

StreamOne® Security Operations (SecOps) Solution

User's Manual

Table of Contents

Solution Overview	4
What is StreamOne® Security Operations (SecOps) solution?	4
What are the key differentiators of the StreamOne® SecOps solution?	4
What is the goal of this guide?.....	5
Prerequisites	6
How to access to the SecOps Solution.....	9
1 st Time Access.....	10
Home Page	11
Home Page Widgets	11
Microsoft Secure Score	11
Risk Level.....	12
Top Critical Security Recommendations	13
High Risk Customers	13
Featured Applications	14
Azure Consumption	14
Customers	16
Customer Details > Overview	18
Widgets	18
Tenant Status and Availability	18
Risk Level.....	19
Microsoft Secure Score	19
Security Recommendations	19
Azure Consumption	19
Customer Details > Security Settings.....	20
Security Type	20
Manage Security Options.....	20
User Based Rules.....	22
Device Based Rules	23
Mail Based Rules	24
Exclusions	25

Conditional Access Policy Management: Post Deployment	26
Azure Budgets	28
Managing your Budget Management and Budget Threshold	28
Budget Alerts.....	29
Azure Policies	30
Azure Policies	30
Authentication.....	32
Authentication Methods.....	32
Password Settings	32
Smart Lockout Settings	33
MFA Settings	33
Password Less Settings	34
Customer Details > Recommended Products	35
Customer Details > Tenant Details	36
Customer Details > Deployment Log	37
Support.....	38

Solution Overview

What is StreamOne® Security Operations (SecOps) solution?

StreamOne® SecOps Solution is a centralized platform designed to offer a comprehensive, unified view of your Microsoft customers' security posture, helping to reduce their risk levels and standardize the deployment of security policies across your entire customer base. It also enables users and organizations to leverage third-party product recommendations, making it easier to address security gaps and enhance overall protection.

This 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 policies, and set budgets within Azure Cost Management.

What are the key differentiators of the StreamOne® SecOps solution?

- Provide a single, centralized, end-to-end solution that integrates all security dashboards, settings and metrics creating a comprehensive security view of your entire customer base
- Standardize the way to apply customer's security settings by reducing the time and effort to handle threats and improve customer's security posture
- Prioritize high-risk customers, allowing users to focus on critical threats and recommended actions
- Offer real-time dashboards that provide actionable insights into security posture, threat trends, and operational metrics
- Scalable and flexible solution that provides a cost-effective solution for SMBs, ensuring it grows with partner and customer's needs and can adapt to changes in the security landscape
- Save time and resources by simplifying the process of maintaining compliance with security policies
- Intuitive and easy-to-use interface tailored to the workflows of security teams which reduces the learning curve to use the portal more effectively
- Leverage our digital upsell mechanisms and recommended products engine


What is the goal of this guide?

This guide is designed to provide users with help to successfully use the SecOps Solution through StreamOne platform.

Prerequisites

In order to pull data from the customers, a GDAP Relationship between the partner and the customer is required. This GDAP relationship needs to include at least the **Cloud Application Administrator role**.

Please make sure that this relationship exists and is approved by the customer. Otherwise, it will not be possible to pull data from that customer and it will be excluded from the aggregated data view.

 Dashboard data is incomplete due to restricted access for 1 of 9 customers. [\(hide details\)](#)
To resolve, establish a GDAP Relationship with the **Cloud Application Administrator** role from **StreamOne**.

- ▶ [Show impacted customers](#)
- ▶ [Dismiss this warning](#)

Here you can find how to request a new GDAP relationship for a given customer:

- For StreamOne ION users, you need to request a GDAP Relationship with **Recommended Access**. [Click here to see how to request it.](#)

INITIATE GDAP REQUEST

Permission Set

Select a permission set below. Regardless of permission level, the GDAP request will be sent for 2 years duration.

☐ Limited Access | GDAP Link Absolute Minimum

- Directory Reader
- Service Support Administrator

☒ Recommended Access | GDAP Link Primary

- Cloud Application Administrator
- Intune Administrator
- License Administrator
- Security Reader
- Helpdesk Administrator
- Privileged Authentication Administrator
- Directory Reader
- Password Administrator
- Billing Administrator
- Service Support Administrator
- Global Reader
- User Administrator

- For StreamOne Stellr users, you need to request a GDAP Relationship with **Recommended Access** or one with **Custom Access** that includes at least the **Cloud Application Administrator role** in it. [Click here to see how to request it.](#)

Request New GDAP Relationship
Cancel
Send request to customer
×

A GDAP relationship may take about 20 minutes to take effect after a customer approved.

Customer Name:
Alyssa Demo April 2021

Admin Relationship Name:
GDAPS-281aa819-47f6-45cd-beb4-2472f8c4c443-063835

*** Duration in days:**

*** Allows platform to perform functions:**

☐ GDAP Limited Access

☒ GDAP Recommended Access

- Global Reader
- Cloud Application Administrator
- Helpdesk Administrator
- Privileged Authentication Administrator
- Billing Administrator
- License Administrator
- User Administrator
- Intune Administrator
- Security Administrator
- Service Support Administrator
- Password Administrator
- Directory Readers

☐ GDAP Custom Access

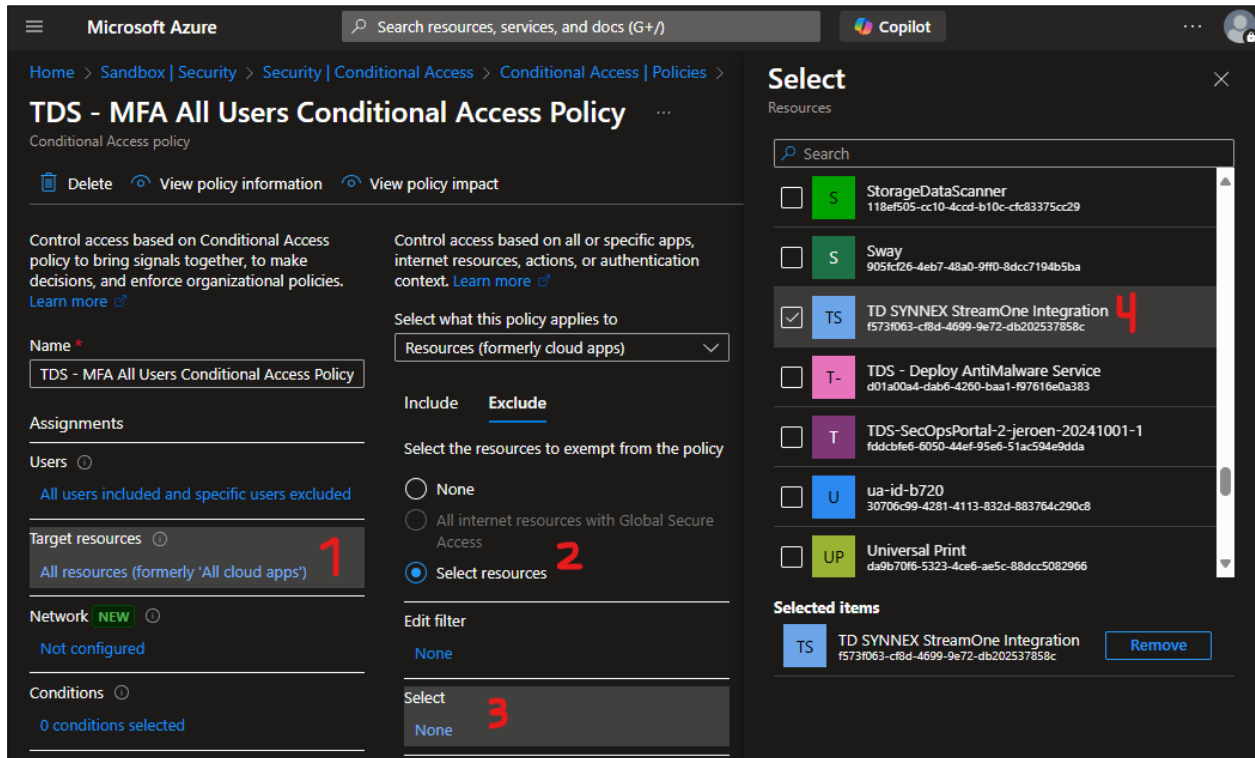
*** Email to:**

Email cc:

Also, please make sure that there is no Conditional Access policy blocking the access to the TD SYNnex StreamOne application (Service Principal) installed in the customer's tenant. You can add an exception in the policy to exclude it. [Open the Conditional Access Policy](#) and follow these steps:

1. Click on **Target Resources**
2. Select resources
3. None
4. Find the **TD SYNnex StreamOne Integration** resource and select it
5. Save

- The next daily synchronization should now be able to connect and pull data from the customer.



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

Home > Sandbox | Security > Security | Conditional Access > Conditional Access | Policies >

TDS - MFA All Users Conditional Access Policy

Conditional Access policy

Delete View policy information View policy impact

Control access based on Conditional Access policy to bring signals together, to make decisions, and enforce organizational policies. [Learn more](#)

Control access based on all or specific apps, internet resources, actions, or authentication context. [Learn more](#)

Select what this policy applies to

Name *
TDS - MFA All Users Conditional Access Policy

Assignments

Users
All users included and specific users excluded

Target resources
All resources (formerly 'All cloud apps') **1**

Network **NEW**
Not configured

Conditions
0 conditions selected

Include **Exclude**

Select the resources to exempt from the policy

☐ None
☐ All internet resources with Global Secure Access
☒ Select resources **2**

Edit filter
None

Select **3**
None

Select

Resources

Search

- ☐ **S** StorageDataScanner 118ef505-cc10-4ccd-b10c-cfc83375cc29
- ☐ **S** Sway 9051c226-4eb7-48a0-9ff0-8dcc7194b5ba
- ☒ **TS** TD SYNnex StreamOne Integration f573f063-cf8d-4699-9e72-db202537858c **4**
- ☐ **T-** TDS - Deploy AntiMalware Service d01a00a4-dab6-4260-baa1-f97616e0a383
- ☐ **T** TDS-SecOpsPortal-2-jeroen-20241001-1 fddcbfe6-6050-44ef-95e6-51ac594e9dda
- ☐ **U** ua-id-b720 30706c99-4281-4113-832d-883764c290c8
- ☐ **UP** Universal Print da9b70f6-5323-4ce6-ae5c-88dcc5082966

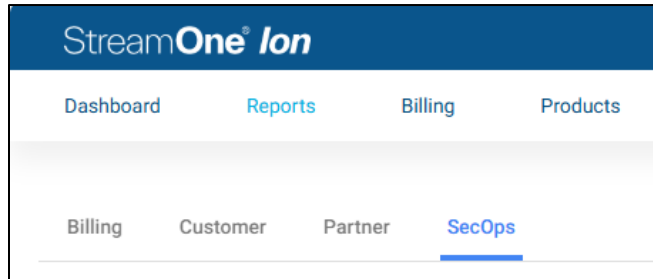
Selected items

TS TD SYNnex StreamOne Integration f573f063-cf8d-4699-9e72-db202537858c [Remove](#)

How to access to the SecOps Solution

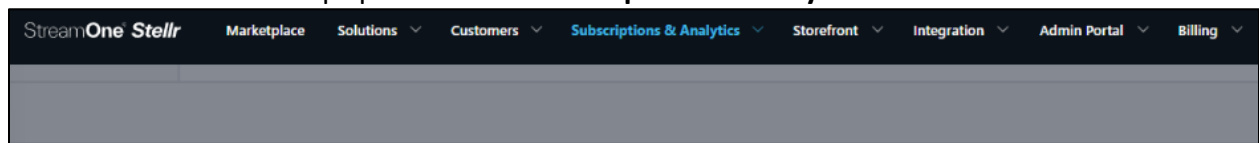
StreamOne ION

You can access the SecOps portal under **Reports > SecOps**



StreamOne Stellr

You can access the SecOps portal under **Subscriptions & Analytics**



Contact your TD SYNnex representative to know more about this program and how to participate.

