microsoft.com/en-us/azure/mysql/single-server/how-to-configure-audit-logs-portal>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-3-enable-logging-for-security-investigation>

**Additional Information:**

There is also a CLI version: <https://docs.microsoft.com/en-us/azure/mysql/single-server/how-to-configure-audit-logs-cli>

There are numerous settings and event types and it might be helpful to discuss which of these may be appropriate to have a separate check item for.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 Collect Audit Logs</b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	<b>6.2 Activate audit logging</b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

## 4.4.4 Ensure server parameter 'audit\_log\_events' has 'CONNECTION' set for MySQL Database Server (Manual)

### Profile Applicability:

- Level 2

### Description:

Set `audit_log_enabled` to include `CONNECTION` on MySQL Servers.

### Rationale:

Enabling `CONNECTION` helps MySQL Database to log items such as successful and failed connection attempts to the server. Log data can be used to identify, troubleshoot, and repair configuration errors and suboptimal performance.

### Impact:

There are further costs incurred for storage of logs. For high traffic databases these logs will be significant. Determine your organization's needs before enabling.

### Audit:

#### From Azure Portal

1. From Azure Home select the Portal Menu.
2. Select Azure Database for MySQL servers.
3. Select a database.
4. Under Settings, select Server parameters.
5. Ensure `audit_log_enabled` parameter is set to `ON`.
6. Ensure `audit_log_events` parameter has `CONNECTION` checked.

### Remediation:

#### From Azure Portal

1. From Azure Home select the Portal Menu.
2. Select Azure Database for MySQL servers.
3. Select a database.
4. Under Settings, select Server parameters.
5. Update `audit_log_enabled` parameter to `ON`.
6. Update `audit_log_events` parameter to have at least `CONNECTION` checked.
7. Click Save.
8. Under Monitoring, select Diagnostic settings.
9. Select + Add diagnostic setting.
10. Provide a diagnostic setting name.
11. Under Categories, select MySQL Audit Logs.

12. Specify destination details.
13. Click `Save`.

It may take up to 10 minutes for the logs to appear in the configured destination.

**Default Value:**

By default `audit_log_events` is disabled.

**References:**

1. <https://docs.microsoft.com/en-us/azure/mysql/single-server/how-to-configure-audit-logs-portal>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-3-enable-logging-for-security-investigation>

**Additional Information:**

There is also a CLI version: <https://docs.microsoft.com/en-us/azure/mysql/single-server/how-to-configure-audit-logs-cli>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.2 <u>Collect Audit Logs</u></b> Collect audit logs. Ensure that logging, per the enterprise's audit log management process, has been enabled across enterprise assets.	●	●	●
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●

## 4.5 Cosmos DB

This section groups security best practices/recommendations for Azure Cosmos DB Database Servers.

DRAFT

## 4.5.1 Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks (Manual)

### Profile Applicability:

- Level 2

### Description:

Limiting your Cosmos DB to only communicate on whitelisted networks lowers its attack footprint.

### Rationale:

Selecting certain networks for your Cosmos DB to communicate restricts the number of networks including the internet that can interact with what is stored within the database.

### Impact:

Failure to whitelist the correct networks will result in a connection loss.

### Audit:

#### From Azure Portal

1. Open the portal menu.
2. Select the Azure Cosmos DB blade
3. Select a Cosmos DB to audit.
4. Select `Networking`.
5. Under `Public network access`, ensure `Selected networks` is selected.
6. Under `Virtual networks`, ensure appropriate virtual networks are configured.

#### From Azure CLI

```
az cosmosdb database list
az cosmosdb show <database id>
isVirtualNetworkFilterEnabled should be set to true
```

#### From PowerShell

## Remediation:

### From Azure Portal

1. Open the portal menu.
2. Select the Azure Cosmos DB blade.
3. Select a Cosmos DB account to audit.
4. Select `Networking`.
5. Under `Public network access`, select `Selected networks`.
6. Under `Virtual networks`, select `+ Add existing virtual network` **OR** `+ Add a new virtual network`.
7. For existing networks, select subscription, virtual network, subnet and click `Add`. For new networks, provide a name, update the default values if required, and click `Create`.
8. Click `Save`.

### From Azure CLI

### From PowerShell

### Default Value:

By default, Cosmos DBs are set to have access all networks.

### References:

1. <https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints>
2. <https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-vnet-service-endpoint>
3. <https://docs.microsoft.com/en-us/cli/azure/cosmosdb?view=azure-cli-latest#az-cosmosdb-show>
4. <https://docs.microsoft.com/en-us/cli/azure/cosmosdb/database?view=azure-cli-latest#az-cosmosdb-database-list>
5. <https://docs.microsoft.com/en-us/powershell/module/az.cosmosdb/?view=azps-8.1.0>
6. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-2-secure-cloud-services-with-network-controls>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>4.4 <u>Implement and Manage a Firewall on Servers</u></b>            Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.</p>	●	●	●
v8	<p><b>12.2 <u>Establish and Maintain a Secure Network Architecture</u></b>            Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.</p>		●	●
v7	<p><b>9.4 <u>Apply Host-based Firewalls or Port Filtering</u></b>            Apply host-based firewalls or port filtering tools on end systems, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.</p>	●	●	●
v7	<p><b>14.1 <u>Segment the Network Based on Sensitivity</u></b>            Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).</p>		●	●

DRAFT



## 4.5.2 Ensure That Private Endpoints Are Used Where Possible (Manual)

### Profile Applicability:

- Level 2

### Description:

Private endpoints limit network traffic to approved sources.

### Rationale:

For sensitive data, private endpoints allow granular control of which services can communicate with Cosmos DB and ensure that this network traffic is private. You set this up on a case by case basis for each service you wish to be connected.

### Impact:

Only whitelisted services will have access to communicate with the Cosmos DB.

### Audit:

#### From Azure Portal

1. Open the portal menu.
2. Select the Azure Cosmos DB blade.
3. Select the Azure Cosmos DB account.
4. Select `Networking`.
5. Ensure `Public network access` is set to `Selected networks`.
6. Ensure the listed networks are set appropriately.
7. Select `Private access`.
8. Ensure a private endpoint exists and `Connection state` is `Approved`.

### Remediation:

#### From Azure Portal

1. Open the portal menu.
2. Select the Azure Cosmos DB blade.
3. Select the Azure Cosmos DB account.
4. Select `Networking`.
5. Select `Private access`.
6. Click `+ Private Endpoint`.
7. Provide a Name.
8. Click `Next`.
9. From the `Resource type` drop down, select `Microsoft.AzureCosmosDB/databaseAccounts`.

10. From the Resource drop down, select the Cosmos DB account.
11. Click `Next`.
12. Provide appropriate Virtual Network details.
13. Click `Next`.
14. Provide appropriate DNS details.
15. Click `Next`.
16. Optionally provide Tags.
17. Click `Next : Review + create`.
18. Click `Create`.

### Default Value:

By default Cosmos DB does not have private endpoints enabled and its traffic is public to the network.

### References:

1. <https://docs.microsoft.com/en-us/azure/cosmos-db/how-to-configure-private-endpoints>
2. <https://docs.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-cosmosdb-portal>
3. <https://docs.microsoft.com/en-us/cli/azure/cosmosdb/private-endpoint-connection?view=azure-cli-latest>
4. <https://docs.microsoft.com/en-us/cli/azure/network/private-endpoint?view=azure-cli-latest#az-network-private-endpoint-create>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-2-secure-cloud-services-with-network-controls>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>12.2 <u>Establish and Maintain a Secure Network Architecture</u></b>            Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.</p>		●	●
v7	<p><b>14.1 <u>Segment the Network Based on Sensitivity</u></b>            Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).</p>		●	●

### 4.5.3 Use Azure Active Directory (AAD) Client Authentication and Azure RBAC where possible. (Manual)

#### Profile Applicability:

- Level 1

#### Description:

Cosmos DB can use tokens or AAD for client authentication which in turn will use Azure RBAC for authorization. Using AAD is significantly more secure because AAD handles the credentials and allows for MFA and centralized management, and the Azure RBAC better integrated with the rest of Azure.

#### Rationale:

AAD client authentication is considerably more secure than token-based authentication because the tokens must be persistent at the client. AAD does not require this.

#### Audit:

```
$cosmosdbname = "cosmos-db-account-name"
$resourcegroup = "resource-group-name"
$cosmosdb = az cosmosdb show --name $cosmosdbname --resource-group
$resourcegroup | ConvertFrom-Json
In the resulting output, disableLocalAuth should be true
```

#### Remediation:

Map all the resources that currently access to the Azure Cosmos DB account with keys or access tokens.

Create an Azure Active Directory (AAD) identity for each of these resources:

For Azure resources, you can create a managed identity . You may choose between system-assigned and user-assigned managed identities.

For non-Azure resources, create an AAD identity.

Grant each AAD identity the minimum permission it requires. When possible, we recommend you use one of the 2 built-in role definitions: Cosmos DB Built-in Data Reader or Cosmos DB Built-in Data Contributor.

Validate that the new resource is functioning correctly. After new permissions are granted to identities, it may take a few hours until they propagate. When all resources are working correctly with the new identities, continue to the next step.

You can use the az resource update powershell command:

```
$cosmosdbname = "cosmos-db-account-name"
$resourcegroup = "resource-group-name"
$cosmosdb = az cosmosdb show --name $cosmosdbname --resource-group
$resourcegroup | ConvertFrom-Json
az resource update --ids $cosmosdb.id --set properties.disableLocalAuth=true --latest-include-preview
```

**Default Value:**

The default is to use tokens/keys for client authentication.

**References:**

1. <https://learn.microsoft.com/en-us/azure/cosmos-db/role-based-access-control>

## 5 Logging and Monitoring

This section covers security recommendations to follow to set logging and monitoring policies on an Azure Subscription.

DRAFT

## 5.1 Configuring Diagnostic Settings

The Azure Diagnostic Settings capture control/management activities performed on a subscription or Azure AD Tenant. By default, the Azure Portal retains activity logs only for 90 days. The Diagnostic Settings define the type of events that are stored or streamed and the outputs—storage account, log analytics workspace, event hub, and others. The Diagnostic Settings, if configured properly, can ensure that all logs are retained for longer duration. This section has recommendations for correctly configuring the Diagnostic Settings so that all logs captured are retained for longer periods.

### **Azure Subscriptions**

When configuring Diagnostic Settings, you may choose to export in one of four ways in which you need to ensure appropriate data retention. The options are Log Analytics, Event Hub, Storage Account, and Partner Solutions. It is important to ensure you are aware and have set retention as your organization sees fit.

### **Azure AD Logs**

In order to retain sign in logs, user account changes, application provisioning logs, or other logs that are visible to only on the Tenant in Azure AD, separate Diagnostic settings must be specified.

### **Deployment by Policy**

Deploying Azure diagnostics should ideally be done by policy to ensure a consistent configuration, Microsoft provide a full set of policies for all diagnostic capable resource types in their github repository. If you chose to deploy by policy, it is best to route the diagnostics to a Log Analytics Workspace so that they can be used in Azure Monitor or Azure Sentinel. Be aware that this has a cost attached to it. Future versions of the CIS Azure Foundations Benchmark will aim to cover the use of policy in greater detail.

## 5.1.1 Ensure that a 'Diagnostic Setting' exists (Manual)

### Profile Applicability:

- Level 1

### Description:

Enable Diagnostic settings for exporting activity logs. Diagnostic settings are available for each individual resource within a subscription. Settings should be configured for all appropriate resources for your environment.

### Rationale:

A diagnostic setting controls how a diagnostic log is exported. By default, logs are retained only for 90 days. Diagnostic settings should be defined so that logs can be exported and stored for a longer duration in order to analyze security activities within an Azure subscription.

### Audit:

#### From Azure Portal

To identify Diagnostic Settings on a subscription:

1. Go to Monitor
2. Click Activity Log
3. Click Export Activity Logs
4. Select a Subscription
5. Ensure a Diagnostic settings exists for the selected Subscription

To identify Diagnostic Settings on specific resources:

1. Go to Monitor
2. Click Diagnostic settings
3. Ensure that Diagnostics status is enabled on all appropriate resources.

#### From Azure CLI

To identify Diagnostic Settings on a subscription:

```
az monitor diagnostic-settings subscription list --subscription <subscription ID>
```

To identify Diagnostic Settings on a resource

```
az monitor diagnostic-settings list --resource <resource Id>
```

#### From PowerShell

To identify Diagnostic Settings on a Subscription:

```
Get-AzDiagnosticSetting -SubscriptionId <subscription ID>
```

To identify Diagnostic Settings on a specific resource:

```
Get-AzDiagnosticSetting -ResourceId <resource ID>
```

## Remediation:

### From Azure Portal

To enable Diagnostic Settings on a Subscription:

1. Go to `Monitor`
2. Click on `Activity Log`
3. Click on `Export Activity Logs`
4. Click + `Add diagnostic setting`
5. Enter a `Diagnostic setting name`
6. Select `Categories` for the diagnostic settings
7. Select the appropriate `Destination details` (this may be `Log Analytics/Storage Account/Event Hub` or `Partner solution`)
8. Click `Save`

To enable Diagnostic Settings on a specific resource:

1. Go to `Monitor`
2. Click `Diagnostic settings`
3. Click on the resource that has a diagnostics status of `disabled`
4. Select `Add Diagnostic Setting`
5. Enter a `Diagnostic setting name`
6. Select the appropriate log, metric, and destination. (This may be `Log Analytics/Storage account` or `Event Hub`)
7. Click `save`

Repeat these step for all resources as needed.

### From Azure CLI

To configure Diagnostic Settings on a Subscription:

```
az monitor diagnostic-settings subscription create --subscription <subscription id> --name <diagnostic settings name> --location <location> <[--event-hub <event hub ID> --event-hub-auth-rule <event hub auth rule ID>] [--storage-account <storage account ID>] [--workspace <log analytics workspace ID>] --logs "<JSON encoded categories>" (e.g. [{category:Security,enabled:true},{category:Administrative,enabled:true},{category:Alert,enabled:true},{category:Policy,enabled:true}])
```

To configure Diagnostic Settings on a specific resource:

```
az monitor diagnostic-settings create --subscription <subscription ID> --resource <resource ID> --name <diagnostic settings name> <[--event-hub <event hub ID> --event-hub-rule <event hub auth rule ID>] [--storage-account <storage account ID>] [--workspace <log analytics workspace ID>] --logs <resource specific JSON encoded log settings> --metrics <metric settings (shorthand|json-file|yaml-file)>
```

## From PowerShell

To configure Diagnostic Settings on a subscription:

```
$logCategories = @();
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Administrative -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Security -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category ServiceHealth -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Alert -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Recommendation -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Policy -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Autoscale -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category ResourceHealth -Enabled $true

New-AzSubscriptionDiagnosticSetting -SubscriptionId <subscription ID> -Name
<Diagnostic settings name> <[-EventHubAuthorizationRule <event hub auth rule
ID> -EventHubName <event hub name>] [-StorageAccountId <storage account ID>]
[-WorkspaceId <log analytics workspace ID>] [-MarketplacePartner ID <full ARM
Marketplace resource ID>]> -Log $logCategories
```

To configure Diagnostic Settings on a specific resource:

```
$logCategories = @()
$logCategories += New-AzDiagnosticSettingLogSettingsObject -Category
<resource specific log category> -Enabled $true

Repeat command and variable assignment for each Log category specific to the
resource where this Diagnostic Setting will get configured.

$metricCategories = @()
$metricCategories += New-AzDiagnosticSettingMetricSettingsObject -Enabled
$true [-Category <resource specific metric category | AllMetrics>] [-
RetentionPolicyDay <Integer>] [-RetentionPolicyEnabled $true]

Repeat command and variable assignment for each Metric category or use the
'AllMetrics' category.

New-AzDiagnosticSetting -ResourceId <resource ID> -Name <Diagnostic settings
name> -Log $logCategories -Metric $metricCategories [-
EventHubAuthorizationRuleId <event hub auth rule ID> -EventHubName <event hub
name>] [-StorageAccountId <storage account ID>] [-WorkspaceId <log analytics
workspace ID>] [-MarketplacePartnerId <full ARM marketplace resource ID>]>
```

### Default Value:

By default, diagnostic setting is not set.



## References:

1. <https://docs.microsoft.com/en-us/azure/monitoring-and-diagnostics/monitoring-overview-activity-logs#export-the-activity-log-with-a-log-profile>
2. <https://learn.microsoft.com/en-us/cli/azure/monitor/diagnostic-settings?view=azure-cli-latest>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-3-enable-logging-for-security-investigation>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.9 Centralize Audit Logs</b> Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	<b>6.5 Central Log Management</b> Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●

## 5.1.2 Ensure Diagnostic Setting captures appropriate categories (Automated)

### Profile Applicability:

- Level 1

### Description:

**Prerequisite:** A Diagnostic Setting must exist. If a Diagnostic Setting does not exist, the navigation and options within this recommendation will not be available. Please review the recommendation at the beginning of this subsection titled: "Ensure that a 'Diagnostic Setting' exists."

The diagnostic setting should be configured to log the appropriate activities from the control/management plane.

### Rationale:

A diagnostic setting controls how the diagnostic log is exported. Capturing the diagnostic setting categories for appropriate control/management plane activities allows proper alerting.

### Audit:

#### From Azure Portal

1. Go to Azure Monitor
2. Click Activity log
3. Click on Export Activity Logs
4. Select the appropriate Subscription
5. If there is no Diagnostic Settings listed, generate a finding.
6. Otherwise, click on Edit Settings
7. Ensure that the following categories are checked: Administrative, Alert, Policy, and Security

#### From Azure CLI

Ensure the categories 'Administrative', 'Alert', 'Policy', and 'Security' set to 'enabled: true'

```
az monitor diagnostic-settings subscription list --subscription <subscription ID>
```

#### From Powershell

Ensure the categories Administrative, Alert, Policy, and Security are set to Enabled:True

```
Get-AzSubscriptionDiagnosticSetting -Subscription <subscriptionID>
```

## Remediation:

### From Azure Portal

1. Go to Azure Monitor
2. Click Activity log
3. Click on Export Activity Logs
4. Select the Subscription from the drop down menu
5. Click on Add diagnostic setting
6. Enter a name for your new Diagnostic Setting
7. Check the following categories: Administrative, Alert, Policy, and Security
8. Choose the destination details according to your organization's needs.

### From Az CLI

```
az monitor diagnostic-settings subscription create --subscription
<subscription id> --name <diagnostic settings name> --location <location> <[-
-event-hub <event hub ID> --event-hub-auth-rule <event hub auth rule ID>] [--
storage-account <storage account ID>] [--workspace <log analytics workspace
ID>] --logs
"[{category:Security,enabled:true},{category:Administrative,enabled:true},{ca
tegory:Alert,enabled:true},{category:Policy,enabled:true}]"
```

### From PowerShell

```
$logCategories = @();
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Administrative -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Security -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Alert -Enabled $true
$logCategories += New-AzDiagnosticSettingSubscriptionLogSettingsObject -
Category Policy -Enabled $true

New-AzSubscriptionDiagnosticSetting -SubscriptionId <subscription ID> -Name
<Diagnostic settings name> <[-EventHubAuthorizationRule <event hub auth rule
ID> -EventHubName <event hub name>] [-StorageAccountId <storage account ID>]
[-WorkspaceId <log analytics workspace ID>] [-MarketplacePartner ID <full ARM
Marketplace resource ID>]> -Log $logCategories
```





### Default Value:

When the diagnostic setting is created using Azure Portal, by default no categories are selected.

## References:

1. <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-settings>
2. <https://docs.microsoft.com/en-us/azure/azure-monitor/samples/resource-manager-diagnostic-settings>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-3-enable-logging-for-security-investigation>
4. <https://learn.microsoft.com/en-us/cli/azure/monitor/diagnostic-settings?view=azure-cli-latest>
5. <https://learn.microsoft.com/en-us/powershell/module/az.monitor/new-azsubscriptiondiagnosticsetting?view=azps-9.2.0>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.			
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.			

### 5.1.3 Ensure the Storage Container Storing the Activity Logs is not Publicly Accessible (Automated)

#### Profile Applicability:

- Level 1

#### Description:

The storage account container containing the activity log export should not be publicly accessible.

#### Rationale:

Allowing public access to activity log content may aid an adversary in identifying weaknesses in the affected account's use or configuration.

#### Impact:

Configuring container `Access policy` to `private` will remove access from the container for everyone except owners of the storage account. Access policy needs to be set explicitly in order to allow access to other desired users.

#### Audit:

##### From Azure Portal

1. From Azure Home select the Portal Menu
2. Select `Diagnostic Settings` in the left column.
3. In section `Storage Account`, note the name of the `Storage account`
4. Close `Diagnostic settings`. Close the `Monitor - Activity Log blade`.
5. In left menu, Click `Storage Accounts`
6. For each storage account, go to the `Configuration setting`
7. Check if `Blob public access` is `Disabled`.

##### From Azure CLI

1. Get storage account id configured with Diagnostic Settings:

```
az monitor diagnostic-settings subscription list --subscription  
$subscription.Id --query 'value[*].storageAccountId'
```

2. Ensure the container storing activity logs (`insights-activity-logs`) is not publicly accessible:

```
az storage container list --account-name <Storage Account Name> --query  
"[?name=='insights-activity-logs']"
```

If this command returns output and no errors, the storage account is publicly accessible.

### 3. Otherwise, list `Storage Account Keys` for the storage account.

```
az storage account keys list --resource-group <storage account resource group> --account-name <storage account name>
```

### 4. Use a key to determine if the `Container` is also publicly accessible (in the event the storage account is)

```
az storage container list --account-name <Storage Account Name> --query "[?name=='insights-activity-logs']" --sas-token "<base64 key value from step 3>"
```

Ensure `publicAccess` is set to `null` in the output of the command in step 4.

#### From PowerShell

Create a new storage account context with either a Storage-level SAS token with at least read/list permissions for Blob > Service, Container, Object.

```
$context = New-AzStorageContext -StorageAccountName <storage account name> -SasToken "<SAS token>"
```

Use the newly created storage account context to determine if the `insights-activity-logs` container is publicly accessible.

```
Get-AzStorageContainer -Context $context -name "insights-activity-logs"
```

Ensure `PublicAccess` is empty or set to `null`, `0`, or `off`.

#### Remediation:

##### From Azure Portal

1. From Azure Home select the Portal Menu
2. Search for `Storage Accounts` to access Storage account blade
3. Click on the storage account name
4. Click on `Configuration` under settings
5. Select `Enabled` under "Allow Blob public access"

##### From Azure CLI

```
az storage container set-permission --name insights-activity-logs --account-name <Storage Account Name> --sas-token <SAS token> --public-access off
```

#### From PowerShell

Create a new storage account context for the storage account holding the `insights-activity-logs` container making sure to use a valid Shared Access Signature (SAS) token.

```
$context = New-AzStorageContext -StorageAccountName <storage account name> -SasToken "<SAS token>"
```

Change the `insights-activity-logs` container public access to `off`

```
Set-AzStorageContainerAcl -Context $context -Name "insights-activity-logs" -  
Permission Off -PassThru
```







### Default Value:

By default, public access is set to null (allowing only private access) for a container with activity log export.

### References:

1. <https://docs.microsoft.com/en-us/azure/storage/blobs/anonymous-read-access-configure>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-2-secure-cloud-services-with-network-controls>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 Configure Data Access Control Lists</b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b>14.6 Protect Information through Access Control Lists</b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

## 5.1.4 Ensure the storage account containing the container with activity logs is encrypted with Customer Managed Key (Automated)

### Profile Applicability:

- Level 2

### Description:

Storage accounts with the activity log exports can be configured to use Customer Managed Keys (CMK).

### Rationale:

Configuring the storage account with the activity log export container to use CMKs provides additional confidentiality controls on log data, as a given user must have read permission on the corresponding storage account and must be granted decrypt permission by the CMK.

### Impact:

**NOTE:** You must have your key vault setup to utilize this. All Audit Logs will be encrypted with a key you provide. You will need to set up customer managed keys separately, and you will select which key to use via the instructions here. You will be responsible for the lifecycle of the keys, and will need to manually replace them at your own determined intervals to keep the data secure.

### Audit:

#### From Azure Portal

1. Go to `Activity log`
2. Select `Export`
3. Select `Subscription`
4. In section `Storage Account`, note the name of the Storage account
5. Close the `Export Audit Logs` blade. Close the `Monitor - Activity Log` blade.
6. In right column, Click service `Storage Accounts` to access `Storage account` blade
7. Click on the storage account name noted in step 4. This will open blade specific to that storage account
8. Under `Security + networking`, click `Encryption`.
9. Ensure `Customer-managed keys` is selected and `Key URI` is set.



## From Azure CLI

1. Get storage account id configured with log profile:

```
az monitor diagnostic-settings subscription list --subscription <subscription id> --query 'value[*].storageAccountId'
```

2. Ensure the storage account is encrypted with CMK:

```
az storage account list --query "[?name=='<Storage Account Name>']"
```

In command output ensure `keySource` is set to `Microsoft.Keyvault` and `keyVaultProperties` is not set to `null`

## From PowerShell

```
Get-AzStorageAccount -ResourceGroupName <resource group name> -Name <storage account name>|select-object -ExpandProperty encryption|format-list
```

Ensure the value of `KeyVaultProperties` is not `null` or empty, and ensure `KeySource` is not set to `Microsoft.Storage`.

## Remediation:

### From Azure Portal

1. Navigate to the Storage accounts blade.
2. Click on the storage account.
3. Under **Security + networking**, click **Encryption**.
4. Next to **Encryption type**, select **Customer-managed keys**.
5. Complete the steps to configure a customer-managed key for encryption of the storage account.

## From Azure CLI

```
az storage account update --name <name of the storage account> --resource-group <resource group for a storage account> --encryption-key-source=Microsoft.Keyvault --encryption-key-vault <Key Vault URI> --encryption-key-name <KeyName>--encryption-key-version <Key Version>
```

## From PowerShell

```
Set-AzStorageAccount -ResourceGroupName <resource group name> -Name <storage account name> -KeyvaultEncryption -KeyVaultUri <key vault URI> -KeyName <key name>
```




## Default Value:

By default, for a storage account `keySource` is set to `Microsoft.Storage` allowing encryption with vendor Managed key and not a Customer Managed Key.

