Power Platform
COMMUNITY CONFERENCE

SEPTEMBER 18–20, 2024 • *Workshops: Sept 16, 17 & 21*

MGM GRAND • *Las Vegas, NV*

Exploring the Power Platform's Security Evolution

Rami Mounla

www.linkedin.com/in/ramimounla

Whova

The official event app for the **Power Platform Community Conference**

Join the event app to access:

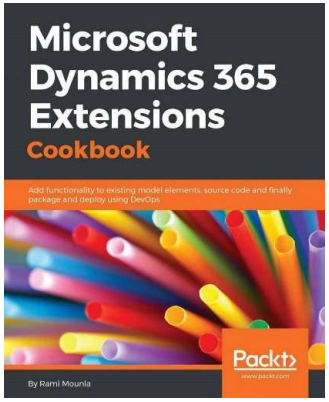
- Event announcements
- Personalized agenda, session details
- Speaker & attendee profiles
- Networking, meet-ups, messages
- Event documents

Event Invitation Code: PPCConf2024

Power Platform COMMUNITY CONFERENCE

Wellington Power Platform UG

DXC TECHNOLOGY



Security in Numbers

350 Million Attacks/year

1.3 Million Dollars loss/successful business attack

8 Trillion Dollars cybercrime global total cost

Probation officer sacked for unauthorised searching of Chinese offenders

Paula Penfold and Louisa Cleave

June 20, 2024 · 10:00am

A Stuff Circuit investigation reveals decades of foreign interference by China in New Zealand. Video credit: Stuff Circuit

A probation officer has been dismissed by the Department of Corrections for accessing information about dozens of offenders "without authority to do so".


CYBER SECURITY
BUDGET BEFORE A BREACH
CYBER SECURITY
BUDGET AFTER A BREACH

The Daily Insecurities

16 SEP 2024

DXC Technology Hit by Major Security Breach, Over 1 Million Accounts Exposed

By PETER PARKER

September 16, 2024 DXC Technology, a global leader in IT services and solutions, confirmed today that a major security breach has compromised the personal data of over one million customer accounts.

The breach, which is believed to have taken place over the course of several weeks in August and September, has affected customers in multiple countries. The stolen data includes names, addresses, social security numbers, and financial information.

DXC has stated that it is working closely with law enforcement and cybersecurity experts to investigate the breach and mitigate its impact. The company has also begun notifying affected customers and has set up a dedicated hotline and website for those concerned about their personal information. In addition, the company is offering affected individuals one year of free credit monitoring and identity protection services.

A DXC spokesperson issued a statement, saying: "We take the privacy and security of our clients extremely seriously. We are working diligently to contain this breach, understand how it occurred, and ensure that similar incidents are prevented in the future."

Potential Impact and Legal Ramifications The breach could have widespread implications, especially

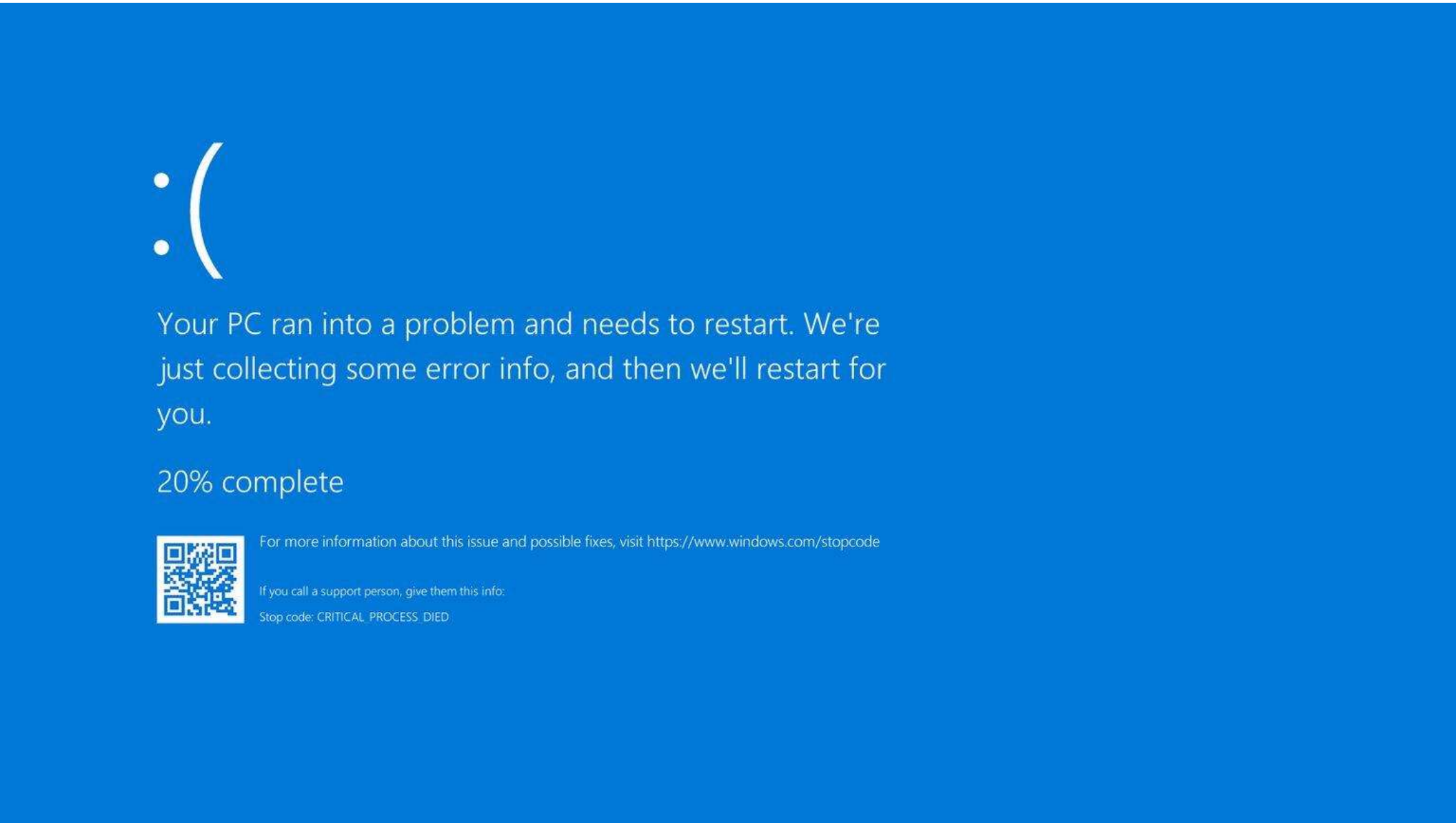
DXC.technology

Reuters

International Moose Count Underway

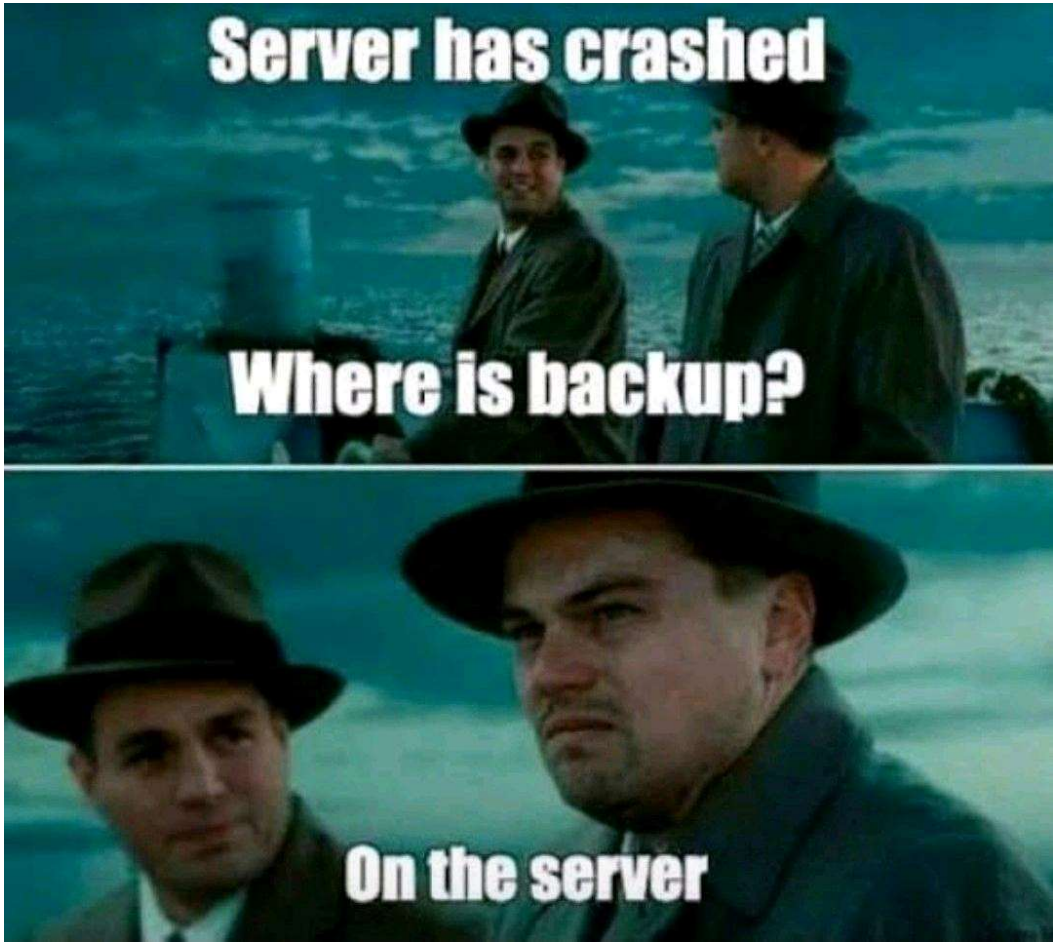
By BOB O'BOBSTON

The UN-sponsored International Moose Census got off to a flying start today with hopes for an increase in the worldwide moose population


:(
Your PC ran into a problem and needs to restart. We're just collecting some error info, and then we'll restart for you.
20% complete
For more information about this issue and possible fixes, visit https://www.windows.com/stopcode
If you call a support person, give them this info:
Stop code: CRITICAL_PROCESS_DIED

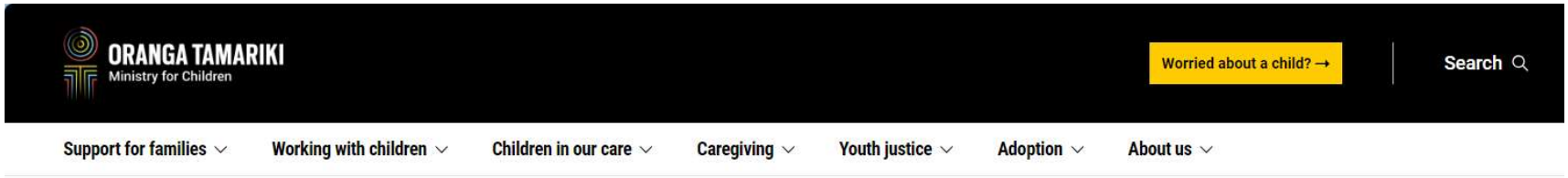

CROWDSTRIKE


246.39 USD
-0.50 (-0.20%) year to date
Closed: 6 Sept, 7:59 pm GMT-4 • Disclaimer
After hours 246.20 −0.19 (0.077%)
1D
5D
1M
6M
YTD
1Y
5Y
Max
217.89 USD Fri, 2 Aug
400
350
300
250
200
Mar 2024
May 2024
Jul 2024
Sept 2024


Server has crashed
Where is backup?
On the server

ORANGA TAMARIKI

Ministry for Children



WORRIED ABOUT A CHILD? TELL US

Worried about a child? Tell us

- Identify abuse
- Community help

Worried about a child? Tell us

He māharahara ōu ki tētahi tamaiti? Whakamōhio mai

Anyone who is worried about a tamaiti or rangatahi can make a report of concern to us or the Police.

TRAVEL

New Zealand passport ranked as most powerful in updated report

The US passport, in comparison, grants access to 92 countries

By Michael Bartiromo · Fox News

New Zealand's passport is now the most powerful in the world, according to the latest Global Passport Index compiled by global financial advisory firm Arton Capital.

The index ranks each country's passport based on its "mobility score" — i.e., the number of countries the passport grants access to — and New Zealand's has recently edged ahead with 129, after Australia agreed to reopen travel with the country earlier this month.

Te Ara Manaaki

In order to provide

the best security protection

to your organisation…

… MASTER your ecosystem’s Security features

Types of Security Controls

Preventative

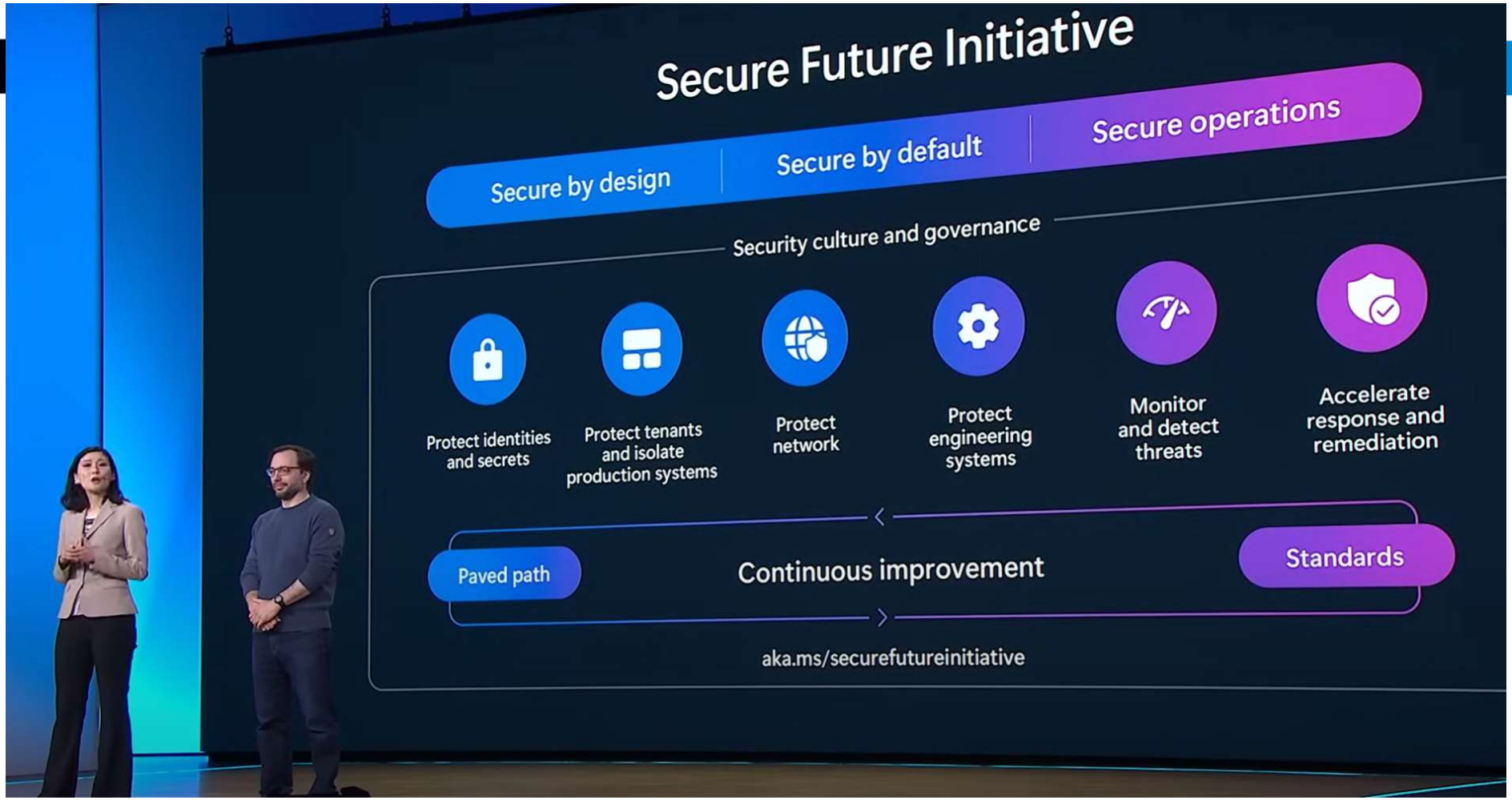
Authentication
Authorisation
Encryption
Firewall

Detective

DoS
Brute Force
Malicious Access
Mass Export

Corrective

Audit Trails
Governance
Notification
Pattern AI


Secure Future Initiative
Secure by design
Secure by default
Secure operations
Security culture and governance
Protect identities and secrets
Protect tenants and isolate production systems
Protect network
Protect engineering systems
Monitor and detect threats
Accelerate response and remediation
Paved path
Continuous improvement
Standards
aka.ms/securefutureinitiative


Security is a team sport

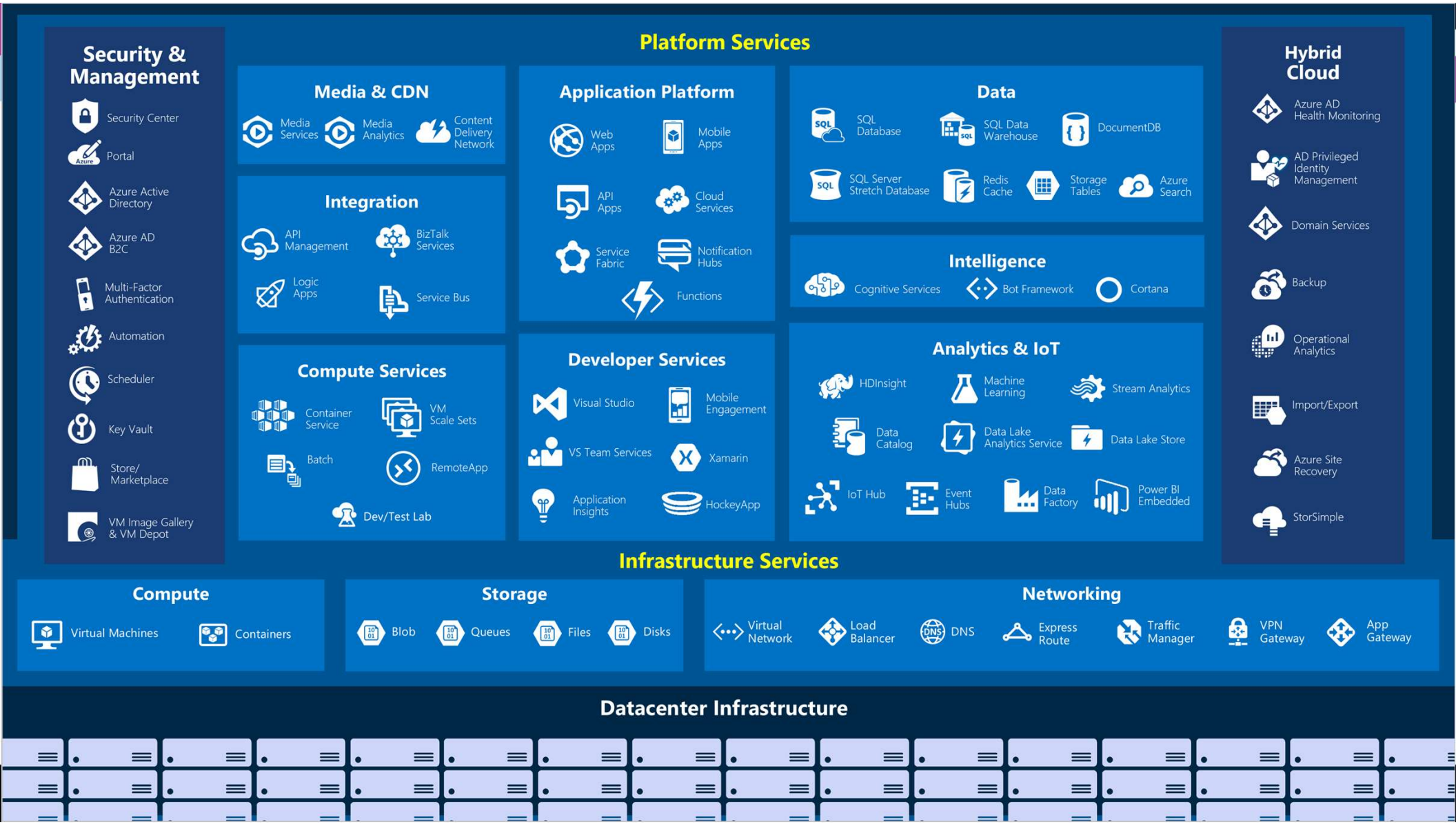
https://learn.microsoft.com/en-us/dynamics365/guidance/implementation-guide/security

Platform Levels

Microsoft	Encryption ISO Certifications Attack Prevention
Azure	Infrastructure Conditional Access SIEM
M365	Security Group Licensing Read Audits
D365	RBAC Field Level Security Access Teams

