



Power Platform

COMMUNITY CONFERENCE

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

MGM GRAND • *Las Vegas, NV*



Power Platform
COMMUNITY CONFERENCE

Exploring the Power Platform's Security Evolution

Rami Mounla

www.linkedin.com/in/ramimounla



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



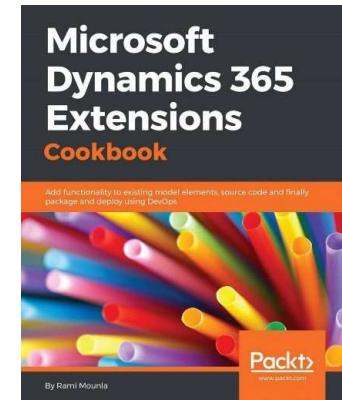
Join the event app to access:

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

**Event Invitation Code:
PPCCConf2024**



Power Platform COMMUNITY CONFERENCE





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

↗ Share



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

sist with the investigation. 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



Reuters

International Moose Count Underway

By BOB O'BOGSTON

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

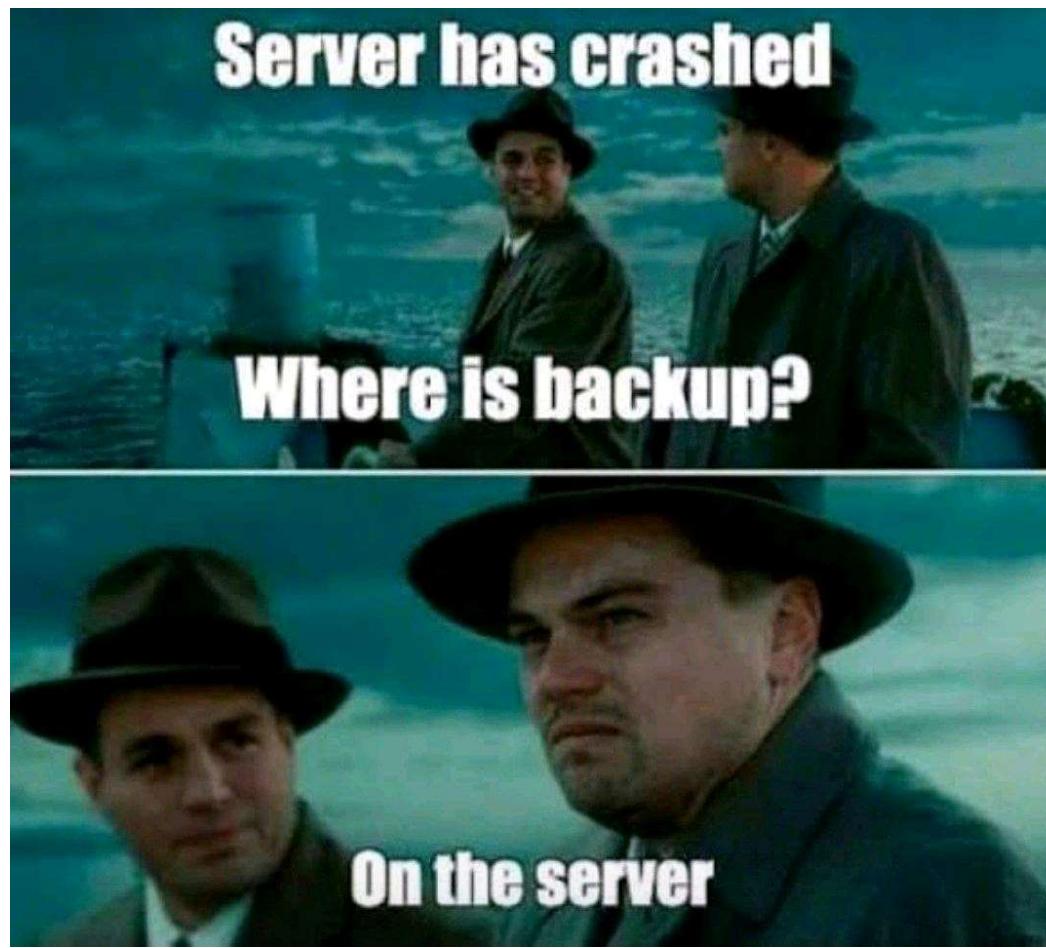


For more information about this issue and possible fixes, visit <https://www.windows.com/stopcode>

If you call a support person, give them this info:

Stop code: CRITICAL_PROCESS_DIED







**ORANGA
TAMARIKI**
Ministry for Children



Worried about a child? →

Search

Support for families ▾

Working with children ▾

Children in our care ▾

Caregiving ▾

Youth justice ▾

Adoption ▾

About us ▾



► 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 or can
make a report of concern to us or the Police.



U.S.

Politics

World

Opinion

Media

Entertainment

Sports

Lifestyle

Video

AI

More :



Login

Watch TV

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.