1st Time Access

When accessing for the first time, you need to accept the Terms & Conditions. This banner will appear. Please read the Terms & Conditions and when you are done click Accept:


Terms & Conditions Agreement

By clicking "Accept", you agree to our Terms and Conditions. Please read them carefully before using our website.

Your continued use of this site constitutes your agreement to be bound by these terms. If you do not agree, please do not use our website.

[See Terms & Conditions](#)

Once accepted, if the reseller has not been used in the SecOps portal yet (so you are the first user under that reseller to access the SecOps portal), a wizard to start importing data will show up, indicating how many customers were found under your reseller:



Welcome to SecOps

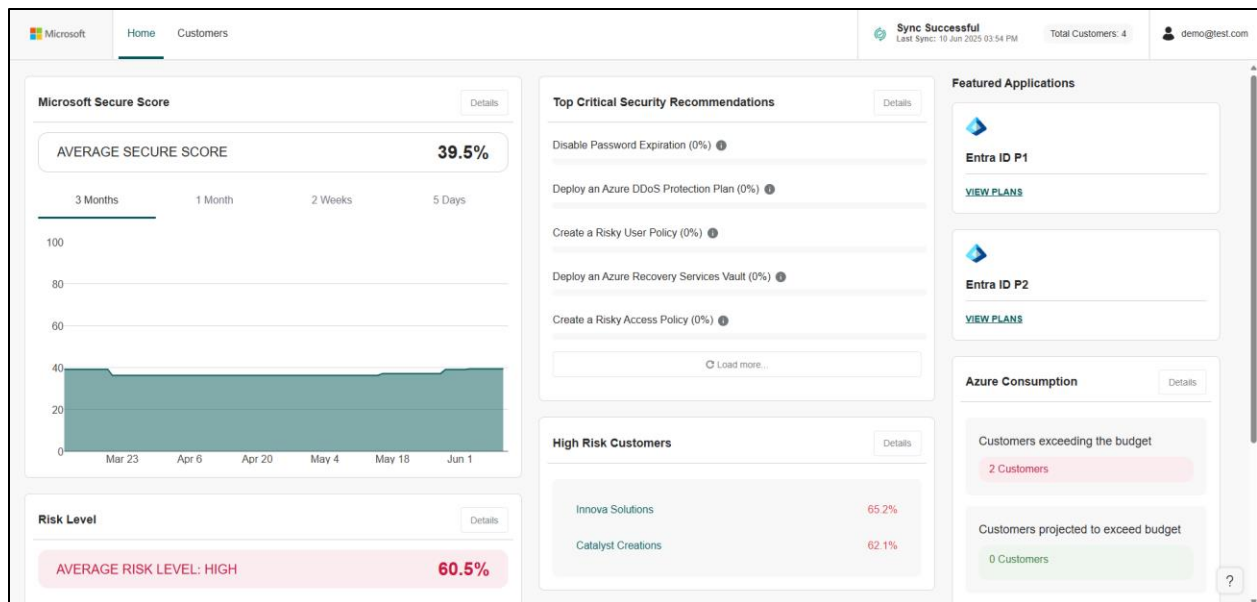
We found 139 customers. Click 'Proceed' to sync their information with the portal.

Clicking PROCEED will start the import process of all the customers data (depending on the number of customers and other aspects of your customers this process can take more or less time). Once the import process reaches 100% you will be able to close the wizard and you will be redirected to the home page with all the data already loaded.

Home Page

Leverage our aggregated security dashboards to monitor your overall security posture through a single interface.

This is displayed as default when you access the portal. It contains aggregated data from all the users so you can easily analyze the overall security by looking at the different widgets. The data represented in this page is refreshed automatically on a daily basis.

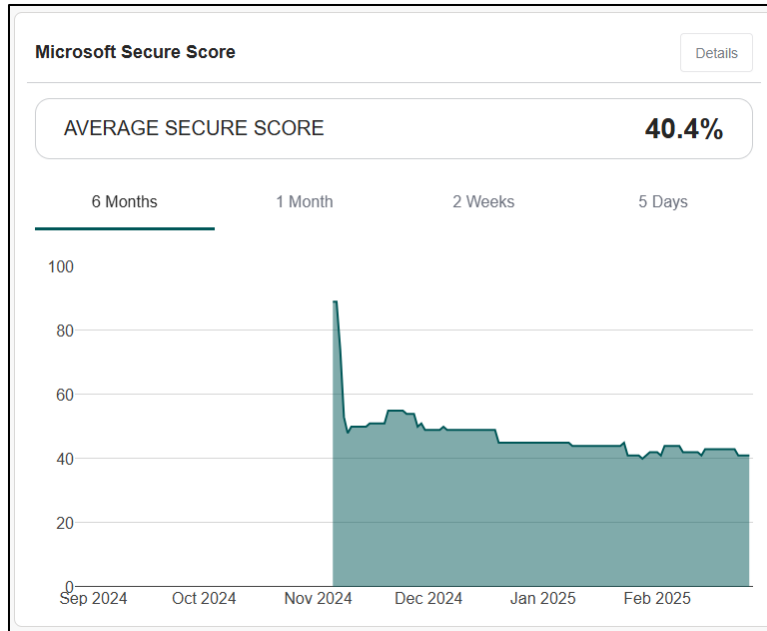


Home Page Widgets

Microsoft Secure Score

This section shows the average Microsoft Secure Score of all your customers. Microsoft Secure Score is a measurement of an organization's security posture, with a higher number indicating more recommended actions taken. It includes Secure Score for Identity, for Apps and for Data.

The graph displayed below shows the historical value of the aggregated Microsoft Secure Score over time. You can use different views in the graph by selecting a different range of time: 6 months, 1 month, 2 weeks or 5 days.



Risk Level

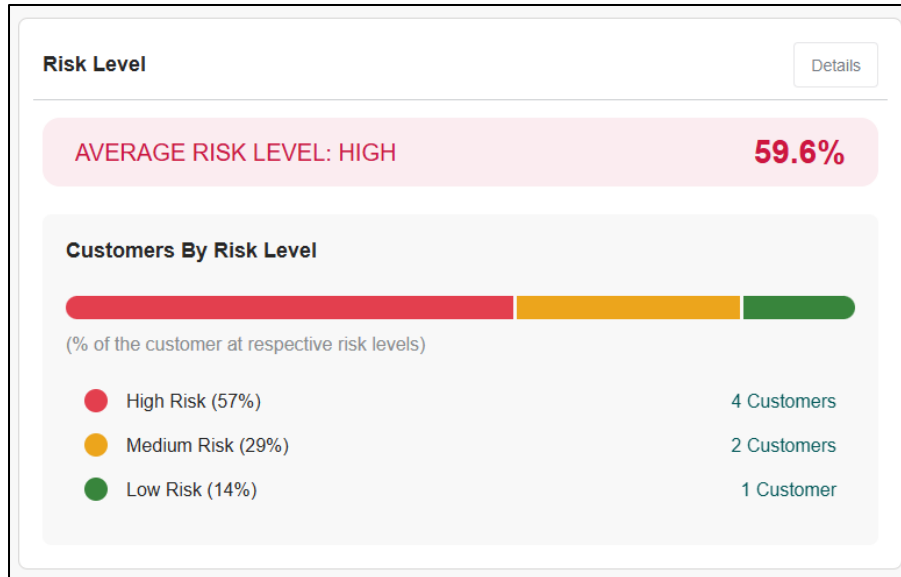
This section shows the average Risk Level of all your customers.

Risk level for a given customer is currently calculated as follows: 100% minus the Microsoft Secure Score. This means that the more % of risk level, the higher the risk.

Each risk level is measured as follows:

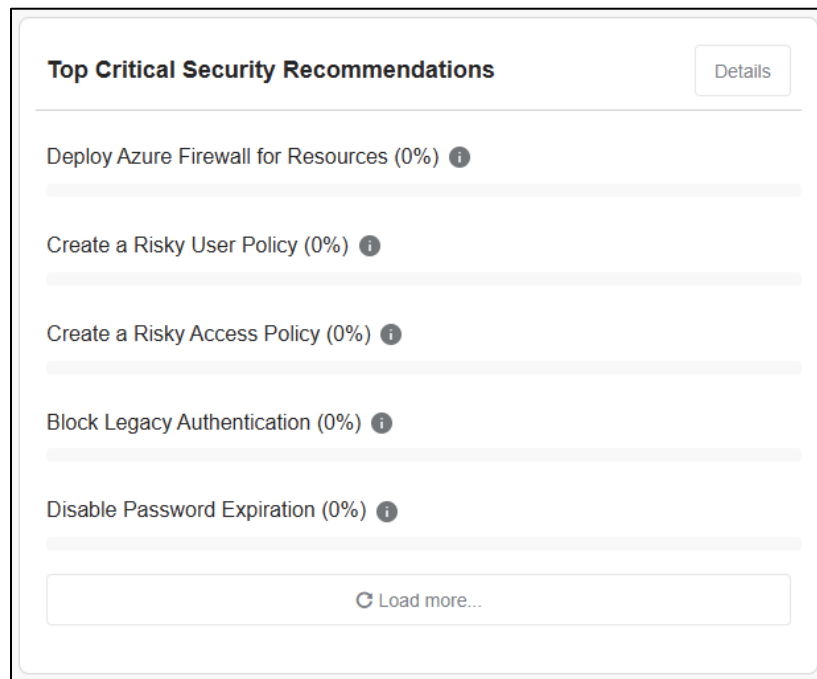
- Low: 0% to 39%
- Medium: 40% to 59%
- High: 60% to 100%

You have the option to click on the number of customers for each risk level so you can see the list of customers filtered by that risk level.