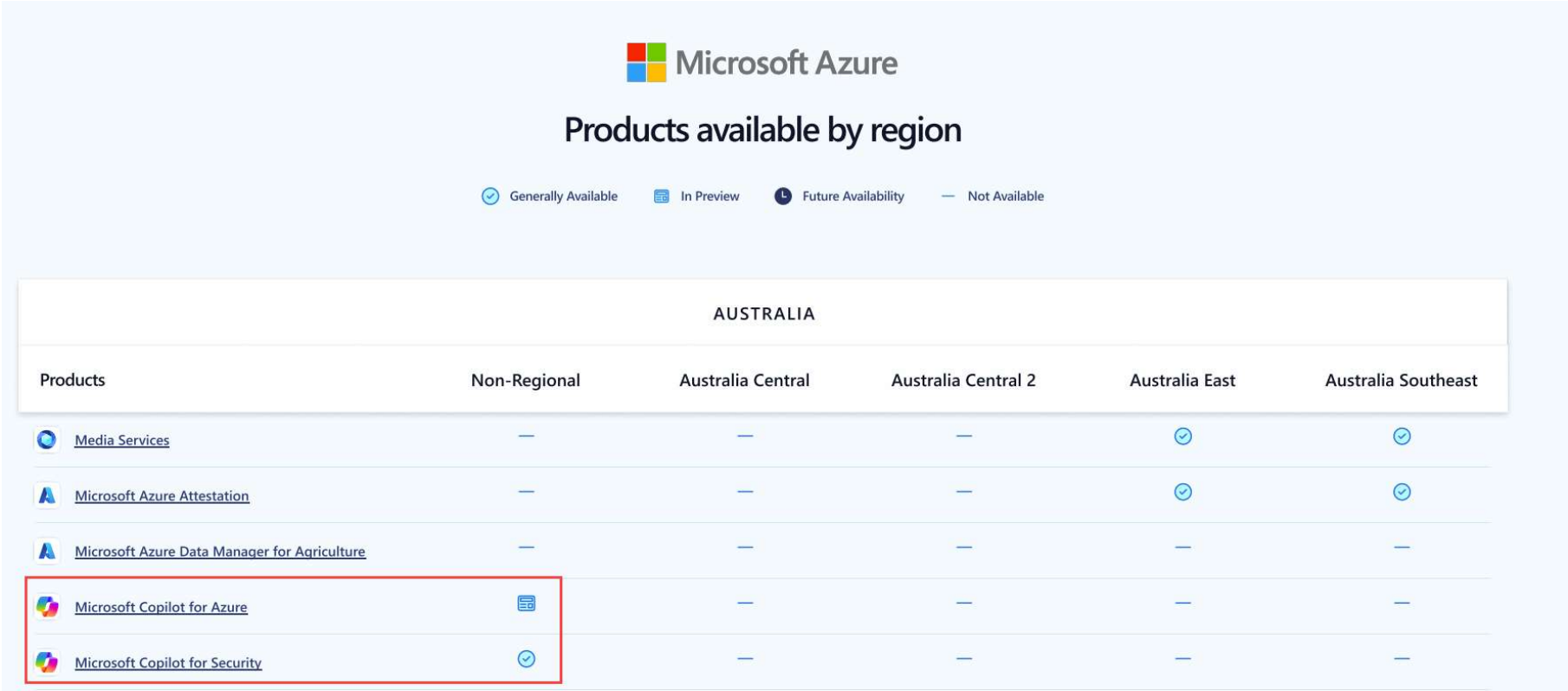
Preventative

Azure


Platform Services
Security & Management
Security Center
Portal
Azure Active Directory
Azure AD B2C
Multi-Factor Authentication
Automation
Scheduler
Key Vault
Store/ Marketplace
VM Image Gallery & VM Depot
Media & CDN
Media Services
Media Analytics
Content Delivery Network
Integration
API Management
BizTalk Services
Logic Apps
Service Bus
Compute Services
Container Service
VM Scale Sets
Batch
RemoteApp
Dev/Test Lab
Application Platform
Web Apps
Mobile Apps
API Apps
Cloud Services
Service Fabric
Notification Hubs
Functions
Developer Services
Visual Studio
Mobile Engagement
VS Team Services
Xamarin
Application Insights
HockeyApp
Data
SQL Database
SQL Data Warehouse
DocumentDB
SQL Server Stretch Database
Redis Cache
Storage Tables
Azure Search
Intelligence
Cognitive Services
Bot Framework
Cortana
Analytics & IoT
HDInsight
Machine Learning
Stream Analytics
Data Catalog
Data Lake Analytics Service
Data Lake Store
IoT Hub
Event Hubs
Data Factory
Power BI Embedded
Hybrid Cloud
Azure AD Health Monitoring
AD Privileged Identity Management
Domain Services
Backup
Operational Analytics
Import/Export
Azure Site Recovery
StorSimple
Infrastructure Services
Compute
Virtual Machines
Containers
Storage
Blob
Queues
Files
Disks
Networking
Virtual Network
Load Balancer
DNS
Express Route
Traffic Manager
VPN Gateway
App Gateway
Datacenter Infrastructure

Check where the services are provided

Check where the services are provided



Microsoft Azure

Products available by region

Generally Available | In Preview | Future Availability | — Not Available

Products	Non-Regional	Australia Central	Australia Central 2	Australia East	Australia Southeast
		AUSTRALIA			
Media Services	—	—	—	✓	✓
Microsoft Azure Attestation	—	—	—	✓	✓
Microsoft Azure Data Manager for Agriculture	—	—	—	—	—
Microsoft Copilot for Azure	▤	—	—	—	—
Microsoft Copilot for Security	✓	—	—	—	—

https://azure.microsoft.com/en-us/global-infrastructure/services

Trust Centre

https://www.microsoft.com/en-us/trustcenter/security/dynamics365-security

Logical Separation

Threat Management (monitoring e.g. DoS)

Physical Security

ISO Certifications

Breach Protocol

TLS 1.2

TDE

Microsoft Security

We secure your data at rest and in transit

With advanced encryption, Microsoft helps protect your data both at rest and in transit. Our encryption protocols erect barriers against unauthorized access to the data, including two or more independent encryption layers to safeguard against compromises of any one layer.

Data at rest

The Microsoft Cloud employs a wide range of encryption capabilities up to AES-256, giving you the flexibility to choose the solution that's best for your business.

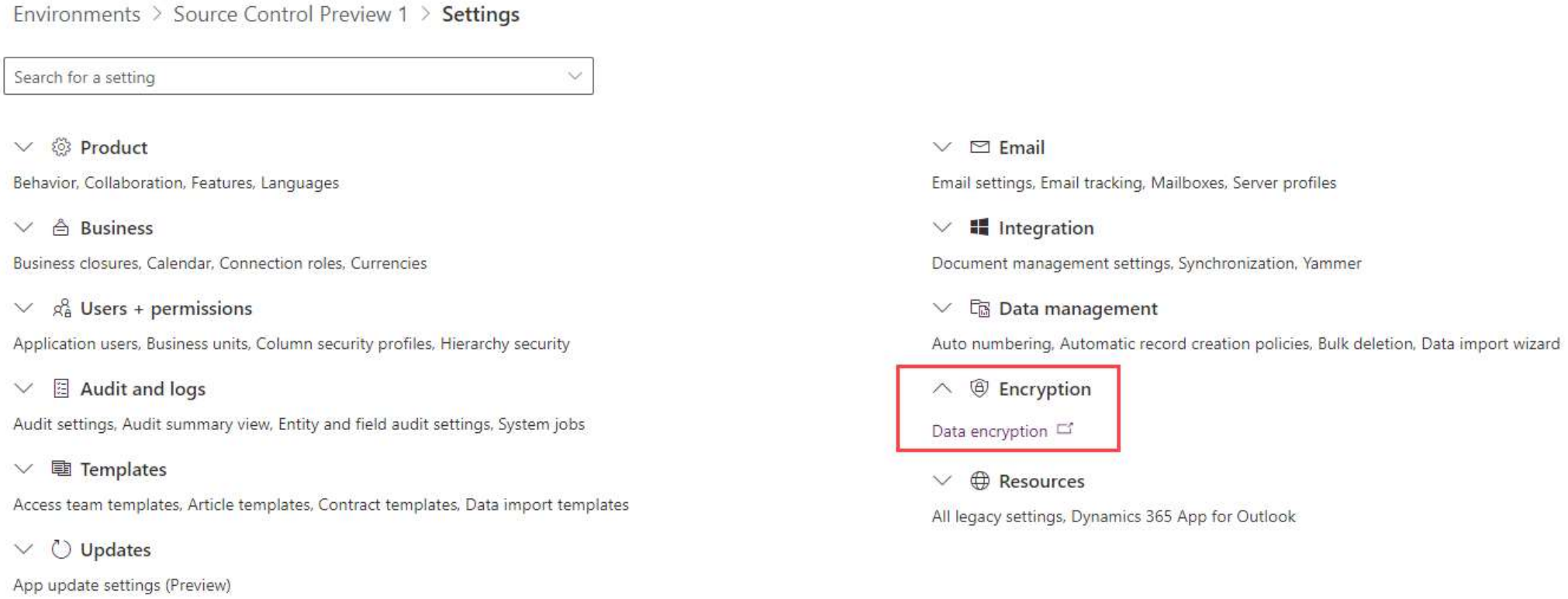
Data in transit

Microsoft uses and enables the use of industry-standard encrypted transport protocols, such as Transport Layer Security (TLS) and Internet Protocol Security (IPsec).

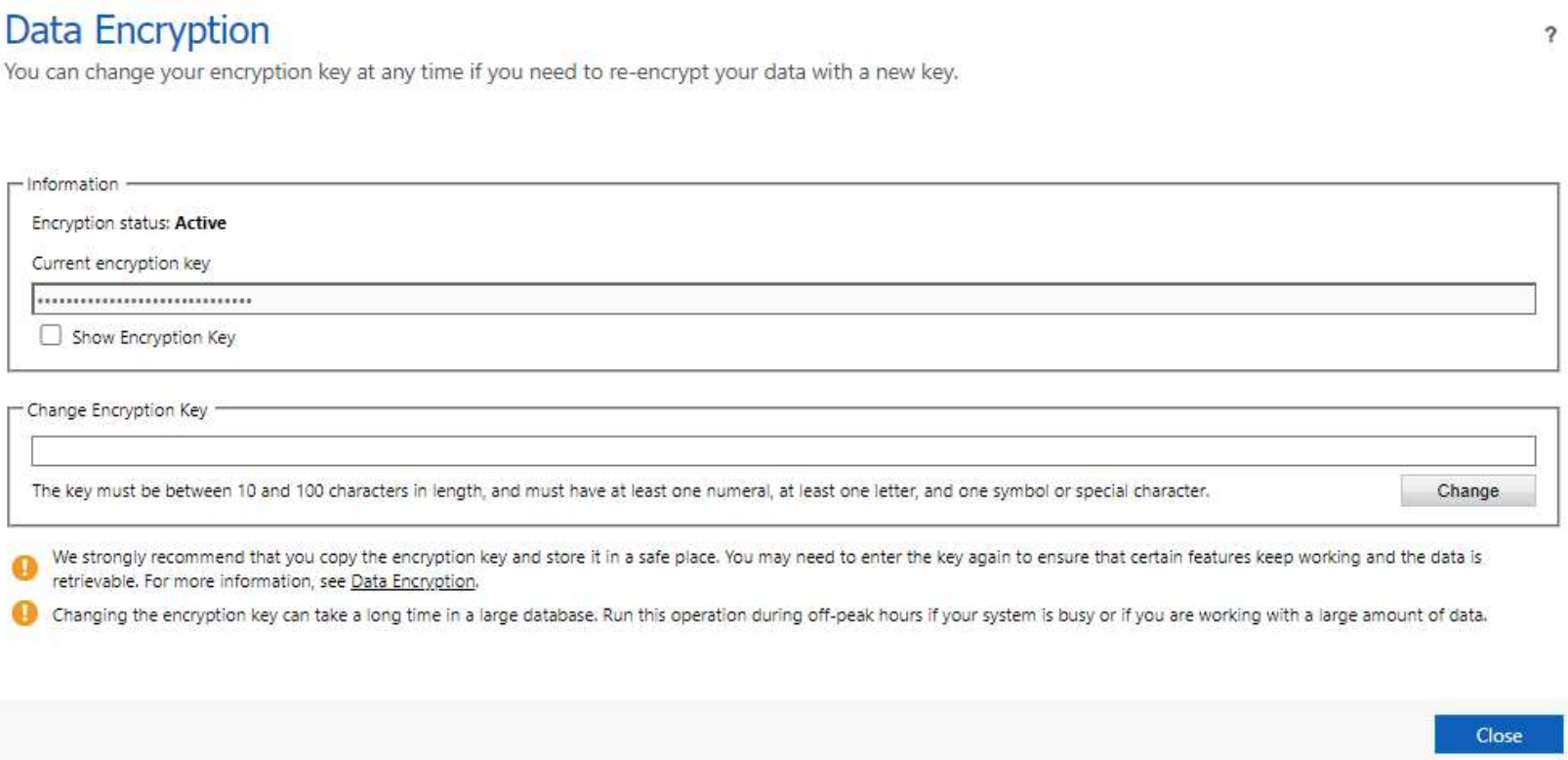
Encryption keys

All Microsoft-managed encryption keys are properly secured and offer the use of technologies such as Azure Key Vault to help you control access to passwords, encryption keys, and other secrets.

Data Encryption



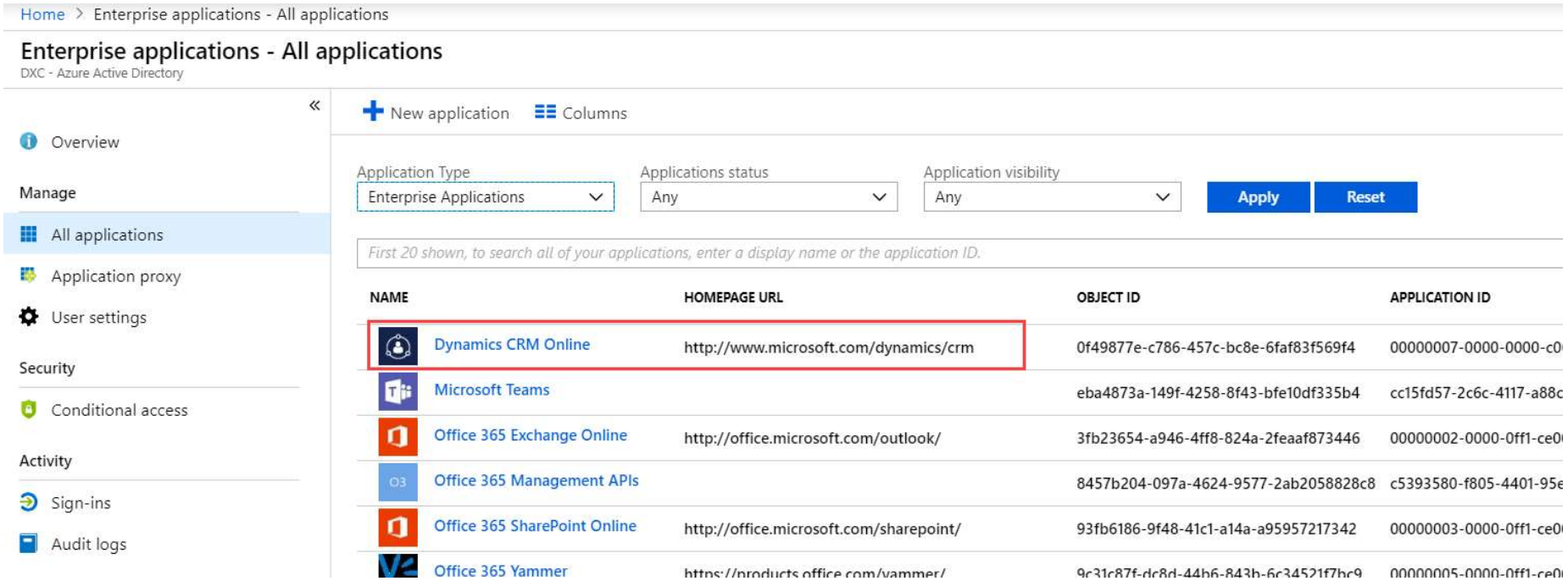
BYO Key


Data Encryption
You can change your encryption key at any time if you need to re-encrypt your data with a new key.
?
Information
Encryption status: Active
Current encryption key
Show Encryption Key
Change Encryption Key
The key must be between 10 and 100 characters in length, and must have at least one numeral, at least one letter, and one symbol or special character.
Change
We strongly recommend that you copy the encryption key and store it in a safe place. You may need to enter the key again to ensure that certain features keep working and the data is retrievable. For more information, see Data Encryption.
Changing the encryption key can take a long time in a large database. Run this operation during off-peak hours if your system is busy or if you are working with a large amount of data.
Close