## References:

1. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-5-encrypt-sensitive-data-at-rest>
2. <https://learn.microsoft.com/en-us/azure/azure-monitor/essentials/activity-log?tabs=cli#managing-legacy-log-profiles>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 Encrypt Sensitive Data at Rest</b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.			
v7	<b>14.8 Encrypt Sensitive Information at Rest</b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			

## 5.1.5 Ensure that logging for Azure Key Vault is 'Enabled' (Automated)

### Profile Applicability:

- Level 1

### Description:

Enable AuditEvent logging for key vault instances to ensure interactions with key vaults are logged and available.

### Rationale:

Monitoring how and when key vaults are accessed, and by whom, enables an audit trail of interactions with confidential information, keys, and certificates managed by Azure Keyvault. Enabling logging for Key Vault saves information in an Azure storage account which the user provides. This creates a new container named insights-logs-auditevent automatically for the specified storage account. This same storage account can be used for collecting logs for multiple key vaults.

### Audit:

#### From Azure Portal

1. Go to Key vaults
2. For each Key vault
3. Go to Diagnostic settings
4. Click on Edit Settings
5. Ensure that Archive to a storage account is Enabled
6. Ensure that AuditEvent is checked, and the retention days is set to 180 days or as appropriate

## From Azure CLI

List all key vaults

```
az keyvault list
```

For each keyvault `id`

```
az monitor diagnostic-settings list --resource <id>
```

Ensure that `storageAccountId` is set as appropriate. Also, ensure that `category` and `days` are set. One of the sample outputs is as below.

```
"logs": [
  {
    "category": "AuditEvent",
    "enabled": true,
    "retentionPolicy": {
      "days": 180,
      "enabled": true
    }
  }
]
```

## From PowerShell

List the key vault(s) in the subscription

```
Get-AzKeyVault
```

For each key vault, run the following:

```
Get-AzDiagnosticSetting -ResourceId <key vault resource ID>
```

Ensure that `StorageAccountId`, `ServiceBusRuleId`, `MarketplacePartnerId`, or `WorkspaceId` is set as appropriate. Also, ensure that `enabled` is set to `true`, and that `category` and `days` are set under the `Log` heading.

## Remediation:

### From Azure Portal

1. Go to `Key vaults`
2. Select a `Key vault`
3. Select `Diagnostic settings`
4. Click on `Edit setting` against an existing diagnostic setting, or `Add diagnostic setting`
5. If creating a new diagnostic setting, provide a name
6. Check `Archive` to a storage account
7. Under `Categories`, check `Audit Logs`
8. Set an appropriate value for `Retention (days)`
9. Click `Save`

## From Azure CLI

To update an existing Diagnostic Settings

```
az monitor diagnostic-settings update --name "<diagnostics settings name>" --resource <key vault resource ID> --set retentionPolicy.days=90
```

To create a new Diagnostic Settings

```
az monitor diagnostic-settings create --name <diagnostic settings name> --resource <key vault resource ID> --logs "[{category:AuditEvents,enabled:true,retention-policy:{enabled:true,days:180}}]" --metrics "[{category:AllMetrics,enabled:true,retention-policy:{enabled:true,days:180}}]" <[--event-hub <event hub ID> --event-hub-rule <event hub auth rule ID> | --storage-account <storage account ID> | --workspace <log analytics workspace ID> | --marketplace-partner-id <full resource ID of third-party solution>]>
```

## From PowerShell

Create the Log settings object

```
$logSettings = @()  
$logSettings += New-AzDiagnosticSettingLogSettingsObject -Enabled $true -RetentionPolicyDay 180 -RetentionPolicyEnabled $true -Category AuditEvent
```

Create the Metric settings object

```
$metricSettings = @()  
$metricSettings += New-AzDiagnosticSettingMetricSettingsObject -Enabled $true -RetentionPolicyDay 180 -RetentionPolicyEnabled $true -Category AllMetrics
```

Create the Diagnostic Settings for each Key Vault

```
New-AzDiagnosticSetting -Name "<diagnostic setting name>" -ResourceId <key vault resource ID> -Log $logSettings -Metric $metricSettings [-StorageAccountId <storage account ID> | -EventHubName <event hub name> -EventHubAuthorizationRuleId <event hub auth rule ID> | -WorkSpaceId <log analytics workspace ID> | -MarketPlacePartnerId <full resource ID for third-party solution>]
```

## Default Value:

By default, Diagnostic AuditEvent logging is not enabled for Key Vault instances.

## References:

1. <https://docs.microsoft.com/en-us/azure/key-vault/general/howto-logging>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-8-ensure-security-of-key-and-certificate-repository>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-3-enable-logging-for-security-investigation>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>8.5 <u>Collect Detailed Audit Logs</u></b>            Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.</p>		●	●
v7	<p><b>6.3 <u>Enable Detailed Logging</u></b>            Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●

DRAFT

## 5.1.6 Ensure that Network Security Group Flow logs are captured and sent to Log Analytics (Manual)

### Profile Applicability:

- Level 2

### Description:

Ensure that network flow logs are captured and fed into a central log analytics workspace.

### Rationale:

Network Flow Logs provide valuable insight into the flow of traffic around your network and feed into both Azure Monitor and Azure Sentinel (if in use), permitting the generation of visual flow diagrams to aid with analyzing for lateral movement, etc.

### Impact:

The impact of configuring NSG Flow logs is primarily one of cost and configuration. If deployed, it will create storage accounts that hold minimal amounts of data on a 5-day lifecycle before feeding to Log Analytics Workspace. This will increase the amount of data stored and used by Azure Monitor.

### Audit:

#### From Azure Portal

1. Navigate to `Network Watcher`.
2. Select `NSG flow logs`
3. For each log you wish to audit select it from this view.

### Remediation:

#### From Azure Portal

1. Navigate to `Network Watcher`.
2. Select `NSG flow logs`.
3. Select `+ Create`.
4. Select the desired `Subscription`.
5. Select `+ Select NSG`.
6. Select a `network security group`.
7. Click `Confirm selection`.
8. Select or create a new `Storage Account`.
9. Input the retention in days to retain the log.
10. Click `Next`.
11. Under `Configuration`, select `Version 2`.

12. If rich analytics are required, select `Enable Traffic Analytics`, a processing interval, and a `Log Analytics Workspace`.
13. Select `Next`.
14. Optionally add Tags.
15. Select `Review + create`.
16. Select `Create`.

### Warning

The remediation policy creates remediation deployment and names them by concatenating the subscription name and the resource group name. The MAXIMUM permitted length of a deployment name is 64 characters. Exceeding this will cause the remediation task to fail.

### Default Value:

By default Network Security Group logs are not sent to Log Analytics.

### References:

1. <https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-portal>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-4-enable-network-logging-for-security-investigation>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	13.6 <u>Collect Network Traffic Flow Logs</u> Collect network traffic flow logs and/or network traffic to review and alert upon from network devices.		●	●
v7	12.8 <u>Deploy NetFlow Collection on Networking Boundary Devices</u> Enable the collection of NetFlow and logging data on all network boundary devices.		●	●



## 5.1.7 Ensure that logging for Azure AppService 'HTTP logs' is enabled (Manual)

### Profile Applicability:

- Level 2

### Description:

Enable AppServiceHTTPLogs diagnostic log category for Azure App Service instances to ensure all http requests are captured and centrally logged.

### Rationale:

Capturing web requests can be important supporting information for security analysts performing monitoring and incident response activities. Once logging, these logs can be ingested into SIEM or other central aggregation point for the organization.

### Impact:

Log consumption and processing will incur additional cost.

### Audit:

#### From Azure Portal

1. Go to App Services

For each App Service:

2. Go to Diagnostic Settings
3. Ensure that 'HTTP logs' is configured to log to a destination aligned to your environments approach to log consumption (event hub, storage account, etc. dependent on what is consuming the logs such as SIEM or other log aggregation utility).

### Remediation:

#### From Azure Portal

1. Go to App Services

For each App Service:

2. Go to Diagnostic Settings
3. Click Add Diagnostic Setting
4. Check the checkbox next to 'HTTP logs'

5. Configure a destination based on your specific logging consumption capability (for example Stream to an event hub and then consuming with SIEM integration for Event Hub logging).





**Default Value:**

Not configured.

**References:**

1. <https://docs.microsoft.com/en-us/azure/app-service/troubleshoot-diagnostic-logs>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-3-enable-logging-for-security-investigation>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.7 Collect URL Request Audit Logs</b> Collect URL request audit logs on enterprise assets, where appropriate and supported.			
v7	<b>7.6 Log all URL requests</b> Log all URL requests from each of the organization's systems, whether onsite or a mobile device, in order to identify potentially malicious activity and assist incident handlers with identifying potentially compromised systems.			

## 5.2 Monitoring using Activity Log Alerts

The recommendations provided in this section are intended to provide entry-level alerting for crucial activities on a tenant account. These recommended activities **should** be tuned to your needs. By default, each of these Activity Log Alerts tends to guide the reader to alerting at the "Subscription-wide" level which will capture and alert on rules triggered by all resources and resource groups contained within a subscription. This is not an ideal rule set for Alerting within larger and more complex organizations.

While this section provides recommendations for the creation of **Activity Log Alerts** specifically, Microsoft Azure supports four different types of alerts:

- Metric Alerts
- Log Alerts
- Activity Log Alerts
- Smart Detection Alerts

All Azure services (Microsoft provided or otherwise) that can generate alerts are assigned a "Resource provider namespace" when they are registered in an Azure tenant. The recommendations in this section are in no way exhaustive of the plethora of available "Providers" or "Resource Types." The Resource Providers that are registered in your Azure Tenant can be located in your Subscription. Each registered Provider in your environment **may** have available "Conditions" to raise alerts via Activity Log Alerts. These providers should be considered for inclusion in Activity Log Alert rules of your own making.

To view the registered resource providers in your Subscription(s), use this guide:

- <https://docs.microsoft.com/en-us/azure/azure-resource-manager/management/resource-providers-and-types>

If you wish to create custom alerting rules for Activity Log Alerts or other alert types, please refer to Microsoft documentation:

- <https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-create-new-alert-rule>

## 5.2.1 Ensure that Activity Log Alert exists for Create Policy Assignment (Automated)

### Profile Applicability:

- Level 1

### Description:

Create an activity log alert for the Create Policy Assignment event.

### Rationale:

Monitoring for create policy assignment events gives insight into changes done in "Azure policy - assignments" and can reduce the time it takes to detect unsolicited changes.

### Audit:

#### From Azure Portal

1. Navigate to the `Monitor` blade
2. Click on `Alerts`
3. In the Alerts window, click on `Alert rules`
4. Hover mouse over the values in the `Condition` column to find an alert where `Operation name=Microsoft.Authorization/policyAssignments/write`
5. Click on the `Alert Name` associated with the previous step
6. Click on the `Condition` name of `Whenever the Activity Log has an event with Category='Administrative', Signal name='Create policy assignment (policyAssignments)`
7. In the `Configure signal logic` window, ensure the following is configured:
  - `Event level`: All selected
  - `Status`: All selected
  - `Event initiated by`: \* (All services and users)
8. Click `Done`
9. Back in the `< Alert Name >` window, review `Actions` to ensure that an `Action` group is assigned to notify the appropriate personnel in your organization.

#### From Azure CLI

```
az monitor activity-log alert list --subscription <subscription ID> --query "[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Authorization/policyAssignments/write` in the output. If it's missing, generate a finding.

## From PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_ .ConditionAllOf.Equal -match
"Microsoft.Authorization/policyAssignments/write"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

If the output is empty, an alert rule for Create Policy Assignments is not configured.

## Remediation:

### From Azure Portal

1. Navigate to the Monitor blade.
2. Select Alerts.
3. Select Create.
4. Select Alert rule.
5. Under Filter by subscription, choose a subscription.
6. Under Filter by resource type, select Policy assignment (policyAssignments).
7. Under Filter by location, select All.
8. From the results, select the subscription.
9. Select Done.
10. Select the Condition tab.
11. Under Signal name, click Create policy assignment (Microsoft.Authorization/policyAssignments).
12. Select the Actions tab.
13. To use an existing action group, click select action groups. To create a new action group, click Create action group. Fill out the appropriate details for the selection.
14. Select the Details tab.
15. Select a Resource group, provide an Alert rule name and an optional Alert rule description.
16. Click Review + create.
17. Click Create.

### From Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Authorization/policyAssignments/write and
level=<verbose | information | warning | error | critical> --scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription ID> --action-group <action group ID> --location
global
```

## From PowerShell

Create the `conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Authorization/policyAssignments/write -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Get the Action Group information and store it in a variable, then create a new Action object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `scope` variable.

```
$scope = "/subscriptions/<subscription ID>"
```

Create the Activity Log Alert Rule for

Microsoft.Authorization/policyAssignments/write

```
New-AzActivityLogAlert -Name "<activity alert rule name>" -ResourceGroupName
"<resource group name>" -Condition $conditions -Scope $scope -Location global
-Action $actionObject -Subscription <subscription ID> -Enabled $true
```

### Default Value:

By default, no monitoring alerts are created.

### References:

1. <https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement>
2. <https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log>
3. <https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate>
4. <https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-3-enable-logging-for-security-investigation>
6. <https://docs.microsoft.com/en-in/rest/api/policy/policy-assignments>
7. <https://docs.microsoft.com/en-us/azure/azure-monitor/alerts/alerts-log>

**CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

DRAFT

## 5.2.2 Ensure that Activity Log Alert exists for Delete Policy Assignment (Automated)

### Profile Applicability:

- Level 1

### Description:

Create an activity log alert for the Delete Policy Assignment event.

### Rationale:

Monitoring for delete policy assignment events gives insight into changes done in "azure policy - assignments" and can reduce the time it takes to detect unsolicited changes.

### Audit:

#### From Azure Portal

1. Navigate to the `Monitor` blade
2. Click on `Alerts`
3. In the Alerts window, click on `Alert rules`
4. Hover mouse over the values in the `Condition` column to find an alert where `Operation name=Microsoft.Authorization/policyAssignments/delete`
5. Click on the `Alert Name` associated with the previous step
6. Click on the `Condition` name of `Whenever the Activity Log has an event with Category='Administrative', Signal name='Delete policy assignment (policyAssignments)'`
7. In the `Configure signal logic` window, ensure the following is configured:
  - `Event level: All` selected
  - `Status: All` selected
  - `Event initiated by: *` (All services and users)
8. Click `Done`
9. Back in the `< Alert Name >` window, review `Actions` to ensure that an `Action` group is assigned to notify the appropriate personnel in your organization.

#### From Azure CLI

```
az monitor activity-log alert list --subscription <subscription ID> --query "[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Authorization/policyAssignments/delete` in the output



## From PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_ .ConditionAllOf.Equal -match
"Microsoft.Authorization/policyAssignments/delete"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

## Remediation:

### From Azure Portal

1. Navigate to the Monitor blade.
2. Select Alerts.
3. Select Create.
4. Select Alert rule.
5. Under Filter by subscription, choose a subscription.
6. Under Filter by resource type, select Policy assignment (policyAssignments).
7. Under Filter by location, select All.
8. From the results, select the subscription.
9. Select Done.
10. Select the Condition tab.
11. Under Signal name, click Delete policy assignment (Microsoft.Authorization/policyAssignments).
12. Select the Actions tab.
13. To use an existing action group, click Select action groups. To create a new action group, click Create action group. Fill out the appropriate details for the selection.
14. Select the Details tab.
15. Select a Resource group, provide an Alert rule name and an optional Alert rule description.
16. Click Review + create.
17. Click Create.

### From Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Authorization/policyAssignments/delete and
level=<verbose | information | warning | error | critical> --scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID> --location
global
```

## From PowerShell

Create the conditions object

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Authorization/policyAssignments/delete -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the Action Group information and store in a variable, then create the Action object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the Scope variable.

```
$scope = "/subscriptions/<subscription id>"
```

Create the Activity Log Alert Rule for

Microsoft.Authorization/policyAssignments/delete.

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

### Default Value:

By default, no monitoring alerts are created.

### References:

1. <https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log>
2. <https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate>
3. <https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-3-enable-logging-for-security-investigation>
5. <https://azure.microsoft.com/en-us/services/blueprints/>

### Additional Information:

This log alert also applies for Azure Blueprints.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>8.5 <u>Collect Detailed Audit Logs</u></b>            Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.</p>		●	●
v7	<p><b>6.3 <u>Enable Detailed Logging</u></b>            Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●

DRAFT

## 5.2.3 Ensure that Activity Log Alert exists for Create or Update Network Security Group (Automated)

### Profile Applicability:

- Level 1

### Description:

Create an Activity Log Alert for the Create or Update Network Security Group event.

### Rationale:

Monitoring for Create or Update Network Security Group events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

### Audit:

#### From Azure Portal

1. Navigate to the `Monitor` blade
2. Click on `Alerts`
3. In the Alerts window, click on `Alert rules`
4. Hover mouse over the values in the `Condition` column to find an alert where `Operation name=Microsoft.Network/networkSecurityGroups/write`
5. Click on the `Alert Name` associated with the previous step
6. Click on the `Condition` name of `Whenever the Activity Log has an event with Category='Administrative', Signal name='Create or Update Network Security Group (networkSecurityGroups)'`
7. In the `Configure signal logic` window, ensure the following is configured:
  - `Event level: All` selected
  - `Status: All` selected
  - `Event initiated by: *` (All services and users)
8. Click `Done`
9. Back in the `< Alert Name >` window, review `Actions` to ensure that an `Action group` is assigned to notify the appropriate personnel in your organization.

#### From Azure CLI

```
az monitor activity-log alert list --subscription <subscription ID> --query "[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Network/networkSecurityGroups/write` in the output

## From PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_ .ConditionAllOf.Equal -match
"Microsoft.Network/networkSecurityGroups/write"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

## Remediation:

### From Azure Portal

1. Navigate to the Monitor blade.
2. Select Alerts.
3. Select Create.
4. Select Alert rule.
5. Under Filter by subscription, choose a subscription.
6. Under Filter by resource type, select Network security groups.
7. Under Filter by location, select All.
8. From the results, select the subscription.
9. Select Done.
10. Select the Condition tab.
11. Under Signal name, click Create or Update Network Security Group (Microsoft.Network/networkSecurityGroups).
12. Select the Actions tab.
13. To use an existing action group, click Select action groups. To create a new action group, click Create action group. Fill out the appropriate details for the selection.
14. Select the Details tab.
15. Select a Resource group, provide an Alert rule name and an optional Alert rule description.
16. Click Review + create.
17. Click Create.

### From Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Network/networkSecurityGroups/write and level=verbose
--scope "/subscriptions/<subscription ID>" --name "<activity log rule name>"
--subscription <subscription id> --action-group <action group ID> --location
global
```

## From PowerShell

Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Network/networkSecurityGroups/write -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription id>"
```

Create the `Activity Log Alert Rule` for  
`Microsoft.Network/networkSecurityGroups/write`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

### Default Value:

By default, no monitoring alerts are created.

### References:

1. <https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement>
2. <https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log>
3. <https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate>
4. <https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-3-enable-logging-for-security-investigation>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>8.5 <u>Collect Detailed Audit Logs</u></b>            Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.</p>		●	●
v7	<p><b>6.3 <u>Enable Detailed Logging</u></b>            Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.</p>		●	●

DRAFT

## 5.2.4 Ensure that Activity Log Alert exists for Delete Network Security Group (Automated)

### Profile Applicability:

- Level 1

### Description:

Create an activity log alert for the Delete Network Security Group event.

### Rationale:

Monitoring for "Delete Network Security Group" events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

### Audit:

#### From Azure Portal

1. Navigate to the `Monitor` blade
2. Click on `Alerts`
3. In the Alerts window, click on `Alert rules`
4. Hover mouse over the values in the Condition column to find an alert where `Operation name=Microsoft.Network/networkSecurityGroups/delete`
5. Click on the `Alert Name` associated with the previous step
6. Click on the Condition name of `Whenever the Activity Log has an event with Category='Administrative', Signal name='Delete Network Security Group (networkSecurityGroups)'`
7. In the Configure signal logic window, ensure the following is configured:
  - Event level: All selected
  - Status: All selected
  - Event initiated by: \* (All services and users)
8. Click `Done`
9. Back in the `< Alert Name >` window, review `Actions` to ensure that an Action group is assigned to notify the appropriate personnel in your organization.

#### From Azure CLI

```
az monitor activity-log alert list --subscription <subscription ID> --query "[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Network/networkSecurityGroups/delete` in the output



## From PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object  
{$_ .ConditionAllOf.Equal -match  
"Microsoft.Network/networkSecurityGroups/delete"}|select-object  
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

## Remediation:

### From Azure Portal

1. Navigate to the Monitor blade.
2. Select Alerts.
3. Select Create.
4. Select Alert rule.
5. Under Filter by subscription, choose a subscription.
6. Under Filter by resource type, select Network security groups.
7. Under Filter by location, select All.
8. From the results, select the subscription.
9. Select Done.
10. Select the Condition tab.
11. Under Signal name, click Delete Network Security Group (Microsoft.Network/networkSecurityGroups).
12. Select the Actions tab.
13. To use an existing action group, click Select action groups. To create a new action group, click Create action group. Fill out the appropriate details for the selection.
14. Select the Details tab.
15. Select a Resource group, provide an Alert rule name and an optional Alert rule description.
16. Click Review + create.
17. Click Create.

### From Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"  
--condition category=Administrative and  
operationName=Microsoft.Network/networkSecurityGroups/delete and  
level=<verbose | information | warning | error | critical>--scope  
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --  
subscription <subscription id> --action-group <action group ID> --location  
global
```

## From PowerShell

Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Network/networkSecurityGroups/delete -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription id>"
```

Create the `Activity Log Alert Rule` for

`Microsoft.Network/networkSecurityGroups/delete`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

### Default Value:

By default, no monitoring alerts are created.

### References:

1. <https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement>
2. <https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log>
3. <https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate>
4. <https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-3-enable-logging-for-security-investigation>

**CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

DRAFT

## 5.2.5 Ensure that Activity Log Alert exists for Create or Update Security Solution (Automated)

### Profile Applicability:

- Level 1

### Description:

Create an activity log alert for the Create or Update Security Solution event.

### Rationale:

Monitoring for Create or Update Security Solution events gives insight into changes to the active security solutions and may reduce the time it takes to detect suspicious activity.

### Audit:

#### From Azure Portal

1. Navigate to the `Monitor` blade
2. Click on `Alerts`
3. In the Alerts window, click on `Alert rules`
4. Hover mouse over the values in the `Condition` column to find an alert where `Operation name=Microsoft.Security/securitySolutions/write`
5. Click on the `Alert Name` associated with the previous step
6. Click on the `Condition` name of `Whenever the Activity Log has an event with Category='Security', Signal name='Create or Update Security Solutions (securitySolutions)'`
7. In the `Configure signal logic` window, ensure the following is configured:
  - `Event level`: All selected
  - `Status`: All selected
  - `Event initiated by`: \* (All services and users)
8. Click `Done`
9. Back in the `< Alert Name >` window, review `Actions` to ensure that an `Action` group is assigned to notify the appropriate personnel in your organization.

#### From Azure CLI

```
az monitor activity-log alert list --subscription <subscription Id> --query "[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Security/securitySolutions/write` in the output

## From PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_ .ConditionAllOf.Equal -match
"Microsoft.Security/securitySolutions/write"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

## Remediation:

### From Azure Portal

1. Navigate to the Monitor blade.
2. Select Alerts.
3. Select Create.
4. Select Alert rule.
5. Under Filter by subscription, choose a subscription.
6. Under Filter by resource type, select Security Solutions (securitySolutions).
7. Under Filter by location, select All.
8. From the results, select the subscription.
9. Select Done.
10. Select the Condition tab.
11. Under Signal name, click Create or Update Security Solutions (Microsoft.Security/securitySolutions).
12. Select the Actions tab.
13. To use an existing action group, click Select action groups. To create a new action group, click Create action group. Fill out the appropriate details for the selection.
14. Select the Details tab.
15. Select a Resource group, provide an Alert rule name and an optional Alert rule description.
16. Click Review + create.
17. Click Create.

### From Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Security/securitySolutions/write and level=<verbose |
information | warning | error | critical>--scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID> --location
global
```

## From PowerShell

Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Security/securitySolutions/write -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription ID>"
```

Create the `Activity Log Alert Rule` for  
`Microsoft.Security/securitySolutions/write`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

### Default Value:

By default, no monitoring alerts are created.

### References:

1. <https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement>
2. <https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log>
3. <https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate>
4. <https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-3-enable-logging-for-security-investigation>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

DRAFT

## 5.2.6 Ensure that Activity Log Alert exists for Delete Security Solution (Automated)

### Profile Applicability:

- Level 1

### Description:

Create an activity log alert for the Delete Security Solution event.

### Rationale:

Monitoring for Delete Security Solution events gives insight into changes to the active security solutions and may reduce the time it takes to detect suspicious activity.

### Audit:

#### From Azure Console

1. Navigate to the `Monitor` blade
2. Click on `Alerts`
3. In the Alerts window, click on `Alert rules`
4. Hover mouse over the values in the `Condition` column to find an alert where `Operation name=Microsoft.Security/securitySolutions/delete`
5. Click on the `Alert Name` associated with the previous step
6. Click on the `Condition` name of `Whenever the Activity Log has an event with Category='Security', Signal name='Delete Security Solutions (securitySolutions)'`
7. In the `Configure signal logic` window, ensure the following is configured:
  - `Event level: All` selected
  - `Status: All` selected
  - `Event initiated by: *` (All services and users)
8. Click `Done`
9. Back in the `< Alert Name >` window, review `Actions` to ensure that an `Action` group is assigned to notify the appropriate personnel in your organization.

#### From Azure CLI

```
az monitor activity-log alert list --subscription <subscription Id> --query "[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Security/securitySolutions/delete` in the output



## From PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_ .ConditionAllOf.Equal -match
"Microsoft.Security/securitySolutions/delete"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

## Remediation:

### From Azure Console

1. Navigate to the Monitor blade.
2. Select Alerts.
3. Select Create.
4. Select Alert rule.
5. Under Filter by subscription, choose a subscription.
6. Under Filter by resource type, select Security Solutions (securitySolutions).
7. Under Filter by location, select All.
8. From the results, select the subscription.
9. Select Done.
10. Select the Condition tab.
11. Under Signal name, click Delete Security Solutions (Microsoft.Security/securitySolutions).
12. Select the Actions tab.
13. To use an existing action group, click Select action groups. To create a new action group, click Create action group. Fill out the appropriate details for the selection.
14. Select the Details tab.
15. Select a Resource group, provide an Alert rule name and an optional Alert rule description.
16. Click Review + create.
17. Click Create.

