TD SYNNEX

SMB Fraud Defense

Click-to-Run™ Solution Deployment Guide

TD SYNNEX

SMB Fraud Defense 3.0

Deployment Guide

This guide is designed to provide our Partners with the deployment steps, which are required to successfully deploy SMB Fraud Defense version 3.0.

TD SYNNEX

Table of Contents

Solution Overview

TD SYNNEX has developed a new pre-configured anti-fraud solution to enable partners to detect, prevent, and remediate against potential attacks in Azure. SMB Fraud Defense helps small and medium sized customers increase their security posture and gain better control of their cloud environment, while reducing risks in day-to-day cloud operations.

This Click-to-Run™ Solution delivers a multi-layer defense against vulnerabilities based on industry security best practice, allowing you to easily enable Security Defaults, implement Conditional Access and Azure polices, and set budgets within Azure Cost Management.

Solution Key Features

MFA & Identity: Options to enforce MFA & identity polices across all users.

Configure Conditional Access: Blocking legacy authentication, risky login restrictions and compliance devices per user or 365 App.

Geo-Restrictions for Logins: Manage locations where data centers can be deployed.

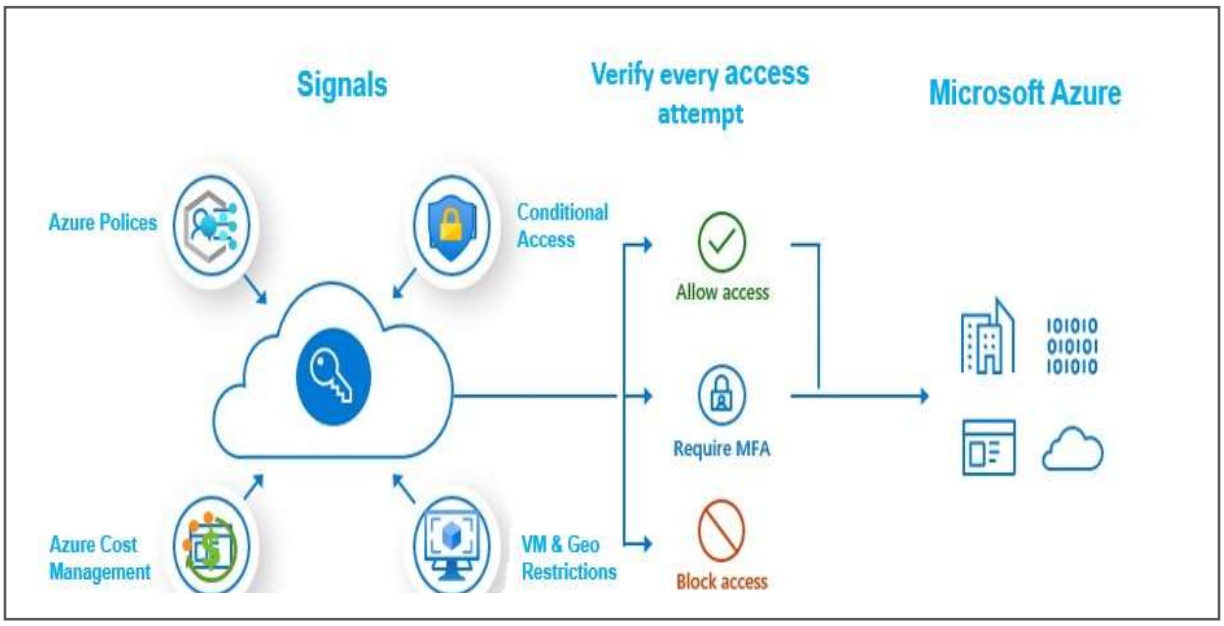
Security 365: Manage security settings and Data Compliance policies for email services.

Security Essentials: Manage security settings and prevention policies.

Azure Cost Management: Set thresholds and alerts to control cost management.

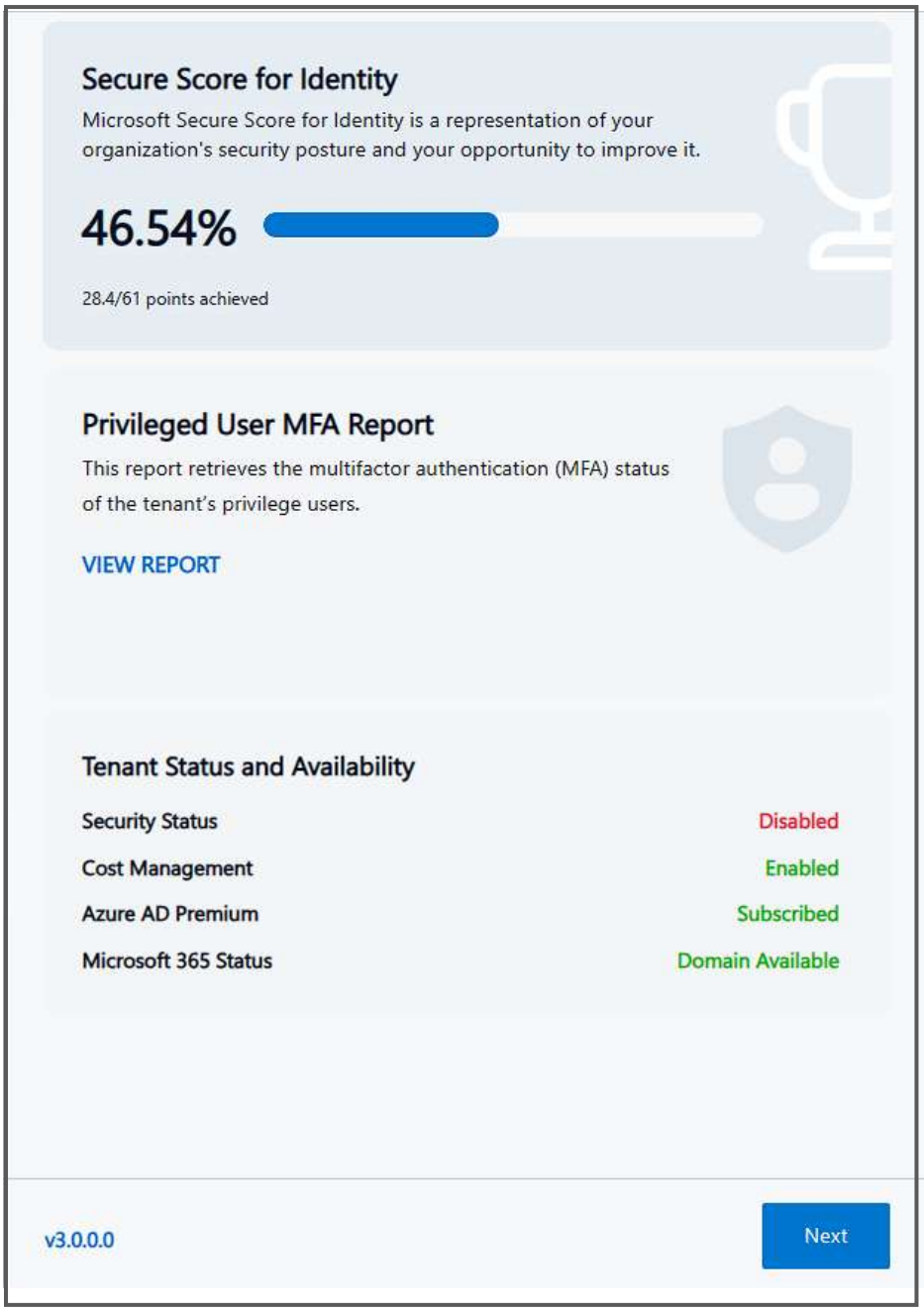
Alerts & Monitoring: Set alerts and audit to control configuration settings and azure activity.

Deployment Architecture



Solutions User Interface Overview

For more details on the UI and a quick explanation of each option and mechanism, you can refer to the Quick Step Guide.



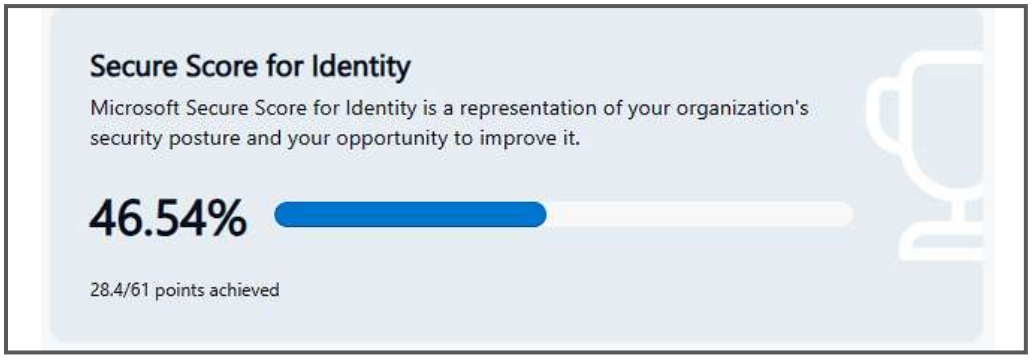
Deployment Options

3rd Party MFA Control

This version of the Click-to-Run ™ Solution is compatible with third party multi-Factor authentication solutions. When a 3rd party MFA is detected, solution will show a warning message, and the Security Tab will be blocked.

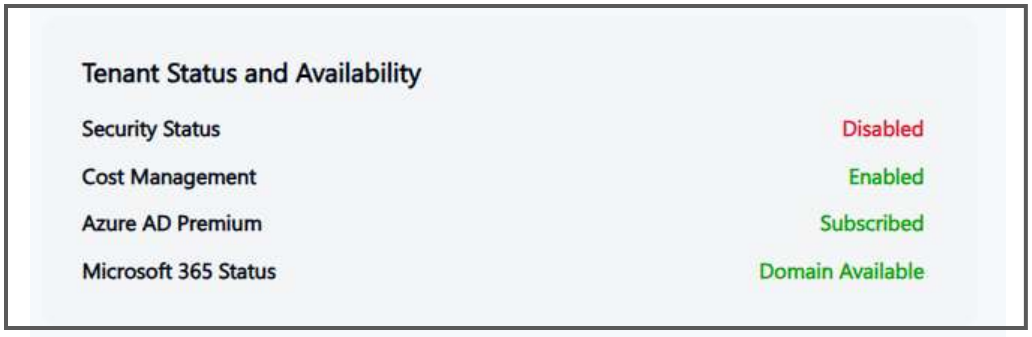
Secure Score for Identity

Secure Score for “Identity" is a component of Microsoft Secure Score, a scoring model that reflects your organization's identity security posture based on your regular activities and settings in Azure Active Directory (Azure AD) and Microsoft 365.



Tenant Status and Availability

The solution will do a complete scan of your Azure environment to identify solution’s requirement as well as security status.



Security Status: Solution will check If Security Defaults is enabled, Conditional Access is deployed, or none of the above.

Cost Management: It will also check to see if cost management has been enabled in your Azure environment, if not this needs to be enabled by clicking on the button “Enable”.

Azure AD Premium: Reports which Azure license you are currently using. Depending on the type of license some features may not be available, “Conditional Access” and “Smart Lockout” options require at least P1.

Microsoft 365 Status: Reports if a Microsoft 365 Email service exists on your Subscription. If you do not have Email service enabled, Microsoft 365 tab will be blocked.

Reports

The solution will do a complete scan of your Azure environment to report Identity security status.

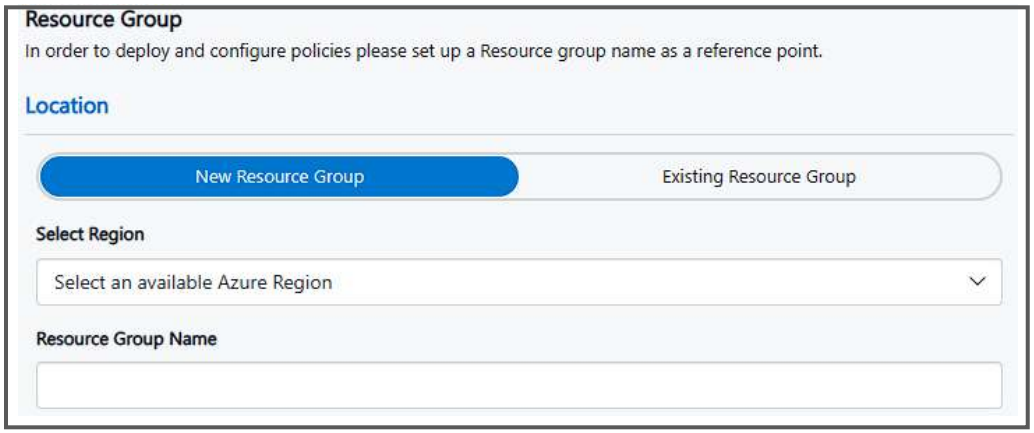
Privileged User Report: A customizable Report of Privileged accounts (Administrators), will provide MFA status per user *.