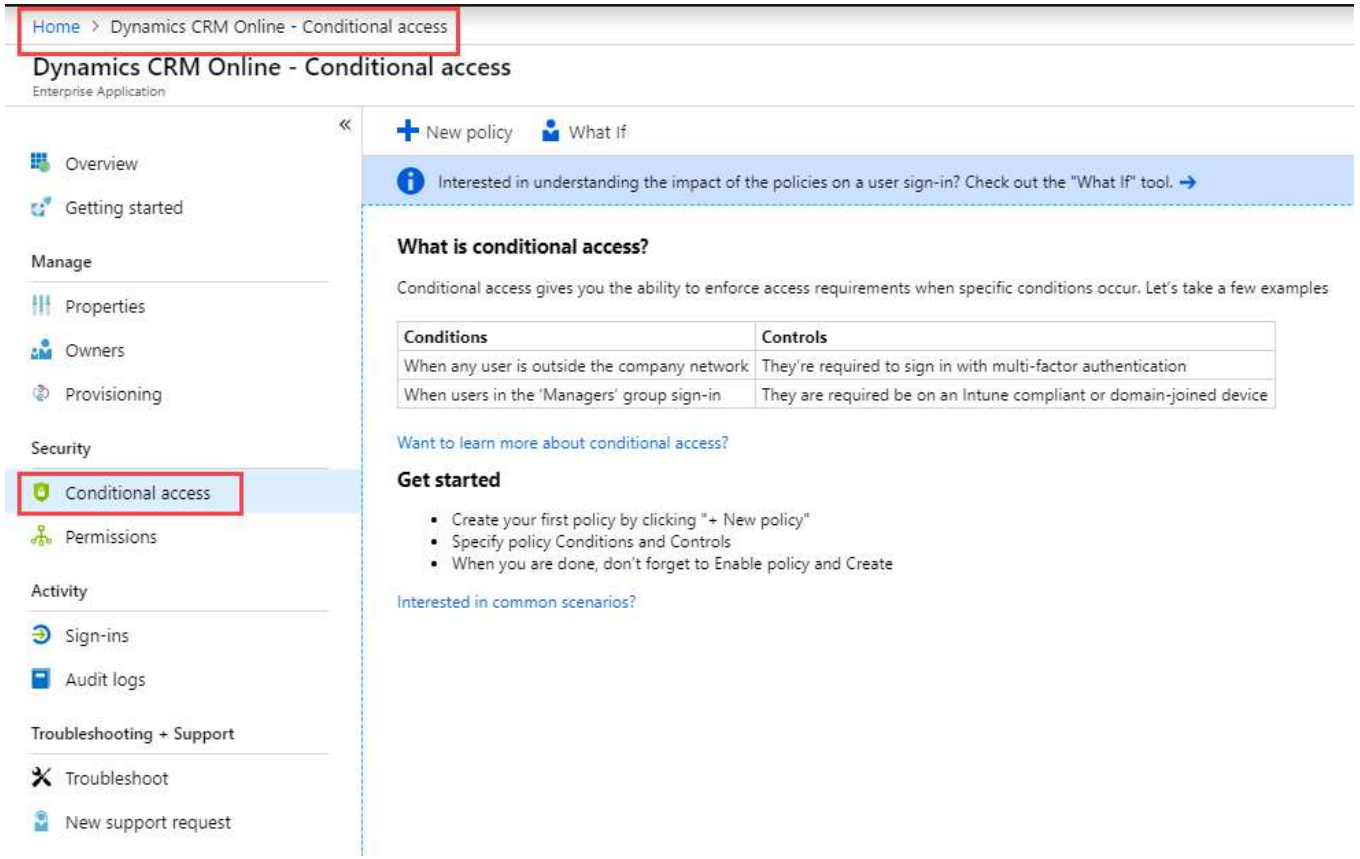
Preventative

Azure Conditional Access

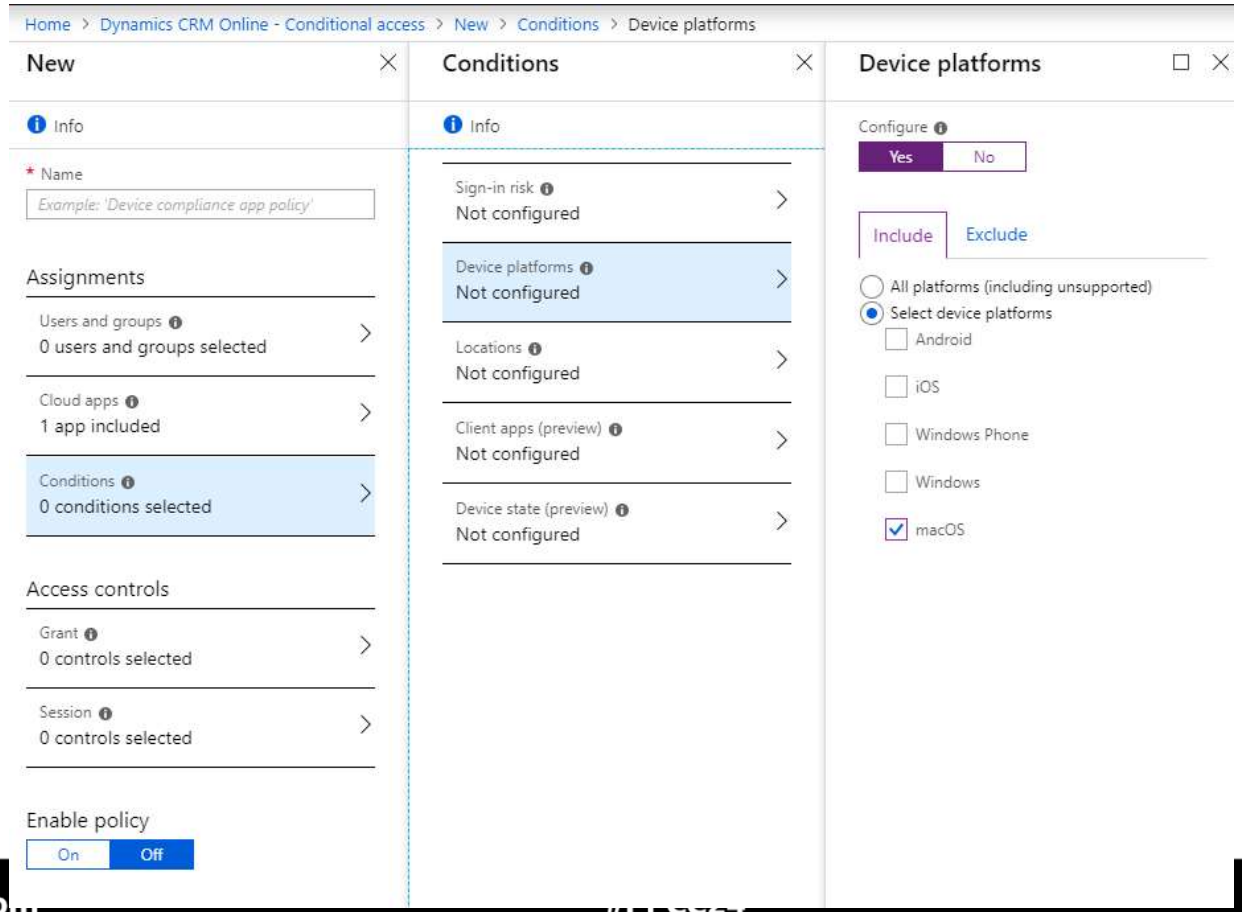
Enterprise Applications



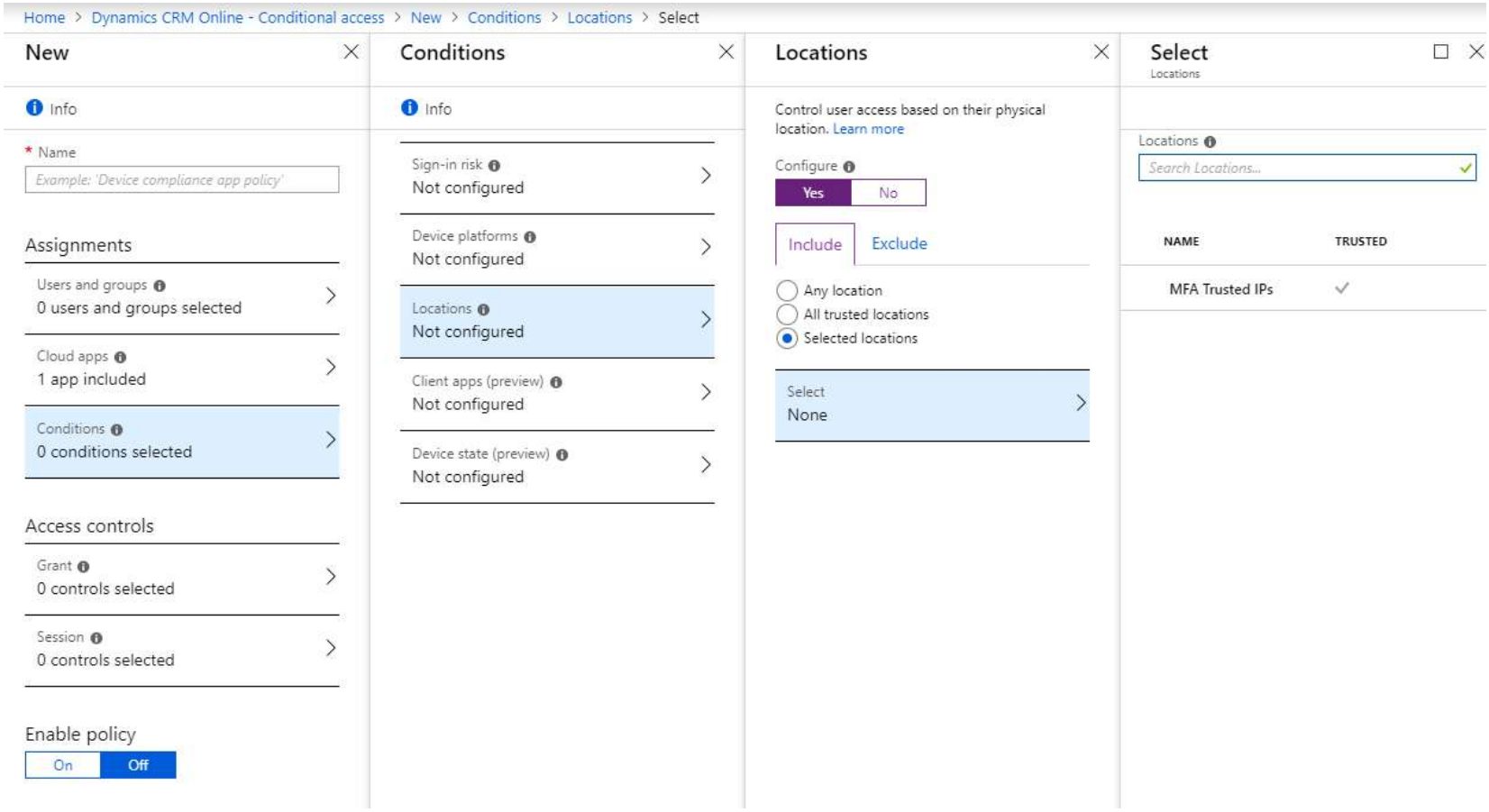
Azure Conditional Access



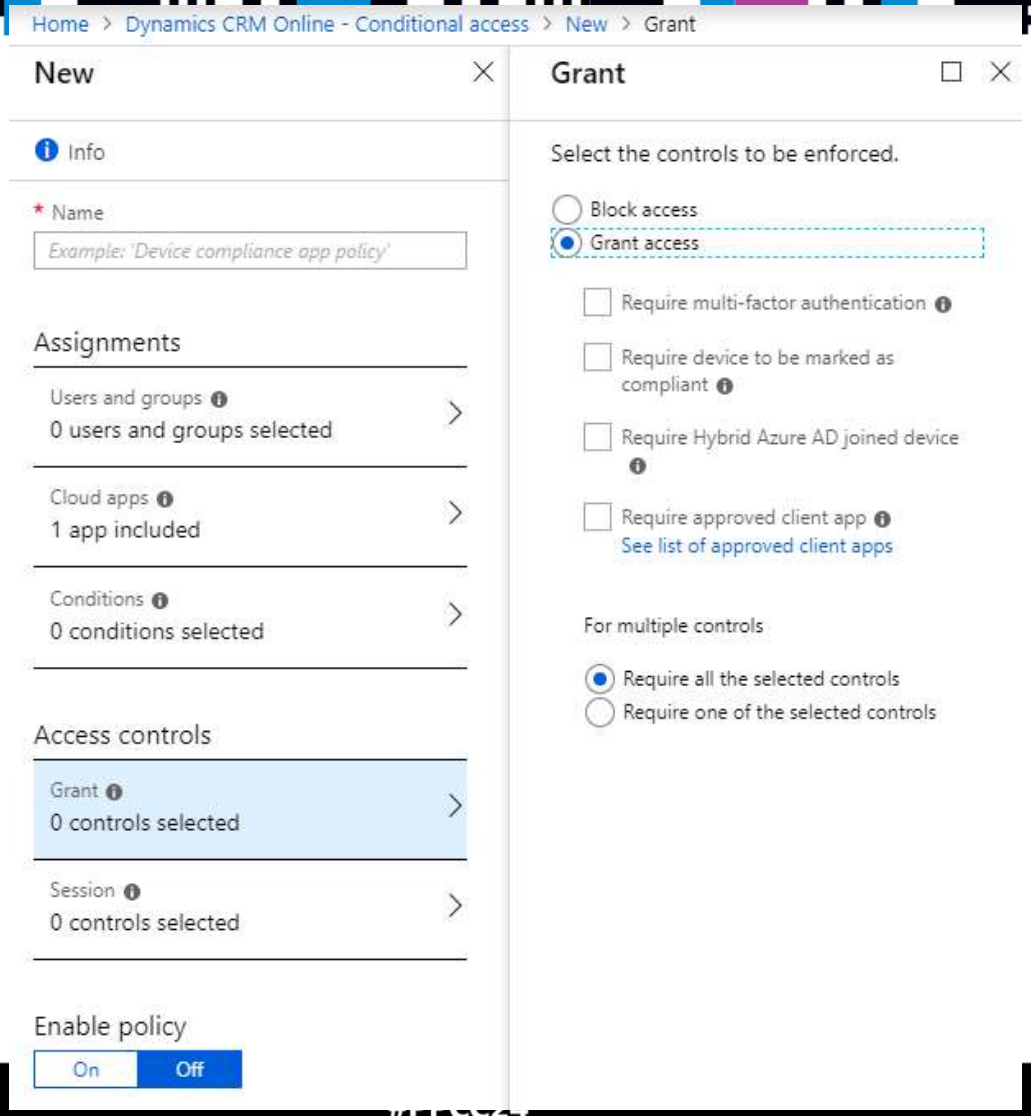
Device Control



IP Control


Home > Dynamics CRM Online - Conditional access > New > Conditions > Locations > Select
New
Info
* Name
Example: 'Device compliance app policy'
Assignments
Users and groups
0 users and groups selected
Cloud apps
1 app included
Conditions
0 conditions selected
Access controls
Grant
0 controls selected
Session
0 controls selected
Enable policy
On
Off
Conditions
Info
Sign-in risk
Not configured
Device platforms
Not configured
Locations
Not configured
Client apps (preview)
Not configured
Device state (preview)
Not configured
Locations
Control user access based on their physical location. Learn more
Configure
Yes
No
Include
Exclude
Any location
All trusted locations
Selected locations
Select
None
Select
Locations
Locations
Search Locations...
NAME
TRUSTED
MFA Trusted IPs

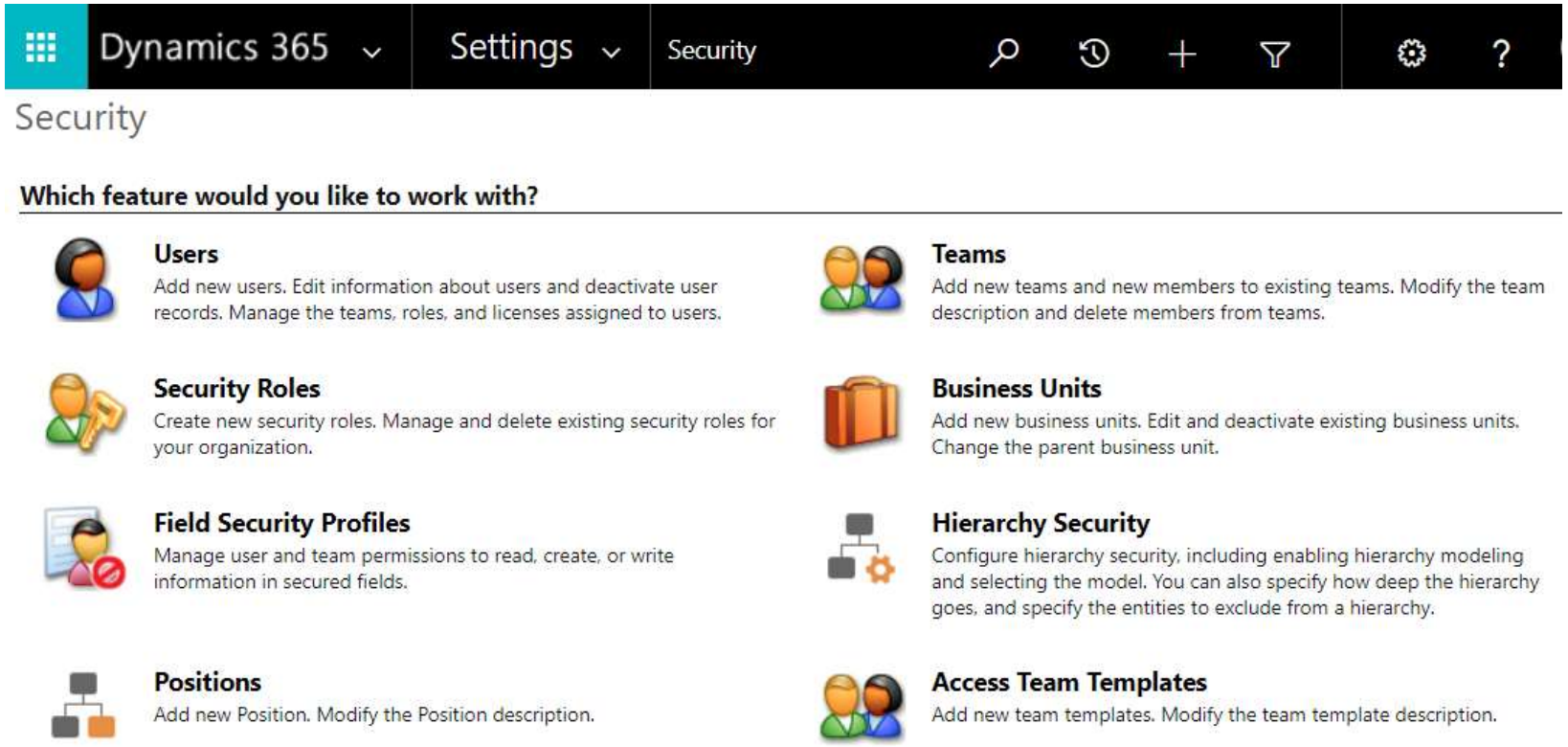
Block / MFA


Home > Dynamics CRM Online - Conditional access > New > Grant
New
Info
* Name
Example: 'Device compliance app policy'
Assignments
Users and groups
0 users and groups selected
Cloud apps
1 app included
Conditions
0 conditions selected
Access controls
Grant
0 controls selected
Session
0 controls selected
Enable policy
On
Off
Grant
Select the controls to be enforced.
Block access
Grant access
Require multi-factor authentication
Require device to be marked as compliant
Require Hybrid Azure AD joined device
Require approved client app
See list of approved client apps
For multiple controls
Require all the selected controls
Require one of the selected controls

Preventative

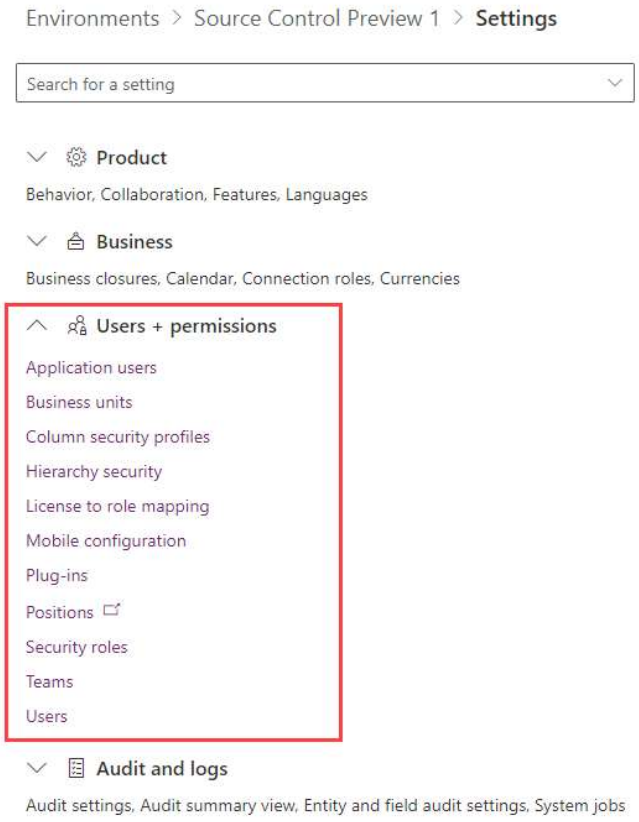
Security Roles

Settings > Security

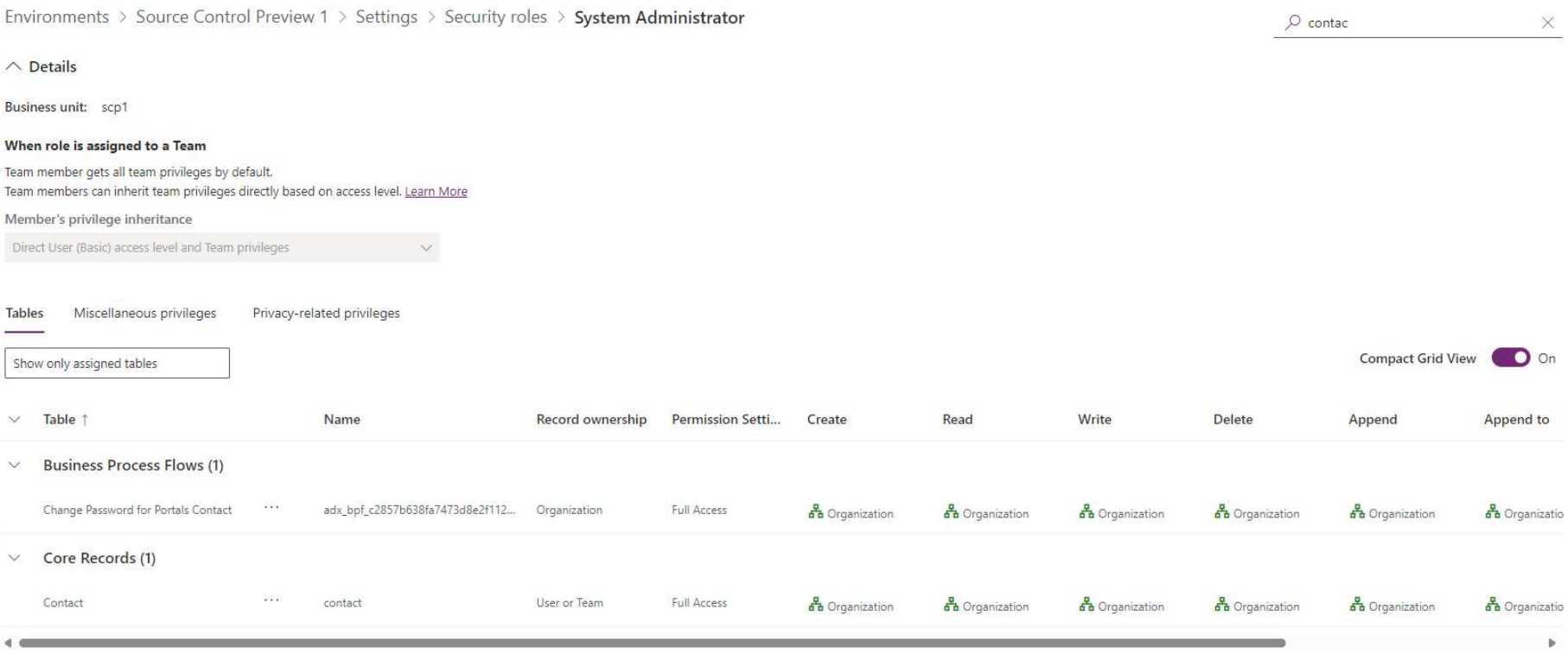


Security Roles

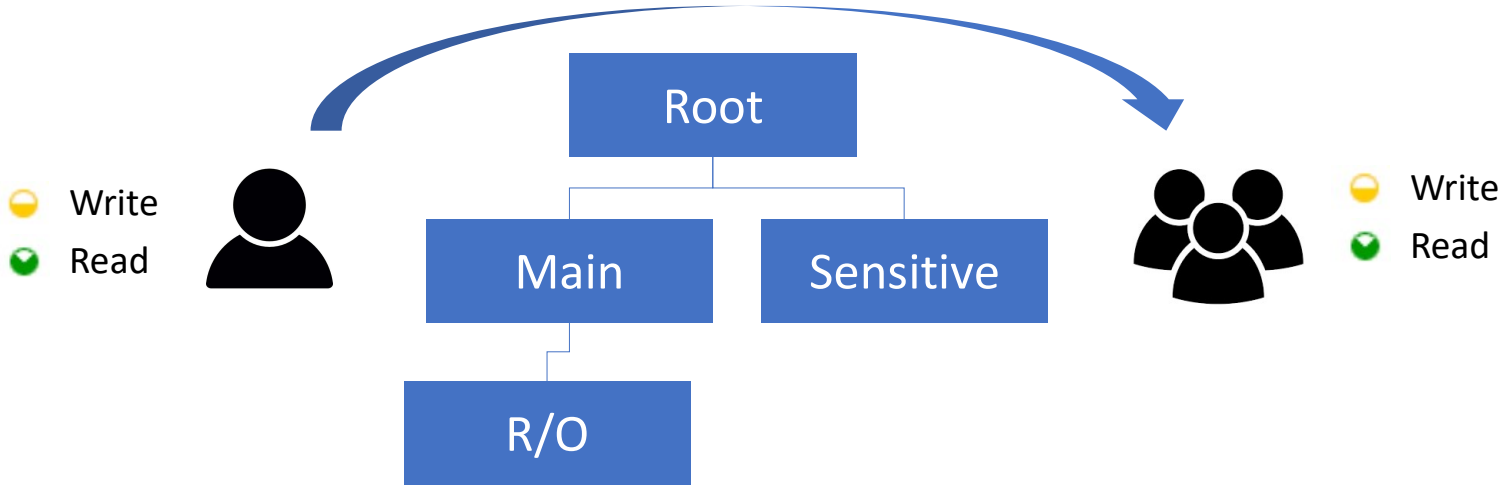
Env > Settings > Users + permissions



Security Roles

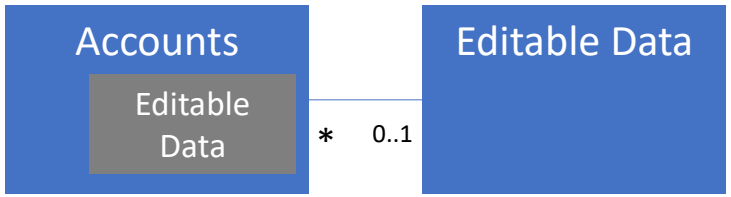


Business Unit and Teams

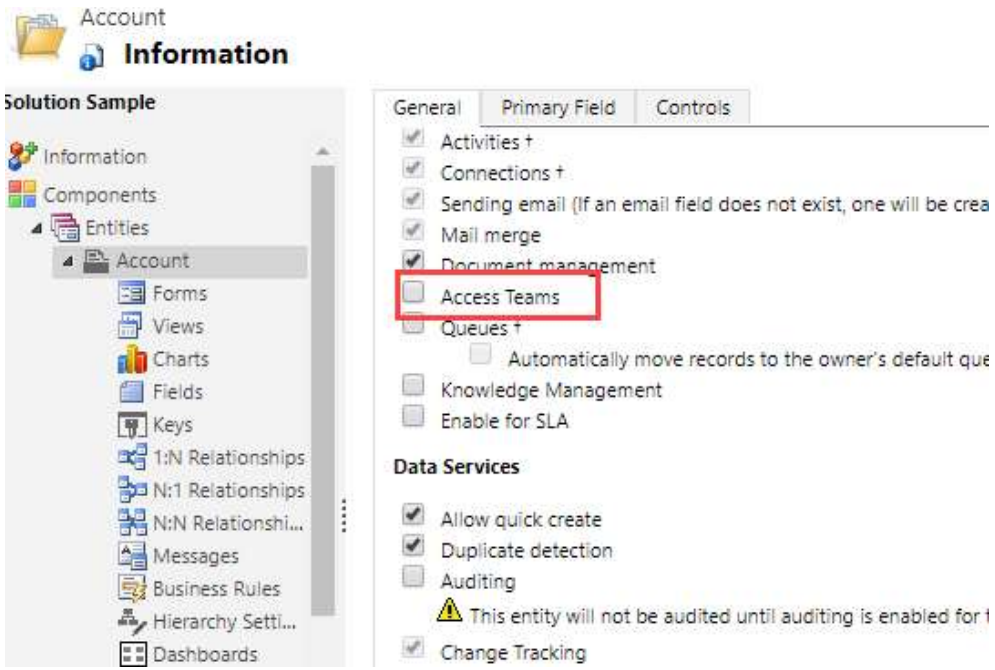


Security Requirement

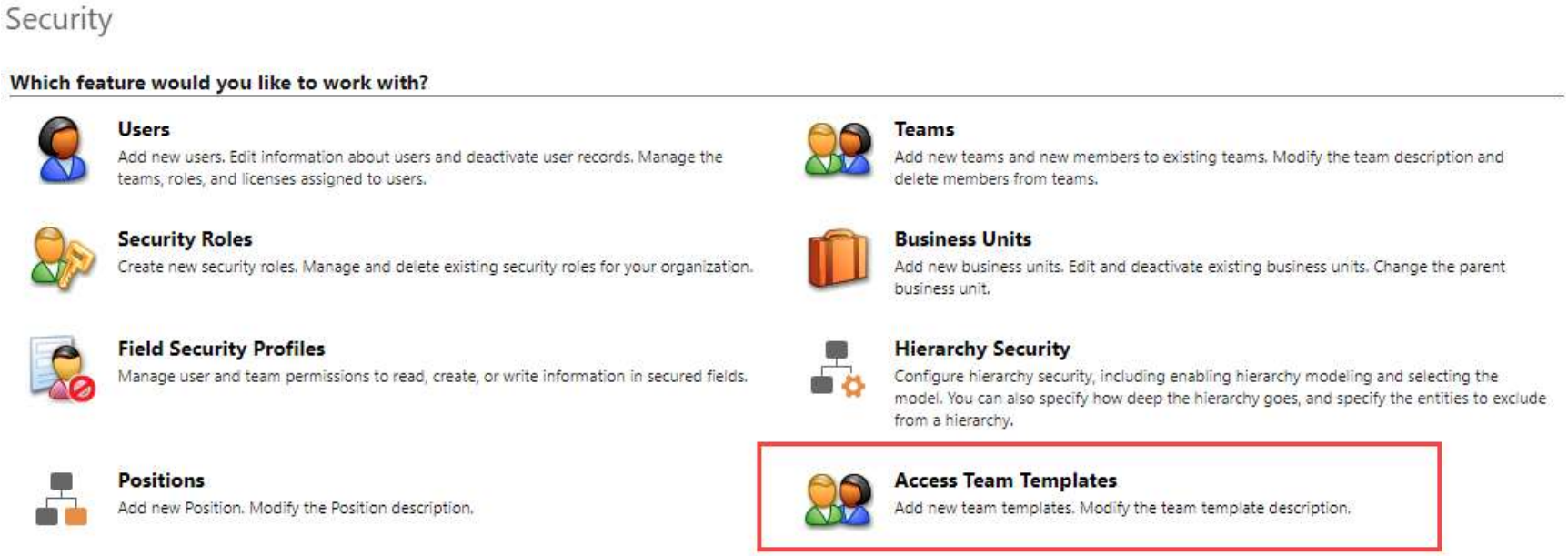
Account are read-only but have Dynamics specific field that can be edited.