Top Critical Security Recommendations

In this section are listed all the security recommendations as an average of all your customers.



High Risk Customers



In this section the most critical customers are listed based on their risk level. Only those that are marked with a high Risk Level are listed.

The box will be empty if no high risk customers were found.

High Risk Customers		Details
Novant Inc	77.3%	
Catalyst Creations	73.2%	
Fadel LLC	72.5%	
Zemlak Inc	65.2%	

Featured Applications

A couple of recommended security applications are displayed with the option to view their plans for purchasing them.

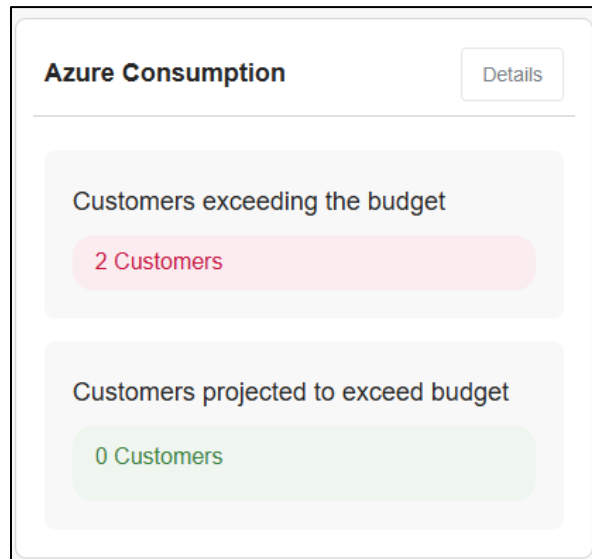
Featured Applications	
	Fortinet FortiAuthenticator ID Access Management VIEW PLANS
	AuthN SSO - phish-proof MFA VIEW PLANS

Azure Consumption

This section shows following information:

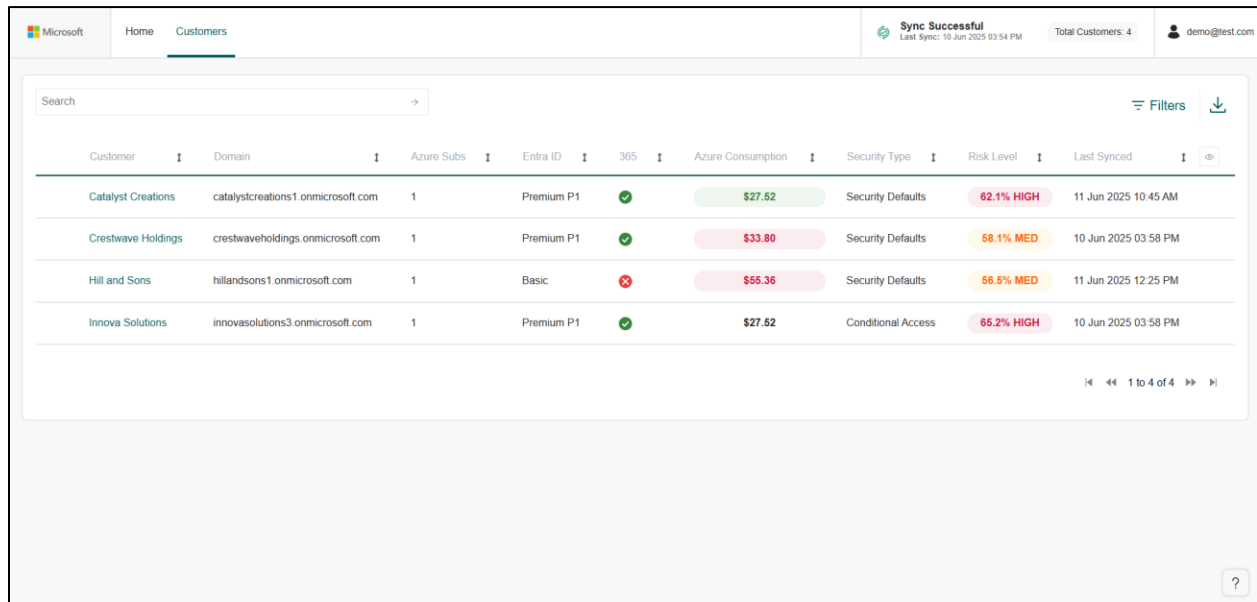
- Number of customers that have at least an Azure Subscription that is exceeding at least one budget.

- Number of customers that have at least an Azure Subscription that is exceeding at least one forecasted budget.



Customers

Monitor your customer's risk exposure through actionable insights. Prioritize high-risk customers, allowing users to focus on critical threats. Same as for the Home page, the data displayed here is automatically refreshed on a daily basis.



Customer	Domain	Azure Subs	Entra ID	365	Azure Consumption	Security Type	Risk Level	Last Synced
Catalyst Creations	catalystcreations1.onmicrosoft.com	1	Premium P1	✓	\$27.52	Security Defaults	62.1% HIGH	11 Jun 2025 10:45 AM
Crestwave Holdings	crestwaveholdings.onmicrosoft.com	1	Premium P1	✓	\$33.80	Security Defaults	68.1% MED	10 Jun 2025 03:58 PM
Hill and Sons	hillandsons1.onmicrosoft.com	1	Basic	✗	\$55.36	Security Defaults	66.6% MED	11 Jun 2025 12:25 PM
Innova Solutions	innovasolutions3.onmicrosoft.com	1	Premium P1	✓	\$27.52	Conditional Access	66.2% HIGH	10 Jun 2025 03:58 PM

For each of them, it shows the following information:

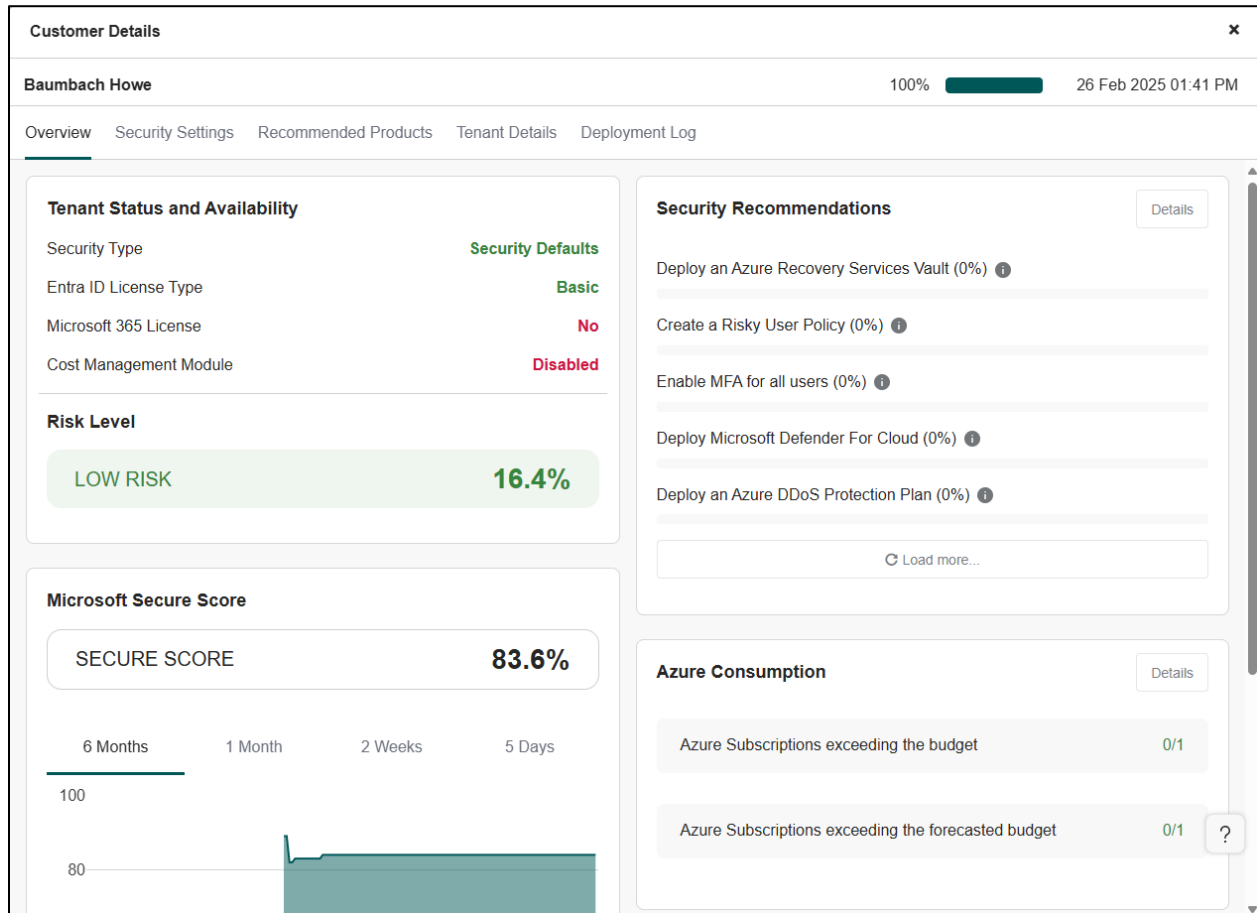
- Customer: customer's name
- Domain: customer's tenant domain name
- Azure Subs: total number of active Azure Subscriptions
- Entra ID: type of Entra ID license. Possible values: Basic/Free, Premium P1, Premium P2
- 365: Active when the tenant has at least one 365 license
- Azure Consumption: accumulated consumption of all the customer's Azure Subscriptions for the current month.
- Security Type: it represents what type of security is currently in place. Possible values:
 - No Security: Customer is not using Security Defaults and has no Conditional Access policy.
 - Security Defaults: Security Defaults is currently enabled.
 - Conditional Access: Customer has at least 1 Conditional Access policy in place. Conditional Access is a feature that is only available for customers with a premium P1 or P2 license.
 - Retrieval Error: there is no connectivity with the customer. In many cases, it can be fixed request a new GDAP relationship and making sure it gets approved.