### From Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Security/securitySolutions/delete and level=<verbose
| information | warning | error | critical>--scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID> --location
global
```

## From PowerShell

Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Security/securitySolutions/delete -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription ID>"
```

Create the `Activity Log Alert Rule` for  
`Microsoft.Security/securitySolutions/delete`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

### Default Value:

By default, no monitoring alerts are created.

### References:

1. <https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement>
2. <https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log>
3. <https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate>
4. <https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-3-enable-logging-for-security-investigation>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

DRAFT

## 5.2.7 Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule (Automated)

### Profile Applicability:

- Level 1

### Description:

Create an activity log alert for the Create or Update SQL Server Firewall Rule event.

### Rationale:

Monitoring for Create or Update SQL Server Firewall Rule events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

### Impact:

There will be a substantial increase in log size if there are a large number of administrative actions on a server.

### Audit:

#### From Azure Portal

1. Navigate to the `Monitor` blade
2. Click on `Alerts`
3. In the Alerts window, click on `Alert rules`
4. Hover mouse over the values in the `Condition` column to find an alert where `Operation name=Microsoft.Sql/servers/firewallRules/write`
5. Click on the `Alert Name` associated with the previous step
6. Click on the `Condition name` of `Whenever the Activity Log has an event with Category='Administrative', Signal name='Create/Update server firewall rule (servers/firewallRules)'`
7. In the `Configure signal logic` window, ensure the following is configured:
  - `Event level`: All selected
  - `Status`: All selected
  - `Event initiated by`: \* (All services and users)
8. Click `Done`
9. Back in the `< Alert Name >` window, review `Actions` to ensure that an `Action group` is assigned to notify the appropriate personnel in your organization.

#### From Azure CLI

```
az monitor activity-log alert list --subscription <subscription Id> --query "[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Sql/servers/firewallRules/write` in the output

## From PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_ .ConditionAllOf.Equal -match
"Microsoft.Sql/servers/firewallRules/write"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

## Remediation:

### From Azure Portal

1. Navigate to the Monitor blade.
2. Select Alerts.
3. Select Create.
4. Select Alert rule.
5. Under Filter by subscription, choose a subscription.
6. Under Filter by resource type, select Server Firewall Rule (servers/firewallRules).
7. Under Filter by location, select All.
8. From the results, select the subscription.
9. Select Done.
10. Select the Condition tab.
11. Under Signal name, click Create/Update server firewall rule (Microsoft.Sql/servers/firewallRules).
12. Select the Actions tab.
13. To use an existing action group, click Select action groups. To create a new action group, click Create action group. Fill out the appropriate details for the selection.
14. Select the Details tab.
15. Select a Resource group, provide an Alert rule name and an optional Alert rule description.
16. Click Review + create.
17. Click Create.

### From Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Sql/servers/firewallRules/write and level=<verbose |
information | warning | error | critical>--scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID> --location
global
```

## From PowerShell

Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Sql/servers/firewallRules/write -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription ID>"
```

Create the `Activity Log Alert Rule` for `Microsoft.Sql/servers/firewallRules/write`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

### Default Value:

By default, no monitoring alerts are created or active.

### References:

1. <https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement>
2. <https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log>
3. <https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate>
4. <https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-3-enable-logging-for-security-investigation>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

DRAFT

## 5.2.8 Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule (Automated)

### Profile Applicability:

- Level 1

### Description:

Create an activity log alert for the "Delete SQL Server Firewall Rule."

### Rationale:

Monitoring for Delete SQL Server Firewall Rule events gives insight into SQL network access changes and may reduce the time it takes to detect suspicious activity.

### Impact:

There will be a substantial increase in log size if there are a large number of administrative actions on a server.

### Audit:

#### From Azure Portal

1. Navigate to the `Monitor` blade
2. Click on `Alerts`
3. In the Alerts window, click on `Alert rules`
4. Hover mouse over the values in the `Condition` column to find an alert where `Operation name=Microsoft.Sql/servers/firewallRules/delete`
5. Click on the `Alert Name` associated with the previous step
6. Click on the `Condition name` of `Whenever the Activity Log has an event with Category='Administrative', Signal name='Delete server firewall rule (servers/firewallRules)'`
7. In the `Configure signal logic` window, ensure the following is configured:
  - `Event level`: All selected
  - `Status`: All selected
  - `Event initiated by`: \* (All services and users)
8. Click `Done`
9. Back in the `< Alert Name >` window, review `Actions` to ensure that an `Action group` is assigned to notify the appropriate personnel in your organization.

#### From Azure CLI

```
az monitor activity-log alert list --subscription <subscription Id> --query "[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Sql/servers/firewallRules/delete` in the output



## From PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_ .ConditionAllOf.Equal -match
"Microsoft.Sql/servers/firewallRules/delete"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

## Remediation:

### From Azure Portal

1. Navigate to the Monitor blade.
2. Select Alerts.
3. Select Create.
4. Select Alert rule.
5. Under Filter by subscription, choose a subscription.
6. Under Filter by resource type, select Server Firewall Rule (servers/firewallRules).
7. Under Filter by location, select All.
8. From the results, select the subscription.
9. Select Done.
10. Select the Condition tab.
11. Under Signal name, click Delete server firewall rule (Microsoft.Sql/servers/firewallRules).
12. Select the Actions tab.
13. To use an existing action group, click Select action groups. To create a new action group, click Create action group. Fill out the appropriate details for the selection.
14. Select the Details tab.
15. Select a Resource group, provide an Alert rule name and an optional Alert rule description.
16. Click Review + create.
17. Click Create.

### From Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Sql/servers/firewallRules/delete and level=<verbose |
information | warning | error | critical>--scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID> --location
global
```

## From PowerShell

Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Sql/servers/firewallRules/delete -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription ID>"
```

Create the `Activity Log Alert Rule` for  
`Microsoft.Sql/servers/firewallRules/delete`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

### Default Value:

By default, no monitoring alerts are created or active.

### References:

1. <https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement>
2. <https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log>
3. <https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate>
4. <https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-3-enable-logging-for-security-investigation>

**CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

DRAFT

## 5.2.9 Ensure that Activity Log Alert exists for Create or Update Public IP Address rule (Automated)

### Profile Applicability:

- Level 1

### Description:

Create an activity log alert for the Create or Update Public IP Addresses rule.

### Rationale:

Monitoring for Create or Update Public IP Address events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

### Impact:

There will be a substantial increase in log size if there are a large number of administrative actions on a server.

### Audit:

#### From Azure Portal

1. Navigate to the `Monitor` blade
2. Click on `Alerts`
3. In the Alerts window, click on `Alert rules`
4. Hover mouse over the values in the `Condition` column to find an alert where `Operation name=Microsoft.Network/publicIPAddresses/write`
5. Click on the `Alert Name` associated with the previous step
6. Click on the `Condition name` of `Whenever the Activity Log has an event with Category='Administrative', Signal name='Create or Update Public Ip Address (publicIPAddresses)'`
7. In the `Configure signal logic` window, ensure the following is configured:
  - `Event level`: All selected
  - `Status`: All selected
  - `Event initiated by`: \* (All services and users)
8. Click `Done`
9. Back in the `< Alert Name >` window, review `Actions` to ensure that an `Action group` is assigned to notify the appropriate personnel in your organization.

#### From Azure CLI

```
az monitor activity-log alert list --subscription <subscription Id> --query "[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Network/publicIPAddresses/write` in the output

## From PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_ .ConditionAllOf.Equal -match
"Microsoft.Network/publicIPAddresses/write"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

## Remediation:

### From Azure Portal

1. Navigate to the Monitor blade.
2. Select Alerts.
3. Select Create.
4. Select Alert rule.
5. Under Filter by subscription, choose a subscription.
6. Under Filter by resource type, select Public IP addresses.
7. Under Filter by location, select All.
8. From the results, select the subscription.
9. Select Done.
10. Select the Condition tab.
11. Under Signal name, click Create or Update Public Ip Address (Microsoft.Network/publicIPAddresses).
12. Select the Actions tab.
13. To use an existing action group, click Select action groups. To create a new action group, click Create action group. Fill out the appropriate details for the selection.
14. Select the Details tab.
15. Select a Resource group, provide an Alert rule name and an optional Alert rule description.
16. Click Review + create.
17. Click Create.

### From Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Network/publicIPAddresses/write and level=<verbose |
information | warning | error | critical>--scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID> --location
global
```

## From PowerShell

Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Network/publicIPAddresses/write -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription ID>"
```

Create the `Activity Log Alert Rule` for `Microsoft.Network/publicIPAddresses/write`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

### Default Value:

By default, no monitoring alerts are created or active.

### References:

1. <https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement>
2. <https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log>
3. <https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate>
4. <https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-3-enable-logging-for-security-investigation>

**CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

DRAFT

## 5.2.10 Ensure that Activity Log Alert exists for Delete Public IP Address rule (Automated)

### Profile Applicability:

- Level 1

### Description:

Create an activity log alert for the Delete Public IP Address rule.

### Rationale:

Monitoring for Delete Public IP Address events gives insight into network access changes and may reduce the time it takes to detect suspicious activity.

### Impact:

There will be a substantial increase in log size if there are a large number of administrative actions on a server.

### Audit:

#### From Azure Portal

1. Navigate to the `Monitor` blade
2. Click on `Alerts`
3. In the Alerts window, click on `Alert rules`
4. Hover mouse over the values in the `Condition` column to find an alert where `Operation name=Microsoft.Network/publicIPAddresses/delete`
5. Click on the `Alert Name` associated with the previous step
6. Click on the `Condition name` of `Whenever the Activity Log has an event with Category='Administrative', Signal name='Delete Public Ip Address (Microsoft.Network/publicIPAddresses)'`
7. In the `Configure signal logic` window, ensure the following is configured:
  - `Event level`: All selected
  - `Status`: All selected
  - `Event initiated by`: \* (All services and users)
8. Click `Done`
9. Back in the `< Alert Name >` window, review `Actions` to ensure that an `Action group` is assigned to notify the appropriate personnel in your organization.

#### From Azure CLI

```
az monitor activity-log alert list --subscription <subscription Id> --query "[].{Name:name,Enabled:enabled,Condition:condition.allOf,Actions:actions}"
```

Look for `Microsoft.Network/publicIPAddresses/delete` in the output



## From PowerShell

```
Get-AzActivityLogAlert -SubscriptionId <subscription ID>|where-object
{$_ .ConditionAllOf.Equal -match
"Microsoft.Network/publicIPAddresses/delete"}|select-object
Location,Name,Enabled,ResourceGroupName,ConditionAllOf
```

## Remediation:

### From Azure Portal

1. Navigate to the Monitor blade.
2. Select Alerts.
3. Select Create.
4. Select Alert rule.
5. Under Filter by subscription, choose a subscription.
6. Under Filter by resource type, select Public IP addresses.
7. Under Filter by location, select All.
8. From the results, select the subscription.
9. Select Done.
10. Select the Condition tab.
11. Under Signal name, click Delete Public Ip Address (Microsoft.Network/publicIPAddresses).
12. Select the Actions tab.
13. To use an existing action group, click Select action groups. To create a new action group, click Create action group. Fill out the appropriate details for the selection.
14. Select the Details tab.
15. Select a Resource group, provide an Alert rule name and an optional Alert rule description.
16. Click Review + create.
17. Click Create.

### From Azure CLI

```
az monitor activity-log alert create --resource-group "<resource group name>"
--condition category=Administrative and
operationName=Microsoft.Network/publicIPAddresses/delete and level=<verbose |
information | warning | error | critical>--scope
"/subscriptions/<subscription ID>" --name "<activity log rule name>" --
subscription <subscription id> --action-group <action group ID> --location
global
```

## From PowerShell

Create the `Conditions` object.

```
$conditions = @()
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Administrative -Field category
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Microsoft.Network/publicIPAddresses/delete -Field operationName
$conditions += New-AzActivityLogAlertAlertRuleAnyOfOrLeafConditionObject -
Equal Verbose -Field level
```

Retrieve the `Action Group` information and store in a variable, then create the `Actions` object.

```
$actionGroup = Get-AzActionGroup -ResourceGroupName <resource group name> -
Name <action group name>
$actionObject = New-AzActivityLogAlertActionGroupObject -Id $actionGroup.Id
```

Create the `Scope` object

```
$scope = "/subscriptions/<subscription ID>"
```

Create the `Activity Log Alert Rule` for  
`Microsoft.Network/publicIPAddresses/delete`

```
New-AzActivityLogAlert -Name "<activity log alert rule name>" -
ResourceGroupName "<resource group name>" -Condition $conditions -Scope
$scope -Location global -Action $actionObject -Subscription <subscription ID>
-Enabled $true
```

### Default Value:

By default, no monitoring alerts are created or active.

### References:

1. <https://azure.microsoft.com/en-us/updates/classic-alerting-monitoring-retirement>
2. <https://docs.microsoft.com/en-in/azure/azure-monitor/platform/alerts-activity-log>
3. <https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/createorupdate>
4. <https://docs.microsoft.com/en-in/rest/api/monitor/activitylogalerts/listbysubscriptionid>
5. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-3-enable-logging-for-security-investigation>

**CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●

DRAFT

## 5.3 Configuring Application Insights

DRAFT

### 5.3.1 Ensure Application Insights are Configured (Automated)

#### Profile Applicability:

- Level 2

#### Description:

Application Insights within Azure act as an Application Performance Monitoring solution providing valuable data into how well an application performs and additional information when performing incident response. The types of log data collected include application metrics, telemetry data, and application trace logging data providing organizations with detailed information about application activity and application transactions. Both data sets help organizations adopt a proactive and retroactive means to handle security and performance related metrics within their modern applications.

#### Rationale:

Configuring Application Insights provides additional data not found elsewhere within Azure as part of a much larger logging and monitoring program within an organization's Information Security practice. The types and contents of these logs will act as both a potential cost saving measure (application performance) and a means to potentially confirm the source of a potential incident (trace logging). Metrics and Telemetry data provide organizations with a proactive approach to cost savings by monitoring an application's performance, while the trace logging data provides necessary details in a reactive incident response scenario by helping organizations identify the potential source of an incident within their application.

#### Impact:

Because Application Insights relies on a Log Analytics Workspace, an organization will incur additional expenses when using this service.

#### Audit:

##### From Azure Portal

1. Navigate to `Application Insights`
2. Ensure an `Application Insights` service is configured and exists.

##### From Azure CLI

*Note:* The `application-insights` extension to Azure CLI is currently in `Preview`  
Add the `application-insights` extension.

```
az extension add --name application-insights
az monitor app-insights component show --query "[].{ID:appId, Name:name,
Tenant:tenantId, Location:location, Provisioning_State:provisioningState}"
```

Ensure the above command produces output, otherwise Application Insights has not been configured.

### From PowerShell

```
Get-AzApplicationInsights|select
location,name,appid,provisioningState,tenantid
```

## Remediation:

### Remediation Procedures

#### From Azure Portal

1. Navigate to Application Insights
2. Under the Basics tab within the PROJECT DETAILS section, select the Subscription
3. Select the Resource group
4. Within the INSTANCE DETAILS, enter a Name
5. Select a Region
6. Next to Resource Mode, select Workspace-based
7. Within the WORKSPACE DETAILS, select the Subscription for the log analytics workspace
8. Select the appropriate Log Analytics Workspace
9. Click Next:Tags >
10. Enter the appropriate Tags as Name, Value pairs.
11. Click Next:Review+Create
12. Click Create

#### From Azure CLI

```
az monitor app-insights component create --app <app name> --resource-group
<resource group name> --location <location> --kind "web" --retention-time
<INT days to retain logs> --workspace <log analytics workspace ID> --
subscription <subscription ID>
```

#### From PowerShell

```
New-AzApplicationInsights -Kind "web" -ResourceGroupName <resource group
name> -Name <app insights name> -location <location> -RetentionInDays <INT
days to retain logs> -SubscriptionID <subscription ID> -WorkspaceResourceId
<log analytics workspace ID>
```

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v7	<b>6.2 <u>Activate audit logging</u></b> Ensure that local logging has been enabled on all systems and networking devices.	●	●	●
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	<b>18 <u>Application Software Security</u></b> Application Software Security			

DRAFT

## 5.4 Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it (Manual)

### Profile Applicability:

- Level 1

### Description:

Resource Logs capture activity to the data access plane while the Activity log is a subscription-level log for the control plane. Resource-level diagnostic logs provide insight into operations that were performed within that resource itself; for example, reading or updating a secret from a Key Vault. Currently, 95 Azure resources support Azure Monitoring (See the more information section for a complete list), including Network Security Groups, Load Balancers, Key Vault, AD, Logic Apps, and CosmosDB. The content of these logs varies by resource type.

A number of back-end services were not configured to log and store Resource Logs for certain activities or for a sufficient length. It is crucial that monitoring is correctly configured to log all relevant activities and retain those logs for a sufficient length of time. Given that the mean time to detection in an enterprise is 240 days, a minimum retention period of two years is recommended.

### Rationale:

A lack of monitoring reduces the visibility into the data plane, and therefore an organization's ability to detect reconnaissance, authorization attempts or other malicious activity. Unlike Activity Logs, Resource Logs are not enabled by default. Specifically, without monitoring it would be impossible to tell which entities had accessed a data store that was breached. In addition, alerts for failed attempts to access APIs for Web Services or Databases are only possible when logging is enabled.

### Impact:

Costs for monitoring varies with Log Volume. Not every resource needs to have logging enabled. It is important to determine the security classification of the data being processed by the given resource and adjust the logging based on which events need to be tracked. This is typically determined by governance and compliance requirements.

### Audit:

#### From Azure Portal

The specific steps for configuring resources within the Azure console vary depending on resource, but typically the steps are:

1. Go to the resource
2. Click on Diagnostic settings
3. In the blade that appears, click "Add diagnostic setting"
4. Configure the diagnostic settings



## 5. Click on Save

### From Azure CLI

List all `resources` for a `subscription`

```
az resource list --subscription <subscription id>
```

For each `resource` run the following

```
az monitor diagnostic-settings list --resource <resource ID>
```

An empty result means a `diagnostic settings` is not configured for that resource. An error message means a `diagnostic settings` is not supported for that resource.

### From PowerShell

Get a list of `resources` in a `subscription` context and store in a variable

```
$resources = Get-AzResource
```

Loop through each `resource` to determine if a `diagnostic setting` is configured or not.

```
foreach ($resource in $resources) {$diagnosticSetting = Get-AzDiagnosticSetting -ResourceId $resource.id -ErrorAction "SilentlyContinue"; if ([string]::IsNullOrEmpty($diagnosticSetting)) {$message = "Diagnostic Settings not configured for resource: " + $resource.Name; Write-Output $message} else {$diagnosticSetting}}
```

A result of `Diagnostic Settings not configured for resource: <resource name>` means a `diagnostic settings` is not configured for that resource. Otherwise, the output of the above command will show configured `Diagnostic Settings` for a resource.

### Remediation:

Azure Subscriptions should log every access and operation for all resources. Logs should be sent to Storage and a Log Analytics Workspace or equivalent third-party system. Logs should be kept in readily-accessible storage for a minimum of one year, and then moved to inexpensive cold storage for a duration of time as necessary. If retention policies are set but storing logs in a Storage Account is disabled (for example, if only Event Hubs or Log Analytics options are selected), the retention policies have no effect. Enable all monitoring at first, and then be more aggressive moving data to cold storage if the volume of data becomes a cost concern.

### From Azure Portal

The specific steps for configuring resources within the Azure console vary depending on resource, but typically the steps are:

1. Go to the resource
2. Click on Diagnostic settings
3. In the blade that appears, click "Add diagnostic setting"
4. Configure the diagnostic settings
5. Click on Save

## From Azure CLI

For each `resource`, run the following making sure to use a `resource` appropriate JSON encoded `category` for the `--logs` option.

```
az monitor diagnostic-settings create --name <diagnostic settings name> --resource <resource ID> --logs "[{category:<resource specific category>,enabled:true,retention-policy:{enabled:true,days:180}}]" --metrics "[{category:AllMetrics,enabled:true,retention-policy:{enabled:true,days:180}}]" <[--event-hub <event hub ID> --event-hub-rule <event hub auth rule ID> | --storage-account <storage account ID> | --workspace <log analytics workspace ID> | --marketplace-partner-id <full resource ID of third-party solution>]>
```

## From PowerShell

Create the `log` settings object

```
$logSettings = @()
$logSettings += New-AzDiagnosticSettingLogSettingsObject -Enabled $true -RetentionPolicyDay 180 -RetentionPolicyEnabled $true -Category <resource specific category>
$logSettings += New-AzDiagnosticSettingLogSettingsObject -Enabled $true -RetentionPolicyDay 180 -RetentionPolicyEnabled $true -Category <resource specific category number 2>
```

Create the `metric` settings object

```
$metricSettings = @()
$metricSettings += New-AzDiagnosticSettingMetricSettingsObject -Enabled $true -RetentionPolicyDay 180 -RetentionPolicyEnabled $true -Category AllMetrics
```

Create the diagnostic setting for a specific resource

```
New-AzDiagnosticSetting -Name "<diagnostic settings name>" -ResourceId <resource ID> -Log $logSettings -Metric $metricSettings
```

## Default Value:

By default, Azure Monitor Resource Logs are 'Disabled' for all resources.

## References:

1. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-3-enable-logging-for-security-investigation>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-5-centralize-security-log-management-and-analysis>
3. <https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/monitor-azure-resource>
4. Supported Log Categories: <https://docs.microsoft.com/en-us/azure/azure-monitor/essentials/resource-logs-categories>
5. Logs and Audit - Fundamentals: <https://docs.microsoft.com/en-us/azure/security/fundamentals/log-audit>
6. Collecting Logs: <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/collect-activity-logs>

7. Key Vault Logging: <https://docs.microsoft.com/en-us/azure/key-vault/key-vault-logging>
8. Monitor Diagnostic Settings: <https://docs.microsoft.com/en-us/cli/azure/monitor/diagnostic-settings?view=azure-cli-latest>
9. Overview of Diagnostic Logs: <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-logs-overview>
10. Supported Services for Diagnostic Logs: <https://docs.microsoft.com/en-us/azure/azure-monitor/platform/diagnostic-logs-schema>
11. Diagnostic Logs for CDNs: <https://docs.microsoft.com/en-us/azure/cdn/cdn-azure-diagnostic-logs>

**Additional Information:**

Note: The CIS Benchmark covers some specific Diagnostic Logs separately.

Section 3 - Storage Accounts: Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' requests

Section 6 - Network: Ensure that Network Security Group Flow Log retention period is 'greater than 90 days'

For an up-to-date list of Azure resources which support Azure Monitor, refer to the "Supported Log Categories" reference.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.5 <u>Collect Detailed Audit Logs</u></b> Configure detailed audit logging for enterprise assets containing sensitive data. Include event source, date, username, timestamp, source addresses, destination addresses, and other useful elements that could assist in a forensic investigation.		●	●
v8	<b>8.9 <u>Centralize Audit Logs</u></b> Centralize, to the extent possible, audit log collection and retention across enterprise assets.		●	●
v7	<b>6.3 <u>Enable Detailed Logging</u></b> Enable system logging to include detailed information such as an event source, date, user, timestamp, source addresses, destination addresses, and other useful elements.		●	●
v7	<b>6.5 <u>Central Log Management</u></b> Ensure that appropriate logs are being aggregated to a central log management system for analysis and review.		●	●

## *5.5 Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads) (Automated)*

### **Profile Applicability:**

- Level 2

### **Description:**

The use of Basic or Free SKUs in Azure whilst cost effective have significant limitations in terms of what can be monitored and what support can be realized from Microsoft. Typically, these SKU's do not have a service SLA and Microsoft will usually refuse to provide support for them. Consequently Basic/Free SKUs should never be used for production workloads.

### **Rationale:**

Typically, production workloads need to be monitored and should have an SLA with Microsoft, using Basic SKUs for any deployed product will mean that that these capabilities do not exist.

The following resource types should use standard SKUs as a minimum.

- Public IP Addresses
- Network Load Balancers
- REDIS Cache
- SQL PaaS Databases
- VPN Gateways

### **Impact:**

The impact of enforcing Standard SKU's is twofold

1. There will be a cost increase
2. The monitoring and service level agreements will be available and will support the production service.

All resources should be either tagged or in separate Management Groups/Subscriptions

### **Audit:**

This needs to be audited by Azure Policy (one for each resource type) and denied for each artifact that is production.

## From Azure Portal

1. Open Azure Resource Graph Explorer
2. Click New query
3. Paste the following into the query window:

```
Resources
| where sku contains 'Basic' or sku contains 'consumption'
| order by type
```

4. Click Run query then evaluate the results in the results window.

## From Azure CLI

```
az graph query -q "Resources | sku contains 'Basic' or sku contains
'consumption' | order by type"
```

## From PowerShell

```
Get-AzResource | ?{ $_.Sku -EQ "Basic" }
```

## Remediation:

Each artifact has its own process for upgrading from basic to standard SKU's and this should be followed if required.

## Default Value:

Policy should enforce standard SKUs for the following artifacts:

- Public IP Addresses
- Network Load Balancers
- REDIS Cache
- SQL PaaS Databases
- VPN Gateways

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v7	<b><u>5.5 Implement Automated Configuration Monitoring Systems</u></b> Utilize a Security Content Automation Protocol (SCAP) compliant configuration monitoring system to verify all security configuration elements, catalog approved exceptions, and alert when unauthorized changes occur.		●	●

## 6 Networking

This section covers security recommendations to follow in order to set networking policies on an Azure subscription.

DRAFT

## 6.1 Ensure that RDP access from the Internet is evaluated and restricted (Automated)

### Profile Applicability:

- Level 1

### Description:

Network security groups should be periodically evaluated for port misconfigurations. Where certain ports and protocols may be exposed to the Internet, they should be evaluated for necessity and restricted wherever they are not explicitly required.

### Rationale:

The potential security problem with using RDP over the Internet is that attackers can use various brute force techniques to gain access to Azure Virtual Machines. Once the attackers gain access, they can use a virtual machine as a launch point for compromising other machines on an Azure Virtual Network or even attack networked devices outside of Azure.

### Audit:

#### From Azure Portal

1. For each VM, open the `Networking` blade
2. Verify that the `INBOUND PORT RULES` **does not** have a rule for RDP such as
  - port = 3389,
  - protocol = TCP,
  - Source = Any OR Internet

#### From Azure CLI

List Network security groups with corresponding non-default Security rules:

```
az network nsg list --query [*].[name,securityRules]
```

Ensure that none of the NSGs have security rule as below

```
"access" : "Allow"
"destinationPortRange" : "3389" or "*" or "[port range containing 3389]"
"direction" : "Inbound"
"protocol" : "TCP"
"sourceAddressPrefix" : "*" or "0.0.0.0" or "<nw>/0" or "/0" or "internet" or "any"
```

## Remediation:

Where RDP is not explicitly required and narrowly configured for resources attached to the Network Security Group, Internet-level access to your Azure resources should be restricted or eliminated.

For internal access to relevant resources, configure an encrypted network tunnel such as:

[ExpressRoute](#)

[Site-to-site VPN](#)

[Point-to-site VPN](#)

## Default Value:

By default, RDP access from internet is not enabled.

## References:

1. <https://docs.microsoft.com/en-us/azure/security/azure-security-network-security-best-practices#disable-rdpssh-access-to-azure-virtual-machines>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-1-establish-network-segmentation-boundaries>
3. Express Route: <https://docs.microsoft.com/en-us/azure/expressroute/>
4. Site-to-Site VPN: <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>
5. Point-to-Site VPN: <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</b> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	<b>4.5 Implement and Manage a Firewall on End-User Devices</b> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	<b>13.4 Perform Traffic Filtering Between Network Segments</b> Perform traffic filtering between network segments, where appropriate.		●	●
v7	<b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●



## 6.2 Ensure that SSH access from the Internet is evaluated and restricted (Automated)

### Profile Applicability:

- Level 1

### Description:

Network security groups should be periodically evaluated for port misconfigurations. Where certain ports and protocols may be exposed to the Internet, they should be evaluated for necessity and restricted wherever they are not explicitly required.

### Rationale:

The potential security problem with using SSH over the Internet is that attackers can use various brute force techniques to gain access to Azure Virtual Machines. Once the attackers gain access, they can use a virtual machine as a launch point for compromising other machines on the Azure Virtual Network or even attack networked devices outside of Azure.

### Audit:

#### From Azure Portal

1. Open the `Networking` blade for the specific Virtual machine in Azure portal
2. Verify that the `INBOUND PORT RULES` **does not** have a rule for SSH such as
  - port = 22,
  - protocol = TCP,
  - Source = Any OR Internet

#### From Azure CLI

List Network security groups with corresponding non-default Security rules:

```
az network nsg list --query [*].[name,securityRules]
```

Ensure that none of the NSGs have security rule as below

```
"access" : "Allow"
"destinationPortRange" : "22" or "*" or "[port range containing 22]"
"direction" : "Inbound"
"protocol" : "TCP"
"sourceAddressPrefix" : "*" or "0.0.0.0" or "<nw>/0" or "/0" or "internet" or "any"
```

## Remediation:

Where SSH is not explicitly required and narrowly configured for resources attached to the Network Security Group, Internet-level access to your Azure resources should be restricted or eliminated.

For internal access to relevant resources, configure an encrypted network tunnel such as:

[ExpressRoute](#)

[Site-to-site VPN](#)

[Point-to-site VPN](#)

## Default Value:

By default, SSH access from internet is not `enabled`.

## References:

1. <https://docs.microsoft.com/en-us/azure/security/azure-security-network-security-best-practices#disable-rdpssh-access-to-azure-virtual-machines>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-1-establish-network-segmentation-boundaries>
3. Express Route: <https://docs.microsoft.com/en-us/azure/expressroute/>
4. Site-to-Site VPN: <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>
5. Point-to-Site VPN: <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</b> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.	●	●	●
v8	<b>4.5 Implement and Manage a Firewall on End-User Devices</b> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.	●	●	●
v8	<b>13.4 Perform Traffic Filtering Between Network Segments</b> Perform traffic filtering between network segments, where appropriate.		●	●
v7	<b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

## 6.3 Ensure that UDP access from the Internet is evaluated and restricted (Automated)

### Profile Applicability:

- Level 1

### Description:

Network security groups should be periodically evaluated for port misconfigurations. Where certain ports and protocols may be exposed to the Internet, they should be evaluated for necessity and restricted wherever they are not explicitly required.

### Rationale:

The potential security problem with broadly exposing UDP services over the Internet is that attackers can use DDoS amplification techniques to reflect spoofed UDP traffic from Azure Virtual Machines. The most common types of these attacks use exposed DNS, NTP, SSDP, SNMP, CLDAP and other UDP-based services as amplification sources for disrupting services of other machines on the Azure Virtual Network or even attack networked devices outside of Azure.

### Audit:

#### From Azure Portal

1. Open the `Networking` blade for the specific Virtual machine in Azure portal
2. Verify that the `INBOUND PORT RULES` **does not** have a rule for UDP such as
  - protocol = UDP,
  - Source = Any OR Internet

#### From Azure CLI

List Network security groups with corresponding non-default Security rules:

```
az network nsg list --query [*].[name,securityRules]
```

Ensure that none of the NSGs have security rule as below

```
"access" : "Allow"  
"destinationPortRange" : "*" or "[port range containing 53, 123, 161, 389, 1900, or other vulnerable UDP-based services]"  
"direction" : "Inbound"  
"protocol" : "UDP"  
"sourceAddressPrefix" : "*" or "0.0.0.0" or "<nw>/0" or "/0" or "internet" or "any"
```

## Remediation:

Where UDP is not explicitly required and narrowly configured for resources attached to the Network Security Group, Internet-level access to your Azure resources should be restricted or eliminated.

For internal access to relevant resources, configure an encrypted network tunnel such as:

[ExpressRoute](#)

[Site-to-site VPN](#)

[Point-to-site VPN](#)









## Default Value:

By default, UDP access from internet is not enabled.

## References:

1. <https://docs.microsoft.com/en-us/azure/security/fundamentals/network-best-practices#secure-your-critical-azure-service-resources-to-only-your-virtual-networks>
2. <https://docs.microsoft.com/en-us/azure/security/fundamentals/ddos-best-practices>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-1-establish-network-segmentation-boundaries>
4. ExpressRoute: <https://docs.microsoft.com/en-us/azure/expressroute/>
5. Site-to-site VPN: <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>
6. Point-to-site VPN: <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</b> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	<b>4.5 Implement and Manage a Firewall on End-User Devices</b> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v8	<b>13.4 Perform Traffic Filtering Between Network Segments</b> Perform traffic filtering between network segments, where appropriate.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p>9.2 <u>Ensure Only Approved Ports, Protocols and Services Are Running</u></p> <p>Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.</p>		●	●

DRAFT

## 6.4 Ensure that HTTP(S) access from the Internet is evaluated and restricted (Automated)

### Profile Applicability:

- Level 1

### Description:

Network security groups should be periodically evaluated for port misconfigurations. Where certain ports and protocols may be exposed to the Internet, they should be evaluated for necessity and restricted wherever they are not explicitly required and narrowly configured.

### Rationale:

The potential security problem with using HTTP(S) over the Internet is that attackers can use various brute force techniques to gain access to Azure resources. Once the attackers gain access, they can use the resource as a launch point for compromising other resources within the Azure tenant.

### Audit:

#### From Azure Portal

1. For each VM, open the Networking blade
2. Verify that the INBOUND PORT RULES does not have a rule for HTTP such as
  - port = 80,
  - protocol = TCP,
  - Source = Any OR Internet

#### From Azure CLI

List Network security groups with corresponding non-default Security rules:

```
az network nsg list --query [*].[name,securityRules]
```

Ensure that none of the NSGs have security rule as below

```
"access" : "Allow"
"destinationPortRange" : "80" or "*" or "[port range containing 80]"
"direction" : "Inbound"
"protocol" : "TCP"
"sourceAddressPrefix" : "*" or "0.0.0.0" or "<nw>/0" or "/0" or "internet" or "any"
```

## Remediation:

Where HTTP(S) is not explicitly required and narrowly configured for resources attached to the Network Security Group, Internet-level access to your Azure resources should be restricted or eliminated.

For internal access to relevant resources, configure an encrypted network tunnel such as:

[ExpressRoute](#)











[Site-to-site VPN](#)

[Point-to-site VPN](#)

## References:

1. Express Route: <https://docs.microsoft.com/en-us/azure/expressroute/>
2. Site-to-Site VPN: <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-site-to-site-resource-manager-portal>
3. Point-to-Site VPN: <https://docs.microsoft.com/en-us/azure/vpn-gateway/vpn-gateway-howto-point-to-site-resource-manager-portal>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-1-establish-network-segmentation-boundaries>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>4.4 Implement and Manage a Firewall on Servers</b> Implement and manage a firewall on servers, where supported. Example implementations include a virtual firewall, operating system firewall, or a third-party firewall agent.			
v8	<b>4.5 Implement and Manage a Firewall on End-User Devices</b> Implement and manage a host-based firewall or port-filtering tool on end-user devices, with a default-deny rule that drops all traffic except those services and ports that are explicitly allowed.			
v8	<b>13.4 Perform Traffic Filtering Between Network Segments</b> Perform traffic filtering between network segments, where appropriate.			
v7	<b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.			

## 6.5 Ensure that Network Security Group Flow Log retention period is 'greater than 90 days' (Automated)

### Profile Applicability:

- Level 2

### Description:

Network Security Group Flow Logs should be enabled and the retention period set to greater than or equal to 90 days.

### Rationale:

Flow logs enable capturing information about IP traffic flowing in and out of network security groups. Logs can be used to check for anomalies and give insight into suspected breaches.

### Impact:

This will keep IP traffic logs for longer than 90 days. As a level 2, first determine your need to retain data, then apply your selection here. As this is data stored for longer, your monthly storage costs will increase depending on your data use.

### Audit:

#### From Azure Portal

1. Go to `Network Watcher`
2. Select `NSG flow logs` blade in the `Logs` section
3. Select each `Network Security Group` from the list
4. Ensure `Status` is set to `On`
5. Ensure `Retention (days)` setting greater than 90 days

#### From Azure CLI

```
az network watcher flow-log show --resource-group <resourceGroup> --nsg <NameorID of the NetworkSecurityGroup> --query 'retentionPolicy'
```

Ensure that `enabled` is set to `true` and `days` is set to greater then or equal to 90.

### Remediation:

#### From Azure Portal

1. Go to `Network Watcher`
2. Select `NSG flow logs` blade in the `Logs` section
3. Select each `Network Security Group` from the list
4. Ensure `Status` is set to `On`
5. Ensure `Retention (days)` setting greater than 90 days



6. Select your storage account in the `Storage account` field
7. Select `Save`

### From Azure CLI

Enable the NSG flow logs and set the Retention (days) to greater than or equal to 90 days.

```
az network watcher flow-log configure --nsg <NameorID of the Network Security Group> --enabled true --resource-group <resourceGroupName> --retention 91 --storage-account <NameorID of the storage account to save flow logs>
```

### Default Value:

By default, Network Security Group Flow Logs are disabled.

### References:

1. <https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-nsg-flow-logging-overview>
2. <https://docs.microsoft.com/en-us/cli/azure/network/watcher/flow-log?view=azure-cli-latest>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-logging-threat-detection#lt-6-configure-log-storage-retention>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>8.3 Ensure Adequate Audit Log Storage</b> Ensure that logging destinations maintain adequate storage to comply with the enterprise's audit log management process.	●	●	●
v8	<b>8.10 Retain Audit Logs</b> Retain audit logs across enterprise assets for a minimum of 90 days.		●	●
v7	<b>6.4 Ensure adequate storage for logs</b> Ensure that all systems that store logs have adequate storage space for the logs generated.		●	●

## 6.6 Ensure that Network Watcher is 'Enabled' (Automated)

### Profile Applicability:

- Level 2

### Description:

Enable Network Watcher for Azure subscriptions.

### Rationale:

Network diagnostic and visualization tools available with Network Watcher help users understand, diagnose, and gain insights to the network in Azure.

### Impact:

There are additional costs per transaction to run and store network data. For high-volume networks these charges will add up quickly.

### Audit:

#### From Azure Portal

1. Go to `Network Watcher`
2. Ensure that the `STATUS` is set to `Enabled`

#### From Azure CLI

```
az network watcher list
```

This will list all regions where `provisioningState` is `Succeeded`.

Then run

```
az account list-locations
```

This will list all regions that exist in the subscription. Compare this list to the previous one to ensure that for all regions, `provisioningState` is set to `Succeeded`.

#### From PowerShell

Get a list of Network Watchers

```
Get-AzNetworkWatcher
```

Make sure each watcher is set with the `ProvisioningState` setting set to `Succeeded` and all `Locations` are set with a watcher.

### Remediation:

Opting out of Network Watcher automatic enablement is a permanent change. Once you opt-out you cannot opt-in without contacting support.

## Default Value:

Network Watcher is automatically enabled. When you create or update a virtual network in your subscription, Network Watcher will be enabled automatically in your Virtual Network's region. There is no impact to your resources or associated charge for automatically enabling Network Watcher.

## References:

1. <https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-monitoring-overview>
2. [https://docs.azure.cn/zh-cn/cli/network/watcher?view=azure-cli-latest#az\\_network\\_watcher\\_list](https://docs.azure.cn/zh-cn/cli/network/watcher?view=azure-cli-latest#az_network_watcher_list)
3. [https://docs.azure.cn/zh-cn/cli/network/watcher?view=azure-cli-latest#az\\_network\\_watcher\\_configure](https://docs.azure.cn/zh-cn/cli/network/watcher?view=azure-cli-latest#az_network_watcher_configure)
4. <https://docs.microsoft.com/en-us/azure/network-watcher/network-watcher-create>
5. <https://docs.microsoft.com/en-us/azure/security/benchmarks/security-controls-v2-logging-threat-detection#lt-3-enable-logging-for-azure-network-activities>
6. <https://azure.microsoft.com/en-ca/pricing/details/network-watcher/>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>12.2 <u>Establish and Maintain a Secure Network Architecture</u></b> Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v8	<b>12.4 <u>Establish and Maintain Architecture Diagram(s)</u></b> Establish and maintain architecture diagram(s) and/or other network system documentation. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.		●	●
v7	<b>11.2 <u>Document Traffic Configuration Rules</u></b> All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.		●	●
v7	<b>12.1 <u>Maintain an Inventory of Network Boundaries</u></b> Maintain an up-to-date inventory of all of the organization's network boundaries.	●	●	●

## 6.7 Ensure that Public IP addresses are Evaluated on a Periodic Basis (Manual)

### Profile Applicability:

- Level 1

### Description:

Public IP Addresses provide tenant accounts with Internet connectivity for resources contained within the tenant. During the creation of certain resources in Azure, a Public IP Address may be created. All Public IP Addresses within the tenant should be periodically reviewed for accuracy and necessity.

### Rationale:

Public IP Addresses allocated to the tenant should be periodically reviewed for necessity. Public IP Addresses that are not intentionally assigned and controlled present a publicly facing vector for threat actors and significant risk to the tenant.

### Audit:

#### From Azure Portal

1. Open the `All Resources` blade
2. Click on `Add Filter`
3. In the `Add Filter` window, select the following:  
Filter: `Type`  
Operator: `Equals`  
Value: `Public IP address`
4. Click the `Apply` button
5. For each Public IP address in the list, use `Overview` (or `Properties`) to review the `"Associated to:"` field and determine if the associated resource is still relevant to your tenant environment. If the associated resource is relevant, ensure that additional controls exist to mitigate risk (e.g. Firewalls, VPNs, Traffic Filtering, Virtual Gateway Appliances, Web Application Firewalls, etc.) on all subsequently attached resources.

#### From Azure CLI

List all Public IP addresses:

```
az network public-ip list
```

For each Public IP address in the output, review the `"name"` property and determine if the associated resource is still relevant to your tenant environment. If the associated resource is relevant, ensure that additional controls exist to mitigate risk (e.g. Firewalls, VPNs, Traffic Filtering, Virtual Gateway Appliances, Web Application Firewalls, etc.) on all subsequently attached resources.

### Remediation:

Remediation will vary significantly depending on your organization's security requirements for the resources attached to each individual Public IP address.

### Default Value:

During Virtual Machine and Application creation, a setting may create and attach a public IP.

### References:

1. <https://docs.microsoft.com/en-us/cli/azure/network/public-ip?view=azure-cli-latest>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>12.1 <u>Ensure Network Infrastructure is Up-to-Date</u></b> Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	●	●	●
v7	<b>12.1 <u>Maintain an Inventory of Network Boundaries</u></b> Maintain an up-to-date inventory of all of the organization's network boundaries.	●	●	●

## 7 Virtual Machines

This section covers security recommendations to follow for the configuration of Virtual Machines on an Azure subscription.

DRAFT

## 7.1 Ensure Virtual Machines are utilizing Managed Disks (Automated)

### Profile Applicability:

- Level 1

### Description:

Migrate blob-based VHDs to Managed Disks on Virtual Machines to exploit the default features of this configuration. The features include:

1. Default Disk Encryption
2. Resilience, as Microsoft will managed the disk storage and move around if underlying hardware goes faulty
3. Reduction of costs over storage accounts

### Rationale:

Managed disks are by default encrypted on the underlying hardware, so no additional encryption is required for basic protection. It is available if additional encryption is required. Managed disks are by design more resilient that storage accounts.

For ARM-deployed Virtual Machines, Azure Adviser will at some point recommend moving VHDs to managed disks both from a security and cost management perspective.

### Impact:

There are additional costs for managed disks based off of disk space allocated. When converting to managed disks, VMs will be powered off and back on.

### Audit:

#### From Azure Portal

1. Using the search feature, go to `Virtual Machines`
2. Click the `Manage view` dropdown, then select `Edit columns`
3. Add `Uses managed disks` to the selected columns
4. Select `Save`
5. Ensure all virtual machines listed are using managed disks

#### From PowerShell

```
Get-AzVM | ForEach-Object {"Name: " + $_.Name;"ManagedDisk Id: " +  
$_.StorageProfile.OsDisk.ManagedDisk.Id;""}
```

## Example output:

```
Name: vm1
ManagedDisk Id: /disk1/id

Name: vm2
ManagedDisk Id: /disk2/id
```

If the 'ManagedDisk Id' field is empty the os disk for that vm is not managed.

## Remediation:

### From Azure Portal

1. Using the search feature, go to `Virtual Machines`
2. Select the virtual machine you would like to convert
3. Select `Disks` in the menu for the VM
4. At the top select `Migrate to managed disks`
5. You may follow the prompts to convert the disk and finish by selecting `Migrate to start the process`

**NOTE** VMs will be stopped and restarted after migration is complete.

### From PowerShell

```
Stop-AzVM -ResourceGroupName $rgName -Name $vmName -Force
ConvertTo-AzVMManagedDisk -ResourceGroupName $rgName -VMName $vmName
Start-AzVM -ResourceGroupName $rgName -Name $vmName
```

## Default Value:

Managed disks or are an option upon the creation of VMs.

## References:

1. <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/convert-unmanaged-to-managed-disks>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-4-enable-data-at-rest-encryption-by-default>
3. <https://docs.microsoft.com/en-us/azure/virtual-machines/faq-for-disks>
4. <https://azure.microsoft.com/en-us/pricing/details/managed-disks/>



**CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>3.11 <u>Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	<b>14.8 <u>Encrypt Sensitive Information at Rest</u></b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

DRAFT

## 7.2 Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK) (Automated)

### Profile Applicability:

- Level 2

### Description:

Ensure that OS disks (boot volumes) and data disks (non-boot volumes) are encrypted with CMK (Customer Managed Keys). Customer Managed keys can be either ADE or Server Side Encryption (SSE).

### Rationale:

Encrypting the IaaS VM's OS disk (boot volume) and Data disks (non-boot volume) ensures that the entire content is fully unrecoverable without a key, thus protecting the volume from unwanted reads. PMK (Platform Managed Keys) are enabled by default in Azure-managed disks and allow encryption at rest. CMK is recommended because it gives the customer the option to control which specific keys are used for the encryption and decryption of the disk. The customer can then change keys and increase security by disabling them instead of relying on the PMK key that remains unchanging. There is also the option to increase security further by using automatically rotating keys so that access to disk is ensured to be limited. Organizations should evaluate what their security requirements are, however, for the data stored on the disk. For high-risk data using CMK is a must, as it provides extra steps of security. If the data is low risk, PMK is enabled by default and provides sufficient data security.

### Impact:

Using CMK/BYOK will entail additional management of keys.

**NOTE:** You must have your key vault set up to utilize this.

### Audit:

#### From Azure Portal

1. Go to `Virtual machines`
2. For each virtual machine, go to `Settings`
3. Click on `Disks`
4. Ensure that the `OS disk` and `Data disks` have encryption set to CMK.

## From PowerShell

```
$ResourceGroupName="yourResourceGroupName"
$DiskName="yourDiskName"

$disk=Get-AzDisk -ResourceGroupName $ResourceGroupName -DiskName $DiskName
$disk.Encryption.Type
```

## Remediation:

### From Azure Portal

**Note:** Disks must be detached from VMs to have encryption changed.

1. Go to `Virtual machines`
2. For each virtual machine, go to `Settings`
3. Click on `Disks`
4. Click the ellipsis (...), then click `Detach` to detach the disk from the VM
5. Now search for `Disks` and locate the unattached disk
6. Click the disk then select `Encryption`
7. Change your encryption type, then select your encryption set
8. Click `Save`
9. Go back to the VM and re-attach the disk

## From PowerShell

```
$KVRGname = 'MyKeyVaultResourceGroup';
$VMRGName = 'MyVirtualMachineResourceGroup';
$vmName = 'MySecureVM';
$KeyVaultName = 'MySecureVault';
$KeyVault = Get-AzKeyVault -VaultName $KeyVaultName -ResourceGroupName
$KVRGname;
$diskEncryptionKeyVaultUrl = $KeyVault.VaultUri;
$KeyVaultResourceId = $KeyVault.ResourceId;

Set-AzVMDiskEncryptionExtension -ResourceGroupName $VMRGname -VMName $vmName
-DiskEncryptionKeyVaultUrl $diskEncryptionKeyVaultUrl -
DiskEncryptionKeyVaultId $KeyVaultResourceId;
```

**NOTE:** During encryption it is likely that a reboot will be required. It may take up to 15 minutes to complete the process.

**NOTE 2:** This may differ for Linux machines as you may need to set the `-skipVmBackup` parameter

## Default Value:

By default, Azure disks are encrypted using SSE with PMK.

**References:**

1. <https://docs.microsoft.com/azure/security/fundamentals/azure-disk-encryption-vms-vmss>
2. <https://docs.microsoft.com/en-us/azure/security-center/security-center-disk-encryption?toc=%2fazure%2fsecurity%2ftoc.json>
3. <https://docs.microsoft.com/azure/security/fundamentals/data-encryption-best-practices#protect-data-at-resthttps://docs.microsoft.com/azure/virtual-machines/windows/disk-encryption-portal-quickstart>
4. <https://docs.microsoft.com/en-us/rest/api/compute/disks/delete>
5. <https://docs.microsoft.com/en-us/rest/api/compute/disks/update#encryptionsettings>
6. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-5-use-customer-managed-key-option-in-data-at-rest-encryption-when-required>
7. <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disks-enable-customer-managed-keys-powershell>
8. <https://docs.microsoft.com/en-us/azure/virtual-machines/disk-encryption>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.11 <u>Encrypt Sensitive Data at Rest</u></b>            Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.</p>		●	●
v7	<p><b>14.8 <u>Encrypt Sensitive Information at Rest</u></b>            Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.</p>			●

## 7.3 Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK) (Automated)

### Profile Applicability:

- Level 2

### Description:

Ensure that unattached disks in a subscription are encrypted with a Customer Managed Key (CMK).

### Rationale:

Managed disks are encrypted by default with Platform-managed keys. Using Customer-managed keys may provide an additional level of security or meet an organization's regulatory requirements. Encrypting managed disks ensures that its entire content is fully unrecoverable without a key and thus protects the volume from unwarranted reads. Even if the disk is not attached to any of the VMs, there is always a risk where a compromised user account with administrative access to VM service can mount/attach these data disks, which may lead to sensitive information disclosure and tampering.

### Impact:

**NOTE:** You must have your key vault set up to utilize this. Encryption is available only on Standard tier VMs. This might cost you more.

Utilizing and maintaining Customer-managed keys will require additional work to create, protect, and rotate keys.

### Audit:

#### From Azure Portal

1. Go to `Disks`
2. Click on `Add Filter`
3. In the `filter` field select `Disk state`
4. In the `Value` field select `Unattached`
5. Click `Apply`
6. for each disk listed ensure that `Encryption type` in the `encryption` blade is `'Encryption at-rest with a customer-managed key'`

#### From Azure CLI

Ensure command below does not return any output.