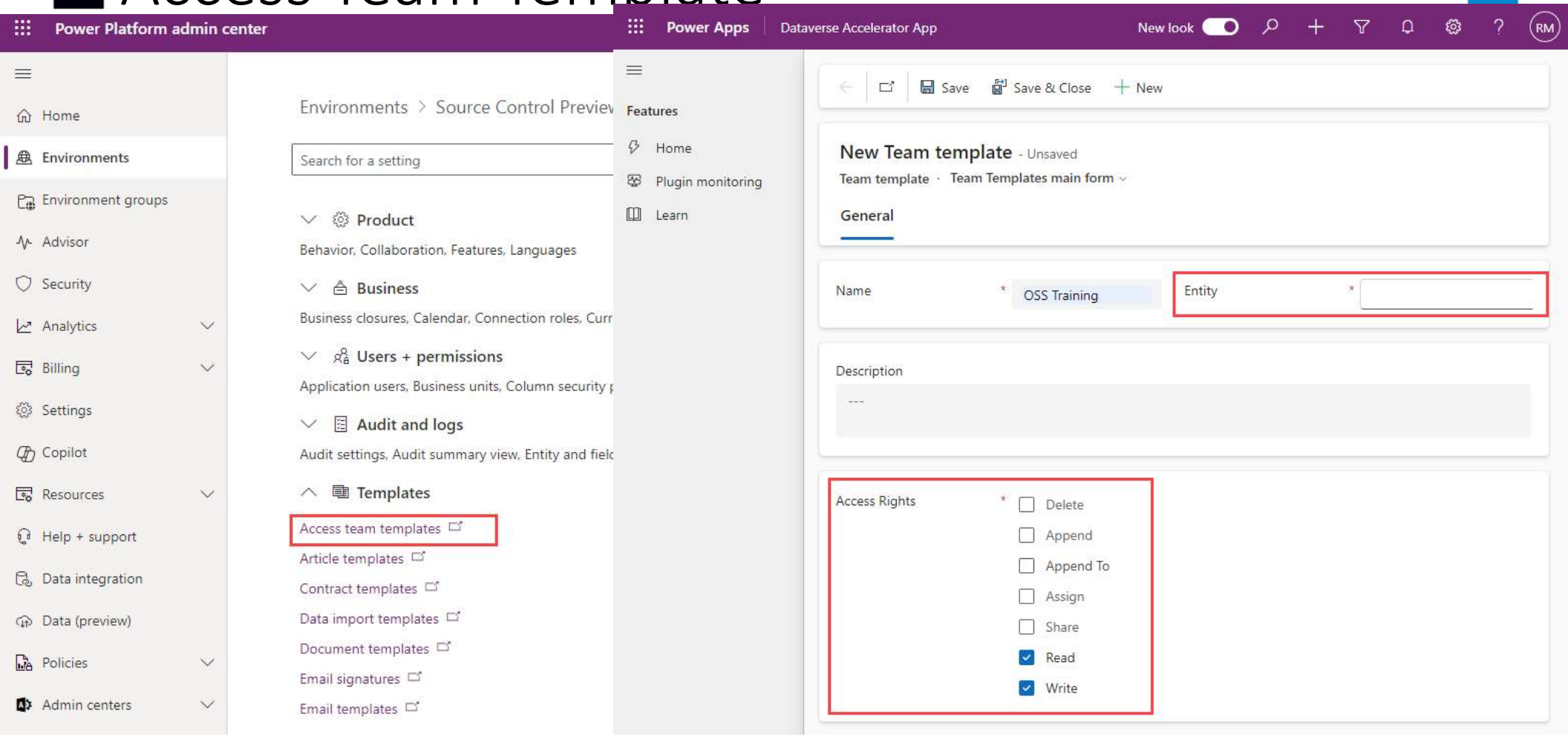
Enable Access Teams



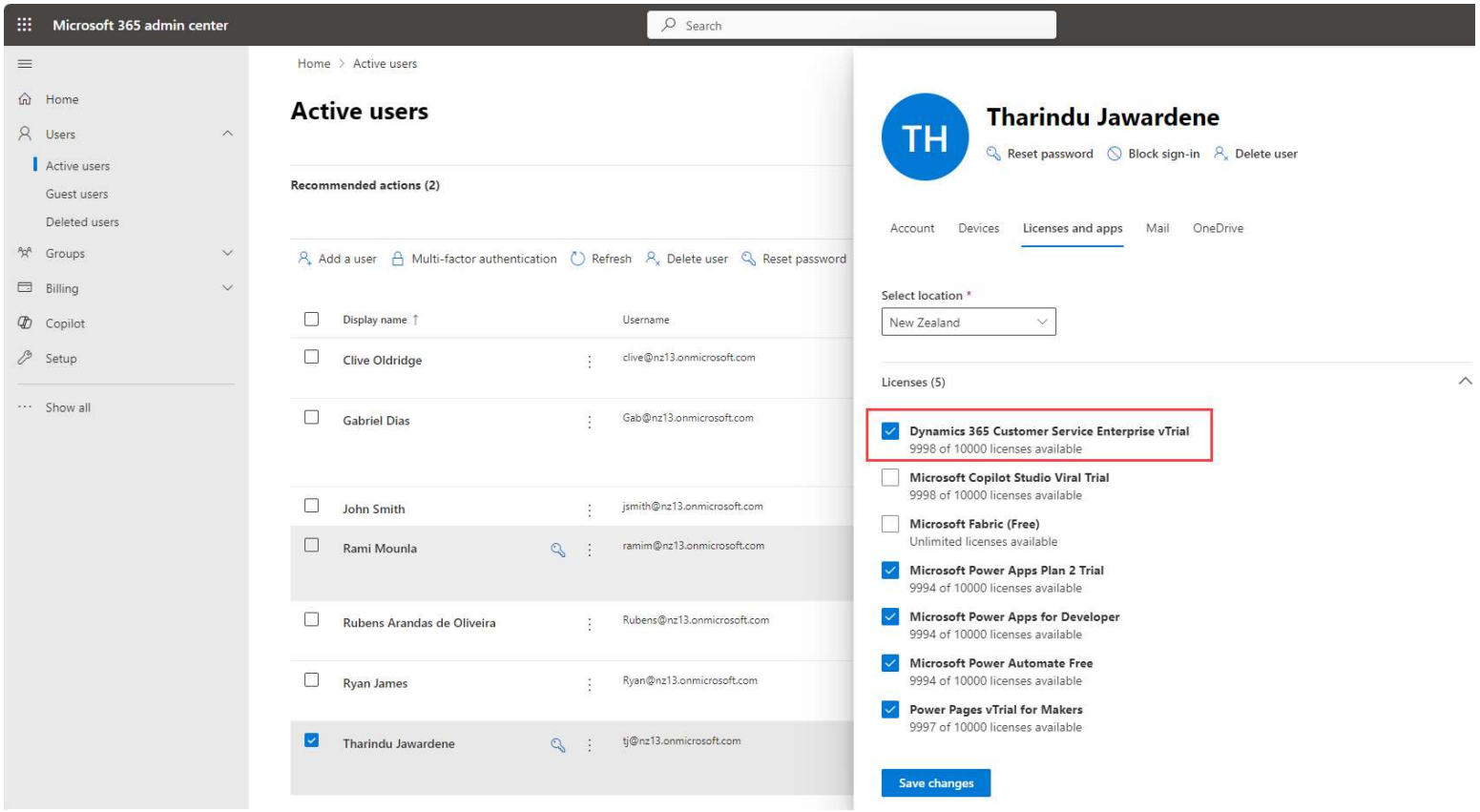
Access Team Template



Access Team Template



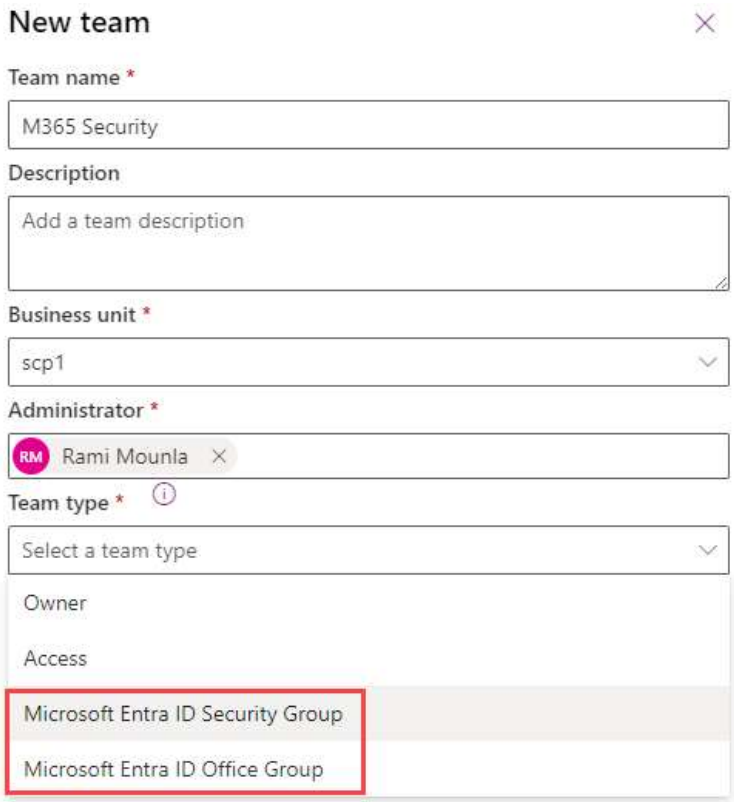
Remove their Licence - admin.microsoft.com



Preventative

Entra ID Security Groups

Entra ID Security Groups



Preventative

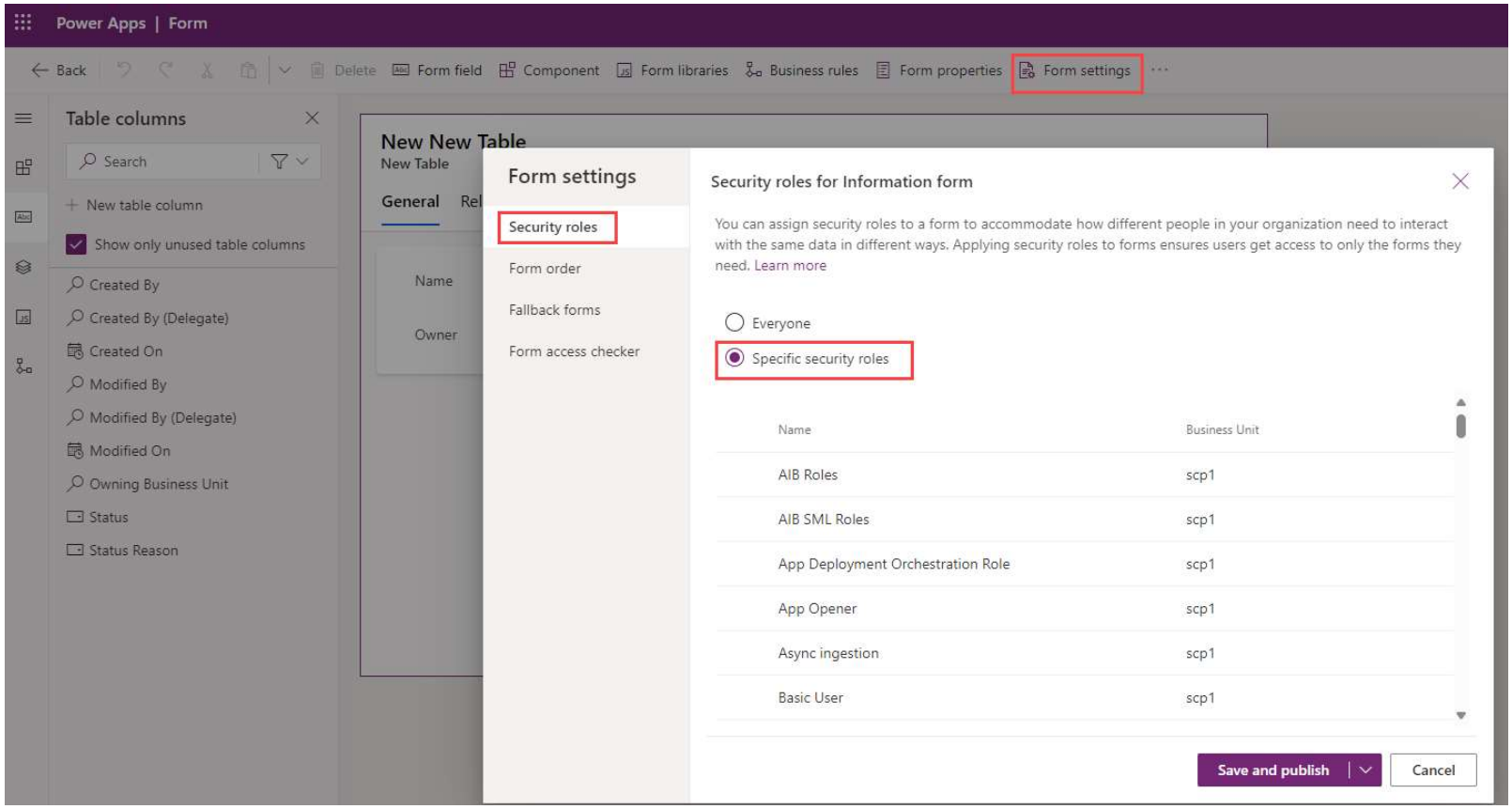
Forms and Apps Restriction

Preventative
Authentication
Authorisation
Encryption
Firewall

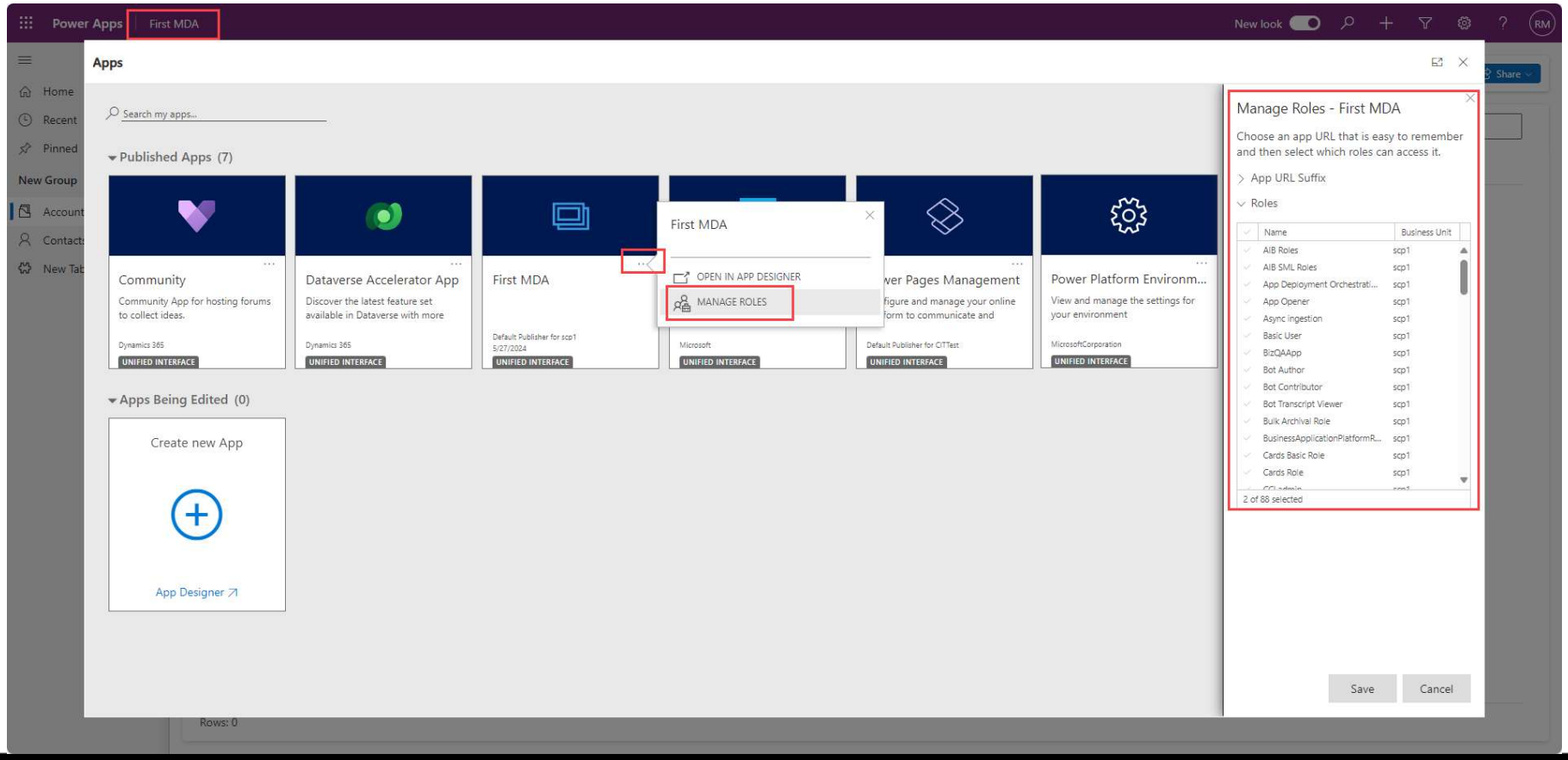
Detective
DoS
Brute Force
Malicious Access
Mass Export

Corrective
Audit Trails
Governance
Notification
Pattern AI

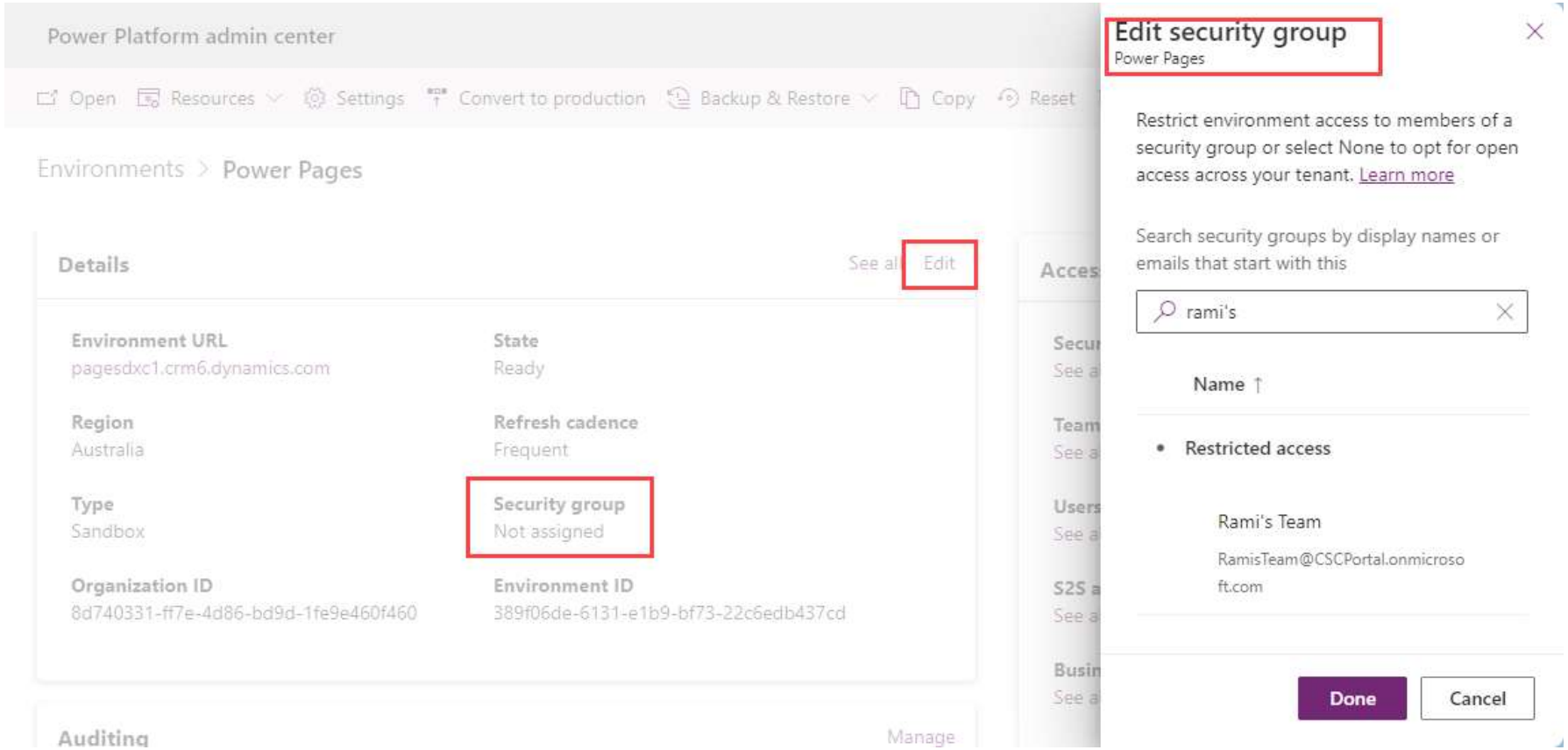
Restrict Access to Forms using Security Roles