- Risk Level: it represents the % risk level which is calculated as the opposite of the Microsoft Secure Score, so $100\% - \text{Microsoft Secure Score}$. A high risk level will be obtained when the Microsoft Secure Score is low and vice versa.
- Top Threats: list with all the potential security threats that the customer could have.
- Last Synched: date of the last time that the data was refreshed for that customer (it should not be more than 24 hours since it is automatically refreshed on a daily basis).

Customer Details > Overview

Get an extensive view of your customer's security posture, risk level, tenant status and security threats

By clicking any of the customers either in the home page or customer list you will get individual details of that particular customer as displayed in the screenshot below.



Widgets

Tenant Status and Availability

- Security Type (No Security, Security Defaults or Conditional Access)
- Entra ID License Type (Basic/Free, Premium P1, Premium P2)
- Microsoft 365 License: Yes/No

Risk Level

It represents the % risk level which is calculated as the opposite of the Microsoft Secure Score, so $100\% - \text{Microsoft Secure Score}$. A high risk level will be obtained when the Microsoft Secure Score is low and vice versa.

Microsoft Secure Score

It displays the historical value of the customer's Microsoft Secure Score over time.

Security Recommendations

It is a list of different security recommendations that are intended to help increase customer's security posture. The progress bar and % represents what is the achievement of that recommendation for the customer. For example, "Enable MFA for all users" at 60% means that 60% of your customers have MFA and 40% don't.

Click on the info icon to get more details about each recommendation.

Azure Consumption

It displays how many Azure Subscriptions are exceeding the budget and the forecasted budget. In case a given subscription has more than one configured budget, the one with the lowest value is used for the calculation.

Customer Details > Security Settings

In this section, we will cover the Security Settings, how to configure them and what they do.

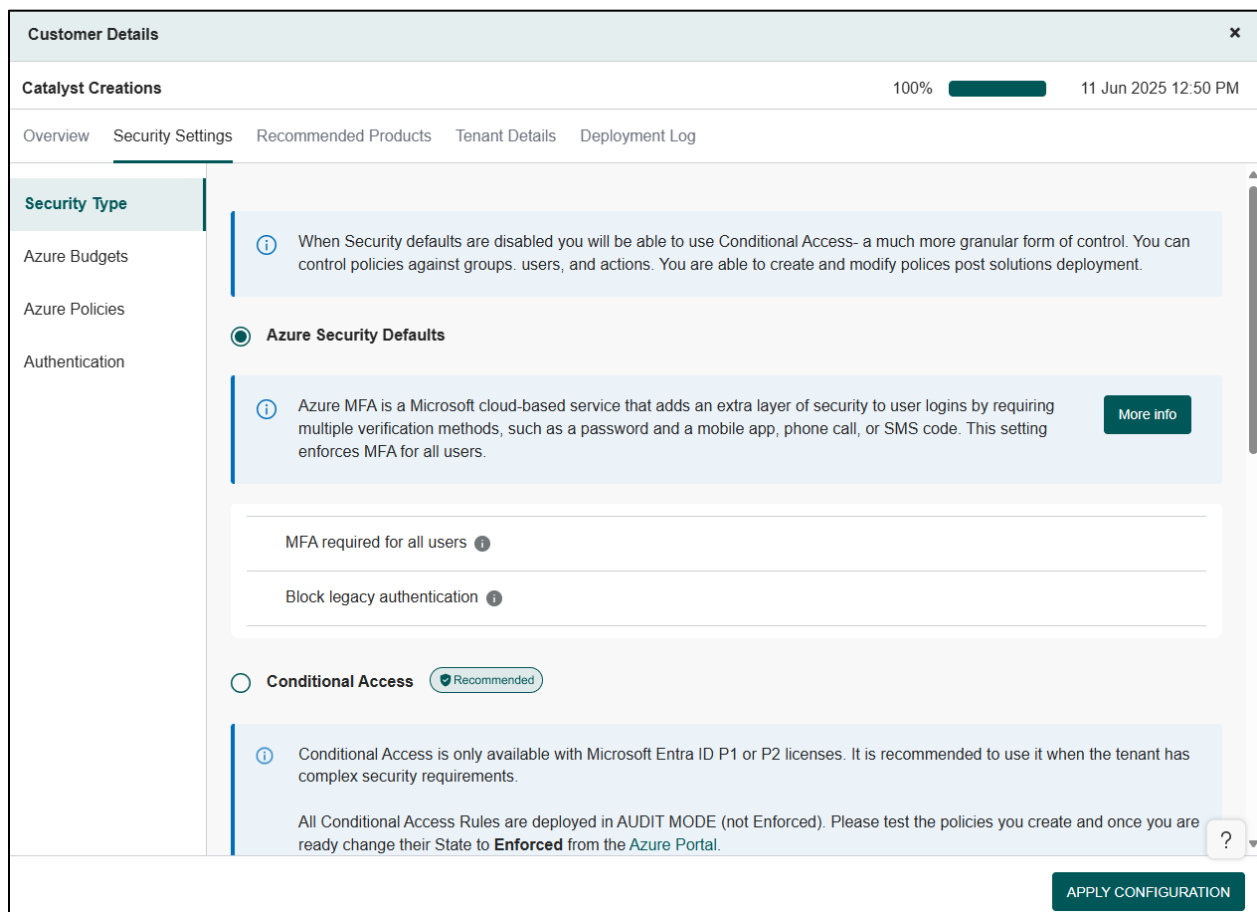
Standardize the way to apply customer's security policies and settings by reducing the time and effort to handle threats and improve customer's security posture

Please keep in mind that once you are done configuring, you need to click on the button to **"Apply configuration"**.

Security Type

Manage Security Options

This 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.



Customer Details [Close]

Catalyst Creations 100% [Progress Bar] 11 Jun 2025 12:50 PM

Overview **Security Settings** Recommended Products Tenant Details Deployment Log

Security Type

- Azure Budgets
- Azure Policies
- Authentication

Azure Security Defaults

When Security defaults are disabled you will be able to use Conditional Access- a much more granular form of control. You can control policies against groups, users, and actions. You are able to create and modify policies post solutions deployment.

Azure MFA is a Microsoft cloud-based service that adds an extra layer of security to user logins by requiring multiple verification methods, such as a password and a mobile app, phone call, or SMS code. This setting enforces MFA for all users. [More info](#)

MFA required for all users ⓘ

Block legacy authentication ⓘ

Conditional Access Recommended

Conditional Access is only available with Microsoft Entra ID P1 or P2 licenses. It is recommended to use it when the tenant has complex security requirements.

All Conditional Access Rules are deployed in AUDIT MODE (not Enforced). Please test the policies you create and once you are ready change their State to **Enforced** from the [Azure Portal](#). ⓘ

APPLY CONFIGURATION

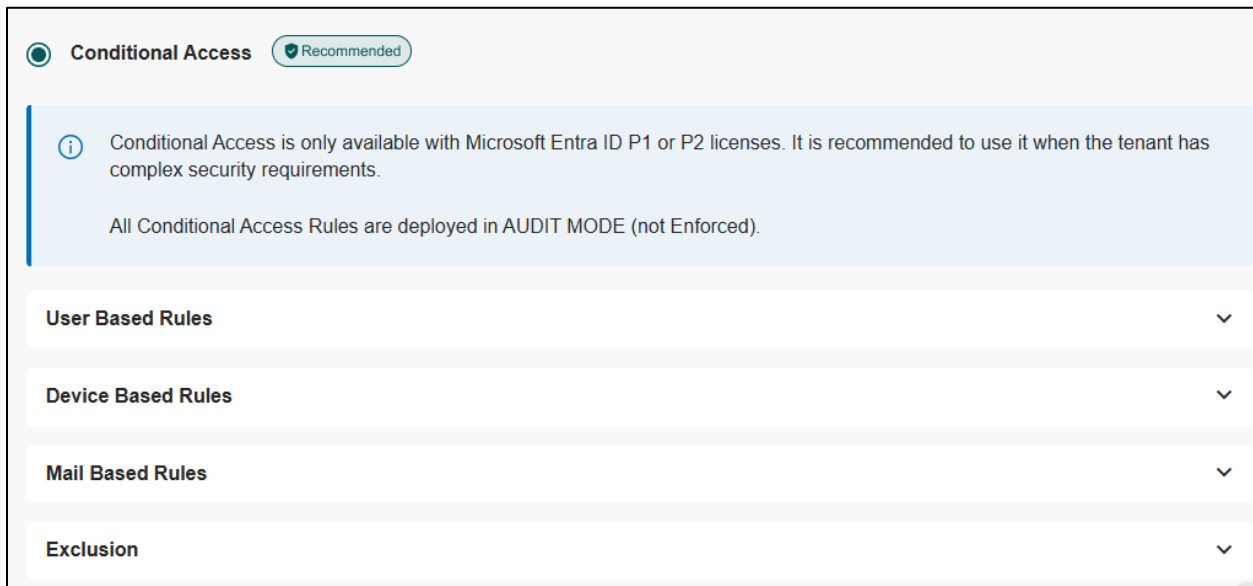
Azure Security Defaults is a set of basic security settings that help protect organizations from common threats. They include requiring multi-factor authentication (MFA) for all users, blocking

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.