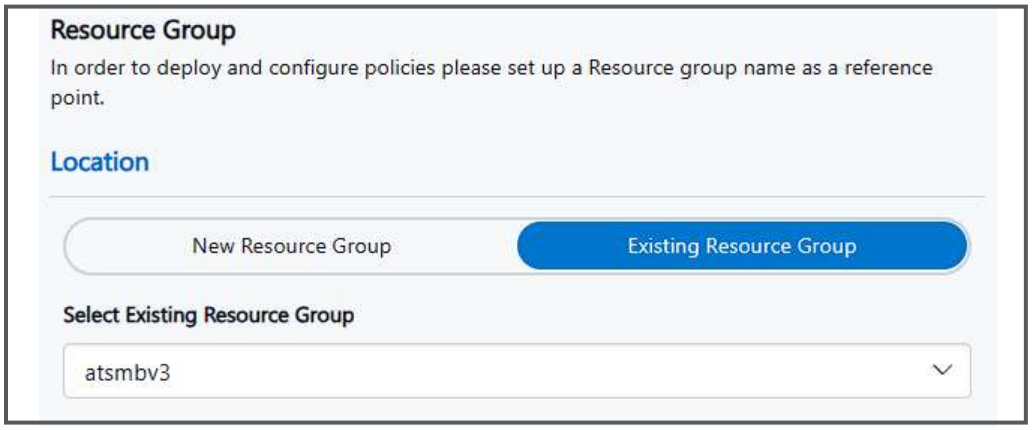
*Current Microsoft Report does not allow retrieving MFA data set by Conditional access, only MFA enabled manually on each user is available.

Location and Resource Group

In “location and resource group”, you will need to choose between create a new resource group or select an existing one with an old deployment of SMB Fraud (version 1.5 or higher).

Information: Resource group will remain empty; nothing will physically be deployed into this resource group.





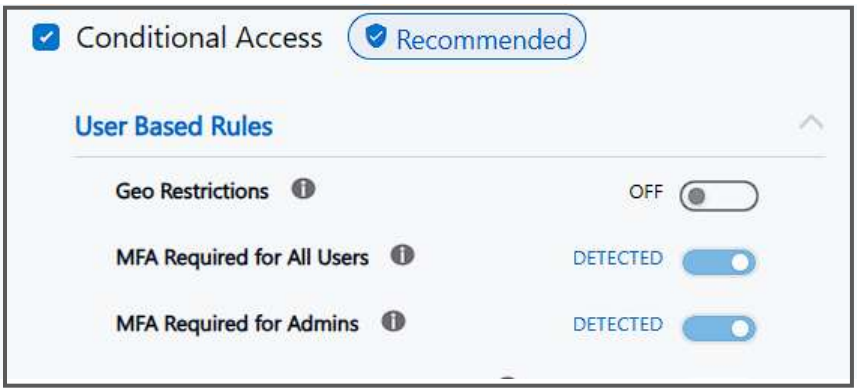
Create Resource Group in Azure

To create a new Resource Group, choose desired location where you would like the Resource Group to be created, this is a drop-down box please choose your desired location and then name this Resource Group.

Use Existing Group in Azure

To select an old deployment of SMB Fraud Defense, select Existing Resource Group option, system will search for existing deployments and then in a drop-down box, please choose your desired deployment and proceed.

When this option has been selected, the solution will perform a check of the existing configuration. If Conditional Access policies or Azure policies are detected, they will appear as "DETECTED" and blocked for deployment. Additionally, if the access policies are in "Audit" mode, an error message will be displayed with the list of affected policies to be corrected.

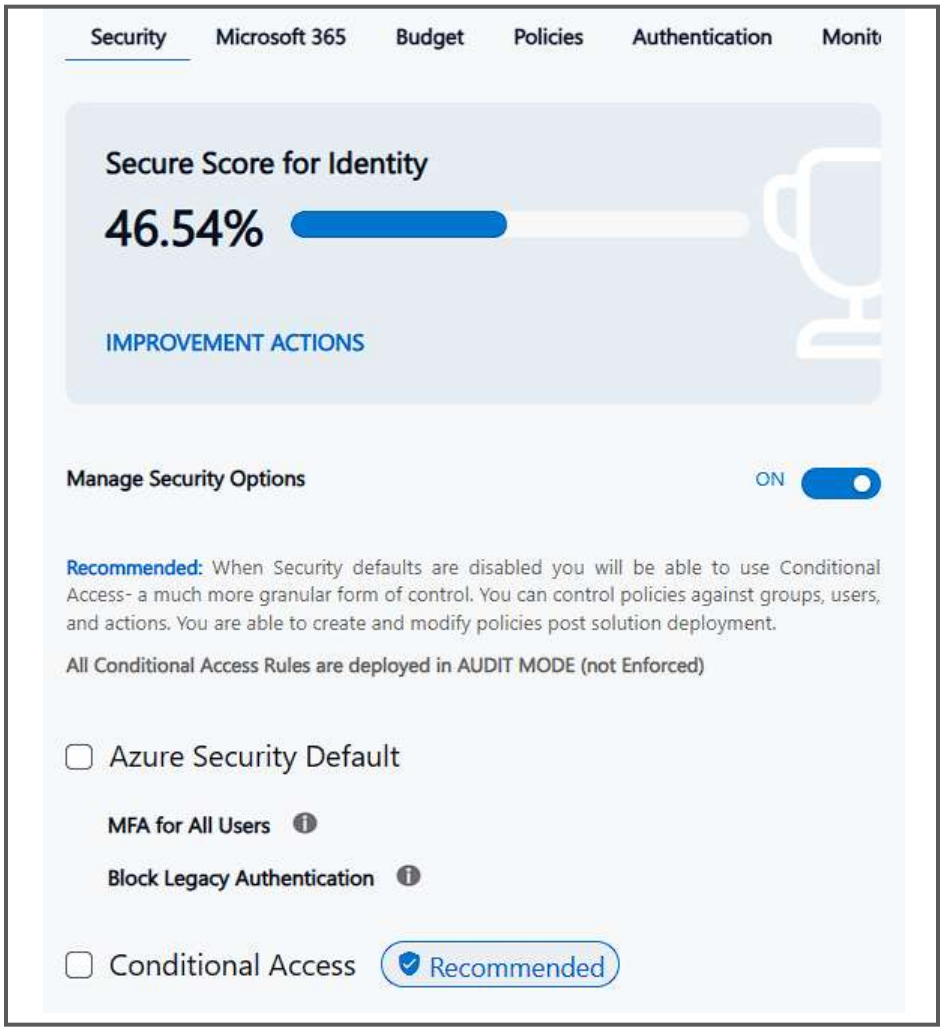


Information: Only available for Version 1.5 or above.

SECURITY

Manage Security Options

The security section will allow us to choose what type of access control we want to implement. If you have a Premium license (P1 or P2), the recommendation from Microsoft and TD SYNNEX is to use Conditional Access, which includes different types of policies adaptable to any environment.

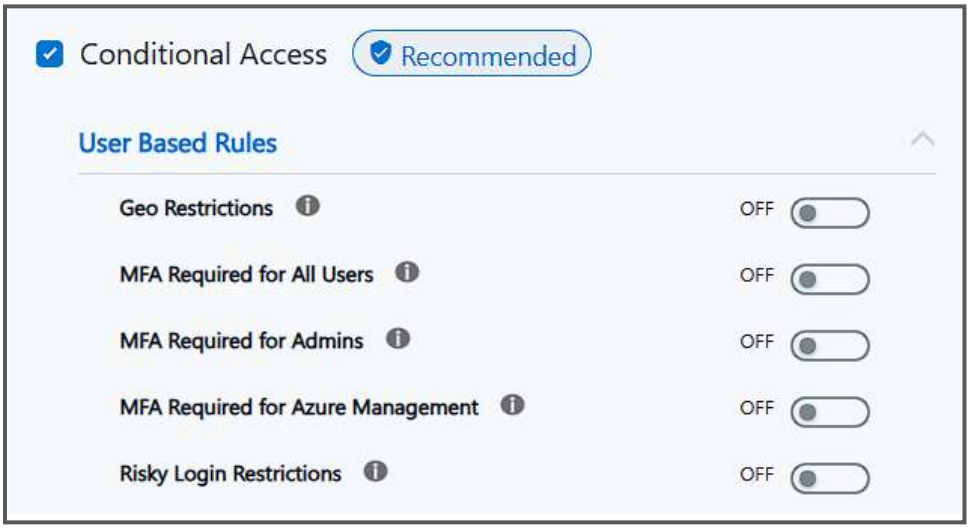


Azure Security Defaults is a set of basic security settings that help protect organizations from common threats. They include requiring multi-factor authentication (MFA) for all users, blocking legacy authentication protocols, and requiring administrators to perform risk-based MFA. It's an easy, one-click solution for a baseline level of security.

Conditional Access Policies in Microsoft Azure are rules that provide security measures when users attempt to access applications and data. Based on conditions like user identity, device status, or location, these policies determine whether access should be allowed, denied, or require further authentication, like multi-factor authentication. They offer a granular, adaptable approach to secure access control.

All of our Conditional Access Polices are created in **Audit Mode** and are not enforced.

Signals that are included in this version include two categories User based rules and Device based rules:



User Based Rules

Geo Restrictions, toggle this option to allow you to add locations you want to set as trusted locations, the list contains those regions recognized by Microsoft. You have no restriction on how many countries you wish to add.

Link to Microsoft Docs for More Info on Geo restrictions: [Microsoft GEO Conditional Access]

MFA for All Users, toggle this option to enforce MFA for all users that have been assigned to that tenant.

Link to Microsoft Docs for More Info on MFA for all Users: Microsoft MFA for All users

MFA for All Admins, toggle this option to enforce MFA for All admins that have been assigned to that tenant.

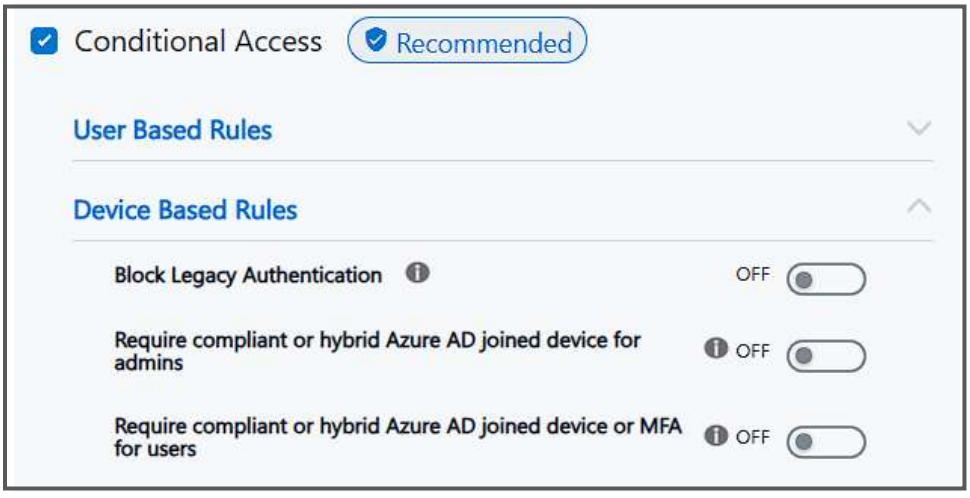
Link to Microsoft Docs for More Info on MFA for all Users: List of Admins being secure. - List of Admins being secure.

MFA for Azure Management, toggle this option to enforce MFA for Azure Management. This means users who are looking to make any changes in Azure, for example, creating or deleting a new resource group, then MFA would be required for this.

Link to Microsoft Docs for More Info on MFA for Azure Management: Microsoft MFA for Privilege Actions

Blocks Risky Login Restrictions, when you enable this option, it will block users who are classified as suspicious because of an uncommon behavior. Azure will manage the risk level, analyze any suspicious behavior, and block the user from logging in. This will force the user to reset their password.

Link to Microsoft Docs for More Info for Block Risky Log Restrictions: Microsoft Risky Login



Device Based Rules

Block Legacy Authentication, this option focuses on devices not users, enable this toggle for this option to block all superseded tenants using M365, POP3 SMTP and IMAP.