```
az disk list --query '[? diskstate == `Unattached`].{encryptionSettings: encryptionSettings, name: name}' -o json
```

## Sample Output:

```
[
  {
    "encryptionSettings": null,
    "name": "<Disk1>"
  },
  {
    "encryptionSettings": null,
    "name": "<Disk2>"
  }
]
```

## Remediation:

If data stored in the disk is no longer useful, refer to Azure documentation to delete unattached data disks at:

```
-https://docs.microsoft.com/en-us/rest/api/compute/disks/delete
-https://docs.microsoft.com/en-us/cli/azure/disk?view=azure-cli-latest#az-disk-delete
```

If data stored in the disk is important, To encrypt the disk refer azure documentation at:

```
-https://docs.microsoft.com/en-us/azure/virtual-machines/disks-enable-customer-managed-keys-portal
-https://docs.microsoft.com/en-us/rest/api/compute/disks/update#encryptionsettings
```

## Default Value:

By default, managed disks are encrypted with a Platform-managed key.

## References:

1. <https://docs.microsoft.com/en-us/azure/security/fundamentals/azure-disk-encryption-vmss-vmss>
2. <https://docs.microsoft.com/en-us/azure/security-center/security-center-disk-encryption?toc=%2fazure%2fsecurity%2ftoc.json>
3. <https://docs.microsoft.com/en-us/rest/api/compute/disks/delete>
4. <https://docs.microsoft.com/en-us/cli/azure/disk?view=azure-cli-latest#az-disk-delete>
5. <https://docs.microsoft.com/en-us/rest/api/compute/disks/update#encryptionsettings>
6. <https://docs.microsoft.com/en-us/cli/azure/disk?view=azure-cli-latest#az-disk-update>
7. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-5-encrypt-sensitive-data-at-rest>

**CIS Controls:**

<b>Controls Version</b>	<b>Control</b>	<b>IG 1</b>	<b>IG 2</b>	<b>IG 3</b>
v8	<b>3.11 <u>Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	<b>14.8 <u>Encrypt Sensitive Information at Rest</u></b> Encrypt all sensitive information at rest using a tool that requires a secondary authentication mechanism not integrated into the operating system, in order to access the information.			●

DRAFT

## 7.4 Ensure that Only Approved Extensions Are Installed (Manual)

### Profile Applicability:

- Level 1

### Description:

For added security, only install organization-approved extensions on VMs.

### Rationale:

Azure virtual machine extensions are small applications that provide post-deployment configuration and automation tasks on Azure virtual machines. These extensions run with administrative privileges and could potentially access anything on a virtual machine. The Azure Portal and community provide several such extensions. Each organization should carefully evaluate these extensions and ensure that only those that are approved for use are actually implemented.

### Impact:

Functionality by unsupported extensions will be disabled.

### Audit:

#### From Azure Portal

1. Go to `Virtual machines`.
2. For each virtual machine, click on the server name to select it go to
3. In the new column menu, under `Settings` Click on `Extensions + applications`.
4. Ensure that all the listed extensions are approved by your organization for use.

#### From Azure CLI

Use the below command to list the extensions attached to a VM, and ensure the listed extensions are approved for use.

```
az vm extension list --vm-name <vmName> --resource-group <sourceGroupName> --query [*].name
```

#### From PowerShell

Get a list of VMs.

```
Get-AzVM
```

For each VM run the following command.

```
Get-AzVMExtension -ResourceGroupName <VM Resource Group> -VMName <VM Name>
```

Review each `Name`, `ExtensionType`, and `ProvisioningState` to make sure no unauthorized extensions are installed on any virtual machines.



## Remediation:

### From Azure Portal

1. Go to `Virtual machines`
2. For each virtual machine, go to `Settings`
3. Click on `Extensions + applications`
4. If there are unapproved extensions, uninstall them.

### From Azure CLI

From the audit command identify the unapproved extensions, and use the below CLI command to remove an unapproved extension attached to VM.

```
az vm extension delete --resource-group <resourceGroupName> --vm-name <vmName> --name <extensionName>
```

### From PowerShell

For each VM and each insecure extension from the Audit Procedure run the following command.

```
Remove-AzVMExtension -ResourceGroupName <ResourceGroupName> -Name <ExtensionName> -VMName <VirtualMachineName>
```




### Default Value:

By default, no extensions are added to the virtual machines.

### References:

1. <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/extensions-features>
2. <https://docs.microsoft.com/en-us/powershell/module/az.compute/?view=azps-7.5.0#vm-extensions>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-asset-management#am-2-use-only-approved-services>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-asset-management#am-5-use-only-approved-applications-in-virtual-machine>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>2.1 <u>Establish and Maintain a Software Inventory</u></b> Establish and maintain a detailed inventory of all licensed software installed on enterprise assets. The software inventory must document the title, publisher, initial install/use date, and business purpose for each entry; where appropriate, include the Uniform Resource Locator (URL), app store(s), version(s), deployment mechanism, and decommission date. Review and update the software inventory bi-annually, or more frequently.			

Controls Version	Control	IG 1	IG 2	IG 3
v7	<b>2.1 <u>Maintain Inventory of Authorized Software</u></b> Maintain an up-to-date list of all authorized software that is required in the enterprise for any business purpose on any business system.	●	●	●

DRAFT

## 7.5 Ensure that Endpoint Protection for all Virtual Machines is installed (Manual)

### Profile Applicability:

- Level 2

### Description:

Install endpoint protection for all virtual machines.

### Rationale:

Installing endpoint protection systems (like anti-malware for Azure) provides for real-time protection capability that helps identify and remove viruses, spyware, and other malicious software. These also offer configurable alerts when known-malicious or unwanted software attempts to install itself or run on Azure systems.

### Impact:

Endpoint protection will incur an additional cost to you.

### Audit:

#### From Azure Portal

1. Go to Security Center
2. Click the Recommendations blade
3. Ensure that there are no recommendations for Endpoint Protection not installed on Azure VMs

#### From Azure CLI

```
az vm show -g MyResourceGroup -n MyVm -d
```

It should list below or any other endpoint extensions as one of the installed extensions.

```
EndpointSecurity || TrendMicroDSA* || Antimalware || EndpointProtection || SCWPAgent || PortalProtectExtension* || FileSecurity*
```

Alternatively, you can employ your own endpoint protection tool for your OS.

### Remediation:

Follow Microsoft Azure documentation to install endpoint protection from the security center. Alternatively, you can employ your own endpoint protection tool for your OS.







### Default Value:

By default Endpoint Protection is disabled.

## References:

1. <https://docs.microsoft.com/en-us/azure/security-center/security-center-install-endpoint-protection>
2. <https://docs.microsoft.com/en-us/azure/security/azure-security-antimalware>
3. [https://docs.microsoft.com/en-us/cli/azure/vm/extension?view=azure-cli-latest#az\\_vm\\_extension\\_list](https://docs.microsoft.com/en-us/cli/azure/vm/extension?view=azure-cli-latest#az_vm_extension_list)
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-endpoint-security#es-1-use-endpoint-detection-and-response-edr>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>10.2 <u>Configure Automatic Anti-Malware Signature Updates</u></b> Configure automatic updates for anti-malware signature files on all enterprise assets.			
v7	<b>8.2 <u>Ensure Anti-Malware Software and Signatures are Updated</u></b> Ensure that the organization's anti-malware software updates its scanning engine and signature database on a regular basis.			

## 7.6 [Legacy] Ensure that VHDs are Encrypted (Manual)

### Profile Applicability:

- Level 2

### Description:

**NOTE: This is a legacy recommendation. Managed Disks are encrypted by default and recommended for all new VM implementations.**

VHD (Virtual Hard Disks) are stored in blob storage and are the old-style disks that were attached to Virtual Machines. The blob VHD was then leased to the VM. By default, storage accounts are not encrypted, and Microsoft Defender will then recommend that the OS disks should be encrypted. Storage accounts can be encrypted as a whole using PMK or CMK. This should be turned on for storage accounts containing VHDs.

### Rationale:

While it is recommended to use Managed Disks which are encrypted by default, "legacy" VHDs may exist for a variety of reasons and may need to remain in VHD format. VHDs are not encrypted by default, so this recommendation intends to address the security of these disks. In these niche cases, VHDs should be encrypted using the procedures in this recommendation to encrypt and protect the data content.

If a virtual machine is using a VHD and can be converted to a managed disk, instructions for this procedure can be found in the resources section of this recommendation under the title "Convert VHD to Managed Disk."

### Impact:

Depending on how the encryption is implemented will change the size of the impact. If provider-managed keys (PMK) are utilized, the impact is relatively low, but processes need to be put in place to regularly rotate the keys. If Customer-managed keys (CMK) are utilized, a key management process needs to be implemented to store and manage key rotation, thus the impact is medium to high depending on user maturity with key management.

### Audit:

#### From Azure CLI

For each virtual machine identify if the VM is using a legacy VHD by reviewing the *VHD* parameter in the output of the following command. The *VHD* parameter will contain the Storage Account name used for the VHD.

```
az vm show --name <MyVM> --resource-group <MyResourceGroup>
```

Next, identify if the storage account from the *VHD* parameter is encrypted by reviewing the *encryption --> services --> blob --> enabled* within the output of the following command and make sure its value is *True*.

```
az storage account show --name <storage account name> --resource-group <resource group>
```

### From PowerShell:

Determine whether the VM is using a VHD for the OS Disk and any Data disks.

```
$virtualMachine = Get-AzVM --Name <vm name> --ResourceGroup <resource group name> |Select-Object -ExpandProperty StorageProfile
```

```
$virtualMachine.OsDisk  
$virtualMachine.DataDisks
```

Next, use the value from *VHD* to see if the storage blob holding the VHD is encrypted.

```
$storageAccount = Get-AzStorageAccount -Name <storage account name from VHD setting> -ResourceGroupName <resource group name>
```

```
$storageAccount.Encryption.Services.Blob
```

### Remediation:

#### From Azure Portal

1. Navigate to the `storage account` that you wish to encrypt
2. Select `encryption`
3. Select the `encryption type` that you wish to use

If you wish to use a Microsoft-managed key (the default), you can save at this point and encryption will be applied to the account.

If you select `Customer-managed keys`, it will ask for the location of the key (The default is an Azure Key Vault) and the key name.

Once these are captured, save the configuration and the account will be encrypted using the provided key.

#### From Azure CLI:

##### Create the Key Vault

```
az keyvault create --name <name> --resource-group <resourceGroup> --location <location> --enabled-for-disk-encryption
```

##### Encrypt the disk and store the key in Key Vault

```
az vm encryption enable -g <resourceGroup> --name <name> --disk-encryption-keyvault myKV
```

#### From PowerShell

This process uses a Key Vault to store the keys

##### Create the Key Vault

```
New-AzKeyvault -name <name> -ResourceGroupName <resourceGroup> -Location <location> -EnabledForDiskEncryption
```

## Encrypt the disk and store the key in Key Vault

```
$KeyVault = Get-AzKeyVault -VaultName <name> -ResourceGroupName  
<resourceGroup>  
Set-AzVMDiskEncryptionExtension -ResourceGroupName <resourceGroup> -VMName  
<name> -DiskEncryptionKeyVaultUrl $KeyVault.VaultUri -  
DiskEncryptionKeyVaultId $KeyVault.ResourceId
```

### Default Value:

The default value for encryption is "NO Encryption"

### References:

1. CLI: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-cli-quickstart>
2. Powershell: <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disk-encryption-powershell-quickstart>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-5-encrypt-sensitive-data-at-rest>
4. Convert VHD to Managed Disk: <https://docs.microsoft.com/en-us/previous-versions/azure/virtual-machines/scripts/virtual-machines-powershell-sample-create-managed-disk-from-vhd>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.11 <u>Encrypt Sensitive Data at Rest</u></b> Encrypt sensitive data at rest on servers, applications, and databases containing sensitive data. Storage-layer encryption, also known as server-side encryption, meets the minimum requirement of this Safeguard. Additional encryption methods may include application-layer encryption, also known as client-side encryption, where access to the data storage device(s) does not permit access to the plain-text data.		●	●
v7	<b>13 <u>Data Protection</u></b> Data Protection			

## 7.7 Ensure an Azure Bastion Host Exists (Automated)

### Profile Applicability:

- Level 2

### Description:

The Azure Bastion service allows secure remote access to Azure Virtual Machines over the Internet without exposing remote access protocol ports and services directly to the Internet. The Azure Bastion service provides this access using TLS over 443/TCP, and subscribes to hardened configurations within an organization's Azure Active Directory service.

### Rationale:

The Azure Bastion service allows organizations a more secure means of accessing Azure Virtual Machines over the Internet without assigning public IP addresses to those Virtual Machines. The Azure Bastion service provides Remote Desktop Protocol (RDP) and Secure Shell (SSH) access to Virtual Machines using TLS within a web browser, thus preventing organizations from opening up 3389/TCP and 22/TCP to the Internet on Azure Virtual Machines. Additional benefits of the Bastion service includes Multi-Factor Authentication, Conditional Access Policies, and any other hardening measures configured within Azure Active Directory using a central point of access.

### Impact:

The Azure Bastion service incurs additional costs and requires a specific virtual network configuration. The `Standard` tier offers additional configuration options compared to the `Basic` tier and may incur additional costs for those added features.

### Audit:

#### From Azure Portal

1. Click on `Bastions`
2. Ensure there is at least one `Bastion` host listed under the `Name` column

#### From Azure CLI

**Note:** The Azure CLI `network bastion` module is in `Preview` as of this writing

```
az network bastion list --subscription <subscription ID>
```

Ensure the output of the above command is not empty.



## From PowerShell

Retrieve the Bastion host(s) information for a specific Resource Group

```
Get-AzBastion -ResourceGroupName <resource group name>  
^^^
```

Ensure the output of the above command is not empty.

## Remediation:

### Remediation Procedures

#### From Azure Portal\*

1. Click on Bastions
2. Select the Subscription
3. Select the Resource group
4. Type a Name for the new Bastion host
5. Select a Region
6. Choose Standard next to Tier
7. Use the slider to set the Instance count
8. Select the Virtual network or Create new
9. Select the Subnet named AzureBastionSubnet. Create a Subnet named AzureBastionSubnet using a /26 CIDR range if it doesn't already exist.
10. Select the appropriate Public IP address option.
11. If Create new is selected for the Public IP address option, provide a Public IP address name.
12. If Use existing is selected for Public IP address option, select an IP address from Choose public IP address
13. Click Next: Tags >
14. Configure the appropriate Tags
15. Click Next: Advanced >
16. Select the appropriate Advanced options
17. Click Next: Review + create >
18. Click Create

#### From Azure CLI

```
az network bastion create --location <location> --name <name of bastion host>  
--public-ip-address <public IP address name or ID> --resource-group <resource  
group name or ID> --vnet-name <virtual network containing subnet called  
"AzureBastionSubnet"> --scale-units <integer> --sku Standard [--disable-copy-  
paste true|false] [--enable-ip-connect true|false] [--enable-tunneling  
true|false]
```

## From PowerShell

Create the appropriate Virtual network settings and Public IP Address settings.

```
$subnetName = "AzureBastionSubnet"
$subnet = New-AzVirtualNetworkSubnetConfig -Name $subnetName -AddressPrefix
<IP address range in CIDR notation making sure to use a /26>
$virtualNet = New-AzVirtualNetwork -Name <virtual network name> -
ResourceGroupName <resource group name> -Location <location> -AddressPrefix
<IP address range in CIDR notation> -Subnet $subnet
$publicip = New-AzPublicIpAddress -ResourceGroupName <resource group name> -
Name <public IP address name> -Location <location> -AllocationMethod Dynamic
-Sku Standard
```

Create the Azure Bastion service using the information within the created variables from above.

```
New-AzBastion -ResourceGroupName <resource group name> -Name <bastion name> -
PublicIpAddress $publicip -VirtualNetwork $virtualNet -Sku "Standard" -
ScaleUnit <integer>
```

### Default Value:

By default, the Azure Bastion service is not configured.

### References:

1. <https://learn.microsoft.com/en-us/azure/bastion/bastion-overview#sku>
2. <https://learn.microsoft.com/en-us/powershell/module/az.network/get-azbastion?view=azps-9.2.0>
3. <https://learn.microsoft.com/en-us/cli/azure/network/bastion?view=azure-cli-latest>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>12.1 Ensure Network Infrastructure is Up-to-Date</b> Ensure network infrastructure is kept up-to-date. Example implementations include running the latest stable release of software and/or using currently supported network-as-a-service (NaaS) offerings. Review software versions monthly, or more frequently, to verify software support.	●	●	●
v8	<b>13.4 Perform Traffic Filtering Between Network Segments</b> Perform traffic filtering between network segments, where appropriate.		●	●
v7	<b>9.2 Ensure Only Approved Ports, Protocols and Services Are Running</b> Ensure that only network ports, protocols, and services listening on a system with validated business needs, are running on each system.		●	●

Controls Version	Control	IG 1	IG 2	IG 3
v7	<p><b>11.2 Document Traffic Configuration Rules</b>            All configuration rules that allow traffic to flow through network devices should be documented in a configuration management system with a specific business reason for each rule, a specific individual's name responsible for that business need, and an expected duration of the need.</p>		●	●
v7	<p><b>12.1 Maintain an Inventory of Network Boundaries</b>            Maintain an up-to-date inventory of all of the organization's network boundaries.</p>	●	●	●

DRAFT

## 8 Key Vault

This section covers security recommendations to follow for the configuration and use of Azure Key Vault.

DRAFT

## 8.1 Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults (Automated)

### Profile Applicability:

- Level 1

### Description:

Ensure that all Keys in Role Based Access Control (RBAC) Azure Key Vaults have an expiration time set.

### Rationale:

Azure Key Vault enables users to store and use cryptographic keys within the Microsoft Azure environment. The `exp` (expiration time) attribute identifies the expiration time on or after which the key MUST NOT be used for encryption of new data, wrapping of new keys, and signing. By default, keys never expire. It is thus recommended that keys be rotated in the key vault and set an explicit expiration time for all keys to help enforce the key rotation. This ensures that the keys cannot be used beyond their assigned lifetimes.

### Impact:

Keys cannot be used beyond their assigned expiration times respectively. Keys need to be rotated periodically wherever they are used.

### Audit:

#### From Azure Portal

1. Go to `Key vaults`
2. For each Key vault, click on `Keys`.
3. Under the `Settings` section, Make sure `Enabled?` is set to `Yes`
4. Then ensure that each key in the vault has `EXPIRATION DATE` set as appropriate

#### From Azure CLI

Get a list of all the keyvaults in your Azure environment by running the following command:

```
az keyvault list
```

Then for each keyvault listed ensure that the output of the below command contains Key ID (kid), enabled status as `true` and Expiration date (expires) is not empty or null:

```
az keyvault key list --vault-name <KEYVAULTNAME> --query ' [*].{"kid":kid,"enabled":attributes.enabled,"expires":attributes.expires} '
```

## From Powershell

Retrieve a list of Azure Key Vaults

```
Get-AzKeyVault
```

For each Key Vault run the following command to determine which vaults are configured to use RBAC.

```
Get-AzKeyVault -VaultName <Vault Name>
```

For each Key Vault with the `EnableRbacAuthorization` setting set to `True`, run the following command.

```
Get-AzKeyVaultKey -VaultName <Vault Name>
```

Make sure the `Expires` setting is configured with a value as appropriate wherever the `Enabled` setting is set to `True`.

## Remediation:

### From Azure Portal

1. Go to `Key vaults`
2. For each Key vault, click on `Keys`.
3. Under the `Settings` section, Make sure `Enabled?` is set to `Yes`
4. Set an appropriate `EXPIRATION DATE` on all keys.

### From Azure CLI

Update the `EXPIRATION DATE` for the key using below command.

```
az keyvault key set-attributes --name <keyName> --vault-name <vaultName> --expires Y-m-d'T'H:M:S'Z'
```

## Note:

In order to access expiration time on all keys in Azure Key Vault using Microsoft API requires "List" Key permission.

To provide required access follow below steps,

### For Key Vaults using "Key Vault Access Policy"

1. Go to `Key vaults`
2. For each Key vault, click on `Access Policy`.
3. Add access policy with `Key permission as List`

### For Key Vaults using "Role Based Access Control"

Assign the role of "*Key Vault Secrets Officer*" to the appropriate user

### From Powershell

```
Set-AzKeyVaultKeyAttribute -VaultName <Vault Name> -Name <Key Name> -Expires <DateTime>
```

## Default Value:

By default, keys do not expire.

**References:**

1. <https://docs.microsoft.com/en-us/azure/key-vault/key-vault-what-is>
2. <https://docs.microsoft.com/en-us/rest/api/keyvault/about-keys--secrets-and-certificates#key-vault-keys>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-6-use-a-secure-key-management-process>
4. <https://docs.microsoft.com/en-us/powershell/module/az.keyvault/set-azkeyvaultkeyattribute?view=azps-0.10.0>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.1 Establish and Maintain a Data Management Process</b>                      Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>	●	●	●
v8	<p><b>6.2 Establish an Access Revoking Process</b>                      Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.</p>	●	●	●
v7	<p><b>16.7 Establish Process for Revoking Access</b>                      Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.</p>		●	●

## 8.2 Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults. (Automated)

### Profile Applicability:

- Level 1

### Description:

Ensure that all Keys in Non Role Based Access Control (RBAC) Azure Key Vaults have an expiration time set.

### Rationale:

Azure Key Vault enables users to store and use cryptographic keys within the Microsoft Azure environment. The `exp` (expiration time) attribute identifies the expiration time on or after which the key MUST NOT be used for a cryptographic operation. By default, keys never expire. It is thus recommended that keys be rotated in the key vault and set an explicit expiration time for all keys. This ensures that the keys cannot be used beyond their assigned lifetimes.

### Impact:

Keys cannot be used beyond their assigned expiration times respectively. Keys need to be rotated periodically wherever they are used.

### Audit:

#### From Azure Portal

1. Go to `Key vaults`
2. For each Key vault, click on `Keys`.
3. Under the `Settings` section, Make sure `Enabled?` is set to `Yes`
4. Then ensure that each key in the vault has `EXPIRATION DATE` set as appropriate

#### From Azure CLI

Get a list of all the keyvaults in your Azure environment by running the following command:

```
az keyvault list
```

For each vault ensure that the output of the below command contains Key ID (kid), enabled status as `true` and Expiration date (expires) is not empty or null:

```
az keyvault key list --vault-name <KEYVAULTNAME> --query '[*].{"kid":kid,"enabled":attributes.enabled,"expires":attributes.expires}'
```



## From PowerShell

Retrieve a list of Azure Key Vaults

```
Get-AzKeyVault
```

For each Key Vault run the following command to determine which vaults are configured to use RBAC.

```
Get-AzKeyVault -VaultName <Vault Name>
```

For each Key Vault with the `EnableRbacAuthorization` setting set to `False` or empty, run the following command.

```
Get-AzKeyVaultKey -VaultName <Vault Name>
```

Make sure the `Expires` setting is configured with a value as appropriate wherever the `Enabled` setting is set to `True`.

## Remediation:

### From Azure Portal

1. Go to `Key vaults`
2. For each Key vault, click on `Keys`.
3. Under the `Settings` section, Make sure `Enabled?` is set to `Yes`
4. Set an appropriate `EXPIRATION DATE` on all keys.

### From Azure CLI

Update the `EXPIRATION DATE` for the key using below command.

```
az keyvault key set-attributes --name <keyName> --vault-name <vaultName> --expires Y-m-d'T'H:M:S'Z'
```

## Note:

To access expiration time on all keys in Azure Key Vault using Microsoft API, "List" Key permission is required.

To provide required access follow below steps,

### For Key Vaults using Key Vault Access Policy

1. Go to `Key vaults`
2. For each Key vault, click on `Access Policy`.
3. Add access policy with `Key permission as List`

## From PowerShell

```
Set-AzKeyVaultKeyAttribute -VaultName <Vault Name> -Name <Key Name> -Expires <DateTime>
```

## Default Value:

By default, keys do not expire.

**References:**

1. <https://docs.microsoft.com/en-us/azure/key-vault/key-vault-what-is>
2. <https://docs.microsoft.com/en-us/rest/api/keyvault/about-keys--secrets-and-certificates#key-vault-keys>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-6-use-a-secure-key-management-process>
4. <https://docs.microsoft.com/en-us/powershell/module/az.keyvault/set-azkeyvaultkeyattribute?view=azps-0.10.0>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.1 Establish and Maintain a Data Management Process</b>            Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>	●	●	●
v8	<p><b>6.2 Establish an Access Revoking Process</b>            Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.</p>	●	●	●
v7	<p><b>16.7 Establish Process for Revoking Access</b>            Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.</p>		●	●

## 8.3 Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults (Automated)

### Profile Applicability:

- Level 1

### Description:

Ensure that all Secrets in Role Based Access Control (RBAC) Azure Key Vaults have an expiration time set.

### Rationale:

The Azure Key Vault enables users to store and keep secrets within the Microsoft Azure environment. Secrets in the Azure Key Vault are octet sequences with a maximum size of 25k bytes each. The `exp` (expiration time) attribute identifies the expiration time on or after which the secret MUST NOT be used. By default, secrets never expire. It is thus recommended to rotate secrets in the key vault and set an explicit expiration time for all secrets. This ensures that the secrets cannot be used beyond their assigned lifetimes.

### Impact:

Secrets cannot be used beyond their assigned expiry times respectively. Secrets need to be rotated periodically wherever they are used.

### Audit:

#### From Azure Portal

\*\* Ensure that the user has the role of *Key Vault Secrets Officer* assigned

1. Go to `Key vaults`
2. For each Key vault, click on `Secrets`.
3. Under the `Settings` section, Make sure `Enabled?` is set to `Yes`
4. Ensure that each secret in the vault has `EXPIRATION DATE` set as appropriate

#### From Azure CLI

Ensure that the output of the below command contains ID (`id`), enabled status as `true` and Expiration date (`expires`) is not empty or null:

```
az keyvault secret list --vault-name <KEYVAULTNAME> --query '[*].{"kid":kid,"enabled":attributes.enabled,"expires":attributes.expires}'
```

## From PowerShell

Retrieve a list of Azure Key Vaults

```
Get-AzKeyVault
```

For each Key Vault run the following command to determine which vaults are configured to use RBAC.

```
Get-AzKeyVault -VaultName <Vault Name>
```

For each Key Vault with the `EnableRbacAuthorization` setting set to `True`, run the following command.

```
Get-AzKeyVaultSecret -VaultName <Vault Name>
```

Make sure the `Expires` setting is configured with a value as appropriate wherever the `Enabled` setting is set to `True`.

## Remediation:

### From Azure Portal

1. Go to `Key vaults`
2. For each Key vault, click on `Secrets`.
3. Under the `Settings` section, Make sure `Enabled?` is set to `Yes`
4. Set an appropriate `EXPIRATION DATE` on all secrets.

### From Azure CLI

Use the below command to set `EXPIRATION DATE` on the all secrets.