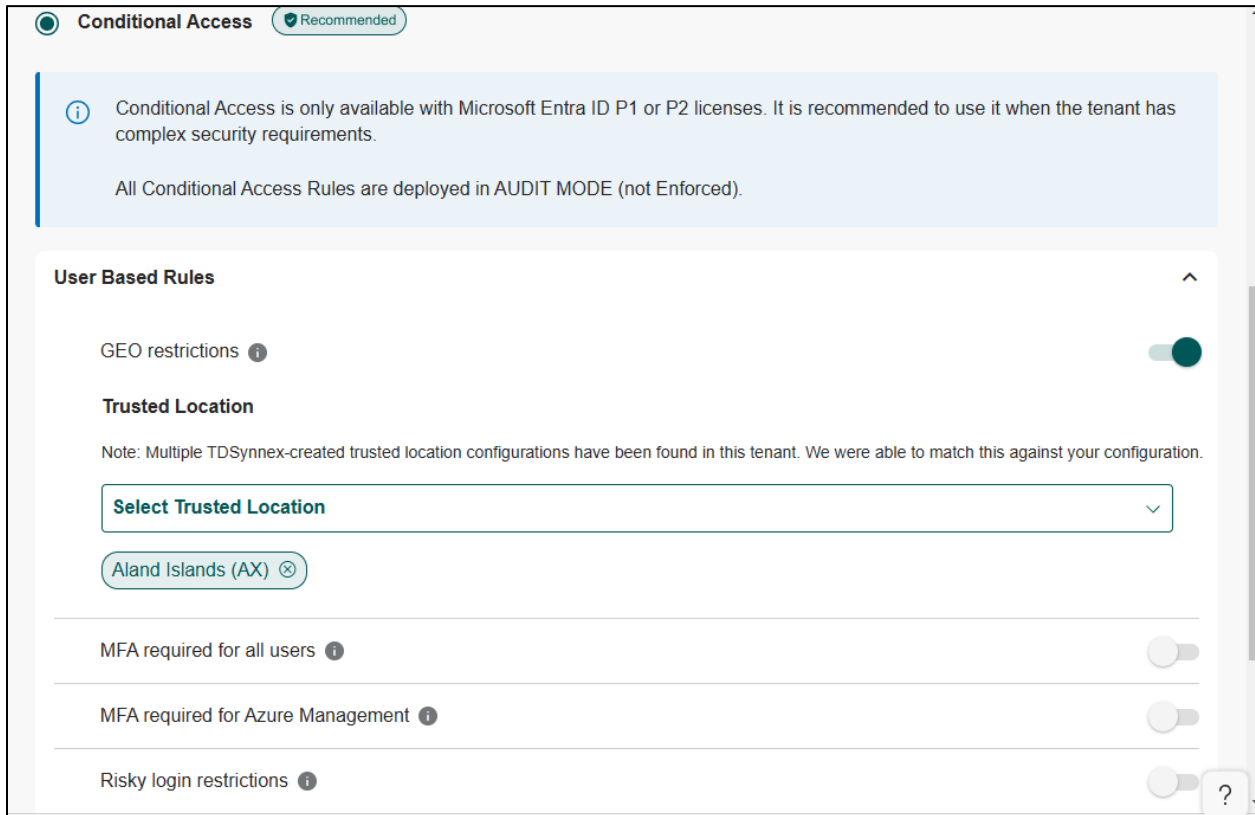
All our Conditional Access Policies are created in Audit Mode and are not enforced.

Signals that are included in this version include three categories User based rules, Device based rules and Mail based rules:



The screenshot shows the Microsoft Conditional Access console. At the top, there is a header with a green circle icon, the text "Conditional Access", and a "Recommended" badge. Below the header, a light blue box contains an information icon and text stating: "Conditional Access is only available with Microsoft Entra ID P1 or P2 licenses. It is recommended to use it when the tenant has complex security requirements." Below this, another line of text says: "All Conditional Access Rules are deployed in AUDIT MODE (not Enforced)." At the bottom, there is a list of four categories, each with a dropdown arrow: "User Based Rules", "Device Based Rules", "Mail Based Rules", and "Exclusion".

User Based Rules



Geo Restrictions, toggle this option allows 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](#)

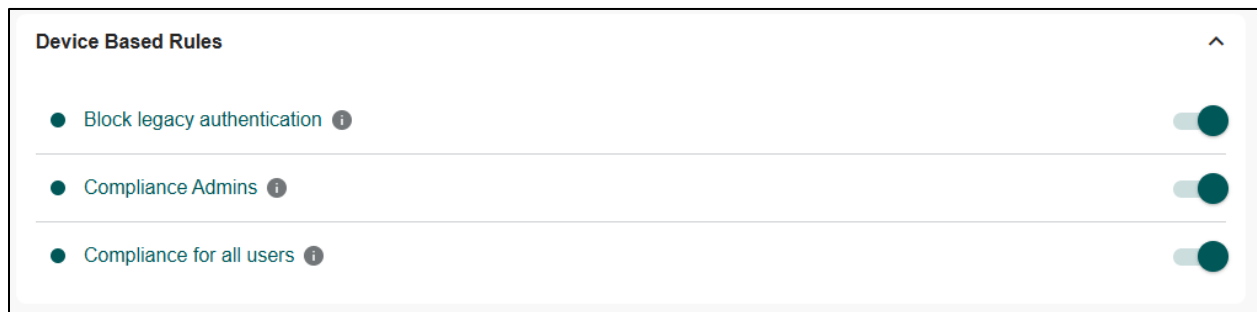
MFA for Azure Management, toggle this option to enforce MFA for Azure Management. This means users who are looking to make any changes in Azure, for example, creating or deleting a new resource group, then MFA would be required for this.

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 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](#)

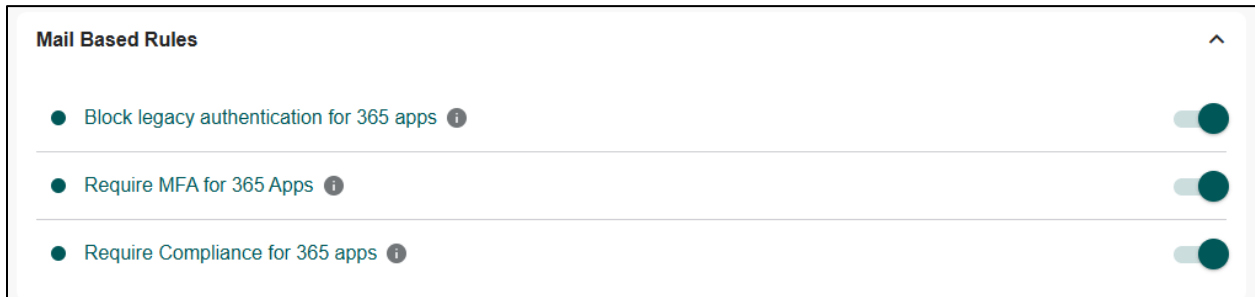
Require compliant or Hybrid Azure AD joined device for Admins, accounts with administrative rights are targeted by attackers. Requiring Admins with these highly privileged rights to perform actions from devices marked as compliant or hybrid Azure AD joined can help limit possible exposure.

Link to Microsoft Docs for more information [Require administrators to 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



Mail Based Rules	
● Block legacy authentication for 365 apps ⓘ	<input checked="" type="checkbox"/>
● Require MFA for 365 Apps ⓘ	<input checked="" type="checkbox"/>
● Require Compliance for 365 apps ⓘ	<input checked="" type="checkbox"/>

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.

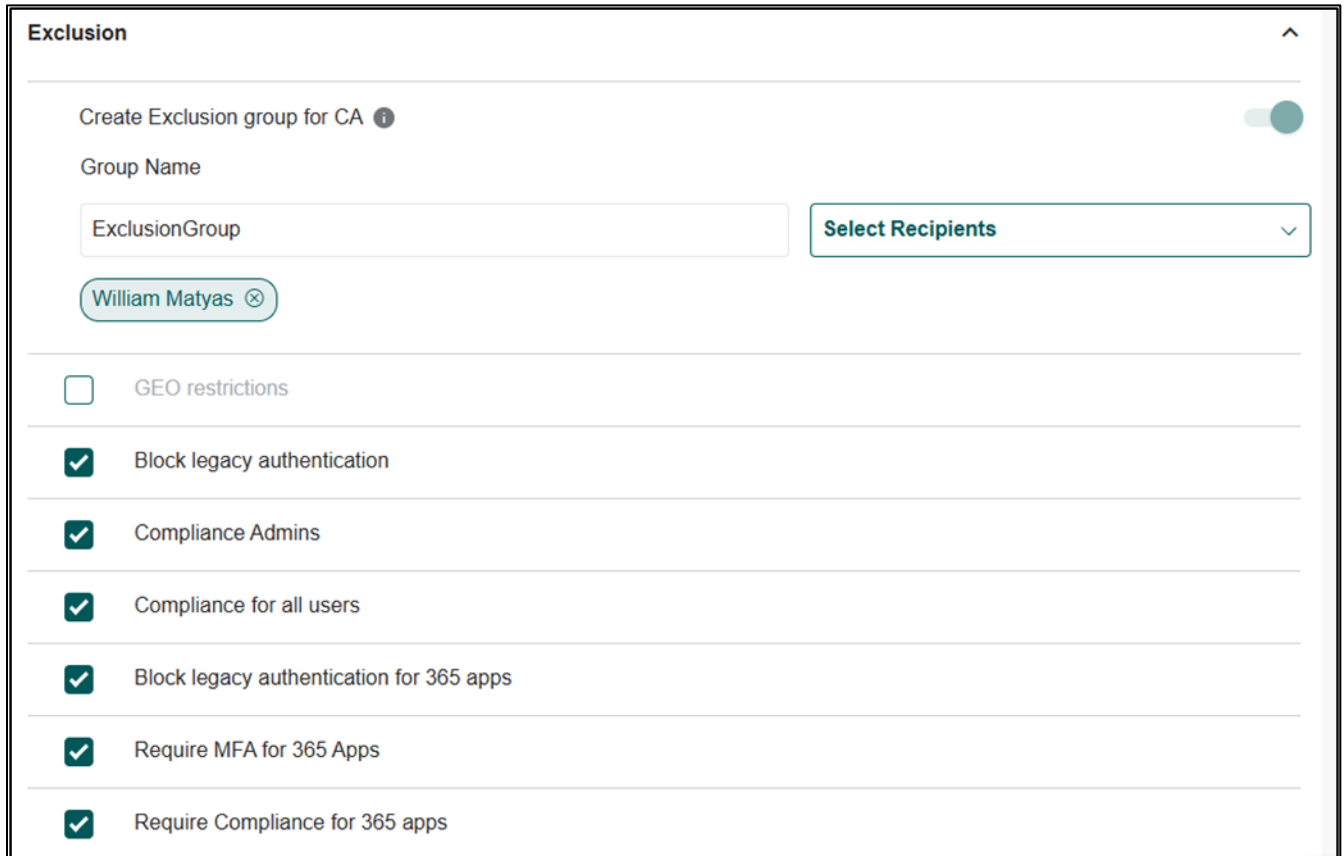
Link to Microsoft Docs for more information [Require administrators to use compliant or hybrid joined devices - Azure Active Directory - Microsoft Entra | Microsoft Learn](#)

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 to the selected policies.



The screenshot shows the 'Exclusion' configuration page in the Azure portal. At the top, there's a toggle for 'Create Exclusion group for CA' which is turned on. Below this, the 'Group Name' field contains 'ExclusionGroup'. To the right of the text input is a 'Select Recipients' button with a dropdown arrow. Below the text input, a tag for 'William Matyas' with a close icon is visible. A list of settings follows, each with a checkbox: 'GEO restrictions' (unchecked), 'Block legacy authentication' (checked), 'Compliance Admins' (checked), 'Compliance for all users' (checked), 'Block legacy authentication for 365 apps' (checked), 'Require MFA for 365 Apps' (checked), and 'Require Compliance for 365 apps' (checked).