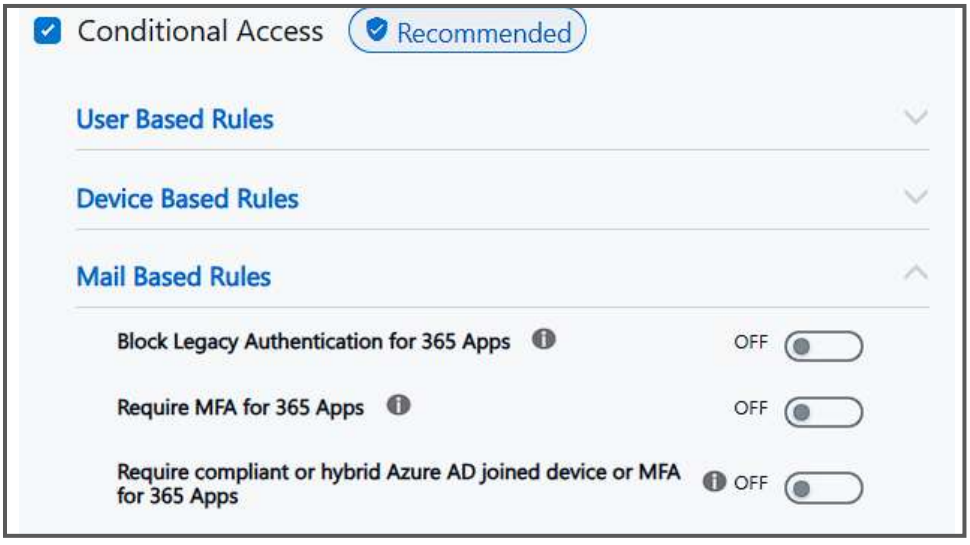
Link to Microsoft Docs for More Info for more information on Block legacy authentication - Azure Active Directory - Microsoft Entra | Microsoft Learn

Require compliant or Hybrid Azure AD joined device for Admins, accounts with administrative rights are targeted by attackers. Requiring Admins with these highly privileged rights to perform actions from devices marked as compliant or hybrid Azure AD joined can help limit possible exposure.

Link to Microsoft Docs for more information Require administrators use compliant or hybrid joined devices - Azure Active Directory - Microsoft Entra | Microsoft Learn

Require compliant or Hybrid Azure AD joined device or MFA for Users, require all users to have at least MFA or connect from a compliant computer.

Link to Microsoft Docs for more information Require compliant, hybrid joined devices, or MFA - Azure Active Directory - Microsoft Entra | Microsoft Learn



Mail Based Rules

Block Legacy Authentication for 365 Apps, this option focuses on devices not users, enable this toggle for this option to block all superseded tenants using M365, POP3 SMTP and IMAP to access Microsoft 365 apps.

Link to Microsoft Docs for more information on Block legacy authentication - Azure Active Directory - Microsoft Entra | Microsoft Learn

Require MFA for 365 Apps, toggle this option to enforce MFA for All users with access to 365 services.

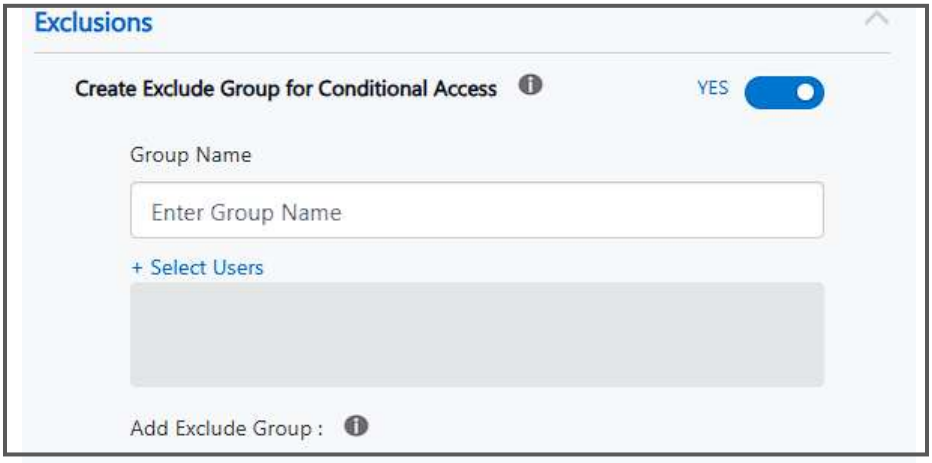
Link to Microsoft Docs for more information Require administrators use compliant or hybrid joined devices - Azure Active Directory - Microsoft Entra | Microsoft Learn

Require compliant or Hybrid Azure AD joined device or MFA for 365 Apps, require all users to have at least MFA or connect from a compliant computer to access 365.

Link to Microsoft Docs for more information Require compliant, hybrid joined devices, or MFA - Azure Active Directory - Microsoft Entra | Microsoft Learn

Exclusions

An exclusion in Conditional Access Policies in Azure is a configuration that allows you to exclude certain users, groups, or applications from the effects of a Conditional Access Policy. Exclusions will create a new Azure AD Group to be added as an exception on the selected policies.



Group Name; Select a name for the Azure AD Group.

Select Users, Solution will check all your available users in Azure AD that can be added to the new group. (Is not required to add users now, they can be added manually later from the Azure Portal).

Add Exclude Group; Allows you to add the exclusion to selected Conditional Access Policies (if applies), click on each CA you want to add the exclusion. (It is not required to add the exclusion now, this can be added manually later from the Azure Portal).

Organization Settings

Allows for modifying the essential configuration parameters of the organization, applying policies for email retention, auditing, and access control.

Client Forward Block Rules, this rule will restrict, or control automatically forwarded messages to external recipients (recipients outside of your organization). Email forwarding can be useful but can also pose a security risk due to the potential disclosure of information. Attackers might use this information to attack your organization or partners.

Link to Microsoft Docs for More Info for more information on 365 - Client Forward Rules

Outbound Spam Filtering, default outbound spam policy automatically applies to all senders recommended settings to avoid unintentional massive email sending by an internal user.

Link to Microsoft Docs for more information on 365 - Outbound Spam Filter

Anonymous Calendar Sharing, the purpose of that policy is to control what kind of information your users share externally.

Link to Microsoft Docs for More Info for more information on 365 - Anonymous Sharing

Mailbox Auditing, you can track logons to a mailbox as well as what actions are taken while the user is logged on. When enabled, some actions performed by administrators and delegates are logged by default.

Link to Microsoft Docs for more information on 365 - Mailbox Audit

Compliance Settings

Compliance options for the organization, requires an E5 license.

Select DLP Country Set, DLP detects sensitive items by using deep content analysis, not by just a simple text scan. Content is analyzed for primary data matches to keywords, by the evaluation of regular expressions, by internal function validation, and by secondary data matches that are in proximity to the primary data match.

Link to Microsoft Docs for More Info for more information on 365 - Data Loss Prevention

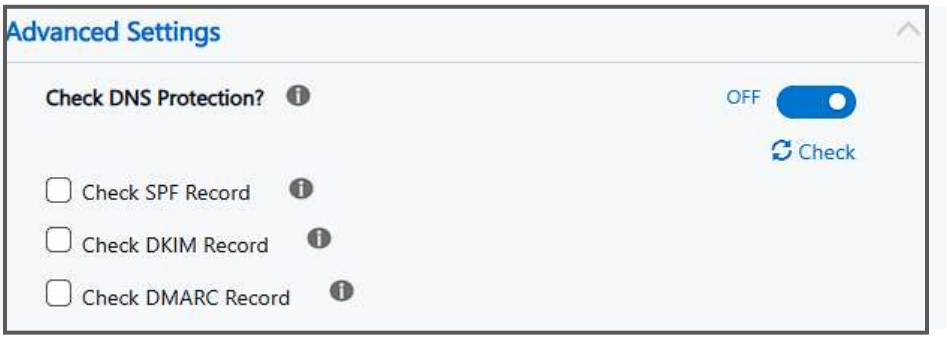
Safe Attachment, after message attachments are scanned by anti-malware protection in Exchange Online Protection (EOP), Safe Attachments opens files in a virtual environment to see what happens (a process known as detonation) before the messages are delivered to recipients.

Link to Microsoft Docs for more information on 365 - Safe Attachment

Safe Link protects your organization from malicious links that are used in phishing and other attacks. Specifically, Safe Links provides URL scanning and rewriting of inbound email messages during mail flow, and time-of-click verification of URLs and links in email messages, Teams, and supported Office 365 apps.

Link to Microsoft Docs for more information on 365 - Safe Links

Advanced Settings



Allows a check on the recommended DNS records to improve email security. These types of records cannot be created manually, so included below is a detailed guide from Microsoft on how to create and add the records in the Microsoft 365 DNS service.

SPF Record, mark this box to validate if you have a SPF in your DNS. SPF record is added as a TXT record that is used by DNS to identify which mail servers can send mail on behalf of your custom domain.

Link to Microsoft Docs for More Info for more information on 365 - Create SPF Record

DKIM Record, mark this box option to validate if you have a DKIM in your DNS. A DKIM record is a specially formatted DNS TXT record that stores the public key the receiving mail server will use to verify a message's signature.

Link to Microsoft Docs for more information 365 - Create DKIM Record

DMARC Record, mark this box option to validate if you have a DMARC in your DNS. A DMARC record defines how strictly you should check messages. Recommended actions for the receiving server when it gets messages that fail authentication checks.

Link to Microsoft Docs for more information 365 - Create DMARC Record

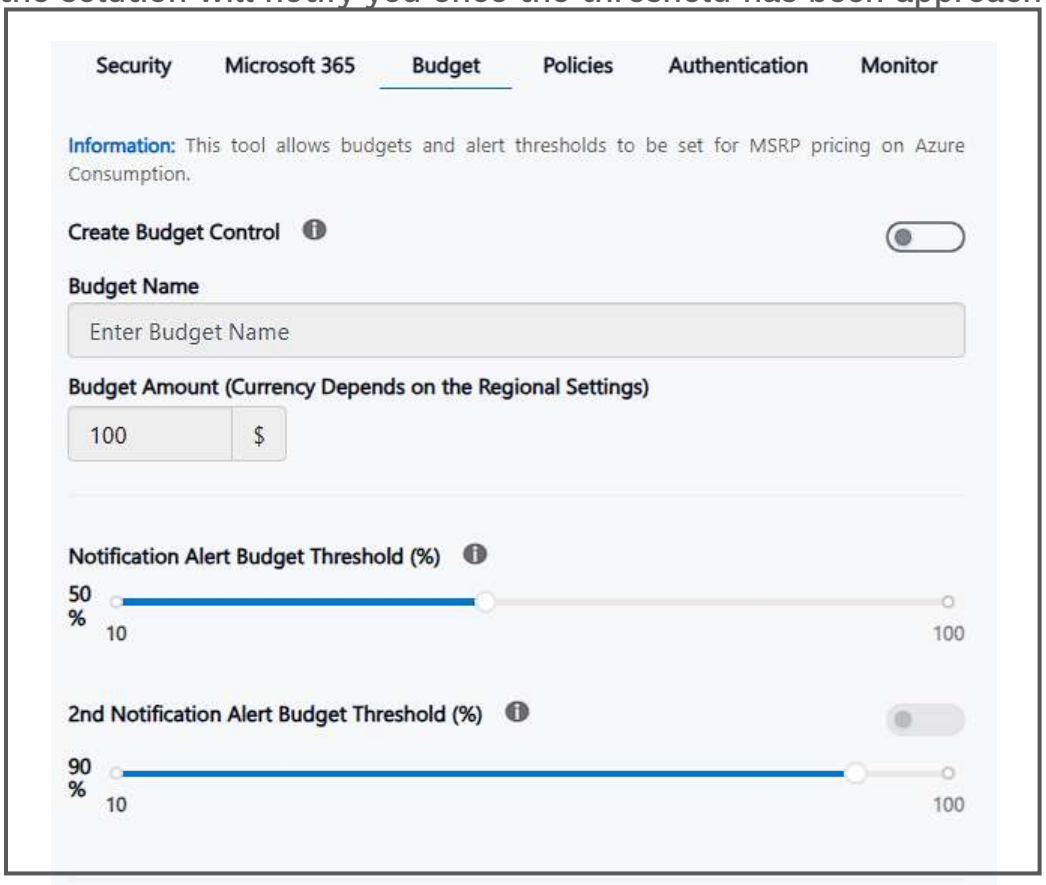
BUDGET

Managing your Budget Management and Budget Threshold

In the “Budget tab,” you will have the option to manage your budget and to set budget thresholds. To use this option, you will need to have Cost Management enabled within your Azure environment.

If you do not have cost management enabled in your tenant, then the “Enable” button will appear allowing the module to be enabled. You can continue to deploy the solution and re-deploy cost management at a later stage once enabled. It will just then add this setting to your Azure tenant.

Once you have the budget enabled you start by creating a budget name, this is your identifier to ensure that your desired monthly amount does not exceed your monthly budget. In the Budget sum, you have the option to input the value with a minimum of 100 (The currency is set based on your regional settings, set-up in Azure). If your tenant is calculated in dollars, sterling, or euros the solution will notify you once the threshold has been approached.