```
az keyvault secret set-attributes --name <secretName> --vault-name <vaultName> --expires Y-m-d'T'H:M:S'Z'
```

### From PowerShell

```
Set-AzKeyVaultSecretAttribute -VaultName <Vault Name> -Name <Secret Name> -Expires <DateTime>
```

## Default Value:

By default, secrets do not expire.

## References:

1. <https://docs.microsoft.com/en-us/azure/key-vault/key-vault-what-is>
2. <https://docs.microsoft.com/en-us/rest/api/keyvault/about-keys--secrets-and-certificates#key-vault-secrets>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-6-use-a-secure-key-management-process>
4. <https://docs.microsoft.com/en-us/powershell/module/az.keyvault/set-azkeyvaultsecretattribute?view=azps-0.10.0>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.1 <u>Establish and Maintain a Data Management Process</u></b>            Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>	●	●	●
v8	<p><b>6.2 <u>Establish an Access Revoking Process</u></b>            Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.</p>	●	●	●
v7	<p><b>16.7 <u>Establish Process for Revoking Access</u></b>            Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.</p>		●	●

DRAFT

## 8.4 Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults (Automated)

### Profile Applicability:

- Level 1

### Description:

Ensure that all Secrets in Non Role Based Access Control (RBAC) Azure Key Vaults have an expiration time set.

### Rationale:

The Azure Key Vault enables users to store and keep secrets within the Microsoft Azure environment. Secrets in the Azure Key Vault are octet sequences with a maximum size of 25k bytes each. The `exp` (expiration time) attribute identifies the expiration time on or after which the secret MUST NOT be used. By default, secrets never expire. It is thus recommended to rotate secrets in the key vault and set an explicit expiration time for all secrets. This ensures that the secrets cannot be used beyond their assigned lifetimes.

### Impact:

Secrets cannot be used beyond their assigned expiry times respectively. Secrets need to be rotated periodically wherever they are used.

### Audit:

#### From Azure Portal

1. Go to `Key vaults`
2. For each Key vault, click on `Secrets`.
3. Under the `Settings` section, Make sure `Enabled?` is set to `Yes`
4. Ensure that each secret in the vault has `EXPIRATION DATE` set as appropriate

#### From Azure CLI

Get a list of all the keyvaults in your Azure environment by running the following command:

```
az keyvault list
```

For each keyvault ensure that the output of the below command contains ID (id), enabled status as `true` and Expiration date (expires) is not empty or null:

```
az keyvault secret list --vault-name <KEYVALUTNAME> --query '[*].{"kid":kid,"enabled":attributes.enabled,"expires":attributes.expires}'
```

## From PowerShell

Retrieve a list of Azure Key Vaults

```
Get-AzKeyVault
```

For each Key Vault run the following command to determine which vaults are configured to use RBAC.

```
Get-AzKeyVault -VaultName <Vault Name>
```

For each Key Vault with the `EnableRbacAuthorization` setting set to `False` or empty, run the following command.

```
Get-AzKeyVaultSecret -VaultName <Vault Name>
```

Make sure the `Expires` setting is configured with a value as appropriate wherever the `Enabled` setting is set to `True`.

## Remediation:

### From Azure Portal

1. Go to Key vaults
2. For each Key vault, click on Secrets.
3. Under the Settings section, Make sure `Enabled?` is set to `Yes`
4. Set an appropriate EXPIRATION DATE on all secrets.

### From Azure CLI

Use the below command to set EXPIRATION DATE on the all secrets.

```
az keyvault secret set-attributes --name <secretName> --vault-name <vaultName> --expires Y-m-d'T'H:M:S'Z'
```

### From PowerShell

For each Key Vault with the `EnableRbacAuthorization` setting set to `False` or empty, run the following command.

```
Set-AzKeyVaultSecret -VaultName <Vault Name> -Name <Secret Name> -Expires <DateTime>
```

## Default Value:

By default, secrets do not expire.

## References:

1. <https://docs.microsoft.com/en-us/azure/key-vault/key-vault-what-is>
2. <https://docs.microsoft.com/en-us/rest/api/keyvault/about-keys--secrets-and-certificates#key-vault-secrets>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-6-use-a-secure-key-management-process>
4. <https://docs.microsoft.com/en-us/powershell/module/az.keyvault/set-azkeyvaultsecret?view=azps-7.4.0>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.1 <u>Establish and Maintain a Data Management Process</u></b>            Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>	●	●	●
v8	<p><b>6.2 <u>Establish an Access Revoking Process</u></b>            Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.</p>	●	●	●
v7	<p><b>16.7 <u>Establish Process for Revoking Access</u></b>            Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.</p>		●	●

DRAFT



## 8.5 Ensure the Key Vault is Recoverable (Automated)

### Profile Applicability:

- Level 1

### Description:

The Key Vault contains object keys, secrets, and certificates. Accidental unavailability of a Key Vault can cause immediate data loss or loss of security functions (authentication, validation, verification, non-repudiation, etc.) supported by the Key Vault objects.

It is recommended the Key Vault be made recoverable by enabling the "Do Not Purge" and "Soft Delete" functions. This is in order to prevent loss of encrypted data, including storage accounts, SQL databases, and/or dependent services provided by Key Vault objects (Keys, Secrets, Certificates) etc. This may happen in the case of accidental deletion by a user or from disruptive activity by a malicious user.

**WARNING:** A current limitation of the soft-delete feature across all Azure services is role assignments disappearing when Key Vault is deleted. All role assignments will need to be recreated after recovery.

### Rationale:

There could be scenarios where users accidentally run delete/purge commands on Key Vault or an attacker/malicious user deliberately does so in order to cause disruption. Deleting or purging a Key Vault leads to immediate data loss, as keys encrypting data and secrets/certificates allowing access/services will become non-accessible. There are 2 Key Vault properties that play a role in permanent unavailability of a Key Vault:

1. `enableSoftDelete`:

Setting this parameter to "true" for a Key Vault ensures that even if Key Vault is deleted, Key Vault itself or its objects remain recoverable for the next 90 days. Key Vault/objects can either be recovered or purged (permanent deletion) during those 90 days. If no action is taken, key vault and its objects will subsequently be purged.

2. `enablePurgeProtection`:

`enableSoftDelete` only ensures that Key Vault is not deleted permanently and will be recoverable for 90 days from date of deletion. However, there are scenarios in which the Key Vault and/or its objects are accidentally purged and hence will not be recoverable. Setting `enablePurgeProtection` to "true" ensures that the Key Vault and its objects cannot be purged.

Enabling both the parameters on Key Vaults ensures that Key Vaults and their objects cannot be deleted/purged permanently.

## Impact:

Once purge-protection and soft-delete are enabled for a Key Vault, the action is irreversible.

## Audit:

### From Azure Portal

1. Go to Key Vaults
2. For each Key Vault
3. Click Properties
4. Ensure the status of soft-delete reads Soft delete has been enabled on this key vault

### From Azure CLI

1. List all Resources of type Key Vaults:

```
az resource list --query "[?type=='Microsoft.KeyVault/vaults']"
```

2. For Every Key Vault ID ensure check parameters `enableSoftDelete` and `enablePurgeProtection` are set to enabled.

```
az resource show --id /subscriptions/xxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx/resourceGroups/<resourceGroupName>/providers/Microsoft.KeyVault/vaults/<keyVaultName>
```

### From PowerShell

Get all Key Vaults.

```
Get-AzKeyVault
```

For each Key Vault run the following command.

```
Get-AzKeyVault -VaultName <Vault Name>
```

Examine the results of the above command for the `EnablePurgeProtection` setting and the `EnableSoftDelete` setting. Make sure both settings are set to `True`.

## Remediation:

To enable "Do Not Purge" and "Soft Delete" for a Key Vault:  
**From Azure Portal**

1. Go to `Key Vaults`
2. For each Key Vault
3. Click `Properties`
4. Ensure the status of soft-delete reads `Soft delete has been enabled on this key vault.`
5. At the bottom of the page, click 'Enable Purge Protection'  
Note, once enabled you cannot disable it.

## From Azure CLI

```
az resource update --id /subscriptions/xxxxxx-xxxx-xxxx-xxxx-  
xxxxxxxxxxxx/resourceGroups/<resourceGroupName>/providers/Microsoft.KeyVault  
/vaults/<keyVaultName> --set properties.enablePurgeProtection=true  
properties.enableSoftDelete=true
```

## From PowerShell

```
Update-AzKeyVault -VaultName <vaultName -ResourceGroupName <resourceGroupName  
-EnablePurgeProtection
```

## Default Value:

When a new Key Vault is created, both the parameters `enableSoftDelete` and `enablePurgeProtection` are set to `null`, disabling both the features.

## References:

1. <https://docs.microsoft.com/en-us/azure/key-vault/key-vault-soft-delete-cli>
2. <https://blogs.technet.microsoft.com/kv/2017/05/10/azure-key-vault-recovery-options/>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-8-define-and-implement-backup-and-recovery-strategy>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-8-ensure-security-of-key-and-certificate-repository>

## Additional Information:

When a key is used for SQL server TDE or Encrypting Storage Account, both the features "Do Not Purge" and "Soft Delete" are enabled for the corresponding Key Vault by default by Azure Backend.

**WARNING:** A current limitation of the soft-delete feature across all Azure services is role assignments disappearing when Key Vault is deleted. All role assignments will need to be recreated after recovery.

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>11.1 <u>Establish and Maintain a Data Recovery Process</u></b>                      Establish and maintain a data recovery process. In the process, address the scope of data recovery activities, recovery prioritization, and the security of backup data. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>	●	●	●
v7	<p><b>10.2 <u>Perform Complete System Backups</u></b>                      Ensure that each of the organization's key systems are backed up as a complete system, through processes such as imaging, to enable the quick recovery of an entire system.</p>	●	●	●

DRAFT

## 8.6 Enable Role Based Access Control for Azure Key Vault (Manual)

### Profile Applicability:

- Level 2

### Description:

WARNING: Role assignments disappear when a Key Vault has been deleted (soft-delete) and recovered. Afterwards it will be required to recreate all role assignments. This is a limitation of the soft-delete feature across all Azure services.

### Rationale:

The new RBAC permissions model for Key Vaults enables a much finer grained access control for key vault secrets, keys, certificates, etc., than the vault access policy. This in turn will permit the use of privileged identity management over these roles, thus securing the key vaults with JIT Access management.

### Impact:

Implementation needs to be properly designed from the ground up, as this is a fundamental change to the way key vaults are accessed/managed. Changing permissions to key vaults will result in loss of service as permissions are re-applied. For the least amount of downtime, map your current groups and users to their corresponding permission needs.

### Audit:

#### From Azure Portal

1. From Azure Home open the Portal Menu in the top left corner
2. Select Key Vaults
3. Select a Key Vault to audit
4. Select Access configuration
5. Ensure the Permission Model radio button is set to `Azure role-based access control`

### Remediation:

#### From Azure Portal

Key Vaults can be configured to use `Azure role-based access control` on creation. For existing Key Vaults:

1. From Azure Home open the Portal Menu in the top left corner
2. Select `Key Vaults`
3. Select a Key Vault to audit

4. Select `Access configuration`
5. Set the Permission model radio button to `Azure role-based access control`, taking note of the warning message
6. Click `Save`
7. Select `Access Control (IAM)`
8. Select the `Role Assignments` tab
9. Reapply permissions as needed to groups or users

**Default Value:**

The default value for Access control in Key Vaults is Vault Policy.

**References:**

1. <https://docs.microsoft.com/en-gb/azure/key-vault/general/rbac-migration#vault-access-policy-to-azure-rbac-migration-steps>
2. <https://docs.microsoft.com/en-gb/azure/role-based-access-control/role-assignments-portal?tabs=current>
3. <https://docs.microsoft.com/en-gb/azure/role-based-access-control/overview>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-8-ensure-security-of-key-and-certificate-repository>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.	●	●	●
v8	<b>6.8 <u>Define and Maintain Role-Based Access Control</u></b> Define and maintain role-based access control, through determining and documenting the access rights necessary for each role within the enterprise to successfully carry out its assigned duties. Perform access control reviews of enterprise assets to validate that all privileges are authorized, on a recurring schedule at a minimum annually, or more frequently.			●
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.	●	●	●

## 8.7 Ensure that Private Endpoints are Used for Azure Key Vault (Manual)

### Profile Applicability:

- Level 2

### Description:

Private endpoints will secure network traffic from Azure Key Vault to the resources requesting secrets and keys.

### Rationale:

Private endpoints will keep network requests to Azure Key Vault limited to the endpoints attached to the resources that are whitelisted to communicate with each other. Assigning the Key Vault to a network without an endpoint will allow other resources on that network to view all traffic from the Key Vault to its destination. In spite of the complexity in configuration, this is recommended for high security secrets.

### Impact:

Incorrect or poorly-timed changing of network configuration could result in service interruption. There are also additional costs tiers for running a private endpoint per petabyte or more of networking traffic.

### Audit:

#### From Azure Portal

1. From Azure Home open the Portal Menu in the top left.
2. Select Key Vaults.
3. Select a Key Vault to audit.
4. Select `Networking` in the left column.
5. Select `Private endpoint connections` from the top row.
6. View if there is an endpoint attached.

#### From Azure CLI

Run the following command within a subscription for each Key Vault you wish to audit.

```
az keyvault private-endpoint-connection show -g <resourceGroup> --vault-name <keyVaultName>
```

## From Powershell

Run the following command within a subscription for each Key Vault you wish to audit.

```
Get-AzPrivateEndpointConnection -PrivateLinkResourceId  
'/subscriptions/<subscriptionNumber>/resourceGroups/<resourceGroup>/providers  
/Microsoft.KeyVault/vaults/<keyVaultName>/'
```

## Remediation:

**Please see the additional information about the requirements needed before starting this remediation procedure.**

### From Azure Portal

1. From Azure Home open the Portal Menu in the top left.
2. Select Key Vaults.
3. Select a Key Vault to audit.
4. Select `Networking` in the left column.
5. Select `Private endpoint connections` from the top row.
6. Select `+ Create`.
7. Select the subscription the Key Vault is within, and other desired configuration.
8. Select `Next`.
9. For resource type select `Microsoft.KeyVault/vaults`.
10. Select the Key Vault to associate the Private Endpoint with.
11. Select `Next`.
12. In the `Virtual Networking` field, select the network to assign the Endpoint.
13. Select other configuration options as desired, including an existing or new application security group.
14. Select `Next`.
15. Select the private DNS the Private Endpoints will use.
16. Select `Next`.
17. Optionally add `Tags`.
18. Select `Next : Review + Create`.
19. Review the information and select `Create`. Follow the Audit Procedure to determine if it has successfully applied.
20. Repeat steps 3-19 for each Key Vault.



## From Azure CLI

1. To create an endpoint, run the following command:

```
az network private-endpoint create --resource-group <resourceGroup> --vnet-name <vnetName> --subnet <subnetName> --name <PrivateEndpointName> --private-connection-resource-id "/subscriptions/<AZURE SUBSCRIPTION ID>/resourceGroups/<resourceGroup>/providers/Microsoft.KeyVault/vaults/<keyVaultName>" --group-ids vault --connection-name <privateLinkConnectionName> --location <azureRegion> --manual-request
```

2. To manually approve the endpoint request, run the following command:

```
az keyvault private-endpoint-connection approve --resource-group <resourceGroup> --vault-name <keyVaultName> -name <privateLinkName>
```

4. Determine the Private Endpoint's IP address to connect the Key Vault to the Private DNS you have previously created:
5. Look for the property `networkInterfaces` then `id`; the value must be placed in the variable `<privateEndpointNIC>` within step 7.

```
az network private-endpoint show -g <resourceGroupName> -n <privateEndpointName>
```

6. Look for the property `networkInterfaces` then `id`; the value must be placed on `<privateEndpointNIC>` in step 7.

```
az network nic show --ids <privateEndpointName>
```

7. Create a Private DNS record within the DNS Zone you created for the Private Endpoint:

```
az network private-dns record-set a add-record -g <resourceGroup> -z "privatelink.vaultcore.azure.net" -n <keyVaultName> -a <privateEndpointNIC>
```

8. `nslookup` the private endpoint to determine if the DNS record is correct:

```
nslookup <keyVaultName>.vault.azure.net  
nslookup <keyVaultName>.privatelink.vaultcore.azure.net
```

### Default Value:

By default, Private Endpoints are not enabled for any services within Azure.

## References:

1. <https://docs.microsoft.com/en-us/azure/private-link/private-endpoint-overview>
2. <https://docs.microsoft.com/en-us/azure/storage/common/storage-private-endpoints>
3. <https://azure.microsoft.com/en-us/pricing/details/private-link/>
4. <https://docs.microsoft.com/en-us/azure/key-vault/general/private-link-service?tabs=portal>
5. <https://docs.microsoft.com/en-us/azure/virtual-network/quick-create-portal>
6. <https://docs.microsoft.com/en-us/azure/private-link/tutorial-private-endpoint-storage-portal>
7. <https://docs.microsoft.com/en-us/azure/bastion/bastion-overview>
8. <https://docs.microsoft.com/azure/dns/private-dns-getstarted-cli#create-an-additional-dns-record>
9. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-8-ensure-security-of-key-and-certificate-repository>

## Additional Information:

This recommendation assumes that you have created a Resource Group containing a Virtual Network that the services are already associated with and configured private DNS. A Bastion on the virtual network is also required, and the service to which you are connecting must already have a Private Endpoint. For information concerning the installation of these services, please see the attached documentation.

Microsoft's own documentation lists the requirements as: A Key Vault. An Azure virtual network. A subnet in the virtual network. Owner or contributor permissions for both the Key Vault and the virtual network.

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>12.2 Establish and Maintain a Secure Network Architecture</b> Establish and maintain a secure network architecture. A secure network architecture must address segmentation, least privilege, and availability, at a minimum.		●	●
v7	<b>14.1 Segment the Network Based on Sensitivity</b> Segment the network based on the label or classification level of the information stored on the servers, locate all sensitive information on separated Virtual Local Area Networks (VLANs).		●	●

## 8.8 Ensure Automatic Key Rotation is Enabled Within Azure Key Vault for the Supported Services (Manual)

### Profile Applicability:

- Level 2

### Description:

Automatic Key Rotation is available in Public Preview. The currently supported applications are Key Vault, Managed Disks, and Storage accounts accessing keys within Key Vault. The number of supported applications will incrementally increased.

### Rationale:

Once set up, Automatic Private Key Rotation removes the need for manual administration when keys expire at intervals determined by your organization's policy. The recommended key lifetime is 2 years. Your organization should determine its own key expiration policy.

### Impact:

There are an additional costs per operation in running the needed applications.

### Audit:

#### From Azure Portal

1. From Azure Portal select the Portal Menu in the top left.
2. Select Key Vaults.
3. Select a Key Vault to audit.
4. Under `Objects` select `Keys`.
5. Select a key to audit.
6. In the top row select `Rotation policy`.
7. Ensure `Enable auto rotation` is set to `Enabled`.
8. Repeat steps 3-7 for each Key Vault and Key.

#### From Azure CLI

Run the following command:

```
az keyvault key rotation-policy show --vaultname <vaultName> --name <keyName>
```

## From PowerShell

Run the following command:

```
Get-AzKeyVaultKeyRotationPolicy -VaultName <vaultName> -Name <keyName>
```

## Remediation:

### Note:

Azure CLI and Powershell use ISO8601 flags to input timespans. Every timespan input will be in the format P<timespanInISO8601Format>(Y,M,D). The leading P is required with it denoting *period*. The (Y,M,D) are for the duration of Year, Month, and Day respectively. A time frame of 2 years, 2 months, 2 days would be (P2Y2M2D).

### From Azure Portal

1. From Azure Portal select the Portal Menu in the top left.
2. Select Key Vaults.
3. Select a Key Vault to audit.
4. Under *Objects* select *Keys*.
5. Select a key to audit.
6. In the top row select *Rotation policy*.
7. Select an *Expiry time*.
8. Set *Enable auto rotation* to *Enabled*.
9. Set an appropriate *Rotation option* and *Rotation time*.
10. Optionally set the *Notification time*.
11. Select *Save*.
12. Repeat steps 3-11 for each Key Vault and Key.

## From Azure CLI

Run the following command for each key to update its policy to be auto-rotated:

```
az keyvault key rotation-policy update -n <keyName> --vault-name <vaultName>
--value <path/to/policy.json>
```

Note: It is easiest to supply the policy flags in a .json file. An example json file would be:

```
{
  "lifetimeActions": [
    {
      "trigger": {
        "timeAfterCreate": "<timespanInISO8601Format>",
        "timeBeforeExpiry" : null
      },
      "action": {
        "type": "Rotate"
      }
    },
    {
      "trigger": {
        "timeBeforeExpiry" : "<timespanInISO8601Format>"
      },
      "action": {
        "type": "Notify"
      }
    }
  ],
  "attributes": {
    "expiryTime": "<timespanInISO8601Format>"
  }
}
```

## From PowerShell

Run the following command for each key to update its policy:

```
Set-AzKeyVaultKeyRotationPolicy -VaultName test-kv -Name test-key -PolicyPath rotation_policy.json
```

Note: It is easiest to supply the policy flags in a .json file. An example json file would be:

```
<#
rotation_policy.json
{
  "lifetimeActions": [
    {
      "trigger": {
        "timeAfterCreate": "P<timespanInISO8601Format>M",
        "timeBeforeExpiry": null
      },
      "action": {
        "type": "Rotate"
      }
    },
    {
      "trigger": {
        "timeBeforeExpiry": "P<timespanInISO8601Format>D"
      },
      "action": {
        "type": "Notify"
      }
    }
  ],
  "attributes": {
    "expiryTime": "P<timespanInISO8601Format>Y"
  }
}
#>
```

## Default Value:

By default, Automatic Key Rotation is not enabled.

## References:

1. <https://docs.microsoft.com/en-us/azure/key-vault/keys/how-to-configure-key-rotation>
2. <https://docs.microsoft.com/en-us/azure/storage/common/customer-managed-keys-overview#update-the-key-version>
3. <https://docs.microsoft.com/en-us/azure/virtual-machines/windows/disks-enable-customer-managed-keys-powershell#set-up-an-azure-key-vault-and-diskencryptionset-optional-with-automatic-key-rotation>
4. <https://azure.microsoft.com/en-us/updates/public-preview-automatic-key-rotation-of-customermanaged-keys-for-encrypting-azure-managed-disks/>
5. <https://docs.microsoft.com/en-us/cli/azure/keyvault/key/rotation-policy?view=azure-cli-latest#az-keyvault-key-rotation-policy-update>

6. <https://docs.microsoft.com/en-us/powershell/module/az.keyvault/set-azkeyvaultkeyrotationpolicy?view=azps-8.1.0>
7. <https://docs.microsoft.com/en-us/azure/data-explorer/kusto/query/scalar-data-types/timespan>
8. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-6-use-a-secure-key-management-process>

**Additional Information:**

Automatic Key Rotation is in public preview, so any configuration will not change upon full release.

**\*\*Note:** \*\* Azure CLI and Powershell use ISO8601 flags to input timespans. Every timespan input will be in the format P<timespanInISO8601Format>(Y,M,D). The leading P is required with it denoting *period*. The (Y,M,D) are for the duration of Year, Month, Day respectively. A time frame of 2 years, 2 months, 2 days would be (P2Y2M2D).

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>3.1 Establish and Maintain a Data Management Process</b>            Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.</p>	●	●	●
v8	<p><b>6.2 Establish an Access Revoking Process</b>            Establish and follow a process, preferably automated, for revoking access to enterprise assets, through disabling accounts immediately upon termination, rights revocation, or role change of a user. Disabling accounts, instead of deleting accounts, may be necessary to preserve audit trails.</p>	●	●	●
v7	<p><b>16.7 Establish Process for Revoking Access</b>            Establish and follow an automated process for revoking system access by disabling accounts immediately upon termination or change of responsibilities of an employee or contractor . Disabling these accounts, instead of deleting accounts, allows preservation of audit trails.</p>		●	●

## 9 AppService

This section covers security recommendations for Azure AppService.

DRAFT



## 9.1 Ensure App Service Authentication is set up for apps in Azure App Service (Automated)

### Profile Applicability:

- Level 2

### Description:

Azure App Service Authentication is a feature that can prevent anonymous HTTP requests from reaching a Web Application or authenticate those with tokens before they reach the app. If an anonymous request is received from a browser, App Service will redirect to a logon page. To handle the logon process, a choice from a set of identity providers can be made, or a custom authentication mechanism can be implemented.

### Rationale:

By Enabling App Service Authentication, every incoming HTTP request passes through it before being handled by the application code. It also handles authentication of users with the specified provider (Azure Active Directory, Facebook, Google, Microsoft Account, and Twitter), validation, storing and refreshing of tokens, managing the authenticated sessions and injecting identity information into request headers.

### Impact:

This is only required for App Services which require authentication. Enabling on site like a marketing or support website will prevent unauthenticated access which would be undesirable.

Adding Authentication requirement will increase cost of App Service and require additional security components to facilitate the authentication.

### Audit:

#### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to App Services
3. Click on each App
4. Under Setting section, Click on Authentication
5. Ensure that App Service authentication set to Enabled (Will only appear once an Identity provider is set up/selected)

## From Azure CLI

To check App Service Authentication status for an existing app, run the following command,

```
az webapp auth show --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME>
--query enabled
```

The output should return `true` if App Service authentication is set to `On`.

## Remediation:

### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to App Services
3. Click on each App
4. Under Setting section, click on Authentication
5. If no identity providers are set up, then click Add identity provider
6. Choose other parameters as per your requirements and click on Add

## From Azure CLI

To set App Service Authentication for an existing app, run the following command:

```
az webapp auth update --resource-group <RESOURCE_GROUP_NAME> --name
<APP_NAME> --enabled true
```

## Note

In order to access App Service authentication settings for Web app using Microsoft API requires Website contributor permission at subscription level. A custom role can be created in place of Website contributor to provide more specific permission and maintain the principle of least privileged access.

## Default Value:

By default, App Service Authentication is disabled when a new app is created using the command-line tool or Azure Portal console.







## References:

1. <https://docs.microsoft.com/en-us/azure/app-service/app-service-authentication-overview>
2. <https://docs.microsoft.com/en-us/azure/role-based-access-control/built-in-roles#website-contributor>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-privileged-access#pa-5-automate-entitlement-management>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-governance-strategy#gs-6-define-identity-and-privileged-access-strategy>

### Additional Information:

You're not required to use App Service for authentication and authorization. Many web frameworks are bundled with security features, and you can use them if you like. If you need more flexibility than App Service provides, you can also write your own utilities. Secure authentication and authorization require deep understanding of security, including federation, encryption, JSON web tokens (JWT) management, grant types, and so on.

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

## 9.2 Ensure Web App Redirects All HTTP traffic to HTTPS in Azure App Service (Automated)

### Profile Applicability:

- Level 1

### Description:

Azure Web Apps allows sites to run under both HTTP and HTTPS by default. Web apps can be accessed by anyone using non-secure HTTP links by default. Non-secure HTTP requests can be restricted and all HTTP requests redirected to the secure HTTPS port. It is recommended to enforce HTTPS-only traffic.

### Rationale:

Enabling HTTPS-only traffic will redirect all non-secure HTTP requests to HTTPS ports. HTTPS uses the TLS/SSL protocol to provide a secure connection which is both encrypted and authenticated. It is therefore important to support HTTPS for the security benefits.

### Impact:

When it is enabled, every incoming HTTP request is redirected to the HTTPS port. This means an extra level of security will be added to the HTTP requests made to the app.

### Audit:

#### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to App Services
3. Click on each App
4. Under Setting section, click on TLS/SSL settings
5. Under the Bindings pane, ensure that HTTPS Only set to On under Protocol Settings

#### From Azure CLI

To check HTTPS-only traffic value for an existing app, run the following command,

```
az webapp show --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME> --query httpsOnly
```

The output should return `true` if HTTPS-only traffic value is set to `On`.

#### From PowerShell

List all the web apps configured within the subscription.