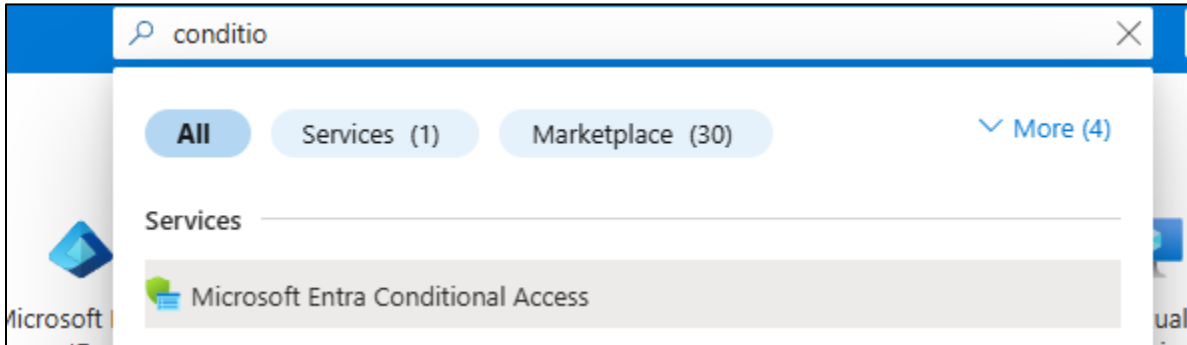
Group Name; Select a name for the Azure AD Group.

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

You can then 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).

Conditional Access Policy Management: Post Deployment

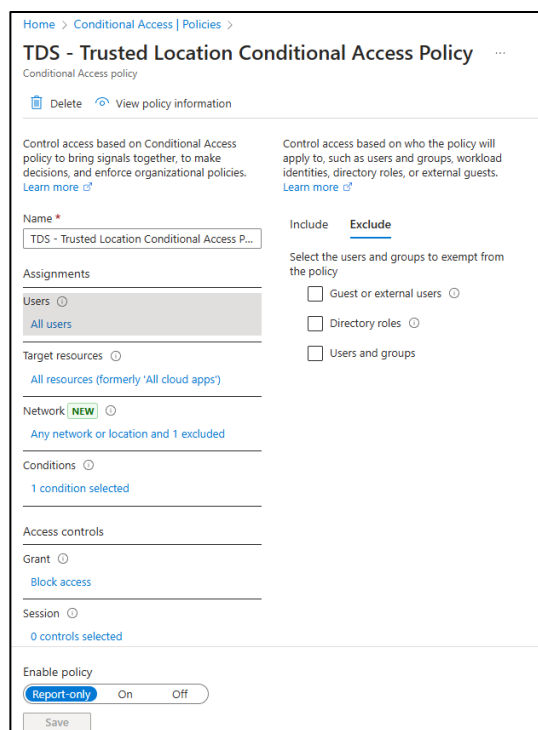
All Conditional Access Policies will be enabled as Report Only. This means Policy will only record which user-devices do not meet the requirements of the policy. Changing the policy to **YES**, once the solution has been deployed is recommended, please be aware that you would need to check the users'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



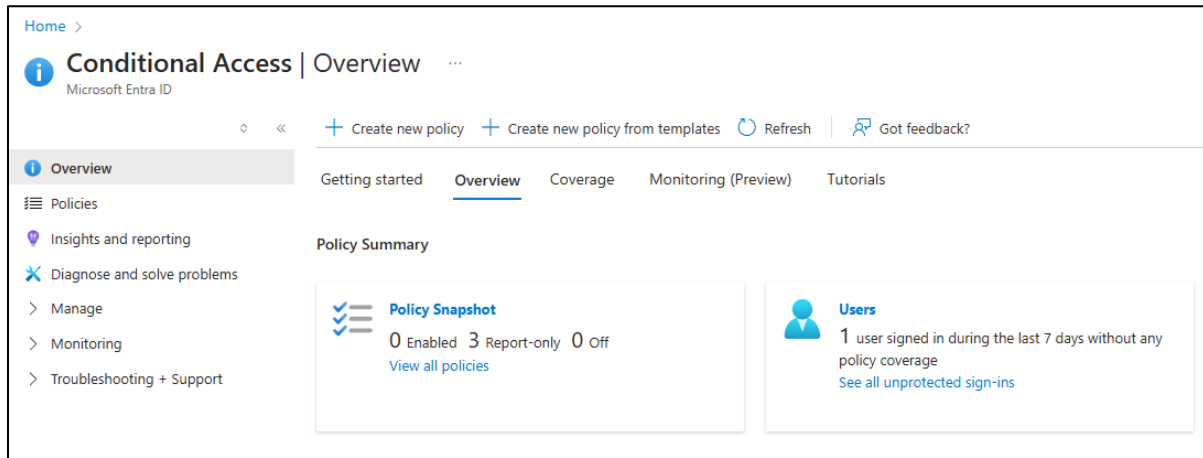
To access Conditional Access Policies, in the search box type “Conditional Access” and select Microsoft Entra Conditional Access.

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

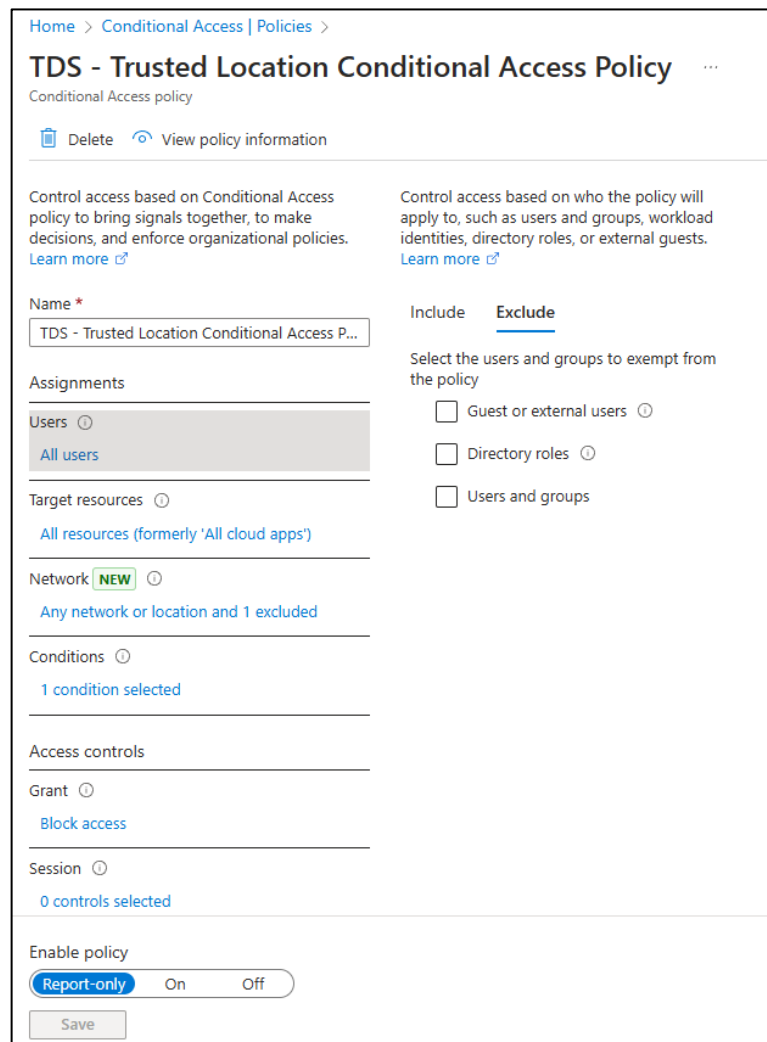
- Add an Exception: **Please be aware that it is very important to NOTE that you need to create an exception to avoid lockout on your own tenant.** In the User/Devices section, select Exclude. Select User or groups to exclude from that policy.



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



The screenshot shows the 'TDS - Trusted Location Conditional Access Policy' editor. The page has a header with 'Home > Conditional Access | Policies >' and the title 'TDS - Trusted Location Conditional Access Policy'. Below the title are links for 'Delete' and 'View policy information'. The main content area is divided into two columns. The left column contains sections for 'Name' (TDS - Trusted Location Conditional Access P...), 'Assignments' (Users: All users), 'Target resources' (All resources (formerly 'All cloud apps')), 'Network' (NEW: Any network or location and 1 excluded), 'Conditions' (1 condition selected), 'Access controls' (Grant: Block access), and 'Session' (0 controls selected). The right column contains sections for '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' (Exclude selected), and 'Select the users and groups to exempt from the policy' (Guest or external users, Directory roles, Users and groups). At the bottom, there is an 'Enable policy' section with 'Report-only' selected, 'On' and 'Off' buttons, and a 'Save' button.

Azure Budgets

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. If your tenant is calculated in dollars, sterling, or euros, the solution will notify you once the threshold has been approached.

Customer Details

Innova Solutions

100%

11 Jun 2025 12:55 PM

Overview

Security Settings

Recommended Products

Tenant Details

Deployment Log

Security Type

Azure Budgets

Azure Policies

Authentication

This tool allows budget and alert thresholds to be set for MSRP pricing on Azure Consumption.

1 out of 1 Azure subscriptions are missing budget configuration. It is highly recommended to create a budget in those subscriptions.

Create New Budget

Budget Name

Name

Budget Amount (\$)

0

Notification Alert Budget Threshold (%)

50

0 50 100

2nd Notification Alert Budget Threshold (%)

70

0 50 100

Send Notification To

Enter email manually

or

Select Recipients

Press Enter to add the email (you can include more than one)

Finally, select the Azure Subscriptions where you want to apply the budget (only for those Subscriptions that have no budget yet)

?