Budget Alerts

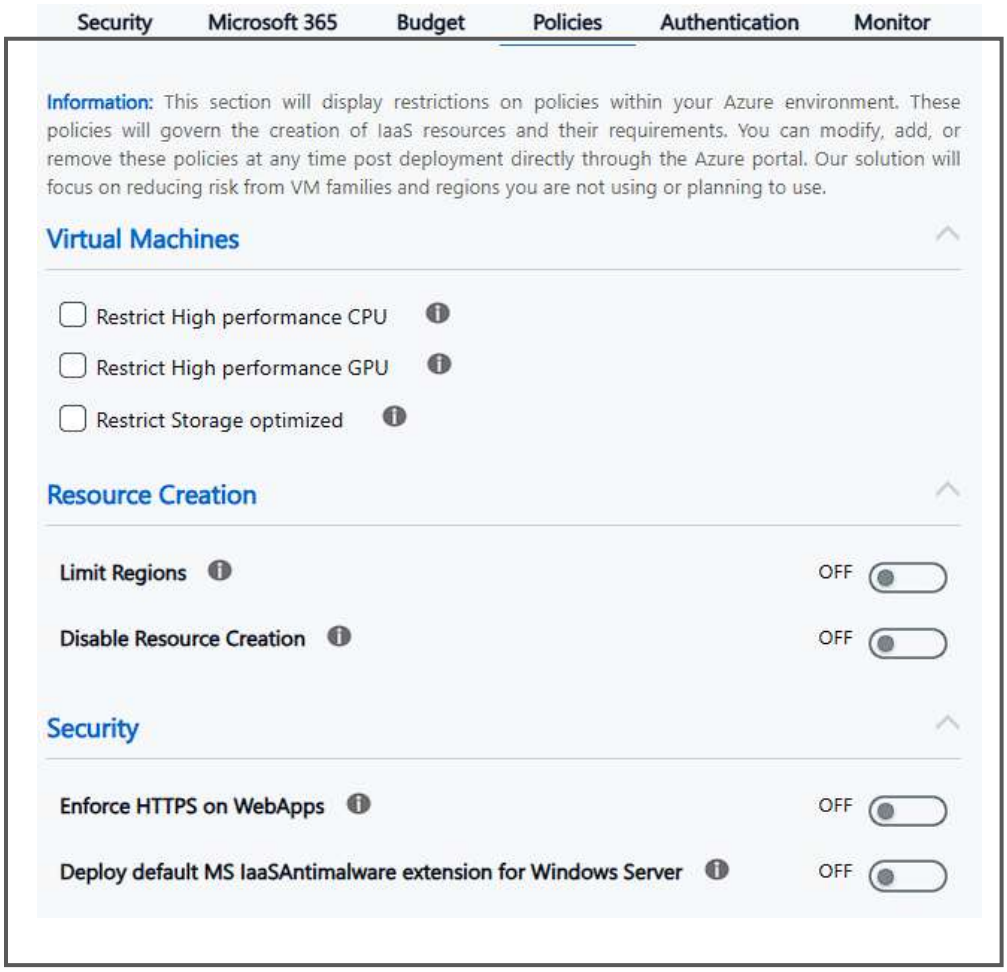
Budget alerts allow you to set up your sender groups. You only have the option to set up one email notification alert, this can be individual email recipients or email groups. This means your Recipients will receive two alerts once the dedicated Budget percentage threshold has been reached. We have set an expiration date of 10 years, which means that this setting will stay in place for 10 years.

POLICIES

Azure Policies

Azure polices includes features which use a JSON format to form a logical evaluation that will determine if a resource is compliant or not. Definitions include metadata and the policy rule. The defined rule can use functions, parameters, logical operators' conditions, and property aliases to match exactly the scenario you want. The policy rule determines which resources in the scope of the assignment are evaluated and blocked or allowed depending on the statement.

When you enable Virtual Machine allowed SKU, this triggers the option to allow you to choose whether you want to enable High Performance CPU – High Performance GPU or Storage Optimized. These are a set of polices to control which type of Resources you want to **DENY** in your tenant. Each policy will deny a family of VMs depending on the resources optimized.



High Performance CPU, toggle this option to **DENY** VMs from the **H** to **F** Families

High Performance GPU, toggle this option to **DENY** VMs from **Nv**, **Nc**, and **Nd** Families

Storage Optimized, toggle this option to **DENY** VMs from **LS** Families

Resource Creation Limit Locations toggle this option to **ALLOW** those locations you want to create a set of Secure Locations; you can choose more than one location, and these will then be added to your list. All other locations will then be blocked.

Resource Creation Disabled toggle this option to **DISABLE** any resource creation in all of the Azure environment.

Security: Enforce HTTPS on WebApps, by default; clients can connect to Azure App Service endpoints by using both HTTP and HTTPS. However, it is always recommended to redirect HTTP to HTTPs because HTTPS uses the SSL/TLS protocol to provide a secure connection, which is both encrypted and authenticated, to enable this restriction toggle this to enable.

Link to Microsoft Docs for more information Enable HTTPS setting on Azure App service using Azure policy (microsoft.com)

Security: Deploy Default Microsoft laaS Antimalware extension for Windows Server, A free real-time protection capability that helps identify and remove viruses, spyware, and other malicious software, with configurable alerts when known malicious or unwanted software attempts to install itself or run on your Azure systems.

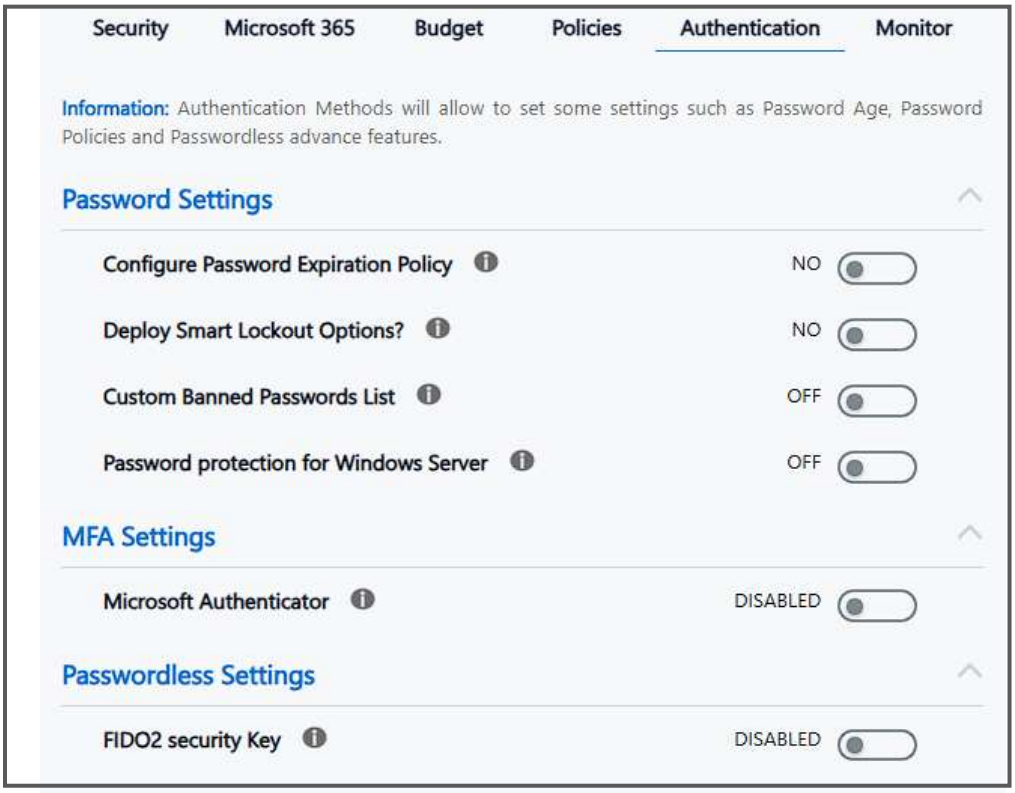
Link to Microsoft Docs for more information, Microsoft Antimalware Extension for Windows VMs on Azure - Azure Virtual Machines | Microsoft Learn

Authentication Methods

Authentication methods allow you to manage your Password age, Password Polices and Passwordless advance features settings.

This has been split into different categories.

- Password Settings
- MFA Settings
- Passwordless Functions



Password Settings

Password Expiration, by default Azure policy will force password to expire after 90 days, toggle this option to disable password expiration for all users.

Microsoft and *TD SYNNEX* recommend disabling password expiration. This will encourage your users to use a complex password.

Smart Lockout; toggle this option to set your lockout threshold. I.e., after three attempts and then set the duration of the lockout, (in seconds).

Link to Microsoft Docs for More Information for Azure Smart Lockout: [Microsoft Smart Lockout]

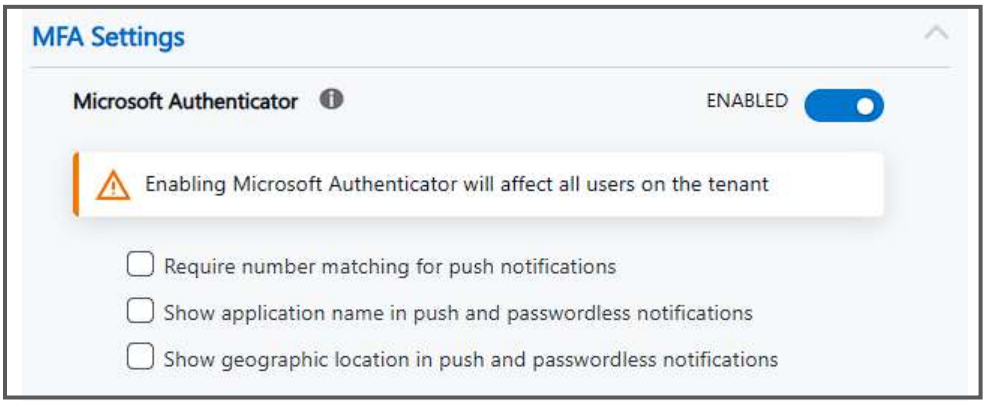
Custom Banned Password List: Azure Custom Banned Password list is a feature of Azure Active Directory (Azure AD) that allows administrators to create a custom list of passwords that cannot be used by users in their organization. This feature is used to enhance the security of user accounts by preventing the use of weak and easily guessable passwords.

By default, the solution will take essential information from your tenant: Location, Zip Code, Domain Name and set as banned words.

Password protection for Windows Server Active Directory, when enabled this protects your on-premises Active Directory Domain Services (AD DS) Hybrid environment. You can install and configure Azure AD Password Protection to work with your on-premises DC. You also have the option to deploy the mode in Audit or Enforced mode.

Link to Microsoft Docs for more information [Enable on-premises Azure AD Password Protection - Microsoft Entra | Microsoft Learn]

MFA Settings



Microsoft Authenticator, Microsoft Authenticator provides an additional level of security to your Azure AD account, with the Microsoft Authenticator app. Users can authenticate in a Passwordless way during sign-in or as an additional verification option during self-service password reset (SSPR) or

multifactor authentication events. Please toggle this feature to enable it then you will have the different options to choose which notifications.

- **Require number matching push notifications**, with this option enabled you will need to match the number on your App against the one that has been given to you by the Authenticator.
- **Show Application name in push and passwordless notifications,** this is going to show which application is trying to connect with Azure and if you want to allow it.
- **Show geographic location and passwordless notifications,** this option will show you in which region you are trying to connect, and if you want to allow it.

If you enable Microsoft Authenticator this will affect all users in the tenant.

Link to Microsoft Docs for more information [Microsoft Authenticator authentication method - Azure Active Directory - Microsoft Entra | Microsoft Learn]

Passwordless Settings

Passwordless Functions, As MFA is a great way to secure organizations, users often get frustrated with the additional security layer on top having to remember passwords. Passwordless authentication is great and provides more convenience because the password it is removed with something you have, plus something you know.

FIDO02, The FIDO (Fast Identity Online), Alliance helps to promote open authentication standards and reduce the use of passwords in form of Authentication. To enable this function toggle this to enabled.

Allow Self Service Setup, once FIDO02 is enabled you can allow self-service set-up.

Enforce attestation, to enforce this function set the toggle to yes.