```
Get-AzWebApp | Select-Object ResourceGroup, Name, HttpsOnly
```

For each web app review the `HttpsOnly` setting and make sure it is set to `True`.

## Remediation:

### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to App Services
3. Click on each App
4. Under Setting section, Click on TLS/SSL settings
5. Under the Bindings pane, set HTTPS Only to On under Protocol Settings section

### From Azure CLI

To set HTTPS-only traffic value for an existing app, run the following command:

```
az webapp update --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME> --set httpsOnly=true
```

### From PowerShell

```
Set-AzWebApp -ResourceGroupName <RESOURCE_GROUP_NAME> -Name <APP_NAME> -HttpsOnly $true
```

### Default Value:

By default, HTTPS-only feature will be disabled when a new app is created using the command-line tool or Azure Portal console.

### References:

1. <https://docs.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-custom-ssl#enforce-https>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-3-encrypt-sensitive-data-in-transit>
3. <https://docs.microsoft.com/en-us/powershell/module/az.websites/set-azwebapp?view=azps-8.1.0>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 <u>Encrypt Sensitive Data in Transit</u></b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	<b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b> Encrypt all sensitive information in transit.		●	●

## 9.3 Ensure Web App is using the latest version of TLS encryption (Automated)

### Profile Applicability:

- Level 1

### Description:

The TLS (Transport Layer Security) protocol secures transmission of data over the internet using standard encryption technology. Encryption should be set with the latest version of TLS. App service allows TLS 1.2 by default, which is the recommended TLS level by industry standards such as PCI DSS.

### Rationale:

App service currently allows the web app to set TLS versions 1.0, 1.1 and 1.2. It is highly recommended to use the latest TLS 1.2 version for web app secure connections.

### Audit:

#### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to App Services
3. Click on each App
4. Under Setting section, Click on TLS/SSL settings
5. Under the Bindings pane, ensure that Minimum TLS Version set to 1.2 under Protocol Settings

#### From Azure CLI

To check TLS Version for an existing app, run the following command,

```
az webapp config show --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME> --query minTlsVersion
```

The output should return 1.2 if TLS Version is set to 1.2 (Which is currently the latest version).

#### From PowerShell

List all web apps.

```
Get-AzWebApp
```

For each web app run the following command.

```
Get-AzWebApp -ResourceGroupName <RESOURCE_GROUP_NAME> -Name <APP_NAME> |Select-Object -ExpandProperty SiteConfig
```

Make sure the `minTlsVersion` is set to at least 1.2.

## Remediation:

### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to App Services
3. Click on each App
4. Under Setting section, Click on SSL settings
5. Under the Bindings pane, set Minimum TLS Version to 1.2 under Protocol Settings section

### From Azure CLI

To set TLS Version for an existing app, run the following command:

```
az webapp config set --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME> --min-tls-version 1.2
```

### From PowerShell

```
Set-AzWebApp -ResourceGroupName <RESOURCE_GROUP_NAME> -Name <APP_NAME> -MinTlsVersion 1.2
```

### Default Value:

By default, TLS Version feature will be set to 1.2 when a new app is created using the command-line tool or Azure Portal console.

### References:

1. <https://docs.microsoft.com/en-us/azure/app-service/app-service-web-tutorial-custom-ssl#enforce-tls-versions>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-3-encrypt-sensitive-data-in-transit>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-network-security#ns-8-detect-and-disable-insecure-services-and--protocols>
4. <https://docs.microsoft.com/en-us/powershell/module/az.websites/set-azwebapp?view=azps-8.1.0>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 <u>Encrypt Sensitive Data in Transit</u></b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	<b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b> Encrypt all sensitive information in transit.		●	●

## 9.4 Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On' (Automated)

### Profile Applicability:

- Level 2

### 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.

### Rationale:

The TLS mutual authentication technique in enterprise environments ensures the authenticity of clients to the server. If incoming client certificates are enabled, then only an authenticated client who has valid certificates can access the app.

### Impact:

Utilizing and maintaining client certificates will require additional work to obtain and manage replacement and key rotation.

### Audit:

#### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to App Services
3. Click on each App
4. Under the Settings section, Click on Configuration, then General settings
5. Ensure that the option Client certificate mode located under Incoming client certificates is set to Require

#### From Azure CLI

To check Incoming client certificates value for an existing app, run the following command,

```
az webapp show --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME> --query clientCertEnabled
```

The output should return `true` if Incoming client certificates value is set to `On`.

#### From PowerShell

List all web apps.

```
Get-AzWebApp
```

For each web app run the following command.

```
Get-AzWebApp -ResourceGroup <app resource group> -Name <app name>
```

Make sure the `ClientCertEnabled` is set to `True`.



## Remediation:

### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to App Services
3. Click on each App
4. Under the Settings section, Click on Configuration, then General settings
5. Set the option Client certificate mode located under Incoming client certificates to Require

### From Azure CLI

To set Incoming client certificates value for an existing app, run the following command:

```
az webapp update --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME> --set clientCertEnabled=true
```







### Default Value:

By default, incoming client certificates will be disabled when a new app is created using the command-line tool or Azure Portal console.

### References:

1. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-4-authenticate-server-and-services>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

## 9.5 Ensure that Register with Azure Active Directory is enabled on App Service (Automated)

### Profile Applicability:

- Level 1

### Description:

Managed service identity in App Service provides more security by eliminating secrets from the app, such as credentials in the connection strings. When registering with Azure Active Directory in App Service, the app will connect to other Azure services securely without the need for usernames and passwords.

### Rationale:

App Service provides a highly scalable, self-patching web hosting service in Azure. It also provides a managed identity for apps, which is a turn-key solution for securing access to Azure SQL Database and other Azure services.

### Audit:

#### From Azure Portal

1. From Azure Portal open the Portal Menu in the top left
2. Go to App Services
3. Click on each App
4. Under the `Setting` section, Click on `Identity`
5. Under the `System assigned` pane, ensure that `Status` set to `On`

#### From Azure CLI

To check Register with Azure Active Directory feature status for an existing app, run the following command,

```
az webapp identity show --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME> --query principalId
```

The output should return unique Principal ID.

If no output for the above command then Register with Azure Active Directory is not set.

#### From PowerShell

List the web apps.

```
Get-AzWebApp
```

For each web app run the following command.

```
Get-AzWebapp -ResourceGroupName <app resource group> -Name <app name>
```

Make sure the `Identity` setting contains a unique Principal ID

## Remediation:

### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to App Services
3. Click on each App
4. Under Setting section, Click on Identity
5. Under the System assigned pane, set Status to On

### From Azure CLI

To set Register with Azure Active Directory feature for an existing app, run the following command:

```
az webapp identity assign --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME>
```

### From PowerShell

To register with Azure Active Directory feature for an existing app, run the following command:

```
Set-AzWebApp -AssignIdentity $True -ResourceGroupName <resource_Group_Name> -Name <App_Name>
```

### Default Value:

By default, Managed service identity via Azure AD is disabled.

### References:

1. <https://docs.microsoft.com/en-gb/azure/app-service/app-service-web-tutorial-connect-msi>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-1-use-centralized-identity-and-authentication-system>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>5.6 Centralize Account Management</b> Centralize account management through a directory or identity service.		●	●
v7	<b>16.2 Configure Centralized Point of Authentication</b> Configure access for all accounts through as few centralized points of authentication as possible, including network, security, and cloud systems.		●	●

## 9.6 Ensure That 'PHP version' is the Latest, If Used to Run the Web App (Manual)

### Profile Applicability:

- Level 1

### Description:

Periodically newer versions are released for PHP software either due to security flaws or to include additional functionality. Using the latest PHP version for web apps is recommended in order to take advantage of security fixes, if any, and/or additional functionalities of the newer version.

### Rationale:

Newer versions may contain security enhancements and additional functionality. Using the latest software version is recommended in order to take advantage of enhancements and new capabilities. With each software installation, organizations need to determine if a given update meets their requirements. They must also verify the compatibility and support provided for any additional software against the update revision that is selected.

### Impact:

If your app is written using version-dependent features or libraries, they may not be available on the latest version. If you wish to upgrade, research the impact thoroughly. Upgrading may have unforeseen consequences that could result in downtime.

### Audit:

#### From Azure Portal

1. From Azure Home open the Portal Menu in the top left
2. Go to `App Services`
3. Click on each App
4. Under `Settings` section, click on `Configuration`
5. Click on the `General settings` pane, ensure that for a `Stack of PHP` the `Major Version` and `Minor Version` reflect the latest stable and supported release.

\*\* The latest stable version can be confirmed by going to `php.net`. Navigate to the downloads, and then find the most recent version that is marked by `Current Stable PHP [version_number]`. \*\*

**NOTE:** No action is required if `PHP version` is set to `Off` as PHP is not used by your web app.

## From Azure CLI

To check PHP version for an existing app, run the following command,

```
az webapp config show --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME> --query "{LinuxFxVersion:linuxFxVersion,PHP_Version:phpVersion}"
```

## From PowerShell

```
$application = Get-AzWebApp -ResourceGroupName <resource group name> -Name <app name>  
$application.SiteConfig | select-object LinuxFXVersion, phpVersion
```

The output should return the latest available version of PHP. Any other version of PHP would be considered a finding.

**NOTE:** No action is required, If the output is empty as PHP is not used by your web app.

## Remediation:

### From Azure Portal

1. From Azure Home open the Portal Menu in the top left
2. Go to App Services
3. Click on each App
4. Under Settings section, click on Configuration
5. Click on the General settings pane, ensure that for a Stack of PHP the Major Version and Minor Version reflect the latest stable and supported release.

**NOTE:** No action is required If PHP version is set to Off or is set with an empty value as PHP is not used by your web app.

## From Azure CLI

List the available PHP runtimes:

```
az webapp list-runtimes
```

To set latest PHP version for an existing app, run the following command:

```
az webapp config set --resource-group <resource group name> --name <app name> [--linux-fx-version <php runtime version>][--php-version <php version>]
```

## From PowerShell

To set latest PHP version for an existing app, run the following command:

```
Set-AzWebApp -ResourceGroupName <resource group name> -Name <app name> -phpVersion <php version>
```

**NOTE:** Currently there is no way to update an existing web app Linux FX Version setting using PowerShell, nor is there a way to create a new web app using PowerShell that configures the PHP runtime in the Linux FX Version setting.







## Default Value:

The version of PHP is whatever was selected upon App creation.

## References:

1. <https://docs.microsoft.com/en-us/azure/app-service/web-sites-configure#general-settings>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-3-establish-secure-configurations-for-compute-resources>
4. <https://www.php.net/downloads>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>2.2 <u>Ensure Authorized Software is Currently Supported</u></b> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			
v7	<b>2.2 <u>Ensure Software is Supported by Vendor</u></b> Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.			

## 9.7 Ensure that 'Python version' is the Latest Stable Version, if Used to Run the Web App (Manual)

### Profile Applicability:

- Level 1

### Description:

Periodically, newer versions are released for Python software either due to security flaws or to include additional functionality. Using the latest full Python version for web apps is recommended in order to take advantage of security fixes, if any, and/or additional functionalities of the newer version.

### Rationale:

Newer versions may contain security enhancements and additional functionality. Using the latest software version is recommended in order to take advantage of enhancements and new capabilities. With each software installation, organizations need to determine if a given update meets their requirements. They must also verify the compatibility and support provided for any additional software against the update revision that is selected. Using the latest full version will keep your stack secure to vulnerabilities and exploits.

### Impact:

If your app is written using version-dependent features or libraries, they may not be available on the latest version. If you wish to upgrade, research the impact thoroughly. Upgrading may have unforeseen consequences that could result in downtime.

### Audit:

#### From Azure Console

1. From Azure Home open the Portal Menu in the top left
2. Go to `App Services`
3. Click on each App
4. Under `Settings` section, click on `Configuration`
5. Click on the General settings pane and ensure that for a Stack of Python, with Major Version of Python 3, that the Minor Version is set to the latest stable version available (Python 3.11, at the time of writing)

NOTE: No action is required if `Python version` is set to `Off`, as Python is not used by your web app.

## From Azure CLI

To check Python version for an existing app, run the following command

```
az webapp config show --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME> --query "{LinuxFxVersion:linuxFxVersion,WindowsFxVersion:windowsFxVersion,PythonVersion:pythonVersion}"
```

The output should return the latest stable version of Python.

**NOTE:** No action is required if the output is empty, as Python is not used by your web app.

## From PowerShell

```
$app = Get-AzWebApp -Name <app name> -ResourceGroup <resource group name>  
$app.SiteConfig |Select-Object LinuxFXVersion, WindowsFxVersion, PythonVersion
```

Ensure the output of the above command shows the latest version of Python.

**NOTE:** No action is required if the output is empty, as Python is not used by your web app.

## Remediation:

### From Azure Portal

1. From Azure Home open the Portal Menu in the top left
2. Go to App Services
3. Click on each App
4. Under Settings section, click on Configuration
5. Click on the General settings pane and ensure that the Major Version and the Minor Version is set to the latest stable version available (Python 3.11, at the time of writing)

**NOTE:** No action is required if Python version is set to Off, as Python is not used by your web app.

## From Azure CLI

To see the list of supported runtimes:

```
az webapp list-runtimes
```

To set latest Python version for an existing app, run the following command:

```
az webapp config set --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME> [--windows-fx-version "PYTHON|3.11"] [--linux-fx-version "PYTHON|3.11"]
```

## From PowerShell

As of this writing, there is no way to update an existing application's SiteConfig or set the a new application's SiteConfig settings during creation via PowerShell.



## Default Value:

The version of Python is whatever was selected upon App creation.







## References:

1. <https://docs.microsoft.com/en-us/azure/app-service/web-sites-configure#general-settings>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-3-establish-secure-configurations-for-compute-resources>
4. <https://www.python.org/downloads/>

## Additional Information:

\*\* The latest stable version can be confirmed by going to python.org. Navigate to the downloads, and then find the most recent version that is marked by `security` in the maintenance column. \*\*

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>2.2 <u>Ensure Authorized Software is Currently Supported</u></b> Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.			
v7	<b>2.2 <u>Ensure Software is Supported by Vendor</u></b> Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.			

## 9.8 Ensure that 'Java version' is the latest, if used to run the Web App (Manual)

### Profile Applicability:

- Level 1

### Description:

Periodically, newer versions are released for Java software either due to security flaws or to include additional functionality. Using the latest Java version for web apps is recommended in order to take advantage of security fixes, if any, and/or new functionalities of the newer version.

### Rationale:

Newer versions may contain security enhancements and additional functionality. Using the latest software version is recommended in order to take advantage of enhancements and new capabilities. With each software installation, organizations need to determine if a given update meets their requirements. They must also verify the compatibility and support provided for any additional software against the update revision that is selected.

### Impact:

If your app is written using version-dependent features or libraries, they may not be available on the latest version. If you wish to upgrade, research the impact thoroughly. Upgrading may have unforeseen consequences that could result in downtime.

### Audit:

#### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to App Services
3. Click on each App
4. Under Settings section, click on Configuration
5. Click on the General settings pane and ensure that for a Stack of Java the Major Version and Minor Version reflect the latest stable and supported release, and that the Java web server version is set to the auto-update option.

NOTE: No action is required if Java version is set to Off, as Java is not used by your web app.

## From Azure CLI

To check Java version for an existing app, run the following command,

```
az webapp config show --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME> --query "{LinuxFxVersion:linuxFxVersion, WindowsFxVersion:windowsFxVersion, JavaVersion:javaVersion, JavaContainerVersion:javaContainerVersion, JavaContainer:javaContainer}"
```

The output should return the latest available version of Java (if java is being used for the web application being audited).

## From PowerShell

For each application, store the application information within an object, and then interrogate the `SiteConfig` information for that application object.

```
$app = Get-AzWebApp -Name <app name> -ResourceGroup <resource group name>
$app.SiteConfig |Select-Object LinuxFXVersion, WindowsFxVersion, JavaVersion, JavaContainerVersion, JavaContainer
```

Ensure the Java version used within the application is a currently supported version (if java is being used for the web application being audited).

## Remediation:

### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to App Services
3. Click on each App
4. Under Settings section, click on Configuration
5. Click on the General settings pane and ensure that for a Stack of Java the Major Version and Minor Version reflect the latest stable and supported release, and that the Java web server version is set to the auto-update option.

NOTE: No action is required if Java version is set to Off, as Java is not used by your web app.

## From Azure CLI

To see the list of supported runtimes:

```
az webapp list-runtimes
```

To set latest Java version for an existing app, run the following command:

```
az webapp config set --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME> [--java-version <JAVA_VERSION> --java-container <JAVA_CONTAINER> --java-container-version <JAVA_CONTAINER_VERSION> [--windows-fx-version <java runtime version>] [--linux-fx-version <java runtime version version>]
```

If creating a new web application to use a currently supported version of Java, run the following commands.

To create an app service plan:

```
az appservice plan create --resource-group <resource group name> --name <plan name> --location <location> [--is-linux --number-of-workers <int> --sku <pricing tier>] [--hyper-v --sku <pricing tier>]
```

Get the app service plan ID:

```
az appservice plan list --query "[].{Name:name, ID:id, SKU:sku, Location:location}"
```

To create a new Java web application using the retrieved app service ID:

```
az webapp create --resource-group <resource group name> --plan <app service plan ID> --name <app name> [--linux-fx-version <java run time version>] [--windows-fx-version <java run time version>]
```

### From PowerShell

As of this writing, there is no way to update an existing application's `SiteConfig` or set a new application's `SiteConfig` settings during creation via PowerShell.

### Default Value:

The default setting is whichever setting was chosen in the creation of the webapp.

### References:

1. <https://docs.microsoft.com/en-us/azure/app-service/web-sites-configure#general-settings>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-3-establish-secure-configurations-for-compute-resources>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-3-establish-secure-configurations-for-compute-resources>
4. <https://www.oracle.com/java/technologies/downloads/#java11>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>2.2 <u>Ensure Authorized Software is Currently Supported</u></b>            Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.</p>	●	●	●
v7	<p><b>2.2 <u>Ensure Software is Supported by Vendor</u></b>            Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.</p>	●	●	●

DRAFT

## 9.9 Ensure that 'HTTP Version' is the Latest, if Used to Run the Web App (Automated)

### Profile Applicability:

- Level 1

### Description:

Periodically, newer versions are released for HTTP either due to security flaws or to include additional functionality. Using the latest HTTP version for web apps to take advantage of security fixes, if any, and/or new functionalities of the newer version.

### Rationale:

Newer versions may contain security enhancements and additional functionality. Using the latest version is recommended in order to take advantage of enhancements and new capabilities. With each software installation, organizations need to determine if a given update meets their requirements. They must also verify the compatibility and support provided for any additional software against the update revision that is selected.

HTTP 2.0 has additional performance improvements on the head-of-line blocking problem of old HTTP version, header compression, and prioritization of requests. HTTP 2.0 no longer supports HTTP 1.1's chunked transfer encoding mechanism, as it provides its own, more efficient, mechanisms for data streaming.

### Audit:

#### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to App Services
3. Click on each App
4. Under Setting section, Click on Configuration
5. Ensure that HTTP Version set to 2.0 version under General settings

NOTE: Most modern browsers support HTTP 2.0 protocol over TLS only, while non-encrypted traffic continues to use HTTP 1.1. To ensure that client browsers connect to your app with HTTP/2, either buy an App Service Certificate for your app's custom domain or bind a third party certificate.

#### From Azure CLI

To check HTTP 2.0 version status for an existing app, run the following command,

```
az webapp config show --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME> --query http20Enabled
```

The output should return `true` if HTTPS 2.0 traffic value is set to `On`.

## From PowerShell

For each application, run the following command:

```
Get-AzWebApp -ResourceGroupName <app resource group> -Name <app name>
|Select-Object -ExpandProperty SiteConfig
```

If the value of the **Http20Enabled** setting is **true**, the application is compliant. Otherwise if the value of the **Http20Enabled** setting is **false**, the application is non-compliant.

## Remediation:

### From Azure Portal

1. Login to Azure Portal using <https://portal.azure.com>
2. Go to App Services
3. Click on each App
4. Under Setting section, Click on Configuration
5. Set HTTP version to 2.0 under General settings

NOTE: Most modern browsers support HTTP 2.0 protocol over TLS only, while non-encrypted traffic continues to use HTTP 1.1. To ensure that client browsers connect to your app with HTTP/2, either buy an App Service Certificate for your app's custom domain or bind a third party certificate.

### From Azure CLI

To set HTTP 2.0 version for an existing app, run the following command:

```
az webapp config set --resource-group <RESOURCE_GROUP_NAME> --name <APP_NAME>
--http20-enabled true
```

### From PowerShell

To enable HTTP 2.0 version support, run the following command:

```
Set-AzWebApp -ResourceGroupName <app resource group> -Name <app name> -
Http20Enabled $true
```

## References:

1. <https://docs.microsoft.com/en-us/azure/app-service/web-sites-configure#general-settings>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities>
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-3-establish-secure-configurations-for-compute-resources>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<p><b>2.2 <u>Ensure Authorized Software is Currently Supported</u></b>            Ensure that only currently supported software is designated as authorized in the software inventory for enterprise assets. If software is unsupported, yet necessary for the fulfillment of the enterprise's mission, document an exception detailing mitigating controls and residual risk acceptance. For any unsupported software without an exception documentation, designate as unauthorized. Review the software list to verify software support at least monthly, or more frequently.</p>	●	●	●
v7	<p><b>2.2 <u>Ensure Software is Supported by Vendor</u></b>            Ensure that only software applications or operating systems currently supported by the software's vendor are added to the organization's authorized software inventory. Unsupported software should be tagged as unsupported in the inventory system.</p>	●	●	●

DRAFT



## 9.10 Ensure FTP deployments are Disabled (Automated)

### Profile Applicability:

- Level 1

### Description:

By default, Azure Functions, Web, and API Services can be deployed over FTP. If FTP is required for an essential deployment workflow, FTPS should be required for FTP login for all App Service Apps and Functions.

### Rationale:

Azure FTP deployment endpoints are public. An attacker listening to traffic on a wifi network used by a remote employee or a corporate network could see login traffic in clear-text which would then grant them full control of the code base of the app or service. This finding is more severe if User Credentials for deployment are set at the subscription level rather than using the default Application Credentials which are unique per App.

### Impact:

Any deployment workflows that rely on FTP or FTPs rather than the WebDeploy or HTTPs endpoints may be affected.

### Audit:

#### From Azure Portal

1. Go to the Azure Portal
2. Select App Services
3. Click on an app
4. Select Settings and then Configuration
5. Under General Settings, for the Platform Settings, the FTP state should not be set to All allowed

#### From Azure CLI

List webapps to obtain the ids.

```
az webapp list
```

List the publish profiles to obtain the username, password and ftp server url.