Restrict Access to Business Apps with Security Roles



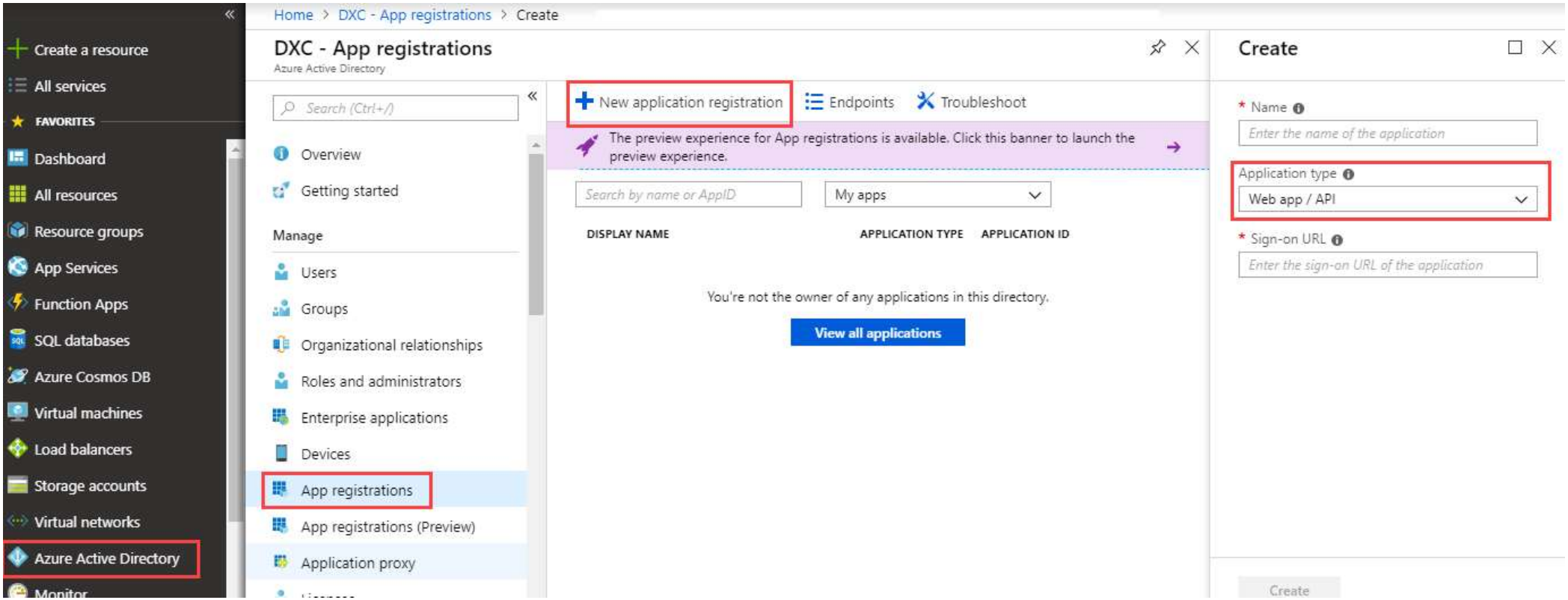
Environment Security Groups



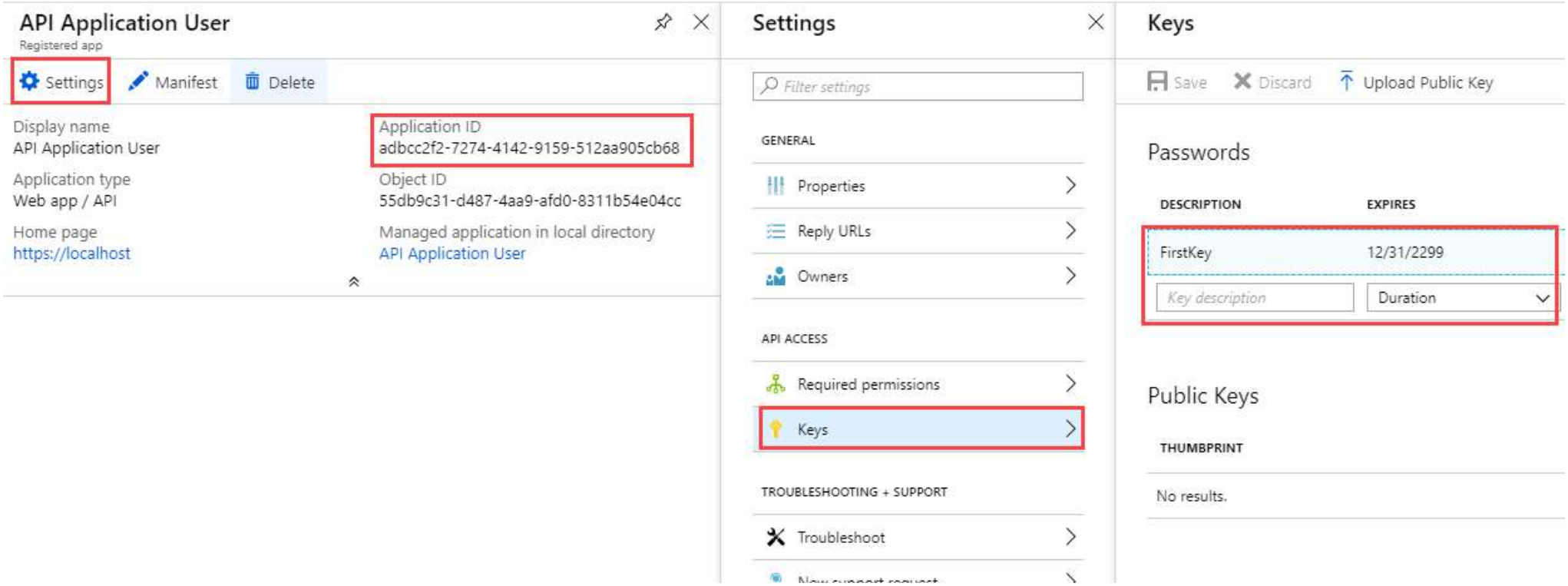
Preventative

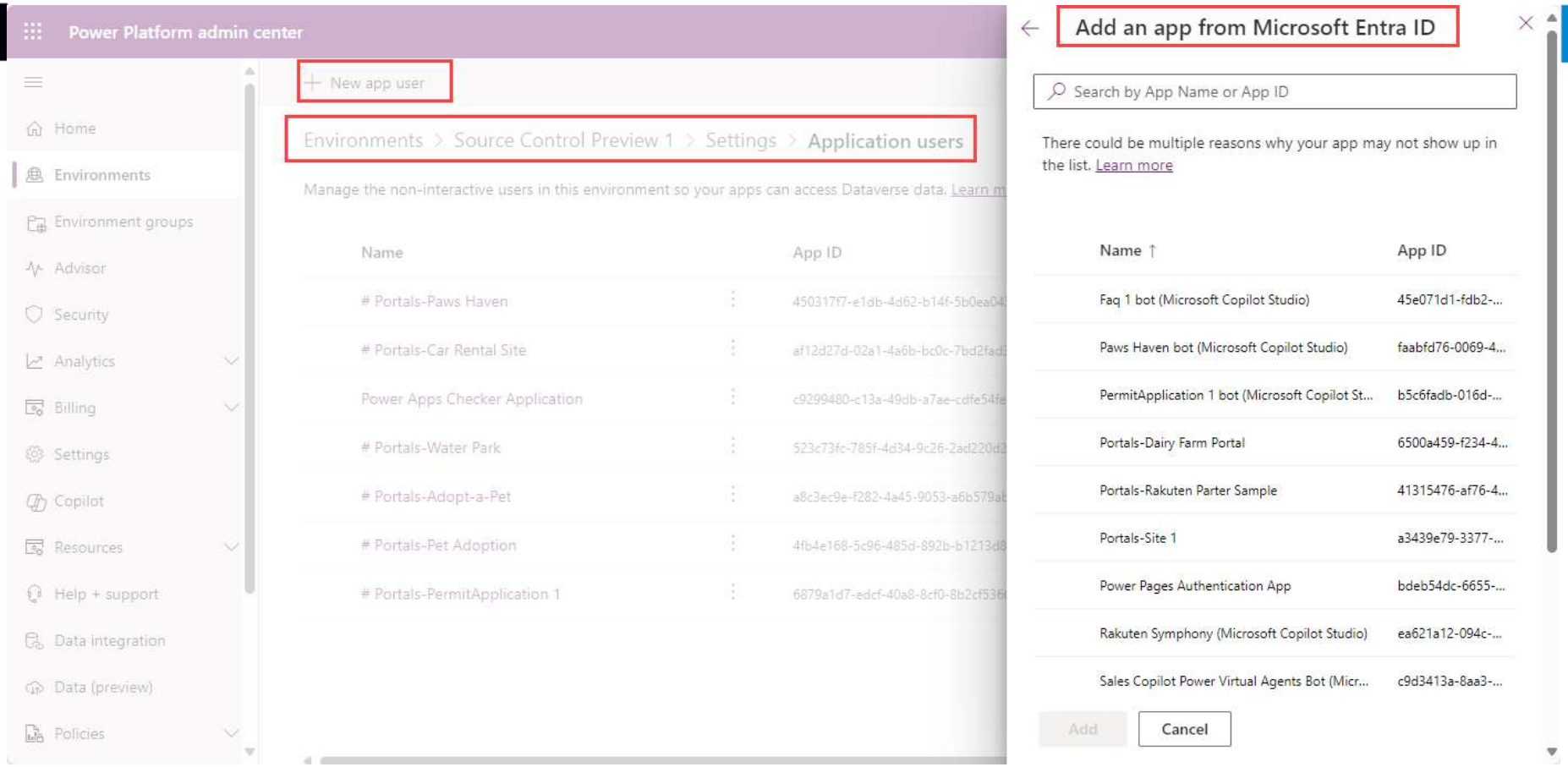
Credential Management

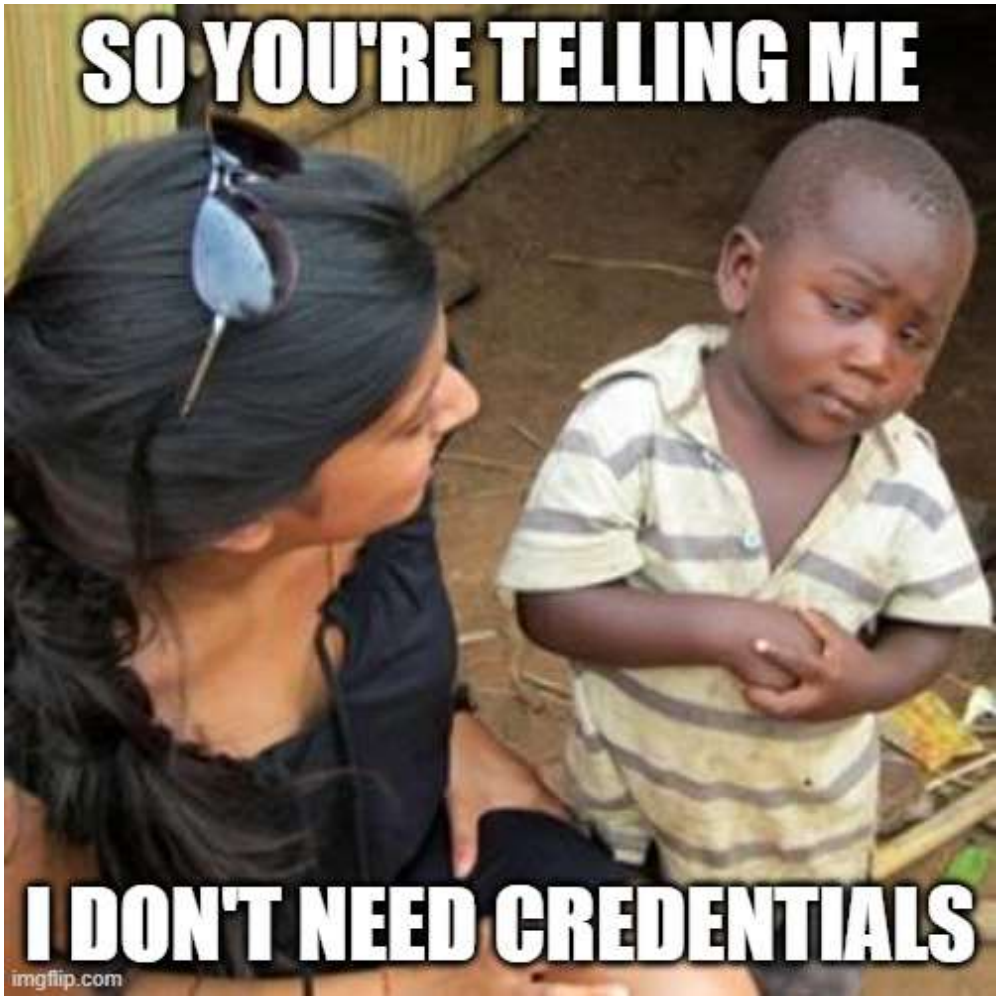
Creating a Web/API account



Create Secret Key




Power Platform admin center
New app user
Home
Environments
Environment groups
Advisor
Security
Analytics
Billing
Settings
Copilot
Resources
Help + support
Data integration
Data (preview)
Policies
Environments > Source Control Preview 1 > Settings > Application users
Manage the non-interactive users in this environment so your apps can access Dataverse data.
Name
App ID
Portals-Paws Haven
Portals-Car Rental Site
Power Apps Checker Application
Portals-Water Park
Portals-Adopt-a-Pet
Portals-Pet Adoption
Portals-PermitApplication 1
Add an app from Microsoft Entra ID
Search by App Name or App ID
There could be multiple reasons why your app may not show up in the list. Learn more
Name ↑
App ID
Faq 1 bot (Microsoft Copilot Studio)
45e071d1-fdb2-...
Paws Haven bot (Microsoft Copilot Studio)
faabfd76-0069-4...
PermitApplication 1 bot (Microsoft Copilot St...
b5c6fadb-016d-...
Portals-Dairy Farm Portal
6500a459-f234-4...
Portals-Rakuten Parter Sample
41315476-af76-4...
Portals-Site 1
a3439e79-3377-...
Power Pages Authentication App
bdeb54dc-6655-...
Rakuten Symphony (Microsoft Copilot Studio)
ea621a12-094c-...
Sales Copilot Power Virtual Agents Bot (Micr...
c9d3413a-8aa3-...
Add
Cancel


SO YOU'RE TELLING ME
I DON'T NEED CREDENTIALS
imgflip.com

Managed Identity

Use managed identities for Dataverse plug-ins

Article • 08/16/2024 • 2 contributors

Feedback

Enabled for	Public preview	General availability
Users, automatically	✔ Aug 6, 2024	Nov 2024

Business value

Power Platform managed identities allow publishers of Dataverse plug-ins to securely connect to Azure resources without having to store or expose credentials. Managed identities eliminate the need for developers to manage these credentials.

Managed Identity

Power Platform managed identity allows enterprises to securely connect with Azure resources that support Azure managed identity from Dataverse plug-ins without the need for managing the credentials.

- Simplifies authentication and reduces the need for credentials management.
- Improves security by reducing the attack surface.
- Enables seamless authentication to other Azure services.

Create managed identity prerequisites

Certificate + thumbprint

Signed Plugin using the certificate

use IManagedIdentityService to acquire a token

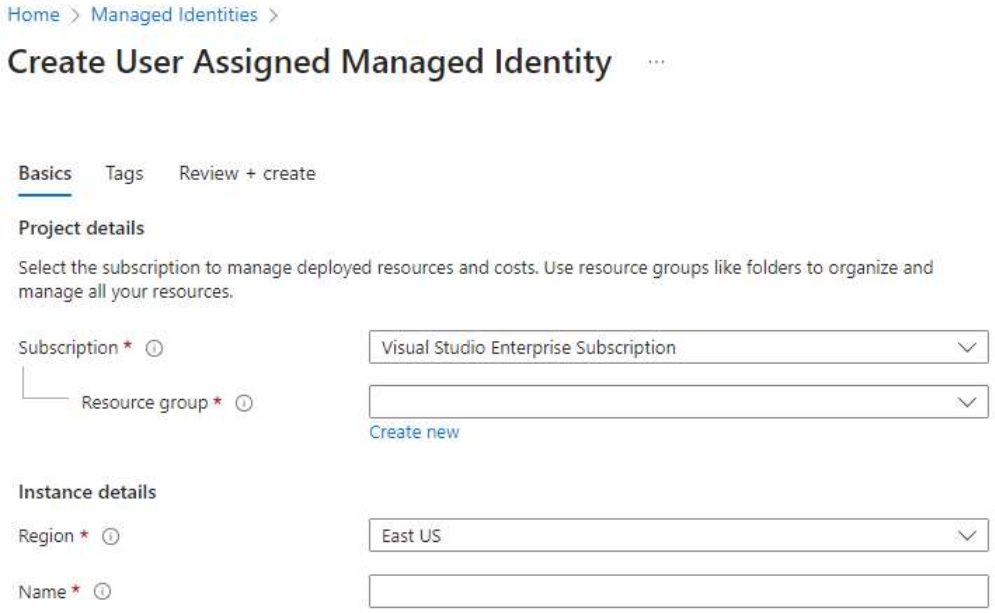
https://learn.microsoft.com/en-us/power-platform/admin/set-up-managed-identity

Managed Identity using the token

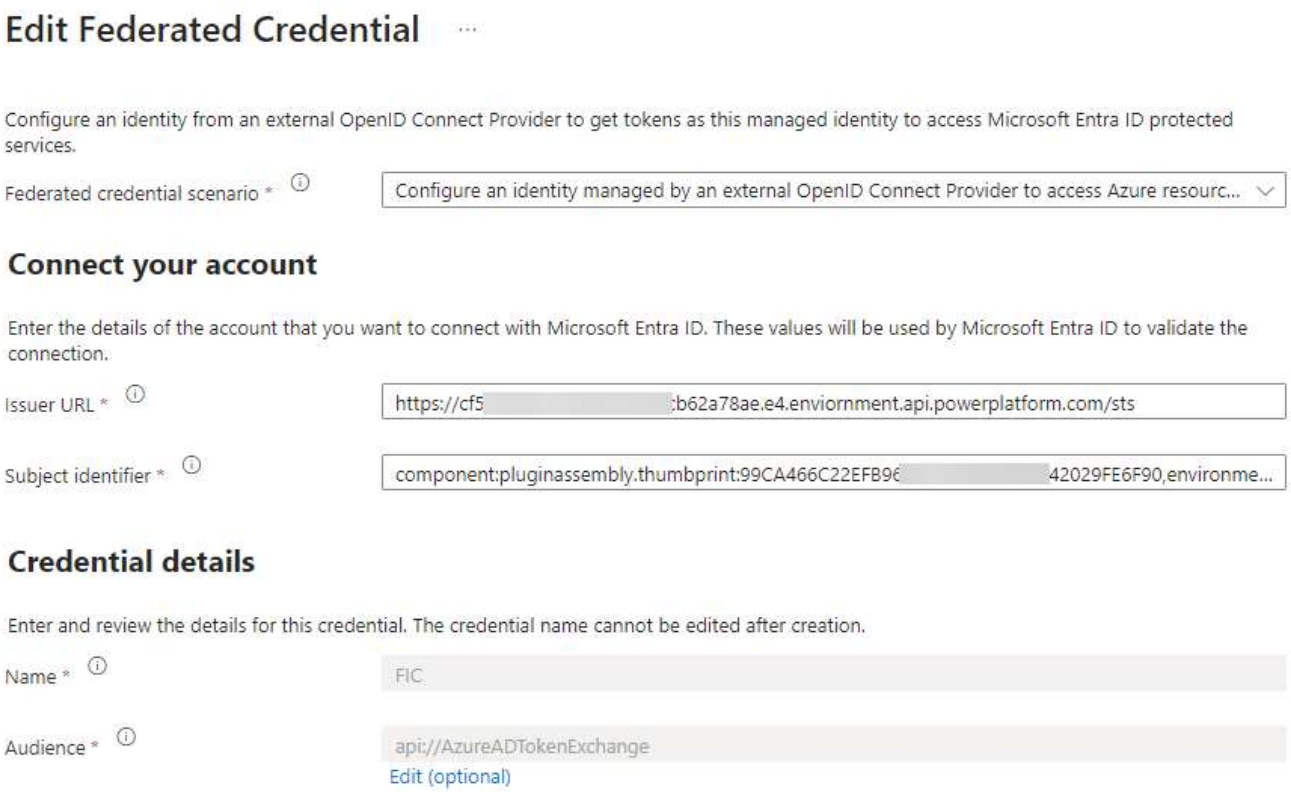
```
using System;
using System.Collections.Generic;
using Microsoft.PowerPlatform.Dataverse.Client;
using Microsoft.PowerPlatform.Dataverse.Client.Auth;
using Microsoft.Xrm.Sdk;

public class SamplePlugin : IPlugin
{
    public void Execute(IServiceProvider serviceProvider)
    {
        IPluginExecutionContext context = (IPluginExecutionContext)serviceProvider.GetService(typeof(IPluginExecutionContext));
        IOrganizationServiceFactory serviceFactory = (IOrganizationServiceFactory)serviceProvider.GetService(typeof(IOrganizationServiceFactory))
        IOrganizationService orgService = serviceFactory.CreateOrganizationService(context.UserId);

        // Retrieve the IManagedIdentityService from the service provider
        var managedIdentityService = (IManagedIdentityService)serviceProvider.GetService(typeof(IManagedIdentityService));

        if (managedIdentityService != null)
        {
            // Define the scopes for acquiring the token
            IEnumerable<string> scopes = new List<string>
            {
                "https://<org>.crm.dynamics.com/.default" // Replace <org> with your Dataverse org URL
            };

            // Call the AcquireToken method
            var token = managedIdentityService.AcquireToken(scopes);
```

Create managed identity 1/3

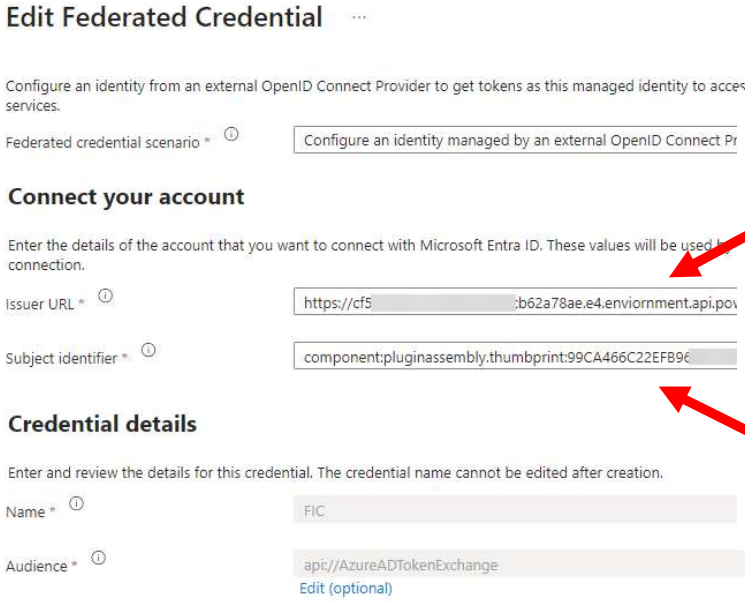
Create App Reg or Managed Identity



Create managed identity 2/3



Create managed identity 2/3



8. Enter the following information:

- **Issuer**: The URL of the token issuer. Format similar to this: `https://[environment ID prefix].[environment ID suffix].enviornment.api.powerplatform.com/sts`
  - **Environment ID prefix** - The environment ID, except for the last two characters.
  - **Environment ID suffix** - The last two characters of the environment ID.