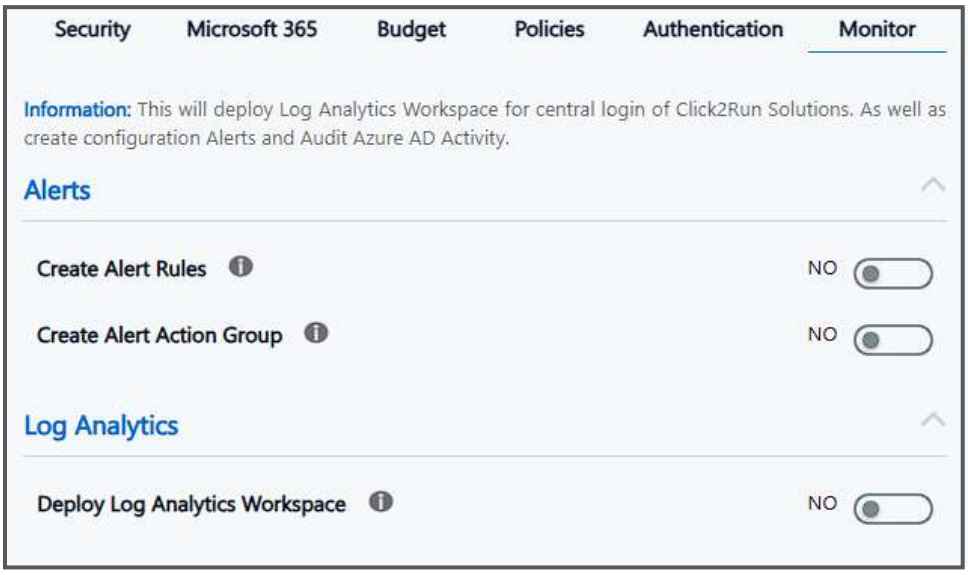
MONITOR

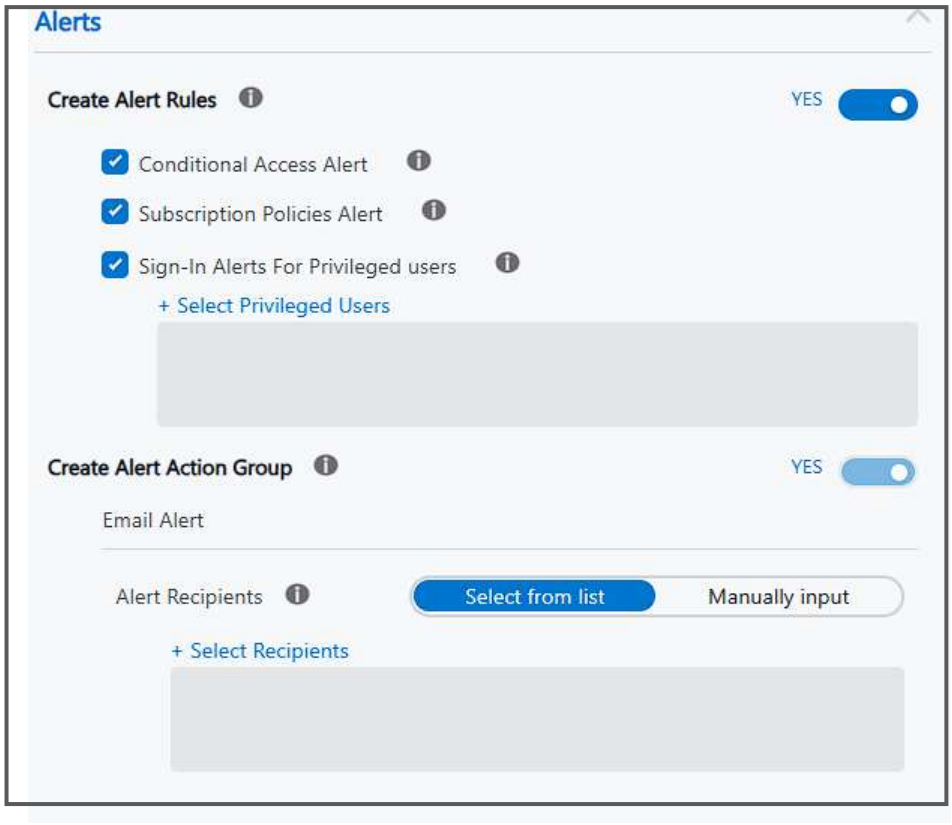
Monitor

Azure Monitor is a cloud-based monitoring and analytics service offered by Microsoft Azure. It provides end-to-end visibility into the performance and health of your applications, infrastructure, and network resources in Azure and on-premises environments. Azure Monitor collects and analyzes telemetry data from various sources, such as application logs, performance metrics, and network traffic, and provides insights into the health, performance, and security of your applications and infrastructure.

The solution offers Monitor and Alert system deploying Log Analytics Workspace; it is required to deploy the service to have all the options available.

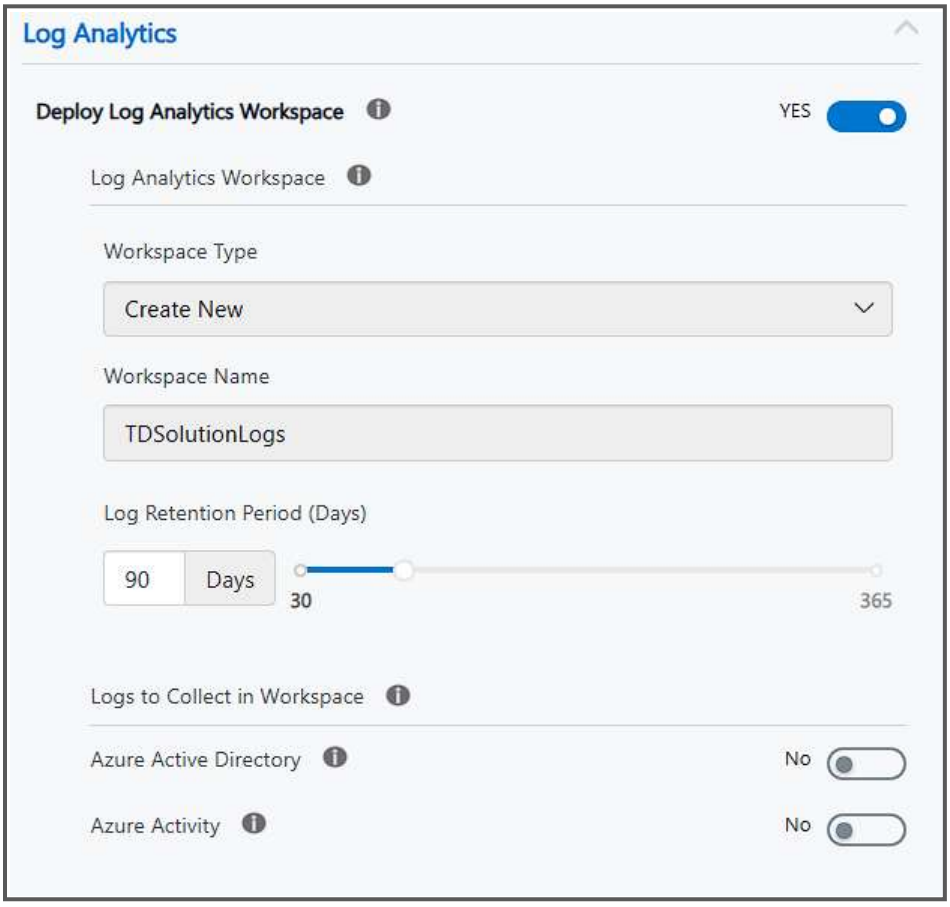
In addition, Log Analytics Workspace will be created on a dedicated resource group tagged and named as "*TDSolutionLogs*" this will allow for future solutions deployed (if desired) to be connected automatically with Analytics Workspace.





Alerts will allow creating alert rules to control any Conditional Access Policy as well as Azure Policies, moreover, it will allow you to audit and control sign-in Azure AD Admin accounts.

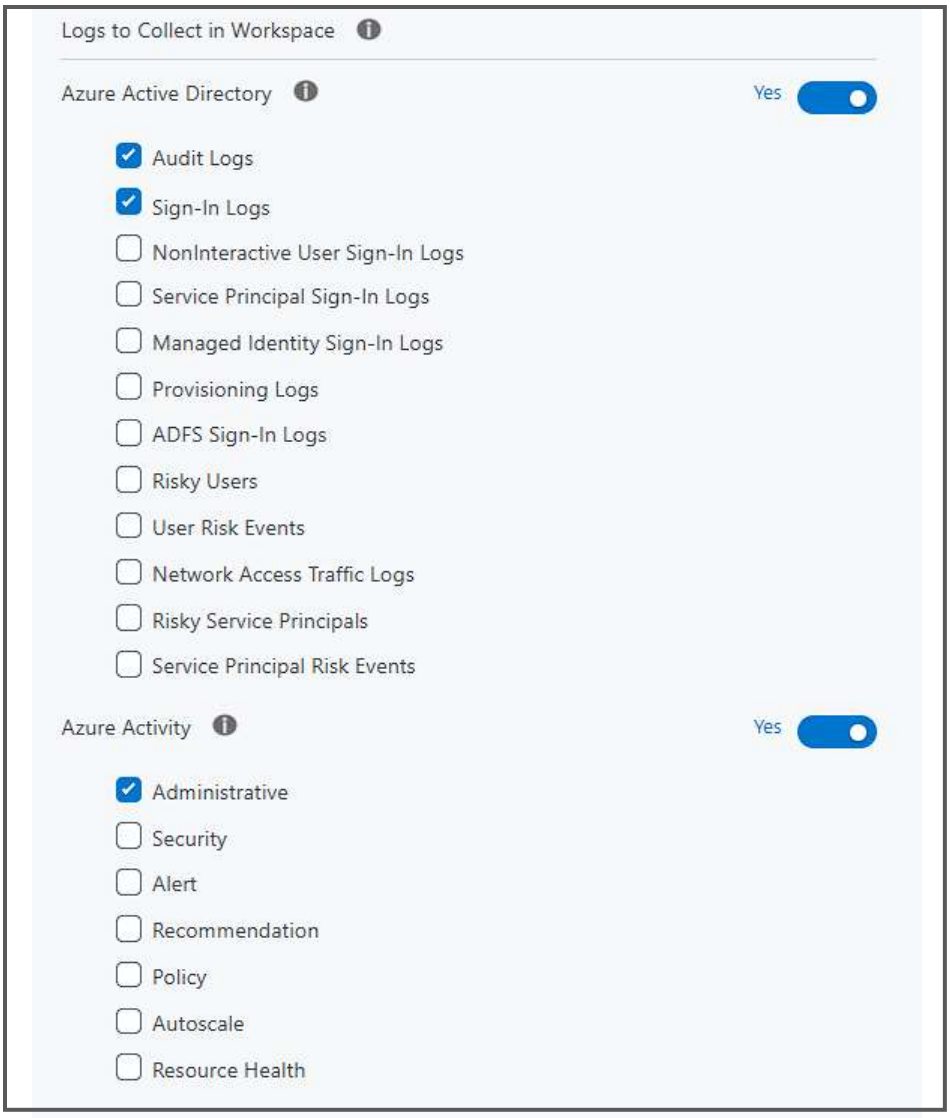
Create Action Group will create a list of emails to receive all the alerts. Recipient list could be retrieved from 365 by selecting “Select from list” or could be added manually by selecting “Manually input”. Both type of emails could be used together. Alert Group is required if Create Alerts is set to “YES.”



Log Analytics will create a new Log Analytics Workspace to retrieve all the desired data. Name of the service cannot be changed to allow future deployments to connect with the service (if desired).

Retention period could have a cost depending on the amount of data and period to archive.

Logs to Collect in Workspace, data to be retrieved from the tenant. The collection of Azure Activity logs (Audit and Sign-In) and Azure Active Directory (administrative) are required if “Alert Rules” are enabled.



Azure Active Directory, capture events and activities that occur within Azure AD. These logs can help you monitor and audit user activity, security events, and other important activities related to your Azure AD environment.

Azure AD logs provide details such as the time of the event, the user account involved, the type of activity, and the result of the activity. Examples of events that can be captured in Azure AD logs include:

1. User sign-ins and sign-outs: Azure AD logs can track user authentication events, such as successful and failed sign-ins, sign-out events, and password reset activity.
2. User and group management: Azure AD logs can capture events related to user and group management, such as creating, deleting, or

modifying users and groups, adding, or removing members, and updating user attributes.

3. Application and service access: Azure AD logs can track events related to application and service access, such as granting or revoking user access to applications and services and managing application roles and permissions.
4. Security-related events: Azure AD logs can help identify security-related events, such as account lockouts, suspicious login attempts, and multi-factor authentication events.

Azure Activity, activity logs provide a historical view of all the activities that have taken place in your Azure resources, including management operations and data-plane events. These logs record details such as who initiated the activity, what the activity was, when it occurred, and the status of the activity.

Activity logs capture data about the following types of events:

1. Control Plane Operations: These are the operations that control and manage Azure resources, such as creating or deleting resources, modifying resource properties, and granting access to resources.
2. Data Plane Operations: These are the operations that are performed on Azure resources themselves, such as reading or writing data to storage accounts, sending, receiving messages to/from a service bus, or executing a query against a database.
3. Resource Provider Operations: These are the operations that are performed by Azure resource providers, such as Azure SQL Database, Azure Virtual Machines, or Azure Storage.