```
az webapp deployment list-publishing-profiles --ids <ids>
{
  "publishUrl": <URL_FOR_WEB_APP>,
  "userName": <USER_NAME>,
  "userPWD": <USER_PASSWORD>,
}
```

## From PowerShell

List all Web Apps:

```
Get-AzWebApp
```

For each app:

```
Get-AzWebApp -ResourceGroupName <resource group name> -Name <app name> |  
Select-Object -ExpandProperty SiteConfig
```

In the output, look for the value of **FtpsState**. If its value is **AllAllowed** the setting is out of compliance. Any other value is considered in compliance with this check.

## Remediation:

### From Azure Portal

1. Go to the Azure Portal
2. Select App Services
3. Click on an app
4. Select Settings and then Configuration
5. Under General Settings, for the Platform Settings, the FTP state should be set to Disabled or FTPS Only

### From Azure CLI

For each out of compliance application, run the following choosing either 'disabled' or 'FtpsOnly' as appropriate:

```
az webapp config set --resource-group <resource group name> --name <app name> --ftps-state [disabled|FtpsOnly]
```

### From PowerShell

For each out of compliance application, run the following:

```
Set-AzWebApp -ResourceGroupName <resource group name> -Name <app name> -  
FtpsState <Disabled or FtpsOnly>
```

## Default Value:

By default, FTP based deployment is All allowed

## References:

1. [Azure Web Service Deploy via FTP](<https://docs.microsoft.com/en-us/azure/app-service/deploy-ftp>)
2. [Azure Web Service Deployment](<https://docs.microsoft.com/en-us/azure/app-service/overview-security>)
3. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-data-protection#dp-4-encrypt-sensitive-information-in-transit>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-posture-vulnerability-management#pv-7-rapidly-and-automatically-remediate-software-vulnerabilities>

**CIS Controls:**

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.10 <u>Encrypt Sensitive Data in Transit</u></b> Encrypt sensitive data in transit. Example implementations can include: Transport Layer Security (TLS) and Open Secure Shell (OpenSSH).		●	●
v7	<b>14.4 <u>Encrypt All Sensitive Information in Transit</u></b> Encrypt all sensitive information in transit.		●	●
v7	<b>16.5 <u>Encrypt Transmittal of Username and Authentication Credentials</u></b> Ensure that all account usernames and authentication credentials are transmitted across networks using encrypted channels.		●	●

DRAFT

## 9.11 Ensure Azure Key Vaults are Used to Store Secrets (Manual)

### Profile Applicability:

- Level 2

### Description:

Azure Key Vault will store multiple types of sensitive information such as encryption keys, certificate thumbprints, and Managed Identity Credentials. Access to these 'Secrets' can be controlled through granular permissions.

### Rationale:

The credentials given to an application have permissions to create, delete, or modify data stored within the systems they access. If these credentials are stored within the application itself, anyone with access to the application or a copy of the code has access to them. Storing within Azure Key Vault as secrets increases security by controlling access. This also allows for updates of the credentials without redeploying the entire application.

### Impact:

Integrating references to secrets within the key vault are required to be specifically integrated within the application code. This will require additional configuration to be made during the writing of an application, or refactoring of an already written one. There are also additional costs that are charged per 10000 requests to the Key Vault.

### Audit:

#### From Azure Portal

1. Login to Azure Portal
2. In the expandable menu on the left go to `Key Vaults`
3. View the Key Vaults listed.

#### From Azure CLI

To list key vaults within a subscription run the following command:

```
Get-AzKeyVault
```

To list the secrets within these key vaults run the following command:

```
Get-AzKeyVaultSecret [-VaultName] <vault name>
```

## From Powershell

To list key vaults within a subscription run the following command:

```
Get-AzKeyVault
```

To list all secrets in a key vault run the following command:

```
Get-AzKeyVaultSecret -VaultName '<vaultName>'
```

## Remediation:

Remediation has 2 steps

1. Setup the Key Vault
2. Setup the App Service to use the Key Vault

## Step 1: Set up the Key Vault

### From Azure CLI

```
az keyvault create --name "<name>" --resource-group "<myResourceGroup>" --  
location myLocation
```

### From Powershell

```
New-AzKeyvault -name <name> -ResourceGroupName <myResourceGroup> -Location  
<myLocation>
```

## Step 2: Set up the App Service to use the Key Vault

Sample JSON Template for App Service Configuration:

```

{
  //...
  "resources": [
    {
      "type": "Microsoft.Storage/storageAccounts",
      "name": "[variables('storageAccountName')]",
      //...
    },
    {
      "type": "Microsoft.Insights/components",
      "name": "[variables('appInsightsName')]",
      //...
    },
    {
      "type": "Microsoft.Web/sites",
      "name": "[variables('functionAppName')]",
      "identity": {
        "type": "SystemAssigned"
      },
      //...
      "resources": [
        {
          "type": "config",
          "name": "appsettings",
          //...
          "dependsOn": [
            "[resourceId('Microsoft.Web/sites',
variables('functionAppName'))]",
            "[resourceId('Microsoft.KeyVault/vaults/',
variables('keyVaultName'))]",
            "[resourceId('Microsoft.KeyVault/vaults/secrets',
variables('keyVaultName'), variables('storageConnectionStringName'))]",
            "[resourceId('Microsoft.KeyVault/vaults/secrets',
variables('keyVaultName'), variables('appInsightsKeyName'))]"
          ],
          "properties": {
            "AzureWebJobsStorage":
"[concat('@Microsoft.KeyVault(SecretUri=',
reference(variables('storageConnectionStringResourceId')).secretUriWithVersio
n, '))]",
            "WEBSITE_CONTENTAZUREFILECONNECTIONSTRING":
"[concat('@Microsoft.KeyVault(SecretUri=',
reference(variables('storageConnectionStringResourceId')).secretUriWithVersio
n, '))]",
            "APPINSIGHTS_INSTRUMENTATIONKEY":
"[concat('@Microsoft.KeyVault(SecretUri=',
reference(variables('appInsightsKeyResourceId')).secretUriWithVersion,
''))]",
            "WEBSITE_ENABLE_SYNC_UPDATE_SITE": "true"
          //...
          }
        },
        {
          "type": "sourcecontrols",
          "name": "web",
          //...
          "dependsOn": [

```

```

        "[resourceId('Microsoft.Web/sites',
variables('functionAppName'))]",
        "[resourceId('Microsoft.Web/sites/config',
variables('functionAppName'), 'appsettings')]"
    ],
    }
]
},
{
    "type": "Microsoft.KeyVault/vaults",
    "name": "[variables('keyVaultName')]",
    //...
    "dependsOn": [
        "[resourceId('Microsoft.Web/sites',
variables('functionAppName'))]"
    ],
    "properties": {
        //...
        "accessPolicies": [
            {
                "tenantId":
"[reference(concat('Microsoft.Web/sites/', variables('functionAppName'),
'/providers/Microsoft.ManagedIdentity/Identities/default'), '2015-08-31-
PREVIEW').tenantId]",
                "objectId":
"[reference(concat('Microsoft.Web/sites/', variables('functionAppName'),
'/providers/Microsoft.ManagedIdentity/Identities/default'), '2015-08-31-
PREVIEW').principalId]",
                "permissions": {
                    "secrets": [ "get" ]
                }
            }
        ]
    },
    "resources": [
        {
            "type": "secrets",
            "name": "[variables('storageConnectionStringName')]",
            //...
            "dependsOn": [
                "[resourceId('Microsoft.KeyVault/vaults/',
variables('keyVaultName'))]",
                "[resourceId('Microsoft.Storage/storageAccounts',
variables('storageAccountName'))]"
            ],
            "properties": {
                "value":
"[concat('DefaultEndpointsProtocol=https;AccountName=',
variables('storageAccountName'), ';AccountKey=',
listKeys(variables('storageAccountResourceId'),'2015-05-01-preview').key1)]"
            }
        },
        {
            "type": "secrets",
            "name": "[variables('appInsightsKeyName')]",
            //...
            "dependsOn": [

```

```

    "[resourceId('Microsoft.KeyVault/vaults/',
variables('keyVaultName'))]",
    "[resourceId('Microsoft.Insights/components',
variables('appInsightsName'))]"
  ],
  "properties": {
    "value":
"[reference(resourceId('microsoft.insights/components/',
variables('appInsightsName')), '2015-05-01').InstrumentationKey]"
  }
}
]
}
]
}

```

### Default Value:

By default, no Azure Key Vaults are created.

### References:

1. <https://docs.microsoft.com/en-us/azure/app-service/app-service-key-vault-references>
2. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-identity-management#im-2-manage-application-identities-securely-and-automatically>
3. <https://docs.microsoft.com/en-us/cli/azure/keyvault?view=azure-cli-latest>
4. <https://docs.microsoft.com/en-us/cli/azure/keyvault?view=azure-cli-latest>

### CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.1 Establish and Maintain a Data Management Process</b> Establish and maintain a data management process. In the process, address data sensitivity, data owner, handling of data, data retention limits, and disposal requirements, based on sensitivity and retention standards for the enterprise. Review and update documentation annually, or when significant enterprise changes occur that could impact this Safeguard.	●	●	●
v7	<b>13.1 Maintain an Inventory Sensitive Information</b> Maintain an inventory of all sensitive information stored, processed, or transmitted by the organization's technology systems, including those located onsite or at a remote service provider.	●	●	●



**10 Miscellaneous**

DRAFT

## 10.1 Ensure that Resource Locks are set for Mission-Critical Azure Resources (Manual)

### Profile Applicability:

- Level 2

### Description:

Resource Manager Locks provide a way for administrators to lock down Azure resources to prevent deletion of, or modifications to, a resource. These locks sit outside of the Role Based Access Controls (RBAC) hierarchy and, when applied, will place restrictions on the resource for all users. These locks are very useful when there is an important resource in a subscription that users should not be able to delete or change. Locks can help prevent accidental and malicious changes or deletion.

### Rationale:

As an administrator, it may be necessary to lock a subscription, resource group, or resource to prevent other users in the organization from accidentally deleting or modifying critical resources. The lock level can be set to `CanNotDelete` or `ReadOnly` to achieve this purpose.

- `CanNotDelete` means authorized users can still read and modify a resource, but they cannot delete the resource.
- `ReadOnly` means authorized users can read a resource, but they cannot delete or update the resource. Applying this lock is similar to restricting all authorized users to the permissions granted by the Reader role.

### Impact:

There can be unintended outcomes of locking a resource. Applying a lock to a parent service will cause it to be inherited by all resources within. Conversely, applying a lock to a resource may not apply to connected storage, leaving it unlocked. Please see the documentation for further information.

### Audit:

#### From Azure Portal

1. Navigate to the specific Azure Resource or Resource Group
2. Click on `Locks`
3. Ensure the lock is defined with name and description, with type `Read-only` or `Delete` as appropriate.

## From Azure CLI

Review the list of all locks set currently:

```
az lock list --resource-group <resourcegroupname> --resource-name  
<resourcename> --namespace <Namespace> --resource-type <type> --parent ""
```

## From Powershell

Run the following command to list all resources.

```
Get-AzResource
```

For each resource, run the following command to check for Resource Locks.

```
Get-AzResourceLock -ResourceName <Resource Name> -ResourceType <Resource  
Type> -ResourceGroupName <Resource Group Name>
```

Review the output of the `Properties` setting. Compliant settings will have the `CanNotDelete` or `ReadOnly` value.

## Remediation:

### From Azure Portal

1. Navigate to the specific Azure Resource or Resource Group
2. For each mission critical resource, click on `Locks`
3. Click `Add`
4. Give the lock a name and a description, then select the type, `Read-only` or `Delete` as appropriate
5. Click `OK`

## From Azure CLI

To lock a resource, provide the name of the resource, its resource type, and its resource group name.

```
az lock create --name <LockName> --lock-type <CanNotDelete/Read-only> --  
resource-group <resourceGroupName> --resource-name <resourceName> --resource-  
type <resourceType>
```

## From Powershell

```
Get-AzResourceLock -ResourceName <Resource Name> -ResourceType <Resource  
Type> -ResourceGroupName <Resource Group Name> -Locktype <CanNotDelete/Read-  
only>
```







## Default Value:

By default, no locks are set.

## References:

1. <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-group-lock-resources>
2. <https://docs.microsoft.com/en-us/azure/azure-resource-manager/resource-manager-subscription-governance#azure-resource-locks>
3. <https://docs.microsoft.com/en-us/azure/governance/blueprints/concepts/resource-locking>
4. <https://docs.microsoft.com/en-us/security/benchmark/azure/security-controls-v3-asset-management#am-4-limit-access-to-asset-management>

## CIS Controls:

Controls Version	Control	IG 1	IG 2	IG 3
v8	<b>3.3 <u>Configure Data Access Control Lists</u></b> Configure data access control lists based on a user's need to know. Apply data access control lists, also known as access permissions, to local and remote file systems, databases, and applications.			
v7	<b>14.6 <u>Protect Information through Access Control Lists</u></b> Protect all information stored on systems with file system, network share, claims, application, or database specific access control lists. These controls will enforce the principle that only authorized individuals should have access to the information based on their need to access the information as a part of their responsibilities.			

# Appendix: Summary Table

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
<b>1</b>	<b>Identity and Access Management</b>		
<b>1.1</b>	<b>Security Defaults</b>		
1.1.1	Ensure Security Defaults is enabled on Azure Active Directory (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.2	Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Privileged Users (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.3	Ensure that 'Multi-Factor Auth Status' is 'Enabled' for all Non-Privileged Users (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.1.4	Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is Disabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>1.2</b>	<b>Conditional Access</b>		
1.2.1	Ensure Trusted Locations Are Defined (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.2	Ensure that an exclusionary Geographic Access Policy is considered (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.3	Ensure that A Multi-factor Authentication Policy Exists for Administrative Groups (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.4	Ensure that A Multi-factor Authentication Policy Exists for All Users (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.5	Ensure Multi-factor Authentication is Required for Risky Sign-ins (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.2.6	Ensure Multi-factor Authentication is Required for Azure Management (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.3	Ensure that 'Users can create Azure AD Tenants' is set to 'No' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.4	Ensure Access Review is Set Up for External Users in Azure AD Privileged Identity Management (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.5	Ensure Guest Users Are Reviewed on a Regular Basis (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.6	Ensure that 'Allow users to remember multi-factor authentication on devices they trust' is 'Disabled' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.7	Ensure That 'Number of methods required to reset' is set to '2' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.8	Ensure that a Custom Bad Password List is set to 'Enforce' for your Organization (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.9	Ensure that 'Number of days before users are asked to re-confirm their authentication information' is not set to '0' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.10	Ensure that 'Notify users on password resets?' is set to 'Yes' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.11	Ensure That 'Notify all admins when other admins reset their password?' is set to 'Yes' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.12	Ensure that 'Users can consent to apps accessing company data on their behalf' is set to 'No' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.13	Ensure That 'Users Can Consent to Apps Accessing Company Data on Their Behalf' Is Set To 'Allow for Verified Publishers' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.14	Ensure that 'Users can add gallery apps to My Apps' is set to 'No' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.15	Ensure That 'Users Can Register Applications' Is Set to 'No' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.16	Ensure That 'Guest users access restrictions' is set to 'Guest user access is restricted to properties and memberships of their own directory objects' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
1.17	Ensure that 'Guest invite restrictions' is set to "Only users assigned to specific admin roles can invite guest users" (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.18	Ensure That 'Restrict access to Azure AD administration portal' is Set to 'Yes' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.19	Ensure that 'Restrict user ability to access groups features in the Access Pane' is Set to 'Yes' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.20	Ensure that 'Users can create security groups in Azure portals, API or PowerShell' is set to 'No' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.21	Ensure that 'Owners can manage group membership requests in the Access Panel' is set to 'No' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.22	Ensure that 'Users can create Microsoft 365 groups in Azure portals, API or PowerShell' is set to 'No' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.23	Ensure that 'Require Multi-Factor Authentication to register or join devices with Azure AD' is set to 'Yes' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.24	Ensure That No Custom Subscription Administrator Roles Exist (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
1.25	Ensure a Custom Role is Assigned Permissions for Administering Resource Locks (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
1.26	Ensure That 'Subscription Entering AAD Directory' and 'Subscription Leaving AAD Directory' Is Set To 'Permit No One' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2</b>	<b>Microsoft Defender</b>		
<b>2.1</b>	<b>Microsoft Defender for Cloud</b>		
2.1.1	Ensure That Microsoft Defender for Servers Is Set to 'On' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.2	Ensure That Microsoft Defender for App Services Is Set To 'On' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.1.3	Ensure That Microsoft Defender for Databases Is Set To 'On' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.4	Ensure That Microsoft Defender for Azure SQL Databases Is Set To 'On' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.5	Ensure That Microsoft Defender for SQL Servers on Machines Is Set To 'On' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.6	Ensure That Microsoft Defender for Open-Source Relational Databases Is Set To 'On' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.7	Ensure That Microsoft Defender for Storage Is Set To 'On' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.8	Ensure That Microsoft Defender for Containers Is Set To 'On' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.9	Ensure That Microsoft Defender for Azure Cosmos DB Is Set To 'On' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.10	Ensure That Microsoft Defender for Key Vault Is Set To 'On' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.11	Ensure That Microsoft Defender for DNS Is Set To 'On' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.12	Ensure That Microsoft Defender for Resource Manager Is Set To 'On' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.13	Ensure that Microsoft Defender Recommendation for 'Apply system updates' status is 'Completed' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.14	Ensure Any of the ASC Default Policy Settings are Not Set to 'Disabled' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.15	Ensure that Auto provisioning of 'Log Analytics agent for Azure VMs' is Set to 'On' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.16	Ensure that Auto provisioning of 'Vulnerability assessment for machines' is Set to 'On' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>



CIS Benchmark Recommendation		Set Correctly	
		Yes	No
2.1.17	Ensure that Auto provisioning of 'Microsoft Defender for Containers components' is Set to 'On' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.18	Ensure That 'All users with the following roles' is set to 'Owner' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.19	Ensure 'Additional email addresses' is Configured with a Security Contact Email (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.20	Ensure That 'Notify about alerts with the following severity' is Set to 'High' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.21	Ensure that Microsoft Defender for Cloud Apps integration with Microsoft Defender for Cloud is Selected (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
2.1.22	Ensure that Microsoft Defender for Endpoint integration with Microsoft Defender for Cloud is selected (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2.2</b>	<b>Microsoft Defender for IoT</b>		
2.2.1	Ensure That Microsoft Defender for IoT Hub Is Set To 'On' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>2.3</b>	<b>Microsoft Defender for External Attack Surface Monitoring</b>		
<b>3</b>	<b>Storage Accounts</b>		
3.1	Ensure that 'Secure transfer required' is set to 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.2	Ensure that 'Enable Infrastructure Encryption' for Each Storage Account in Azure Storage is Set to 'enabled' (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.3	Ensure that 'Enable key rotation reminders' is enabled for each Storage Account (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.4	Ensure that Storage Account Access Keys are Periodically Regenerated (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
3.5	Ensure Storage Logging is Enabled for Queue Service for 'Read', 'Write', and 'Delete' requests (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.6	Ensure that Shared Access Signature Tokens Expire Within an Hour (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.7	Ensure that 'Public access level' is disabled for storage accounts with blob containers (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.8	Ensure Default Network Access Rule for Storage Accounts is Set to Deny (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.9	Ensure 'Allow Azure services on the trusted services list to access this storage account' is Enabled for Storage Account Access (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.10	Ensure Private Endpoints are used to access Storage Accounts (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.11	Ensure Soft Delete is Enabled for Azure Containers and Blob Storage (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.12	Ensure Storage for Critical Data are Encrypted with Customer Managed Keys (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
3.13	Ensure Storage logging is Enabled for Blob Service for 'Read', 'Write', and 'Delete' requests (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.14	Ensure Storage Logging is Enabled for Table Service for 'Read', 'Write', and 'Delete' Requests (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
3.15	Ensure the "Minimum TLS version" for storage accounts is set to "Version 1.2" (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>4</b>	<b>Database Services</b>		
<b>4.1</b>	<b>SQL Server - Auditing</b>		
4.1.1	Ensure that 'Auditing' is set to 'On' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.2	Ensure no Azure SQL Databases allow ingress from 0.0.0.0/0 (ANY IP) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.1.3	Ensure SQL server's Transparent Data Encryption (TDE) protector is encrypted with Customer-managed key (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.4	Ensure that Azure Active Directory Admin is Configured for SQL Servers (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.5	Ensure that 'Data encryption' is set to 'On' on a SQL Database (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.1.6	Ensure that 'Auditing' Retention is 'greater than 90 days' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>4.2</b>	<b>SQL Server - Microsoft Defender for SQL</b>		
4.2.1	Ensure that Microsoft Defender for SQL is set to 'On' for critical SQL Servers (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.2	Ensure that Vulnerability Assessment (VA) is enabled on a SQL server by setting a Storage Account (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.3	Ensure that Vulnerability Assessment (VA) setting 'Periodic recurring scans' is set to 'on' for each SQL server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.4	Ensure that Vulnerability Assessment (VA) setting 'Send scan reports to' is configured for a SQL server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.2.5	Ensure that Vulnerability Assessment (VA) setting 'Also send email notifications to admins and subscription owners' is set for each SQL Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>4.3</b>	<b>PostgreSQL Database Server</b>		
4.3.1	Ensure 'Enforce SSL connection' is set to 'ENABLED' for PostgreSQL Database Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.3.2	Ensure Server Parameter 'log_checkpoints' is set to 'ON' for PostgreSQL Database Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.3.3	Ensure server parameter 'log_connections' is set to 'ON' for PostgreSQL Database Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.3.4	Ensure server parameter 'log_disconnections' is set to 'ON' for PostgreSQL Database Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.3.5	Ensure server parameter 'connection_throttling' is set to 'ON' for PostgreSQL Database Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.3.6	Ensure Server Parameter 'log_retention_days' is greater than 3 days for PostgreSQL Database Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.3.7	Ensure 'Allow access to Azure services' for PostgreSQL Database Server is disabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.3.8	Ensure 'Infrastructure double encryption' for PostgreSQL Database Server is 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>4.4</b>	<b>MySQL Database</b>		
4.4.1	Ensure 'Enforce SSL connection' is set to 'Enabled' for Standard MySQL Database Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.4.2	Ensure 'TLS Version' is set to 'TLSV1.2' for MySQL flexible Database Server (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
4.4.3	Ensure server parameter 'audit_log_enabled' is set to 'ON' for MySQL Database Server (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.4.4	Ensure server parameter 'audit_log_events' has 'CONNECTION' set for MySQL Database Server (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>4.5</b>	<b>Cosmos DB</b>		
4.5.1	Ensure That 'Firewalls & Networks' Is Limited to Use Selected Networks Instead of All Networks (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
4.5.2	Ensure That Private Endpoints Are Used Where Possible (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
4.5.3	Use Azure Active Directory (AAD) Client Authentication and Azure RBAC where possible. (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>5</b>	<b>Logging and Monitoring</b>		
<b>5.1</b>	<b>Configuring Diagnostic Settings</b>		
5.1.1	Ensure that a 'Diagnostic Setting' exists (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.2	Ensure Diagnostic Setting captures appropriate categories (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.3	Ensure the Storage Container Storing the Activity Logs is not Publicly Accessible (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.4	Ensure the storage account containing the container with activity logs is encrypted with Customer Managed Key (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.5	Ensure that logging for Azure Key Vault is 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.6	Ensure that Network Security Group Flow logs are captured and sent to Log Analytics (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.1.7	Ensure that logging for Azure AppService 'HTTP logs' is enabled (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>5.2</b>	<b>Monitoring using Activity Log Alerts</b>		
5.2.1	Ensure that Activity Log Alert exists for Create Policy Assignment (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.2	Ensure that Activity Log Alert exists for Delete Policy Assignment (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.3	Ensure that Activity Log Alert exists for Create or Update Network Security Group (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.4	Ensure that Activity Log Alert exists for Delete Network Security Group (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
5.2.5	Ensure that Activity Log Alert exists for Create or Update Security Solution (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.6	Ensure that Activity Log Alert exists for Delete Security Solution (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.7	Ensure that Activity Log Alert exists for Create or Update SQL Server Firewall Rule (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.8	Ensure that Activity Log Alert exists for Delete SQL Server Firewall Rule (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.9	Ensure that Activity Log Alert exists for Create or Update Public IP Address rule (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.2.10	Ensure that Activity Log Alert exists for Delete Public IP Address rule (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>5.3</b>	<b>Configuring Application Insights</b>		
5.3.1	Ensure Application Insights are Configured (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
5.4	Ensure that Azure Monitor Resource Logging is Enabled for All Services that Support it (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
5.5	Ensure that SKU Basic/Consumption is not used on artifacts that need to be monitored (Particularly for Production Workloads) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>6</b>	<b>Networking</b>		
6.1	Ensure that RDP access from the Internet is evaluated and restricted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.2	Ensure that SSH access from the Internet is evaluated and restricted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.3	Ensure that UDP access from the Internet is evaluated and restricted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.4	Ensure that HTTP(S) access from the Internet is evaluated and restricted (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
6.5	Ensure that Network Security Group Flow Log retention period is 'greater than 90 days' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.6	Ensure that Network Watcher is 'Enabled' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
6.7	Ensure that Public IP addresses are Evaluated on a Periodic Basis (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>7</b>	<b>Virtual Machines</b>		
7.1	Ensure Virtual Machines are utilizing Managed Disks (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.2	Ensure that 'OS and Data' disks are encrypted with Customer Managed Key (CMK) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.3	Ensure that 'Unattached disks' are encrypted with 'Customer Managed Key' (CMK) (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
7.4	Ensure that Only Approved Extensions Are Installed (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
7.5	Ensure that Endpoint Protection for all Virtual Machines is installed (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
7.6	[Legacy] Ensure that VHDs are Encrypted (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
7.7	Ensure an Azure Bastion Host Exists (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
<b>8</b>	<b>Key Vault</b>		
8.1	Ensure that the Expiration Date is set for all Keys in RBAC Key Vaults (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
8.2	Ensure that the Expiration Date is set for all Keys in Non-RBAC Key Vaults. (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
8.3	Ensure that the Expiration Date is set for all Secrets in RBAC Key Vaults (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
8.4	Ensure that the Expiration Date is set for all Secrets in Non-RBAC Key Vaults (Automated)	<input type="checkbox"/>	<input type="checkbox"/>

CIS Benchmark Recommendation		Set Correctly	
		Yes	No
8.5	Ensure the Key Vault is Recoverable (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
8.6	Enable Role Based Access Control for Azure Key Vault (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
8.7	Ensure that Private Endpoints are Used for Azure Key Vault (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
8.8	Ensure Automatic Key Rotation is Enabled Within Azure Key Vault for the Supported Services (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>9</b>	<b>AppService</b>		
9.1	Ensure App Service Authentication is set up for apps in Azure App Service (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.2	Ensure Web App Redirects All HTTP traffic to HTTPS in Azure App Service (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.3	Ensure Web App is using the latest version of TLS encryption (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.4	Ensure the web app has 'Client Certificates (Incoming client certificates)' set to 'On' (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.5	Ensure that Register with Azure Active Directory is enabled on App Service (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.6	Ensure That 'PHP version' is the Latest, If Used to Run the Web App (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
9.7	Ensure that 'Python version' is the Latest Stable Version, if Used to Run the Web App (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
9.8	Ensure that 'Java version' is the latest, if used to run the Web App (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
9.9	Ensure that 'HTTP Version' is the Latest, if Used to Run the Web App (Automated)	<input type="checkbox"/>	<input type="checkbox"/>
9.10	Ensure FTP deployments are Disabled (Automated)	<input type="checkbox"/>	<input type="checkbox"/>



CIS Benchmark Recommendation		Set Correctly	
		Yes	No
9.11	Ensure Azure Key Vaults are Used to Store Secrets (Manual)	<input type="checkbox"/>	<input type="checkbox"/>
<b>10</b>	<b>Miscellaneous</b>		
10.1	Ensure that Resource Locks are set for Mission-Critical Azure Resources (Manual)	<input type="checkbox"/>	<input type="checkbox"/>

DRAFT