  Example: `https://92e1c10d0b34e28ba4a87e3630f46a.06.environment.api.powerplatform.com/sts`

- **Subject identifier**: If a self-signed certificate is used for signing the assembly, use only recommended for non-production use cases.

  Example: `component:pluginassembly,thumbprint:<<Thumbprint>>,environment:<<EnvironmentId>>`

Create managed identity 3/3

Register Managed Identity in Dataverse

```
POST https://<<orgURL>>/api/data/v9.0/managedidentities
```

Be sure to replace **orgURL** with the URL of the organization.

Ensure that **Credentialsource** is set to **2** in the payload and **SubjectScope** is set to **1** for environment-specific scenarios.

Sample

Copy

```
{
   "applicationid":"<<appId>>",
   "managedidentityid":"<<anyGuid>>",
   "credentialsource":2,
   “subjectscope”:1,
   "tenantid":"<<tenantId>>"
}
```

Create managed identity 3/3

Register Managed Identity in Dataverse

```
PATCH https:// <<orgURL>>/api/data/v9.0/pluginassemblies(<<PluginAssemblyId>>)
```

Be sure to replace **orgURL** and **PluginAssemblyId**.

Sample Copy

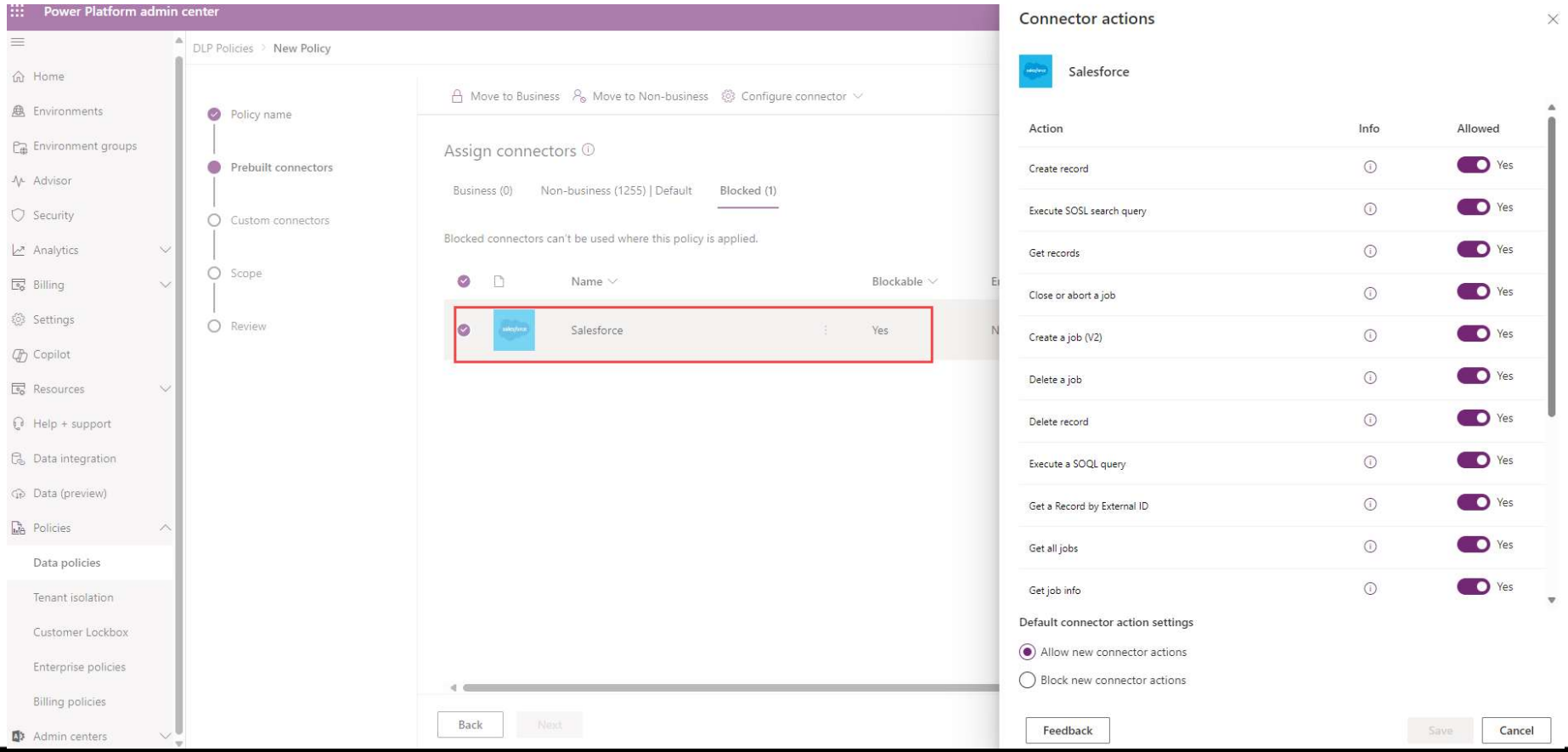
```
{
   "managedidentityid@odata.bind": "/managedidentities(<<ManagedIdentityGuid>>)"
}
```

https://learn.microsoft.com/en-us/power-platform/admin/set-up-managed-identity

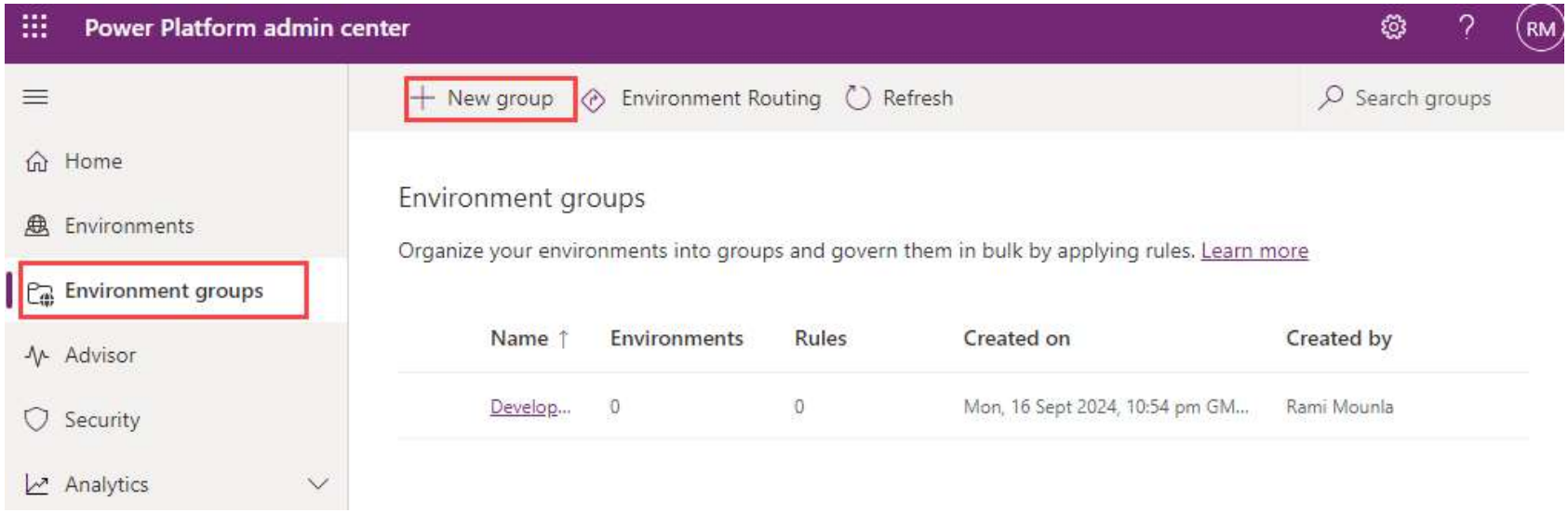
Preventative

Data Policies

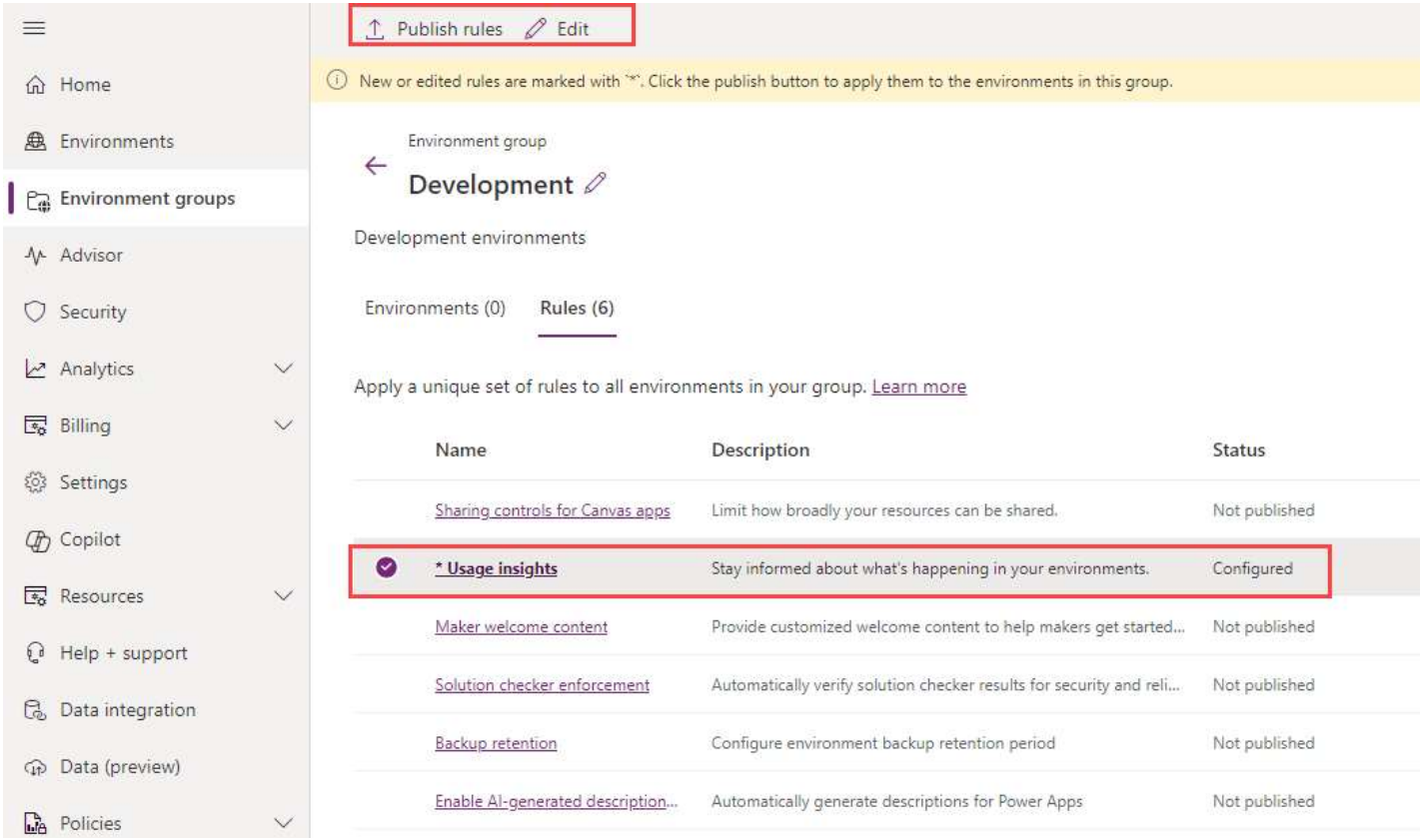
Data Policies



Environment Group



Environment Group



Preventative

Masking Sensitive Data

Inland Revenue says all the details shared with soc

Inland Revenue giving thousands of taxpayers' details to social media platforms for ad campaigns

8:06 am on 9 September 2024

Share this

Phil Pennington, Reporter
@pjppenn phil.pennington@rnz.co.nz

Inland Revenue is giving hundreds of thousands of taxpayers' details to social media platforms for marketing campaigns, using an anonymisation tool that top international regulators say is inadequate at protecting people's personal information.

In a statement, Inland Revenue said all the details were fully protected by anonymisation using a "hashing" process, in which letters are replaced by numbers.

"The lists are of up to 500,000 customers each, with names, DOB, address, phone, and email contacts.

"The data is hashed as it is being uploaded to Facebook, Instagram, or LinkedIn. We do not share any customer details directly with them.

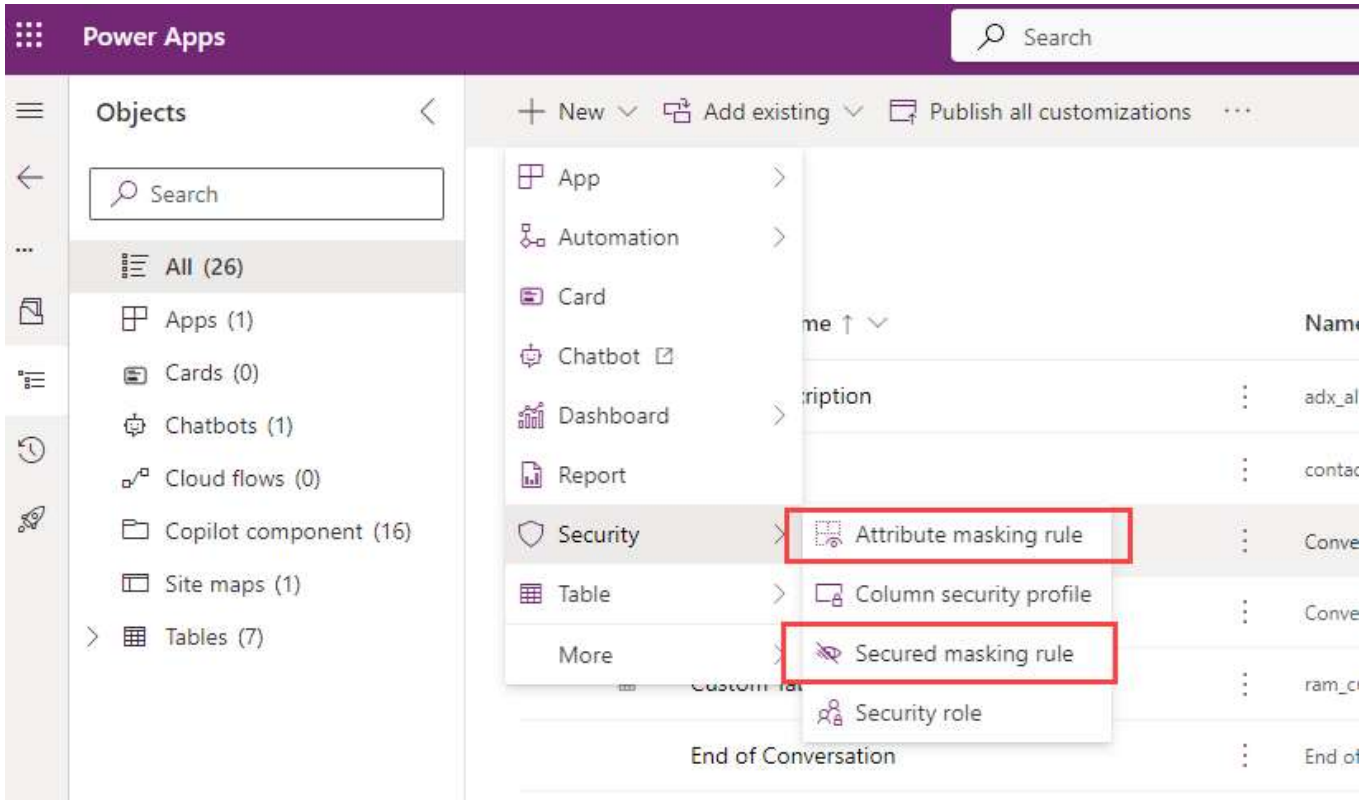
However, in July, the United States Federal Commission said in a press release that hashing was not adequate protection.

"No, hashing still doesn't make your data anonymous," the headline of the statement said.

"Companies often claim that hashing allows them to preserve user privacy.

"This logic is as old as it is flawed - hashes aren't 'anonymous' and can still be used to identify users, and their misuse can lead to harm. Companies should not act or claim as if hashing personal information renders it anonymised."

Masking Sensitive Data



Masking Sensitive Data

ram_maskemail - Saved

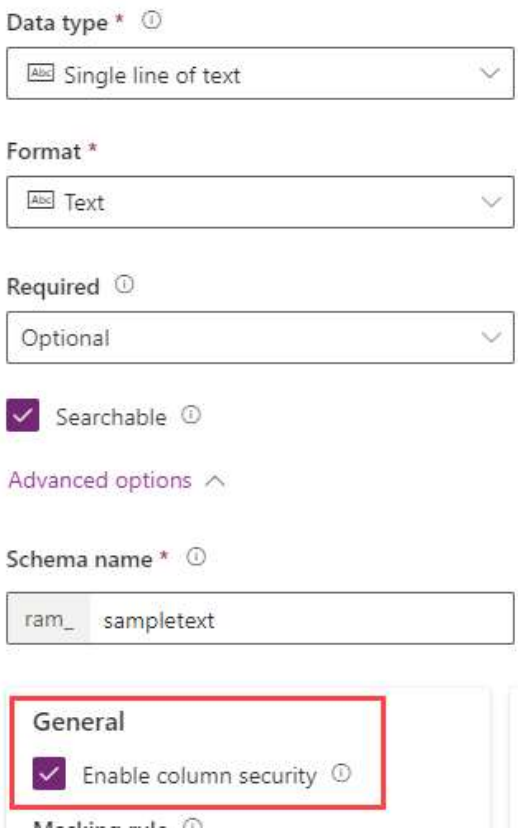
Secured Masking Rule

Summary | Related

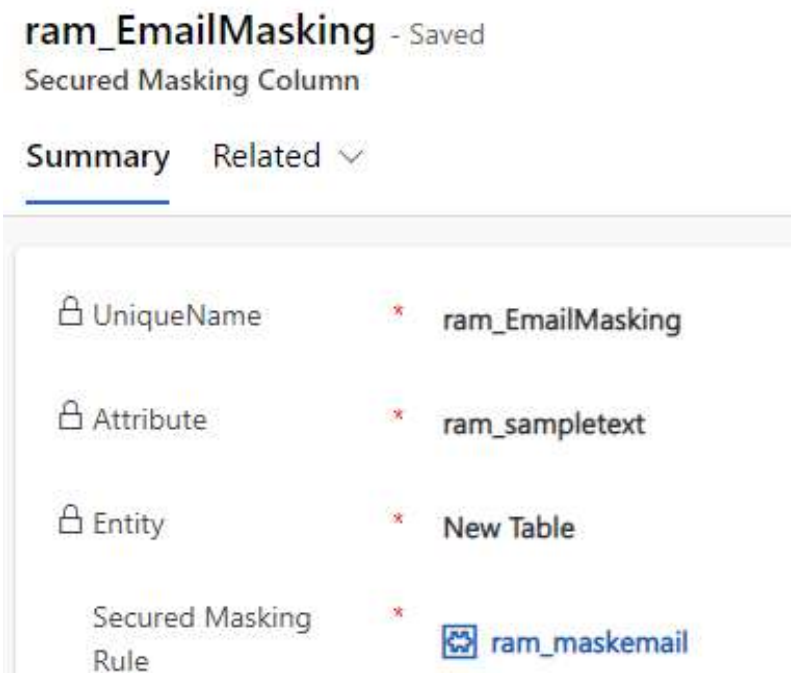
Name *	ram_maskemail
Display Name *	Mask Email
Description *	Mask Email
Regular Expression - Learn more at https://go.microsoft.com/fwlink/p/?linkid=2259742 *	.*?@?[^@]*\.+.*
Masked Character *	*

Enter Plain Text Test Data	test@test.com
Enter Rich Text Test Data	
Masked Plain Text Test Data	*
Masked Rich Text Test Data	