Post Deployment

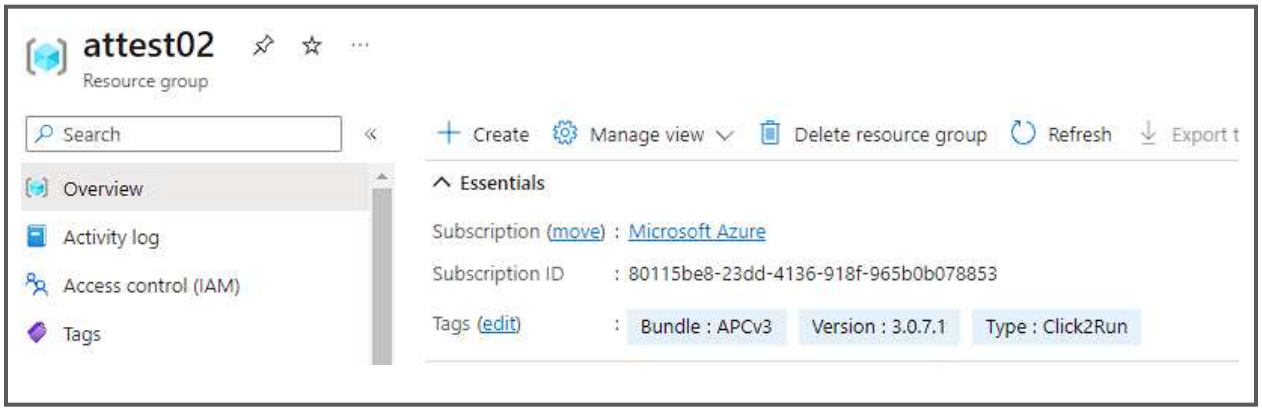
Resource Group Management

New Deployment

Resource Group will be created tagged with version and name of your solution. Do not delete Resource group or tags to allow all functionalities and update capabilities.

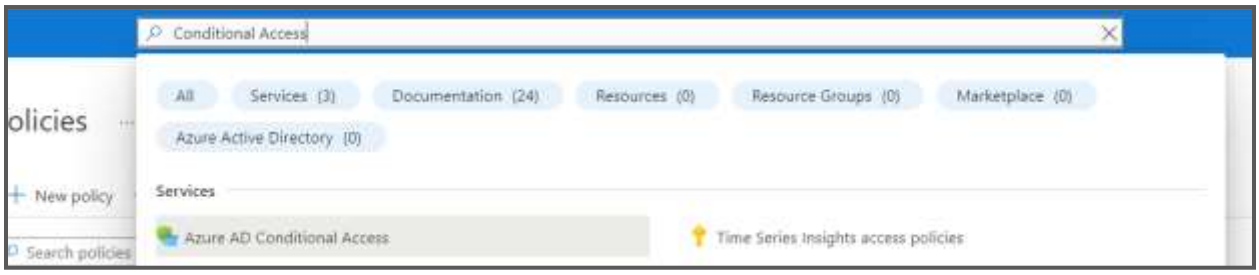
Existing Deployment

If existing Resource Group is selected, TAGS will be updated from previous versions.



Conditional Access Management

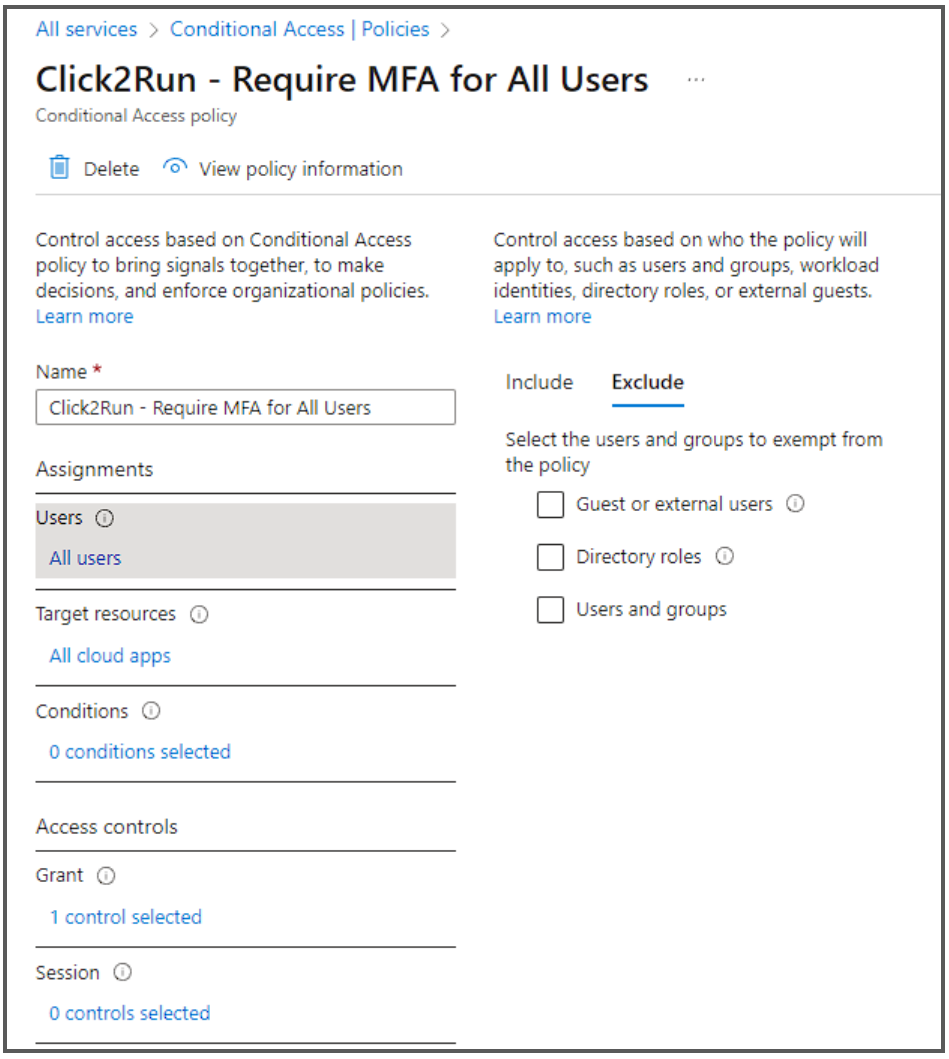
All Conditional Access Policies will be enabled as **Report Only**. This means Policy will only record which user-devices do not meet the requirements of the policy. Changing the policy to **YES**, once the solution has been deployed is recommended, please be aware that you would need to check the users' configurations before you apply this setting to avoid lockouts.



To access Conditional Access Polices, in the search box type "Conditional Access" and select **Azure AD Conditional Access.**

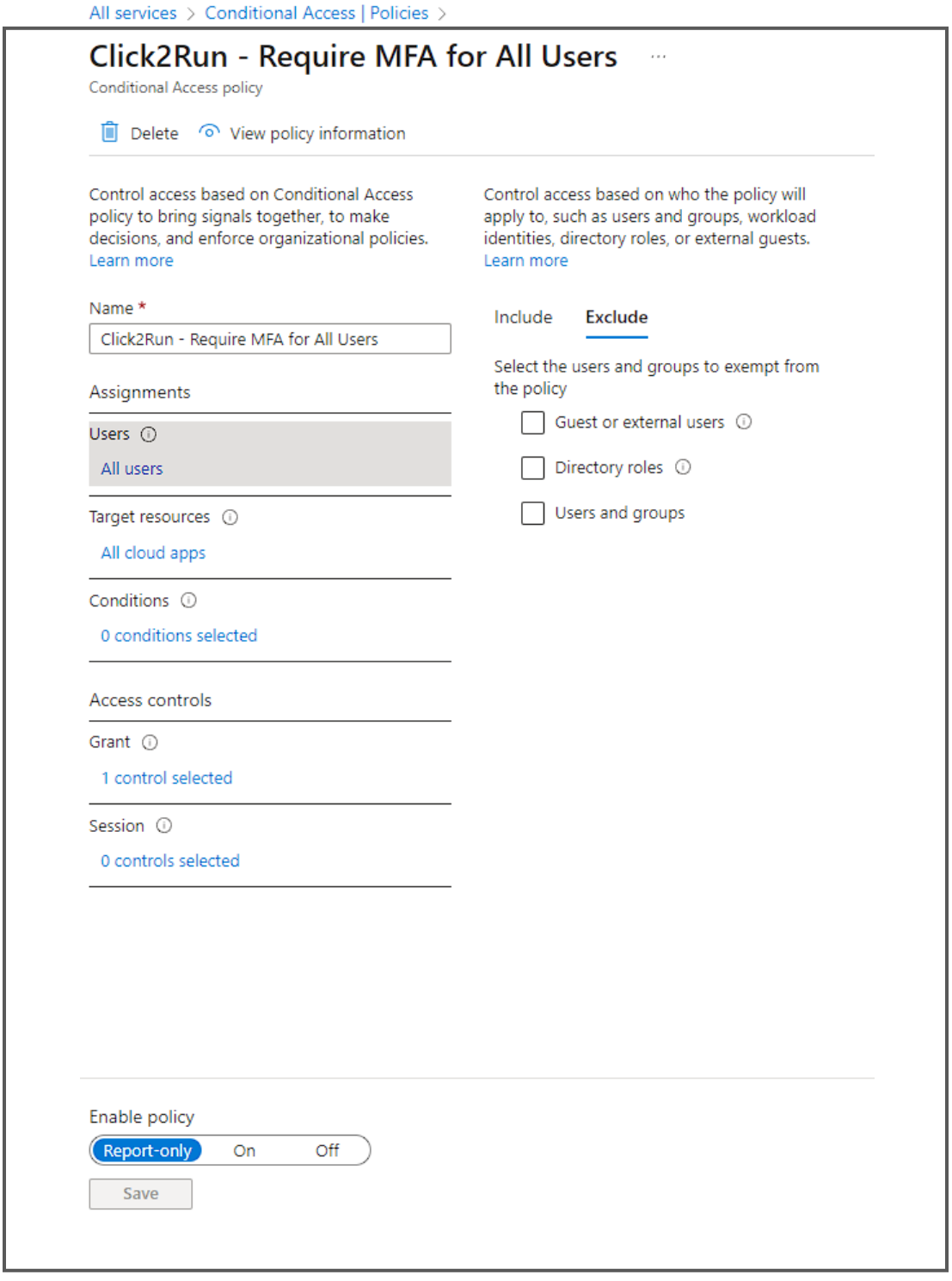
Edit policy: ON Conditional Access Section you will see a list of polices deployed on your tenant either (Enabled or Disabled). To edit these simply click on the desired Policy.

- Add an Exception: Please be aware that it is very important to **NOTE** that you need to create an exception to avoid lockout on your own tenant. In the User/Devices section, select Exclude.
  - Select User or groups to exclude from that policy.



Check Policy Status: You can check the status of every Conditional Access rule that has been created by simply pressing the Overview (preview) tab. In the **Security Alerts,** you can check a quick resume of compliance/noncompliance users-devices.

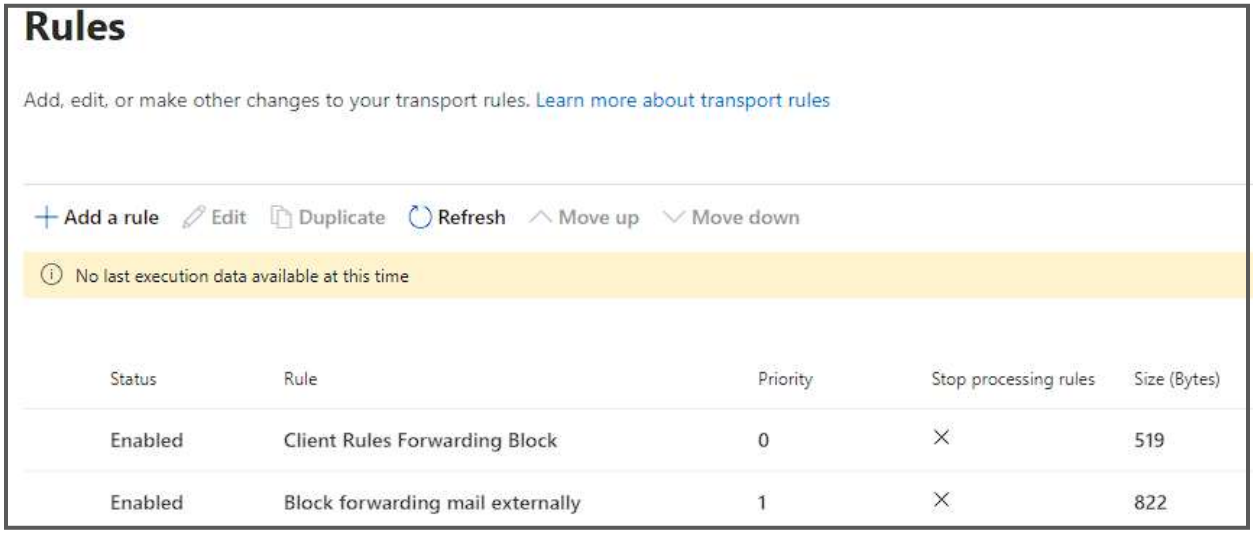
Enforce Policy: On Conditional Access policy editor, you have the option to change the setting from **Report Only** to **Enable** or **Disable**. **This step is mandatory to secure the environment.**