APPLY CONFIGURATION

Budget Alerts

Send Notification To

or

Select Recipients

Press Enter to add the email (you can include more than one)

adele.vance@hillandsons1.com

Finally, select the Azure Subscriptions where you want to apply the budget (only for those Subscriptions that have no budget yet)

☒ Select All

☒ Azure subscription 1 (962f320f-589d-491a-84e8-1dff9f3561b5)

Save new budget

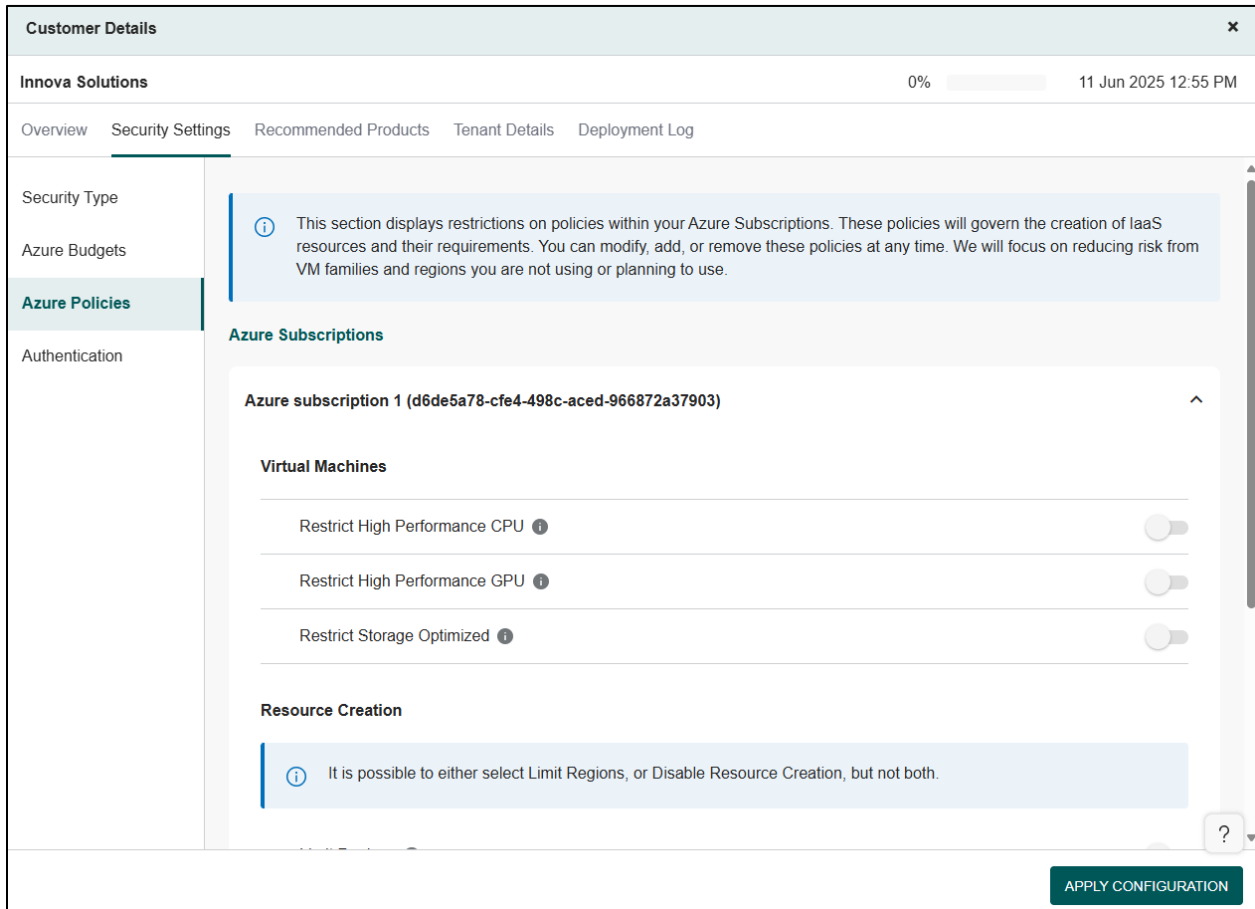
Budget alerts allow you to set up your sender groups. You only have the option to set up one email notification alert, this can be individual email recipients or email groups. This means your Recipients will receive two alerts once the dedicated Budget percentage threshold has been reached. We have set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

Azure Policies

Azure Policies

Azure policies include 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 policies to control which type of Resources you want to DENY in your tenant. Each policy will deny a family of VMs depending on the optimized resources.



The screenshot shows the 'Customer Details' page for 'Innova Solutions'. The 'Security Settings' tab is active, and the 'Azure Policies' section is selected in the left sidebar. A notification box states: 'This section displays restrictions on policies within your Azure Subscriptions. These policies will govern the creation of IaaS resources and their requirements. You can modify, add, or remove these policies at any time. We will focus on reducing risk from VM families and regions you are not using or planning to use.'

Under 'Azure Subscriptions', 'Azure subscription 1 (d6de5a78-cfe4-498c-aced-966872a37903)' is listed. Under 'Virtual Machines', there are three toggle switches:

- Restrict High Performance CPU (toggle is off)
- Restrict High Performance GPU (toggle is off)
- Restrict Storage Optimized (toggle is off)

Under 'Resource Creation', a notification box states: 'It is possible to either select Limit Regions, or Disable Resource Creation, but not both.'

An 'APPLY CONFIGURATION' button is located at the bottom right of the configuration area.

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 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 IaaS 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](#)

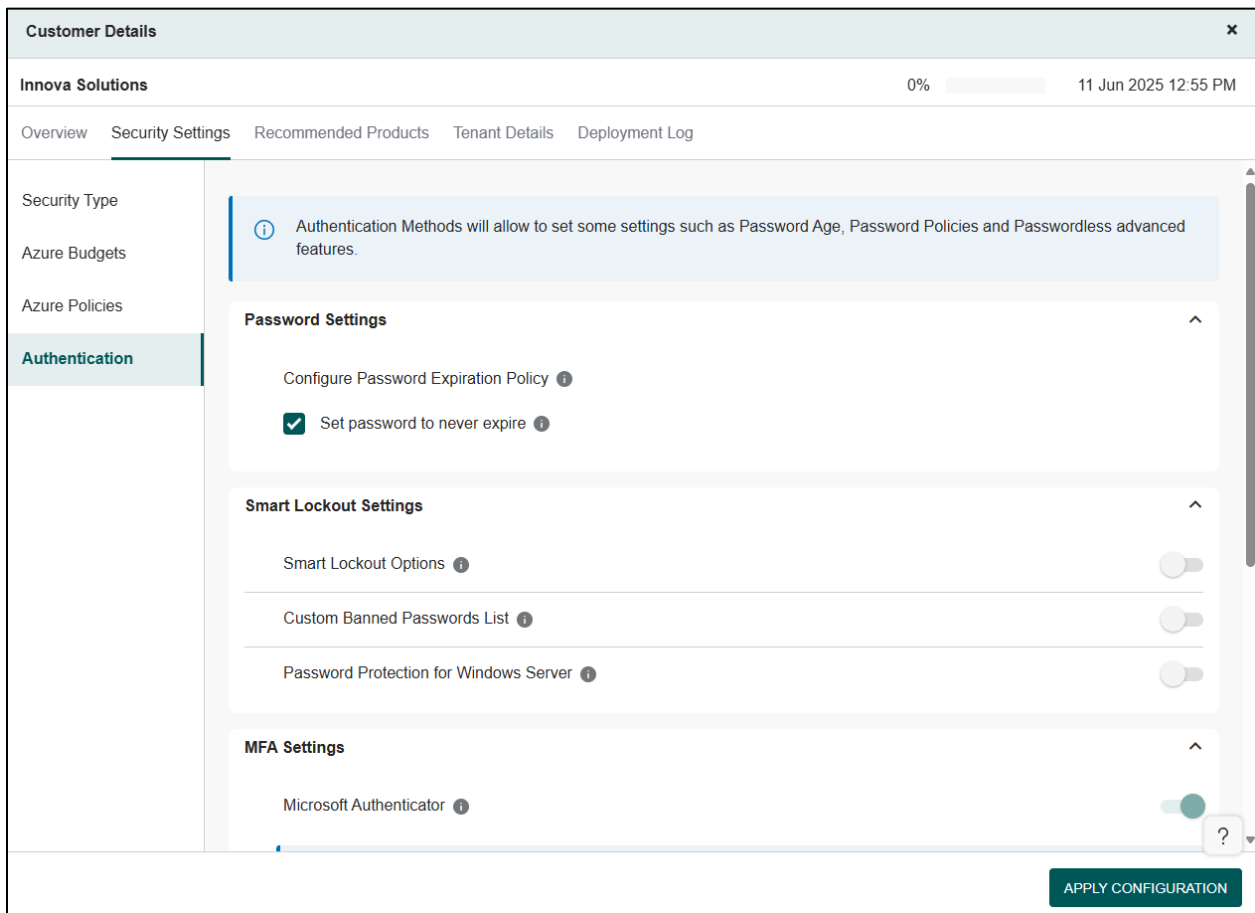
Authentication

Authentication Methods

Authentication methods allow you to manage your Password age, Password Policies and Passwordless advanced features settings.

This has been split into different categories.

- Password Settings
- Smart Lockout Settings
- MFA Settings
- Passwordless Functions



The screenshot shows the 'Customer Details' window for 'Innova Solutions'. The 'Security Settings' tab is active, and the 'Authentication' sub-tab is selected in the left sidebar. A blue informational banner at the top states: 'Authentication Methods will allow to set some settings such as Password Age, Password Policies and Passwordless advanced features.' Below this, the settings are organized into three sections: 'Password Settings' (with a toggle for 'Set password to never expire' which is checked), 'Smart Lockout Settings' (with three toggle switches for 'Smart Lockout Options', 'Custom Banned Passwords List', and 'Password Protection for Windows Server', all currently off), and 'MFA Settings' (with a toggle for 'Microsoft Authenticator' which is on). An 'APPLY CONFIGURATION' button is located at the bottom right of the settings area.

Password Settings

Password Expiration, by default Azure policy will force passwords 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 dissuade users from using similar passwords to ones they have previously created and encourage them to add a second authentication method such as MFA.