Masking Sensitive Data



Masking Sensitive Data



Masking Sensitive Data

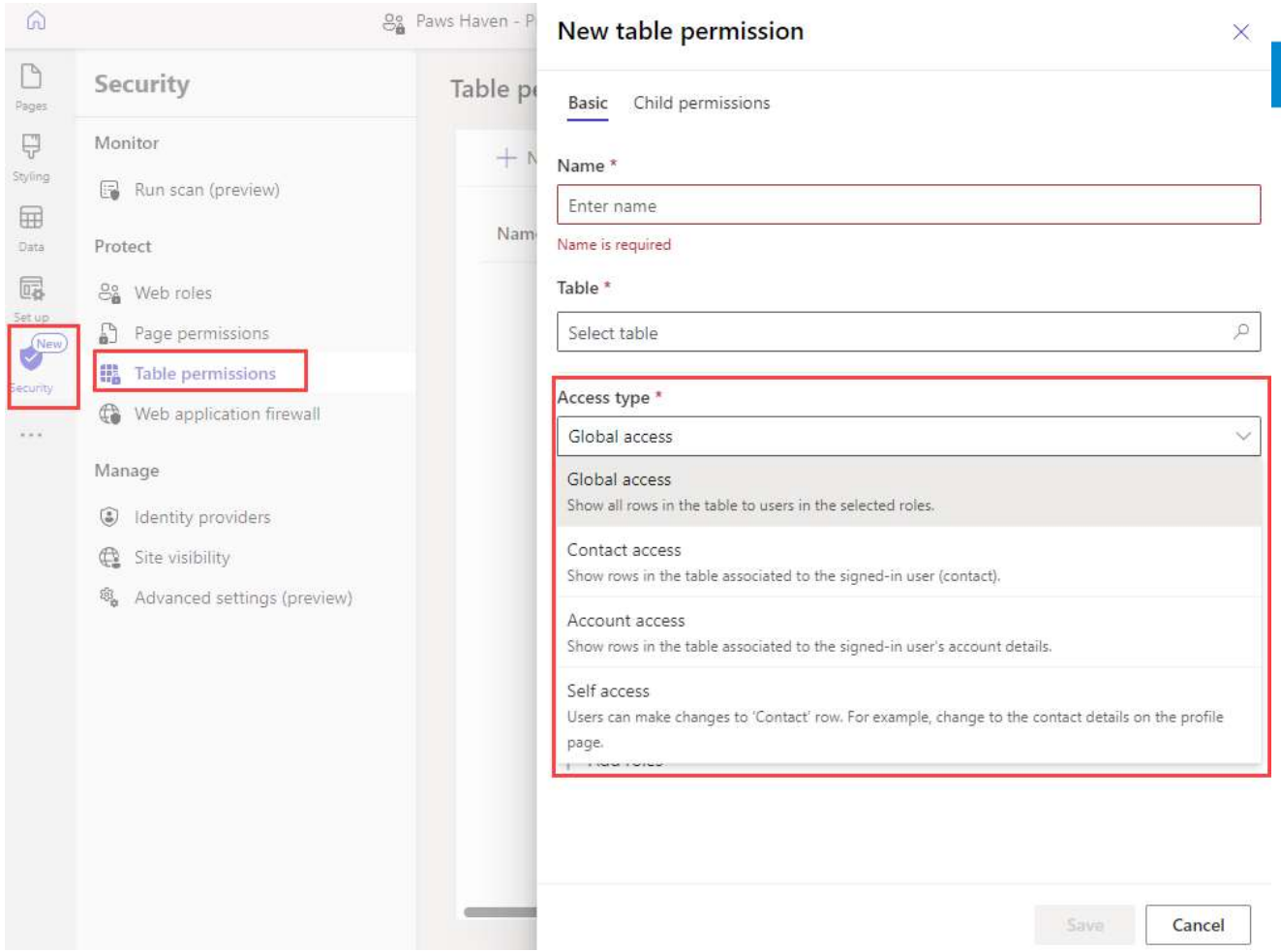
https://scp1.crm.dynamics.com/api/data/v9.2/ram_newtables?$top=50


```
{
    "@odata.context": "https://scp1.crm.dynamics.com/api/data/v9.2/$metadata#ram_newtables",
    "value": [
        {
            "@odata.etag": "W/\"3499795\"",
            "createdon": "2024-09-17T04:41:20Z",
            "_ownerid_value": "ff685a4c-db10-ef11-9f89-0022480c1f28",
            "utcconversiontimezonecode": null,
            "_createdby_value": "ff685a4c-db10-ef11-9f89-0022480c1f28",
            "overriddencreatedon": null,
            "statecode": 0,
            "modifiedon": "2024-09-17T04:41:20Z",
            "statuscode": 1,
            "importsequencenumber": null,
            "_createdonbehalfby_value": null,
            "ram_name": "Hello",
            "timezoneruleversionnumber": null,
            "_modifiedby_value": "ff685a4c-db10-ef11-9f89-0022480c1f28",
            "ram_newtableid": "87d0090f-af74-ef11-ac20-000d3a32e15c",
            "versionnumber": 3499795,
            "_owningbusinessunit_value": "0d625a4c-db10-ef11-9f89-0022480c1f28",
            "_modifiedonbehalfby_value": null,
            "ram_sampletext": "*",
            "_owningteam_value": null,
            "_owninguser_value": "ff685a4c-db10-ef11-9f89-0022480c1f28"
        }
    ]
}
```

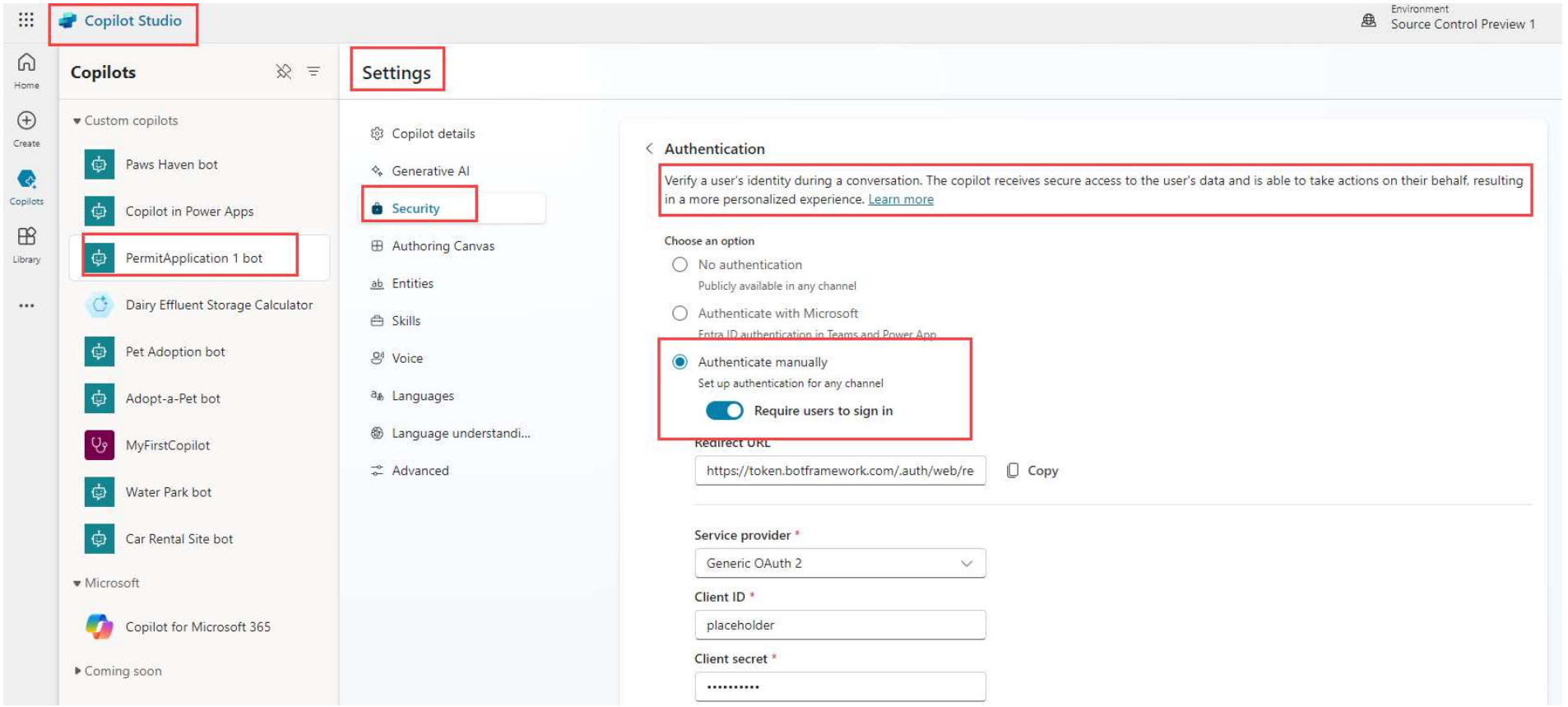
Preventative

Other areas to secure

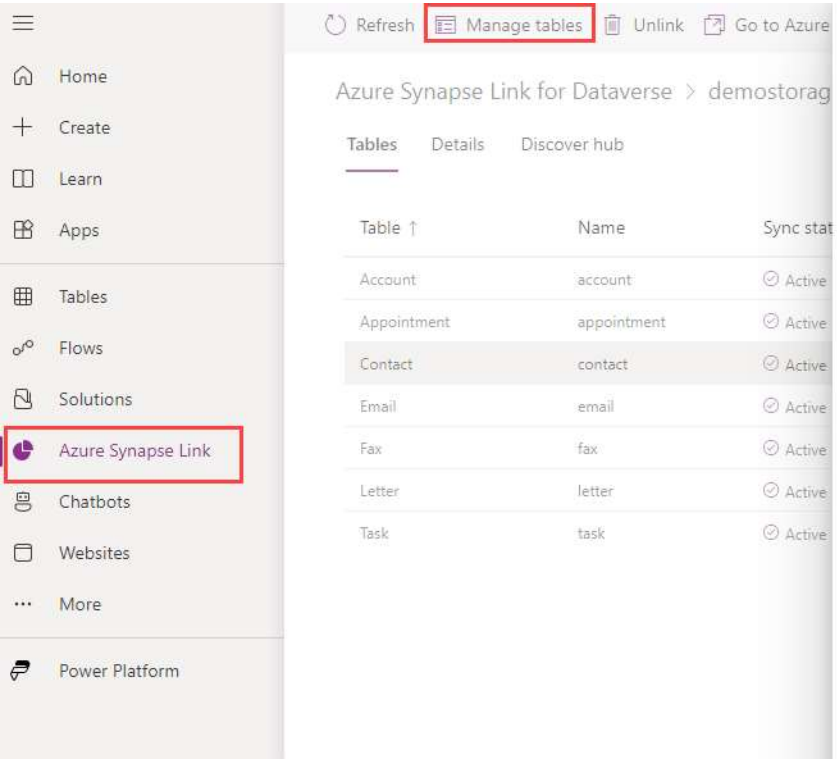
Power Pages

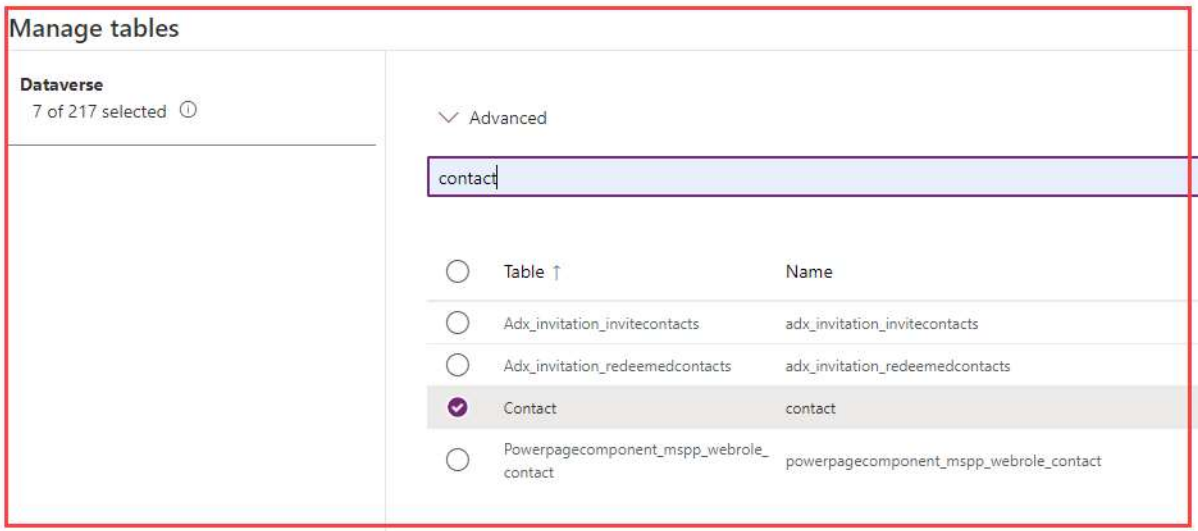

Paws Haven - P
Security
Monitor
Run scan (preview)
Protect
Web roles
Page permissions
Table permissions
Web application firewall
Manage
Identity providers
Site visibility
Advanced settings (preview)
Pages
Styling
Data
Set up
New
Security
New table permission
Basic
Child permissions
Name *
Enter name
Name is required
Table *
Select table
Access type *
Global access
Global access
Show all rows in the table to users in the selected roles.
Contact access
Show rows in the table associated to the signed-in user (contact).
Account access
Show rows in the table associated to the signed-in user's account details.
Self access
Users can make changes to 'Contact' row. For example, change to the contact details on the profile page.
Save
Cancel

CoPilot Studio

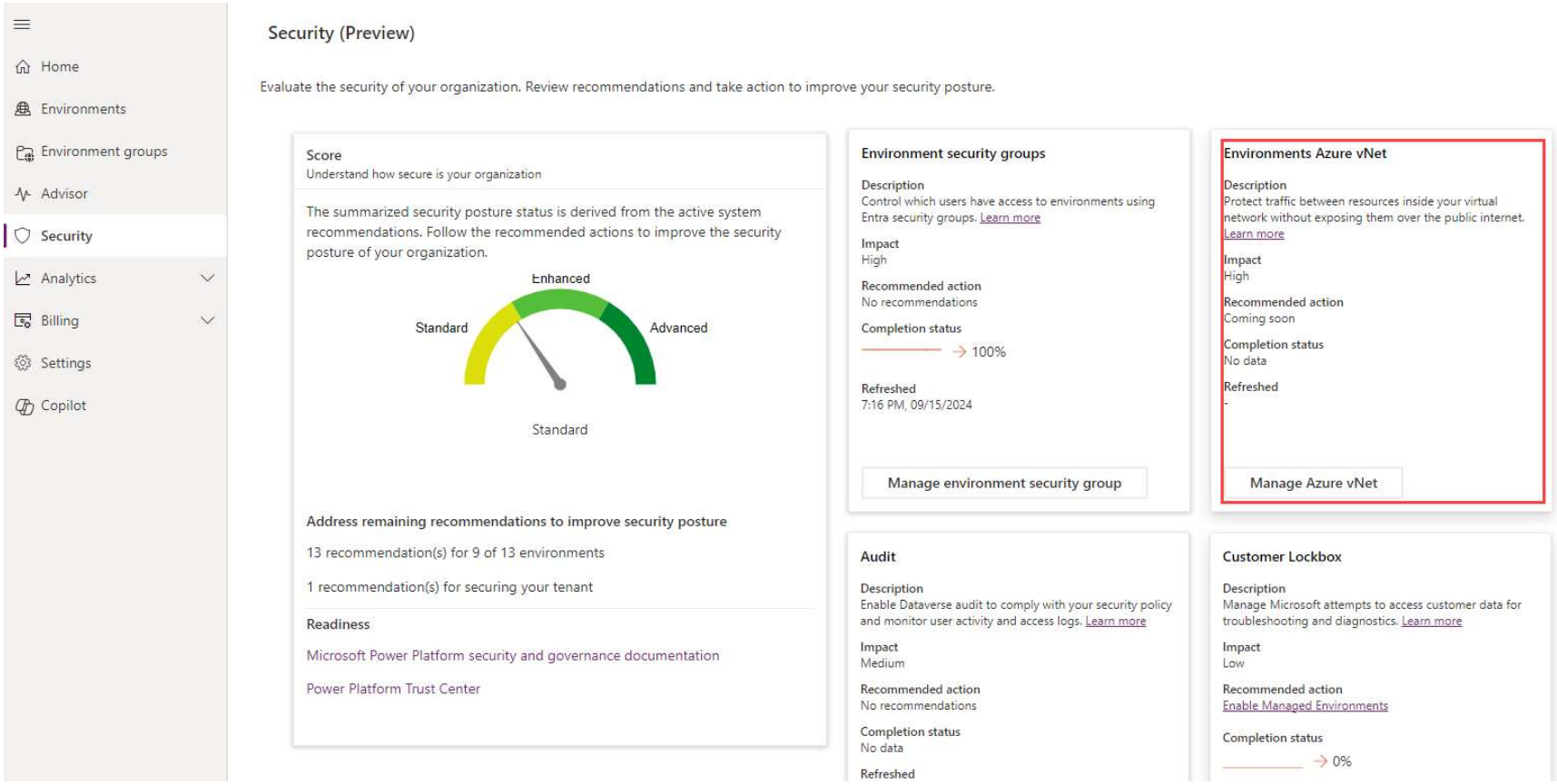


Link to Synapse





Azure Back Bone – Secure Network



Preventative

Power Platform Admin Center

Learn more about Privacy + Security

Privacy preference

Show privacy statement link for this organization

Off

Privacy statement URL

Default action to take when an error occurs

- Ask the user for permission to send an error report to Microsoft
- Automatically send an error report to Microsoft without user interaction
- Never send an error report to Microsoft

Blocked Attachments

Block these file extensions

ade;adp;app;asa;ashx;asmx;asp;bas;bat;cdx;cer;chm;class;cmd;com;config;cpl;crt;csh;dll;exe;fxp;hlp;hta;htr;htw;ida;idc;idq;inf;ins;isp;its;jar;js;jse;ksh;lnk;mad;maf;mag;mam;maq;mar;mas;mat;mau;mav;maw;mda;mdb;mde;mdt;mdw;mdz;msc;msh;msh1;msh1xml;msh2;msh2xml;mshxml;msi;msp;mst;ops;pcd;pif;prf;prg;printer;pst;reg;rem;scf;scr;sct;shb;shs;shtm;shtml;soap;stm;tmp;url;vb;vbe;vbs;vsmacros;vss;vst;vsw;ws;wsc;wsf;wsh

Blocked Mime Types

Block upload of these mime types

Session Expiration

Set custom session timeout

On

Enter maximum session length

Minutes

Enter a value from 60 through 1440.

How long before the session expires do you want to show a timeout warning?

Minutes

Enter a value from 20 through 1440.

Inactivity timeout

Set inactivity timeout

On

Duration of inactivity before timeout

Minutes

Enter a value from 5 through 1440.

How long before the session expires do you want to show an inactivity warning?

Minutes

Enter a value from 1 through 1440.

Enable sharing

Allow users to share read-only links to records with other users from this environment.

On

Learn more about Privacy + Security

Privacy preference

Show privacy statement link for this organization

Off

Privacy statement URL

Default action to take when an error occurs

- Ask the user for permission to send an error report to Microsoft
- Automatically send an error report to Microsoft without user interaction
- Never send an error report to Microsoft

Blocked Attachments

Block these file extensions

ade;adp;app;asa;ashx;asmx;asp;bas;bat;cdx;cer;chm;class;cmd;com;config;cpl;crt;csh;dll;exe;fxp;hlp;hta;htr;htw;ida;idc;idq;inf;ins;isp;its;jar;js;jse;ksh;lnk;mad;maf;mag;mam;maq;mar;mas;mat;mau;mav;maw;mda;mdb;mde;mdt;mdw;mdz;msc;msh;msh1;msh1xml;msh2;msh2xml;mshxml;msi;msp;mst;ops;pcd;pif;prf;prg;printer;pst;reg;rem;scf;scr;sct;shb;shs;shtm;shtml;soap;stm;tmp;url;vb;vbe;vbs;vsmacros;vss;vst;vsw;ws;wsc;wsf;wsh

Blocked Mime Types

Block upload of these mime types

Allowed Mime Types

Allow upload of these mime types. If allowed mime types has value, then blocked mime types is ignored.

Session Expiration

Set custom session timeout

Off

Enter maximum session length

Minutes

How long before the session expires do you want to show a timeout warning?

Minutes

Inactivity timeout

Set inactivity timeout

Off

Enable sharing

Allow users to share read-only links to records with other users from this environment.

On

Show details when unfurling links

Show record name and type to unauthorized users when unfurling links in Teams chats

On

IP address settings

Enable IP address based cookie binding.

Off

Available for managed environments only. Learn more

Enable IP address based firewall rule.

Off

Available for managed environments only. Learn more

Storage Shared Access Signature (SAS) Security Settings (Preview)

Critical Advisory : Prior to activating SAS features customers must first allowlist `https://*.api.powerplatformusercontent.com` domain or most SAS functionalities will NOT work

Enable IP address based Storage Shared Access Signature (SAS) rule

Off

No IP SAS restriction set. Learn more

Enable SAS Logging in Purview

Off

Learn more about Privacy + Security

Privacy preference

Show privacy statement link for this organization

Off

Privacy statement URL

Default action to take when an error occurs

- Ask the user for permission to send an error report to Microsoft
- Automatically send an error report to Microsoft without user interaction
- Never send an error report to Microsoft

Blocked Attachments

Block these file extensions

ade;adp;app;asa;ashx;asmx;asp;bas;bat;cdx;cer;chm;class;cmd;com;config;cpl;crt;csh;dll;exe;fxp;hlp;hta;htr;htw;ida;idc;idq;inf;ins;isp;its;jar;js;jse;ksh;lnk;mad;maf;mag;mam;maq;mar;mas;mat;mau;mav;maw;mda;mdb;mde;mdt;mdw;mdz;msc;msh;msh1;msh1xml;msh2;msh2xml;mshxml;msi;msp;mst;ops;pcd;pif;prf;prg;printer;pst;reg;rem;scf;scr;sct;shb;shs;shtm;shtml;soap;stm;tmp;url;vb;vbe;vbs;vsmacros;vss;vst;vsw;ws;wsc;wsf;wsh

Blocked Mime Types

Block upload of these mime types

Allowed Mime Types

Allow upload of these mime types. If allowed mime types has value, then blocked mime types is ignored.

Session Expiration

Set custom session timeout

Off

Enter maximum session length

Minutes

How long before the session expires do you want to show a timeout warning?

Minutes

Inactivity timeout

Set inactivity timeout

Off

Enable sharing

Allow users to share read-only links to records with other users from this environment.

On

Show details when unfurling links

Show record name and type to unauthorized users when unfurling links in Teams chats

On

IP address settings

Enable IP address based cookie binding.

Off

Available for managed environments only. Learn more

Enable IP address based firewall rule.