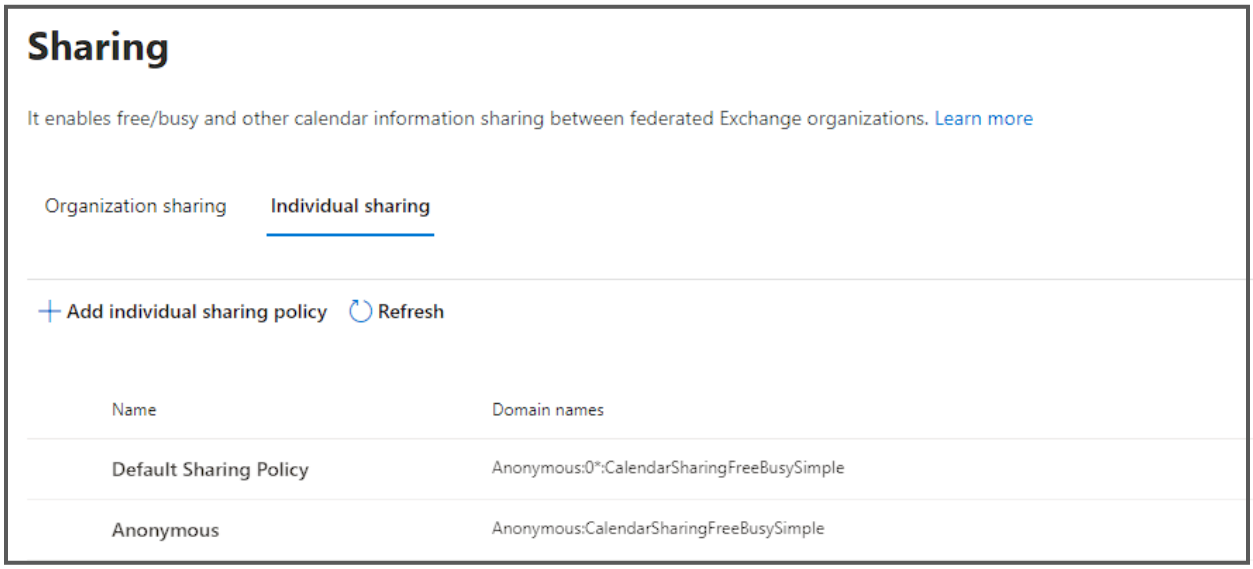

All services > Conditional Access | Policies >
Click2Run - Require MFA for All Users
Conditional Access policy
Delete
View policy information
Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies.
Learn more
Name *
Click2Run - Require MFA for All Users
Assignments
Users
All users
Target resources
All cloud apps
Conditions
0 conditions selected
Access controls
Grant
1 control selected
Session
0 controls selected
Control access based on who the policy will apply to, such as users and groups, workload identities, directory roles, or external guests.
Learn more
Include
Exclude
Select the users and groups to exempt from the policy
Guest or external users
Directory roles
Users and groups
Enable policy
Report-only
On
Off
Save

Organizational Settings Management

To modify the basic parameters of your organization in Microsoft 365, you must access the 365-administration panel. This is where you can make changes to various settings related to your organization's profile, policies, and overall structure.

[365 Administration Panel]





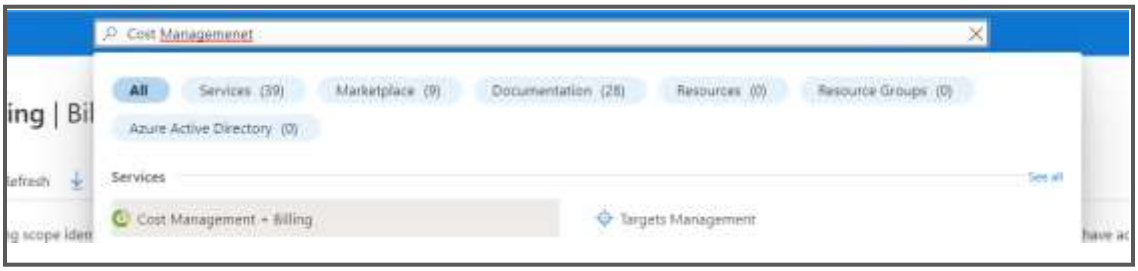
Data Compliance Management

To manage and adjust your organization's data compliance in Microsoft 365, you should use the Data Compliance Center. This tool allows you to manage regulations, set data governance and manage data protection in line with legal and policy requirements.

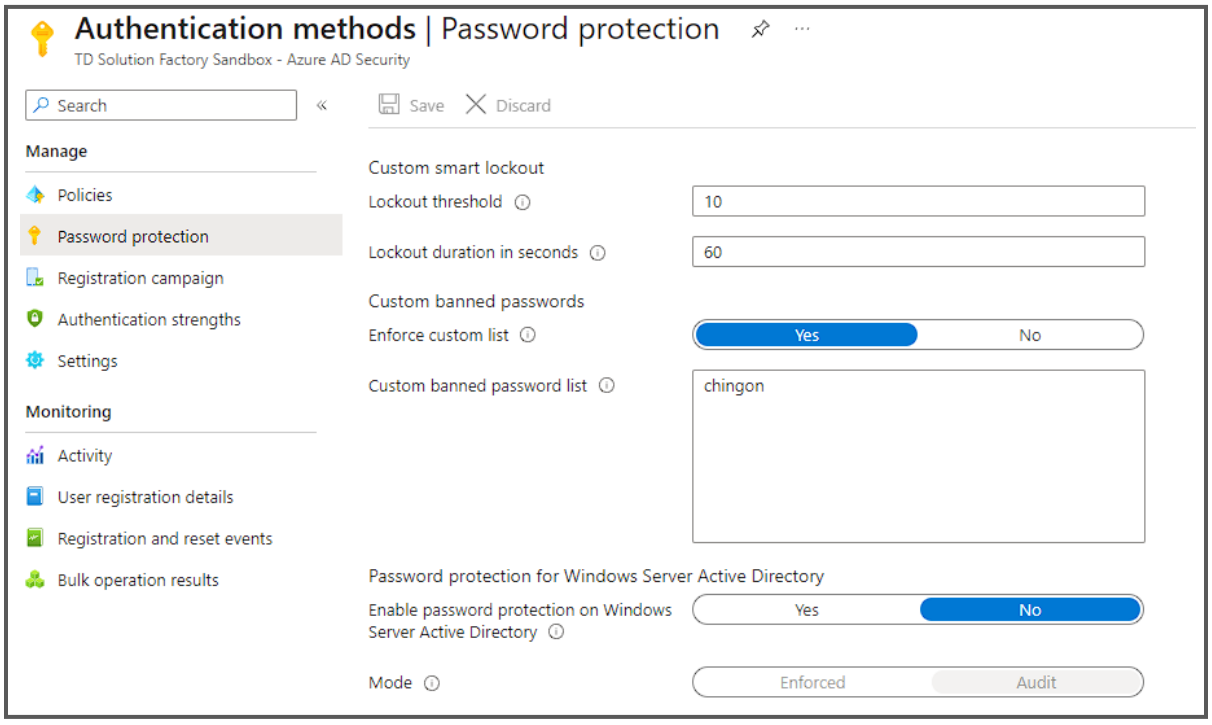
365 Data Compliance Center

Budget Management

In Cost Management you can manage the budget setting you created in the User Interface, you can add or delete recipients for budget alerts, you can also manage the budget thresholds.



To access Smart Lockout and on-premises Password Protection, type in the search box “Authentication Methods” and select “Password Protection”.



Custom smart lockout: You can modify parameters set on the Click-to-Run to allow maximum failed attempts on your tenant and lockout duration.

Password Protection for Windows Server: You can modify parameter for protection in On Premise environments. To allow password control on those systems a Microsoft Agent must be installed. Plan and deploy on-premises Azure Active Directory Password Protection Guide

Azure Policies Management

Azure Polices will be tagged as “Click2Run” remember Azure polices requires approximately 30 min. once the solution has been deployed to take effect.

To access Conditional Access policies type in the search box “Azure Policies” and select “Policy”.

Policies Created: you have options to review the policies that have been deployed with the Click-to-Run, to do this search for the category “Click2Run” in the definitions section.

Removing Assignment: In the Assignment section, you have the option to review the policies that are being assigned and you can remove it.

Adding Assignments: To create additional assignments, in the Definition section, select a policy, click on it and you will be able to check the configuration and assignments.

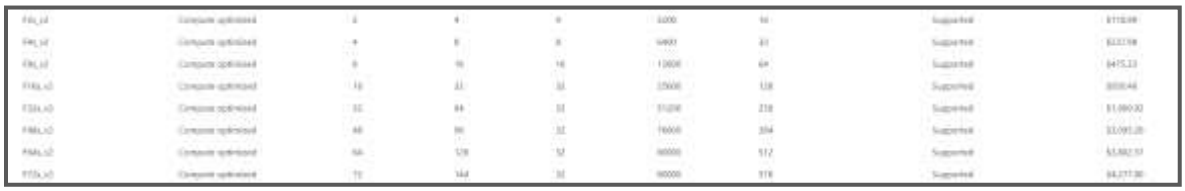
Actions: By default, all Azure Policies are being set as Deny, but “Deploy default Microsoft IaaSAntimalware extension for Windows Server” is not being assigned. Recommended scenario for this policy is set to “Remediate”,

however a managed identity is required to allow this policy to remediate existent VM (available on version 2).

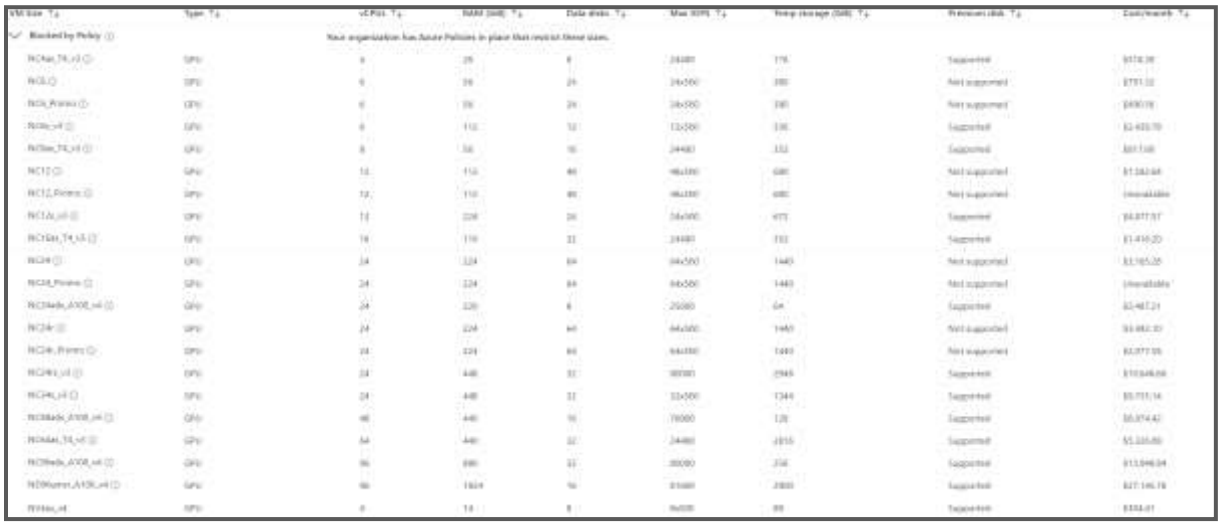
Please follow [Microsoft guide] to add a remediation task.

Index for High Performance Resource Groups

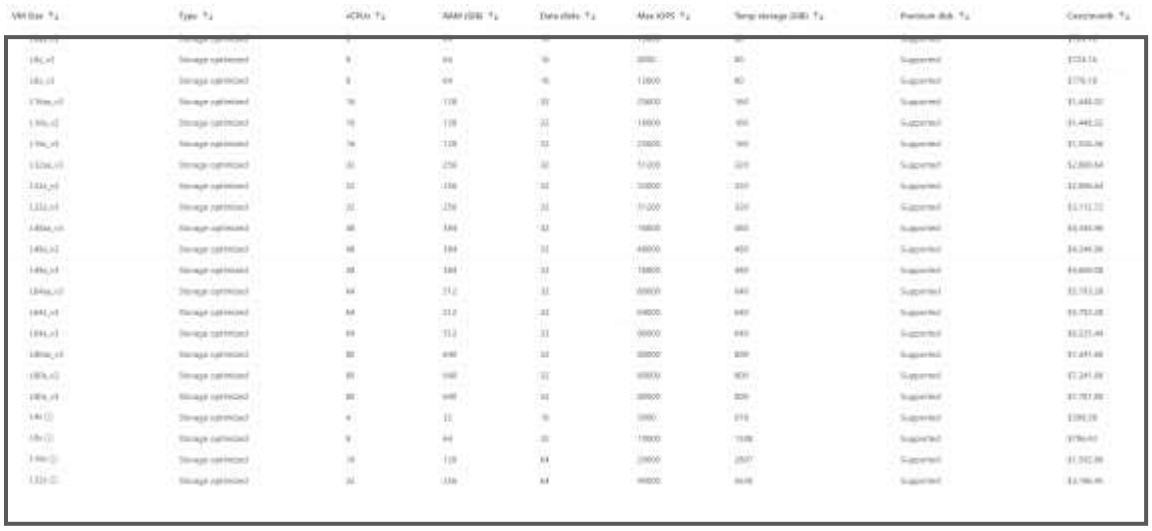
High Performance CPU: This policy will block VM families H_* and F_*



High Performance GPU: This Policy will block VM from families Nv_*, Nc_*, Nd_*.