Smart Lockout Settings

Smart Lockout; toggle this option to set your lockout threshold. 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](#)

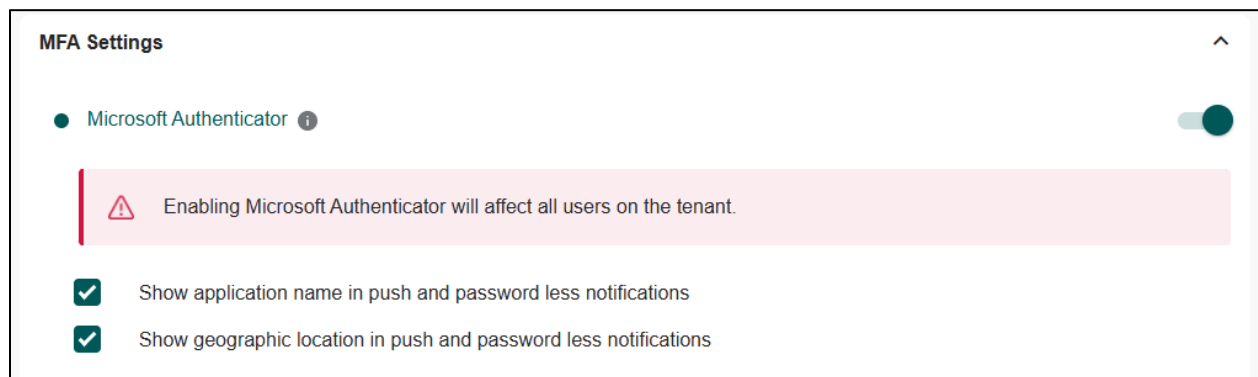
Custom Banned Password List: Azure Custom Banned Password list is a feature of Azure Active Directory (Azure AD) that allows administrators to create a custom list of passwords that cannot be used by users in their organization. This feature is used to enhance the security of user accounts by preventing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

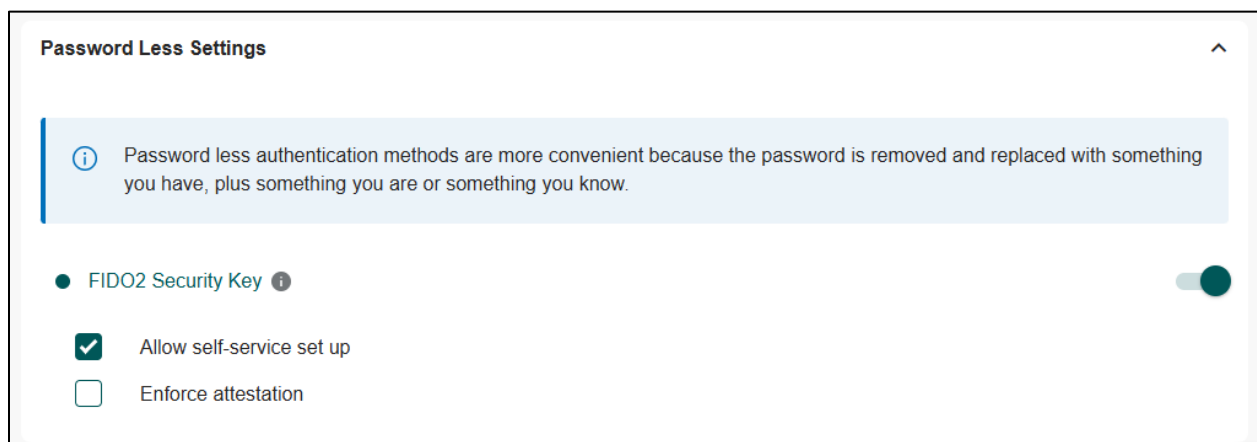
Please toggle this feature to enable it then you will have the different options to choose which notifications.

- 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](#)

Password Less 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 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 the 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.

Customer Details > Recommended Products

Depending on what the customer's security configuration is, different recommended products will be displayed in this page. For each one, there is a link to view the plans and purchase them.

Customer Details

Innova Solutions

0%

11 Jun 2025 12:55 PM

Overview


Security Settings

Recommended Products

Tenant Details

Deployment Log

Enhance your online security and shield yourself from MFA risks




Entra ID P2

Entra ID P2 (previously Azure Active Directory Premium P2) includes all features of Entra ID P1 with advanced capabilities like Identity Protection and Privileged Identity Management (PIM). It is designed to enhance security further by enabling


VIEW PLANS

Elevate your security score for enhanced protection




Trend Micro Worry-Free Services

Designed for overstretched IT teams, Trend Micro Worry-Free Services is an industry leading,




Barracuda SecureEdge Subscription

Barracuda SecureEdge secures your users, sites and things with an easy-to-deploy cloud-first



Sophos Firewall

Sophos Firewall integrates leading technologies into a single next-generation solution



Microsoft Defender for Business

Provides next-generation antivirus, endpoint detection and response (EDR), and threat and vulnerability

35

Next-Gen Solutions Factory

Customer Details > Tenant Details

This page shows extra information about the customer.

Customer Details

Innova Solutions

0%

11 Jun 2025 12:55 PM

Overview

Security Settings

Recommended Products

Tenant Details

Deployment Log

General Information

Company Name

Innova Solutions

Domain Name

innovasolutions3.onmicrosoft.com

Tenant ID

d8d435f2-7407-4148-b41d-762798dce148

Azure Subscriptions

Subscription id	Name	Consumption	Forecasted Consumption	Has Budget?
d6de5a78-cfe4-498c-aced-966872a37903	Azure subscription 1	\$27.52	\$40.60	

1 to 1 of 1

Microsoft 365 Licenses

Name
Microsoft 365 E3

1 to 1 of 1

?

It includes:

General Information

- Company name
- Domain name
- Tenant ID

Azure Subscriptions

List of the customer's active Azure Subscriptions, including their current and forecasted consumption.

Microsoft 365 Licenses

List of all Microsoft 365 licenses that the customer purchased.

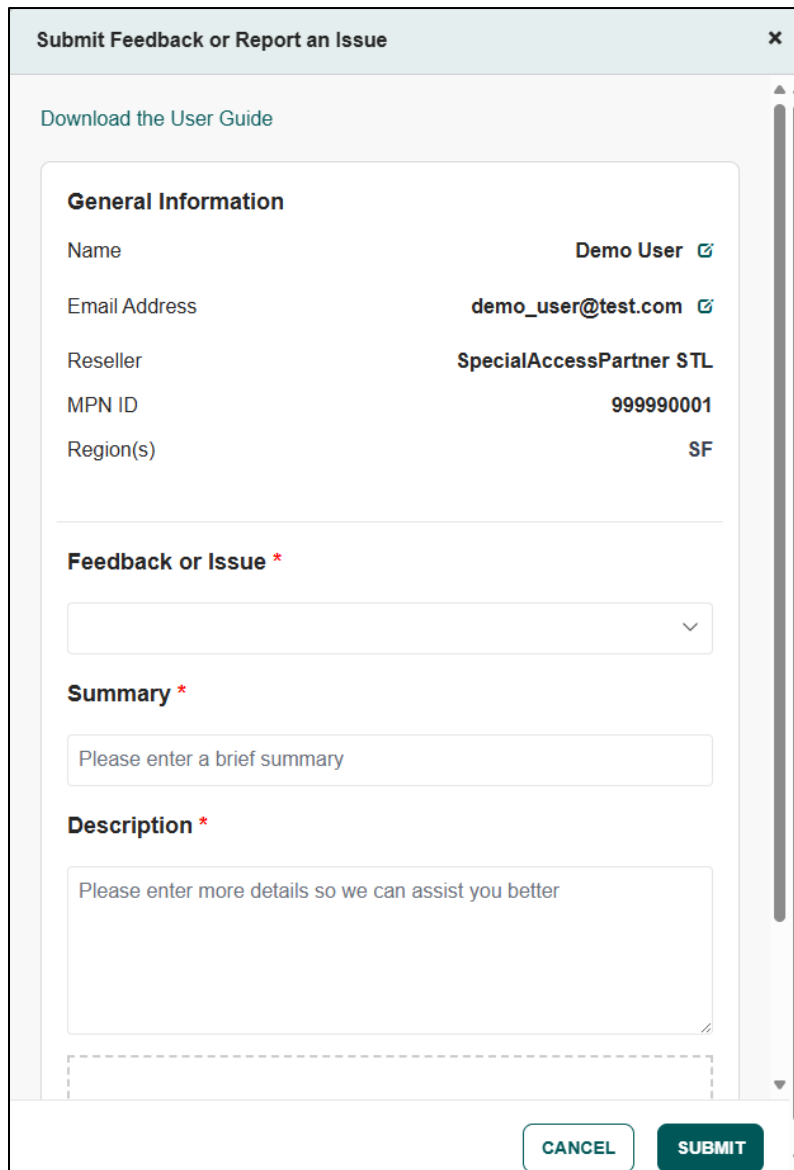
Customer Details > Deployment Log

This tab shows all logs that were generated after a customer synchronization or when a security setting was turned on or off.

Customer Details ×		
Hill and Sons		0% ↺ 02 Jun 2025 11:54 PM
Overview Security Settings Recommended Products Tenant Details Deployment Log		
Message ↑	Status ↑	Timestamp ↑
<input type="text" value="Ab"/>	<input type="text" value="Ab"/>	<input type="text" value="="/> 📅 👁
MenuTabAggregator	Success	06/06/2025 10:11:41
MenuTabFinalizer	Success	06/06/2025 10:11:41
Get Status: Geo Restrictions	Success	06/06/2025 10:11:41
Get Status: No Security Enabled	Success	06/06/2025 10:11:40
Get Status: Security Defaults Enabled	Success	06/06/2025 10:11:40
Get Status: Conditional Access Enabled	Success	06/06/2025 10:11:40
MenuTabFinalizer	Success	06/06/2025 10:11:40
Get Security Type	Success	06/06/2025 10:11:40
Get Status: MFA Azure Management	Success	06/06/2025 10:11:40

Support

You can submit your feedback or report an issue. Please click on the “?” icon you will find on the bottom right corner of the page. The following popup will open:



The screenshot shows a modal window titled "Submit Feedback or Report an Issue" with a close button (X) in the top right corner. Inside the modal, there is a link "Download the User Guide" at the top. Below it is a section titled "General Information" containing a form with the following fields and values:

Field	Value
Name	Demo User
Email Address	demo_user@test.com
Reseller	SpecialAccessPartner STL
MPN ID	999990001
Region(s)	SF

Below the "General Information" section is a section titled "Feedback or Issue *" with a dropdown menu. Underneath is a "Summary *" section with a text input field containing the placeholder "Please enter a brief summary". Below that is a "Description *" section with a larger text input field containing the placeholder "Please enter more details so we can assist you better". At the bottom of the modal are two buttons: "CANCEL" and "SUBMIT".

You need to specify a title for the issue or feedback, a description and optionally you can attach files to the request.

In case of an issue, a Support agent will contact you via email with an update of your case.
In case of feedback, we will review it internally and get back to you once we have an update.

IMPORTANT: Please review the Name and Email Address that is displayed. If it is wrong or is an account that does not belong to you, you can edit both fields. This is important so that replies are sent to your mailbox.