Off

Available for managed environments only. Learn more

Storage Shared Access Signature (SAS) Security Settings (Preview)

Critical Advisory : Prior to activating SAS features customers must first allowlist `https://*.api.powerplatformusercontent.com` domain or most SAS functionalities will NOT work

Enable IP address based Storage Shared Access Signature (SAS) rule

Off

No IP SAS restriction set. Learn more

Enable SAS Logging in Purview

Off

Learn more about Privacy + Security

Privacy preference

Show privacy statement link for this organization

Off

Privacy statement URL

Default action to take when an error occurs

- Ask the user for permission to send an error report to Microsoft
- Automatically send an error report to Microsoft without user interaction
- Never send an error report to Microsoft

Blocked Attachments

Block these file extensions

ade;adp;app;asa;ashx;asmx;asp;bas;bat;cdx;cer;chm;class;cmd;com;config;cpl;crt;csh;dll;exe;fxp;hlp;hta;htr;htw;ida;idc;idq;inf;ins;isp;its;jar;js;jse;ksh;lnk;mad;maf;mag;mam;maq;mar;mas;mat;mau;mav;maw;mda;mdb;mde;mdt;mdw;mdz;msc;msh;msh1;msh1xml;msh2;msh2xml;mshxml;msi;msp;mst;ops;pcd;pif;prf;prg;printer;pst;reg;rem;scf;scr;sct;shb;shs;shtm;shtml;soap;stm;tmp;url;vb;vbe;vbs;vsmacros;vss;vst;vsw;ws;wsc;wsf;wsh

Blocked Mime Types

Block upload of these mime types

Allowed Mime Types

Allow upload of these mime types. If allowed mime types has value, then blocked mime types is ignored.

Session Expiration

Set custom session timeout

Off

Enter maximum session length

Minutes

How long before the session expires do you want to show a timeout warning?

Minutes

Inactivity timeout

Set inactivity timeout

Off

Enable sharing

Allow users to share read-only links to records with other users from this environment.

On

Show details when unfurling links

Show record name and type to unauthorized users when unfurling links in Teams chats

On

IP address settings

Enable IP address based cookie binding.

Off

Available for managed environments only. Learn more

Enable IP address based firewall rule.

Off

Available for managed environments only. Learn more

Storage Shared Access Signature (SAS) Security Settings (Preview)

Critical Advisory : Prior to activating SAS features customers must first allowlist `https://*.api.powerplatformusercontent.com` domain or most SAS functionalities will NOT work

Enable IP address based Storage Shared Access Signature (SAS) rule

Off

No IP SAS restriction set. Learn more

Enable SAS Logging in Purview

Off

Detective

Customer Lockbox

Preventative

Authentication
Authorisation
Encryption
Firewall

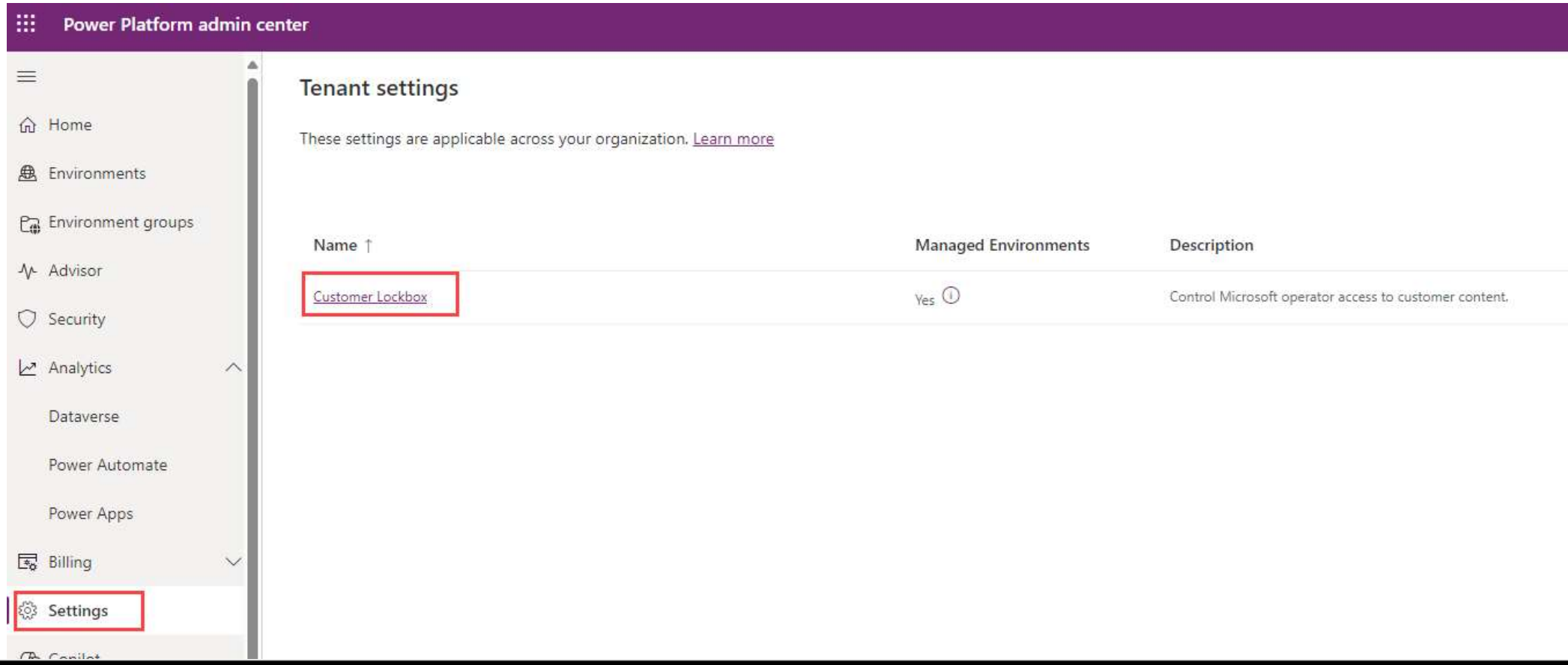
Detective

DoS
Brute Force
Malicious Access
Mass Export

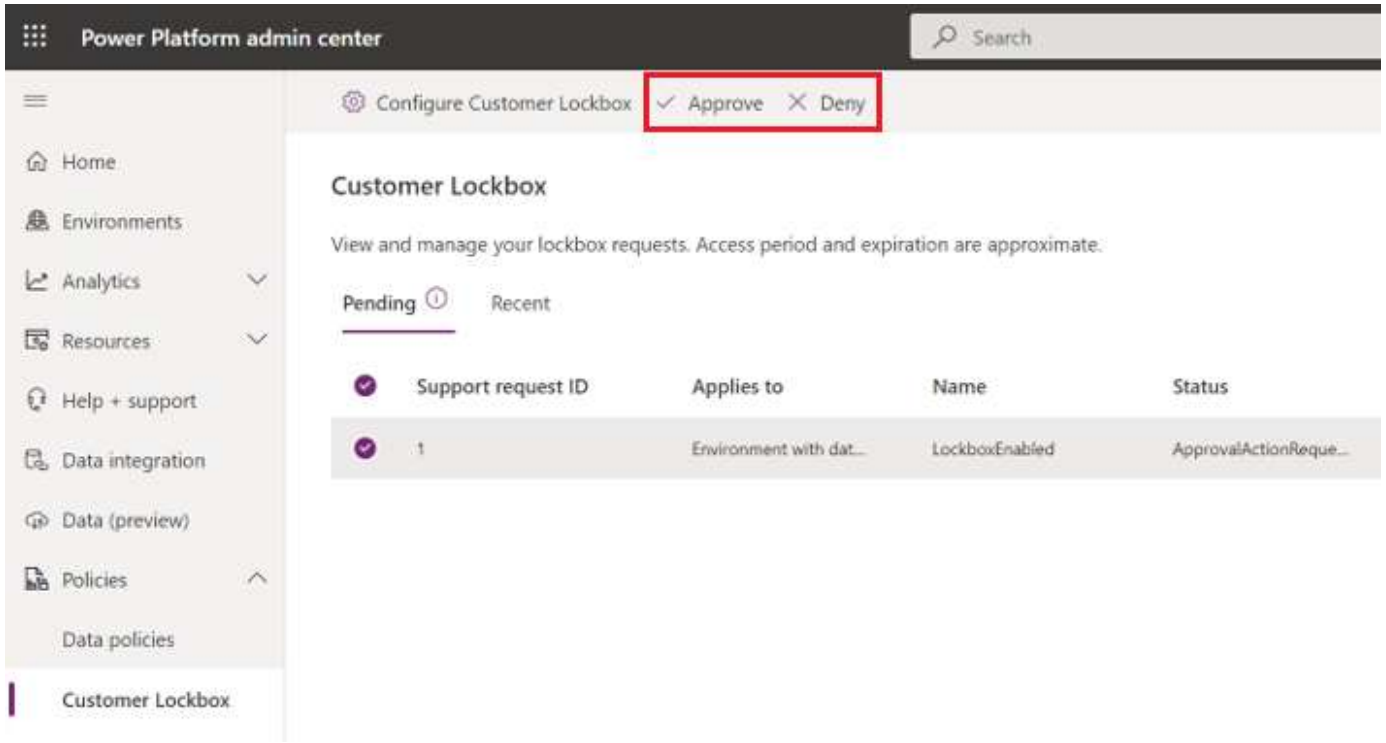
Corrective

Audit Trails
Governance
Notification
Pattern AI

Lockbox


Power Platform admin center
Home
Environments
Environment groups
Advisor
Security
Analytics
Dataverse
Power Automate
Power Apps
Billing
Settings
Tenant settings
These settings are applicable across your organization. Learn more
Name
Managed Environments
Description
Customer Lockbox
Yes
Control Microsoft operator access to customer content.

Lockbox



https://learn.microsoft.com/en-us/power-platform/admin/about-lockbox#enable-the-lockbox-policy

Detective

Sentinel

Preventative

Authentication
Authorisation
Encryption
Firewall

Detective

DoS
Brute Force
Malicious Access
Mass Export

Corrective

Audit Trails
Governance
Notification
Pattern AI

Microsoft Sentinel Solution for Dynamics 365 CE Apps (Preview)

Microsoft Corporation

Overview Plans Ratings + reviews

Get It Now

Pricing information
Cost of deployed template components

Categories
Security
Compute

Support
Support

Legal
Under Microsoft Standard Contract
Privacy Policy

Use Microsoft Sentinel to monitor and protect Dynamics 365 CE apps

The Microsoft Sentinel solution for Dynamics 365 CE apps provides you with ability to collect Dynamics 365 CE Apps logs, gain visibility of activities and analyze them to detect threats and malicious activities.

The solution includes four elements:

Data connector*:

- The Dynamics 365 data connector provides insight into Dataverse audits and activities (CRUD - Create, Read, Update, Delete). By connecting Dynamics 365 CE apps logs into Microsoft Sentinel, you can view this data in workbooks, use it to create custom alerts, and improve your investigation process.

Analytic rules detecting:

- Audit logs data and settings manipulation detection
- Detection of monitored Security and user configuration changes
- Suspicious logins and sign-ins to Dynamics 365
- Detection of new permissions granted to an application identity
- Mass export of Dynamics 365 records to Excel
- Mass deletion of Dynamics 365 records
- Bulk retrieval of data outside of normal activity hours
- Suspicious changes to Dynamics 365 encryption settings
- New user agents accessing Dynamics 365

Workbook dashboard providing visibility into:

- Record retrieval events
- Record deletion events
- Record export events
- Email events
- Other events

Sentinel - Security information and event management

Severity	Name	Rule type	Status	Tactics
High	D365 - Audit log data deletion	Scheduled	Enabled	
High	D365 - Login by a sensitive privileged user	Scheduled	Disabled	
High	D365 - Login from IP in the block list	Scheduled	Disabled	Initial Access
High	D365 - Login from IP not in the allow list	Scheduled	Disabled	Initial Access
Medium	D365 - Audit log configuration change	Scheduled	Enabled	
Medium	D365 - Dormant admin or previously non-admin user conduc...	Scheduled	Enabled	Initial Access
Medium	D365 - Encryption settings changed	Scheduled	Enabled	Defense Evasion
Medium	D365 - Mass deletion of records	Scheduled	Enabled	
Medium	D365 - Mass export of records to Excel	Scheduled	Enabled	
Medium	D365 - Monitored Security configuration changed	Scheduled	Enabled	
Medium	D365 - Monitored User configuration changed	Scheduled	Enabled	
Medium	D365 - Sign-in from an unauthorized domain	Scheduled	Enabled	
Medium	D365 - User bulk retrieval outside normal activity	Scheduled	Enabled	Collection
Low	D365 - New Office user agent detected	Scheduled	Enabled	Initial Access
Low	D365 - New user agent detected	Scheduled	Enabled	Initial Access
Low	D365 - Permissions granted to an application identity	Scheduled	Enabled	

https://techcommunity.microsoft.com/t5/microsoft-sentinel-blog/microsoft-sentinel-solution-for-dynamics-365-news-new-oob/ba-p/3487265

Corrective

Governance and Audit Logs

Preventative

Authentication
Authorisation
Encryption
Firewall

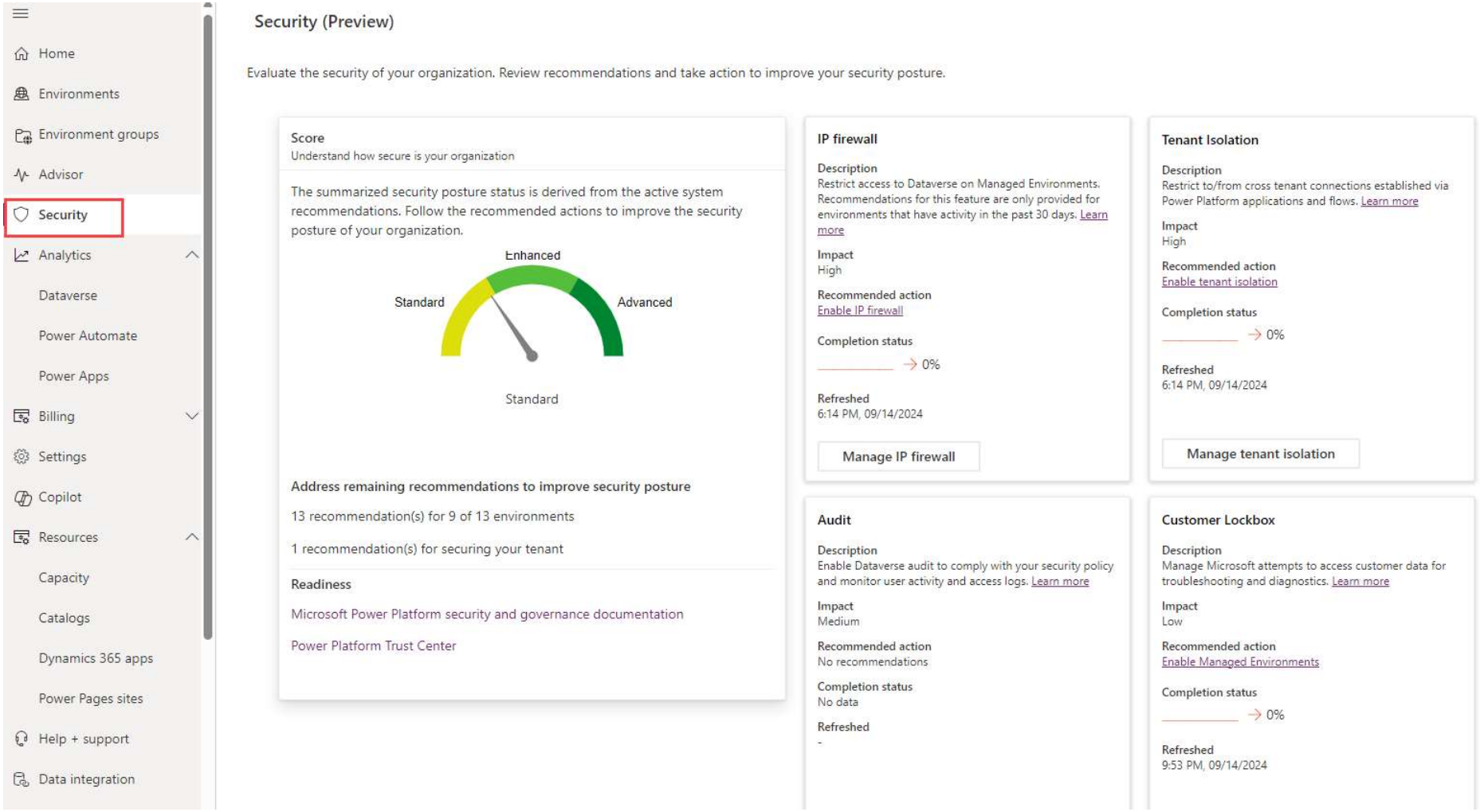
Detective

DoS
Brute Force
Malicious Access
Mass Export

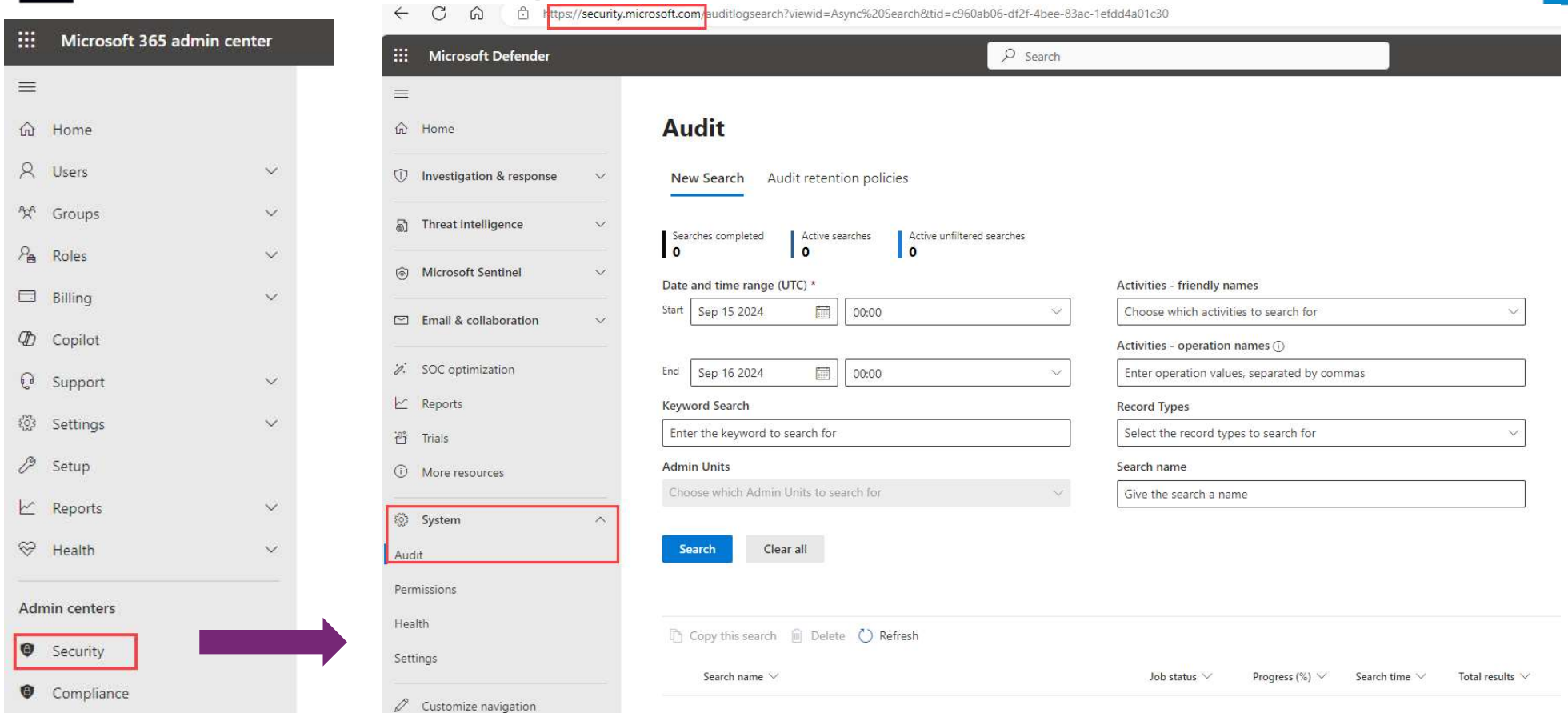
Corrective

Audit Trails
Governance
Notification
Pattern AI

Admin centre security



Read Audit Logs



Honourable Mentions

Mobile Security InTune

Field Level Security

SharePoint Integration

Securing Connector

Virtual Entities

Types of Security Controls

Preventative

Authentication
Authorisation
Encryption
Firewall

Detective

DoS
Brute Force
Malicious Access
Mass Export

Corrective

Audit Trails
Governance
Notification
Pattern AI

Platform Levels

Microsoft	Encryption ISO Certifications Attack Prevention
Azure	Infrastructure Conditional Access SIEM
M365	Security Group Licensing Read Audits
D365	RBAC Field Level Security Access Teams

References

https://learn.microsoft.com/en-us/power-platform/admin/security

https://learn.microsoft.com/en-us/power-platform/admin/wp-compliance-data-privacy

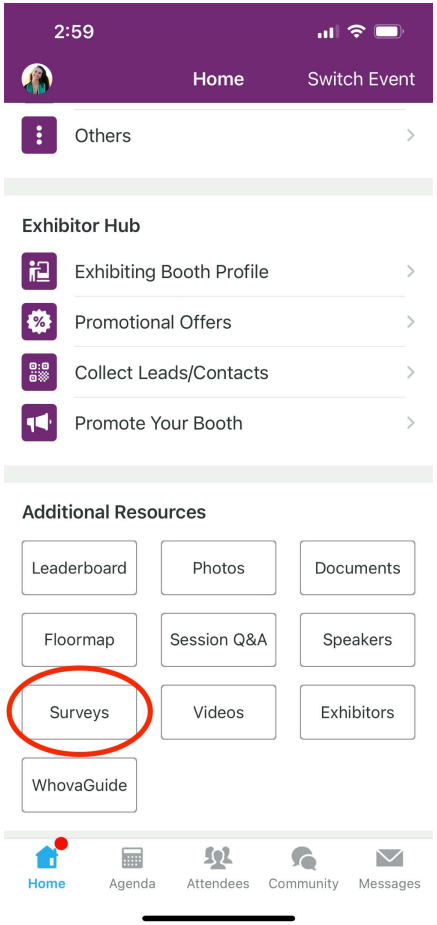
Stay in touch!

https://www.linkedin.com/in/ramimounla/

https://mvp.microsoft.com/en-US/MVP/profile/845a3682-b20f-e511-aa77-6c3be5a8e164

https://www.youtube.com/@rmou008

https://sessionize.com/rami-mounla



Session Feedback Surveys

We really want to hear from YOU!

In the pursuit of making next year's Power Platform Community Conference even better, we want to hear your feedback about this session.

Here's How -

- *Simply go to the Whova App on your smartphone*
- *Scroll down on the Power Platform Community Conference Homepage to 'Additional Resources' to click "Surveys'.*
- *Click Session Feedback.*
- *Scroll down to find this session title.*
- *Complete the session feedback survey.*
- *Finally, click 'Submit'*

It's just that easy!