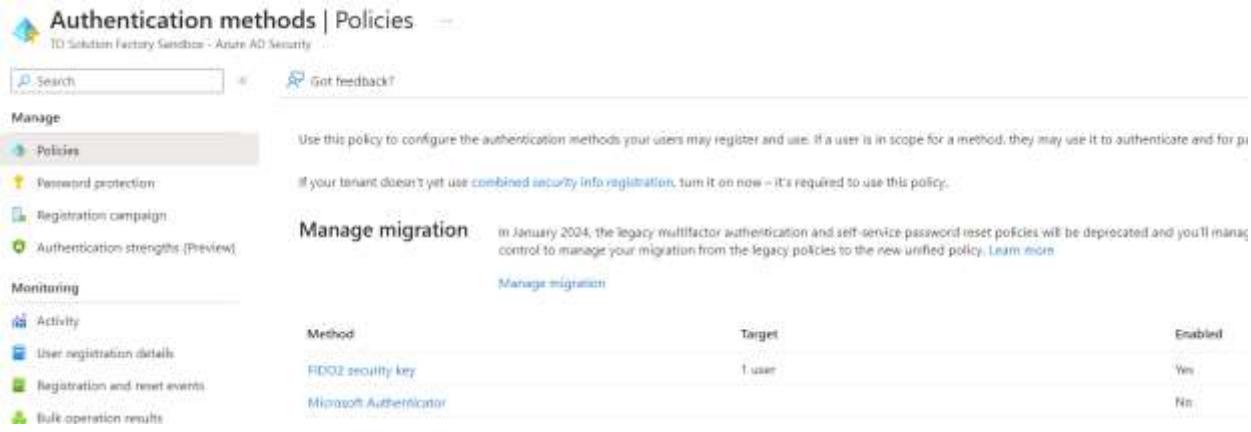
Storage Optimized: This Policy will block VM from Families LS_*



Authentication Management

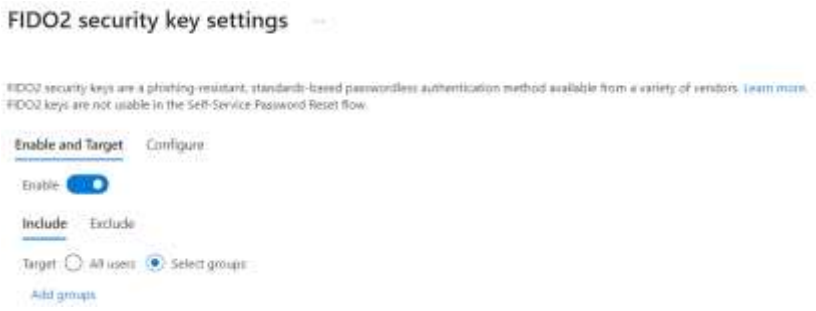
All these settings are being controlled under “Azure Active Directory\Security\Authentication Methods.” All features are built to affect all users. However, some of the options allow changing target and creating some exclusions.

To access Passwordless and Authenticator options, type in the search box “Authentication Methods” and select “Policies”.



Policies: You have different Methods available, select the one you want to change and click on the name.

This will allow you to change target, creation exclusion or modify parameters chosen on the deployment.

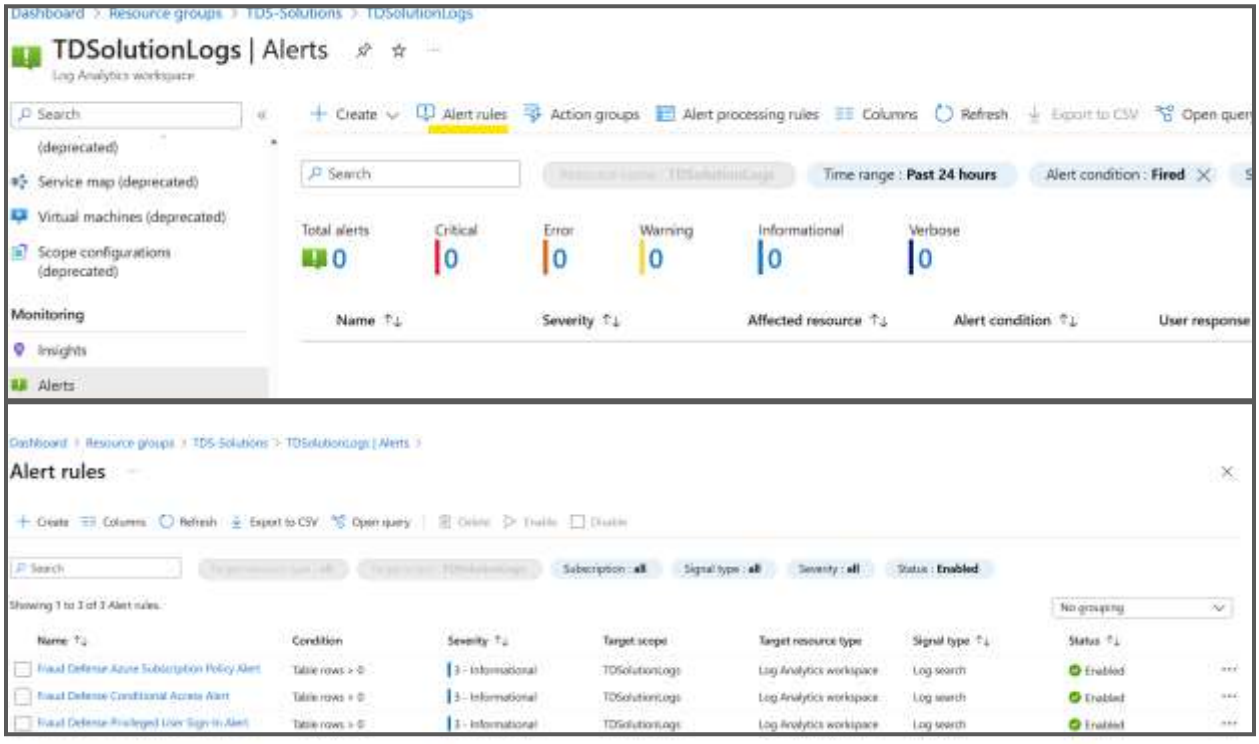


Monitoring Management

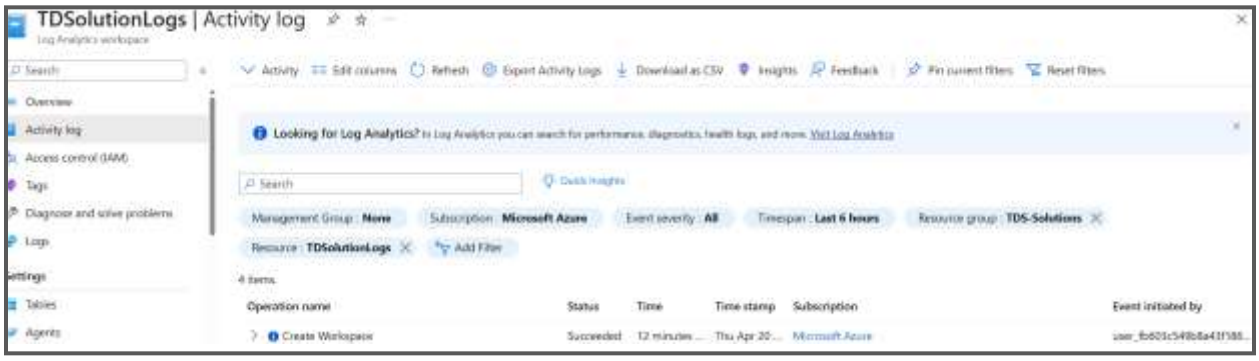
Monitor Option will create different types of Rules and Services under the Resource Group named “TDS-Solutions”. You can find Analytics workspace call “TDS-SolutionLogs” there.

To access Workspace, go to Resource Group, TDS-Solutions.

Alert Rules: On the Alert Section, we can check last trigger alerts as well as configured rules. To check rules (enable, disable, or modify), go to: “TDSolutionLogs|Alerts|Alert Rules”.



Audit Activity Logs: On the Logs Section, we can check last Activity Logs; go to "TDSolutionLogs|Activity log".



Usage and Cost: In the "Usage and estimated Cost" section you can monitor the usage and cost of a Log Analytics workspace. This tool provides real-time insights into the data ingestion and query performance of the workspace, as well as detailed cost analysis and budgeting tools. By monitoring usage and costs, you can optimize your Log Analytics workspace to ensure that it meets your needs while minimizing costs; go to "TDSolutionLogs|Settings|Usage and estimated Cost".

Troubleshooting

The following section compiles a list of error codes that may occur during the deployment of the solution for your investigation and resolution. It is recommended that the error code be provided to the support team to expedite the troubleshooting process and resolve the issue as swiftly as possible.

Please be assured that any potential errors that may arise can often be attributed to communication issues with the Microsoft API or conflicts within the existing configuration. It's important to note that under no circumstances will the solution result in any harm or loss of information within the target tenant. Our priority is to ensure a seamless experience while resolving any hitches that may arise.

Error Code List

Section	Feature	Error Code	Details
Security	Add Members to Group	1101.1	Failed to Create Trusted Location Group
Security	Add Members to Group	1101.2	Failed to Create Conditional Policy
Security	MFA for Users	1102	Failed to Create Conditional Policy
Security	MFA for Admins	1103	Failed to Create Conditional Policy
Security	MFA for Management	1104	Failed to Create Conditional Policy
Security	Risky Login	1105	Failed to Create Conditional Policy
Security	Block Legacy	1106	Failed to Create Conditional Policy
Security	Compliant for Admins	1107	Failed to Create Conditional Policy
Security	Compliant or MFA	1108	Failed to Create Conditional Policy
Security	Block Legacy for 365	1109	Failed to Create Conditional Policy
Security	MFA for 365 App	1110	Failed to Create Conditional Policy
Security	Compliant or MFA 365	1111	Failed to Create Conditional Policy
Security	Exclude Group	1112	Failed to Create Azure AD Group
M365	Check Service Principal	2200	Failed to Validate SP AppSMBFraud
M365	Set App Registration	2200.1	Failed to Create APP SMBFraudApp
M365	Set App Enterprise	2200.2	Failed to Register SMBFraudApp
M365	Client Forward Block	2201	Failed to execute Powershell Script
M365	Outbound Spam	2202	Failed to execute Powershell Script
M365	Anonymous Sharing	2203	Failed to execute Powershell Script

M365	Mailbox Audit	2204	Failed to execute Powershell Script
M365	DLP	2205	Failed to execute Powershell Script
M365	Safe Attachment	2206	Failed to execute Powershell Script
M365	Safe Link	2207	Failed to execute Powershell Script
Budget	Create Budget	3101	Failed to Create Budget
Policies	Define Restrict SKU CPU	4101	Failed to create Policy Definition
Policies	Assign Restrict SKU CPU	4101.1	Failed to assign Azure Policy
Policies	Define Restrict SKU GPU	4102	Failed to create Policy Definition
Policies	Assign Restrict SKU GPU	4102.1	Failed to assign Azure Policy
Policies	Define Restrict SKU DISK	4103	Failed to create Policy Definition
Policies	Assign Restrict SKU DISK	4103.1	Failed to assign Azure Policy
Policies	Define Limit Region	4104	Failed to create Policy Definition
Policies	Assign Limit Region	4104.1	Failed to assign Azure Policy
Policies	Define Deny All	4105	Failed to create Policy Definition
Policies	Assign Deny All	4105.1	Failed to assign Azure Policy
Policies	Enforce HTTPS	4106	Failed to create Policy Definition
Policies	Enforce HTTPS	4106.1	Failed to assign Azure Policy
Policies	IaaSAntimalware	4107	Failed to create Policy Definition
Policies	IaaSAntimalware	4107.1	Failed to assign Azure Policy
Authentication	Expiration Policy	5101	Failed to set Expiration config
Authentication	Smart Lockout	5102	Failed to set Smart Lockout Options
Authentication	MFA Settings	5203	Failed to configure MFA
Authentication	FIDO2 Settings	5204	Failed to configure FIDO2
Monitor	Create Alerts	6101	Failed to create Alerts
Monitor	Create Action Group	6102	Failed to Create Action Group
Monitor	Deploy LAW	6103	Failed to create LAW
Monitor	Deploy AzADDiag	6104	Failed to create Az AD logs
Monitor	Deploy AzDiag	6105	Failed to create AZ Diagnostic logs
Monitor	Create Query Alert	6106	Failed to create Alert Queries