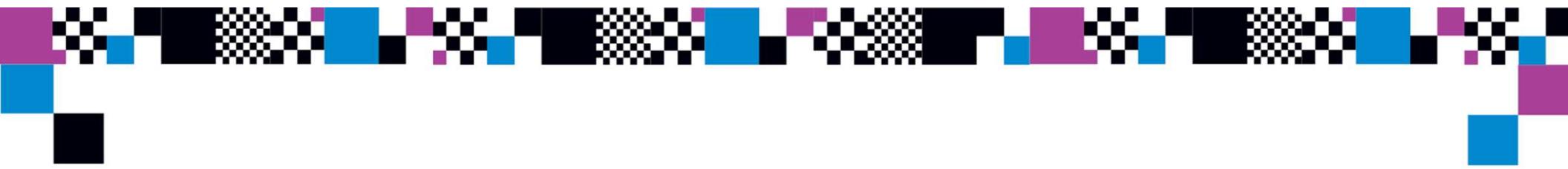
NEW ZEALAND
PASSPORT

URUWHENUA
AOTEAROA



Te Ara Manaaki

1008



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

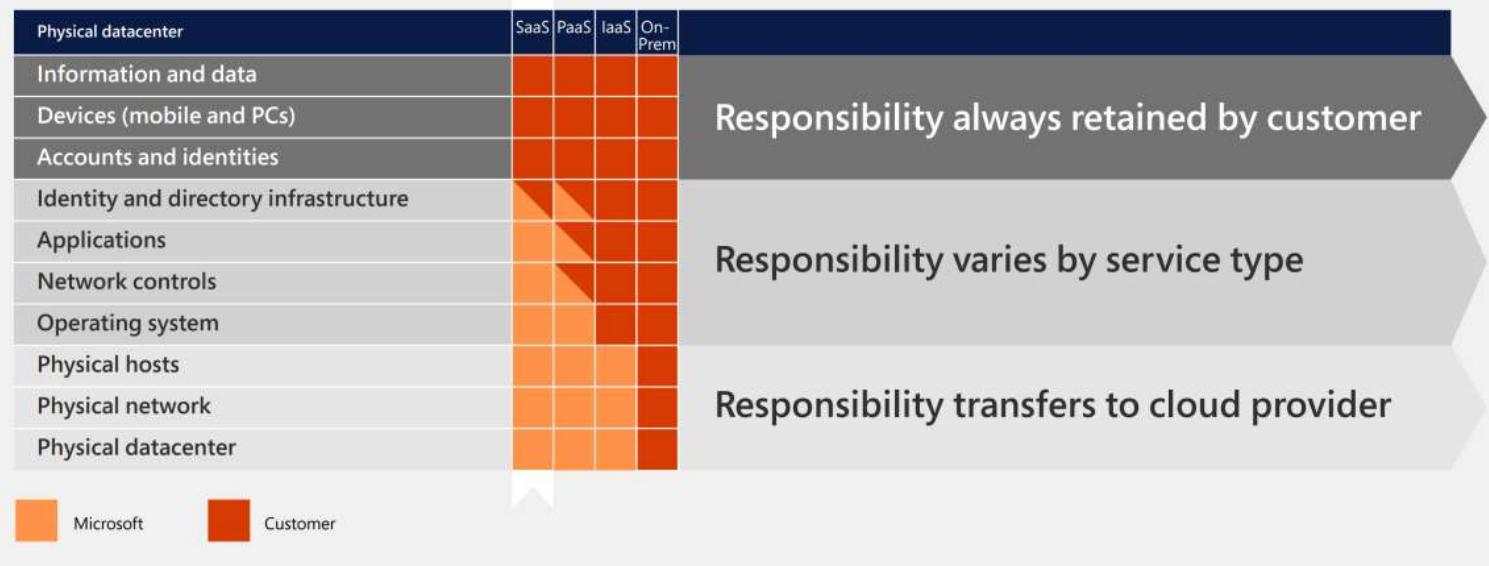
aka.ms/securefutureinitiative





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

Shared responsibility model





Platform Levels

Microsoft

Encryption
ISO Certifications
Attack Prevention

Azure

Infrastructure
Conditional Access
SIEM

M365

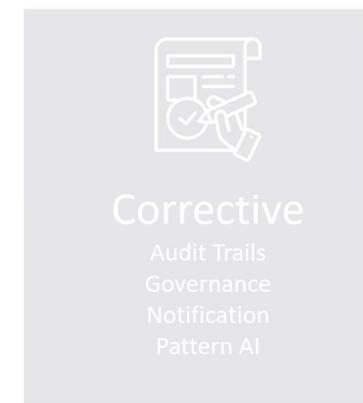
Security Group
Licensing
Read Audits

D365

RBAC
Field Level Security
Access Teams

Preventative

Azure



Security & Management



Platform Services

Application Platform



Data



Intelligence



Analytics & IoT



Hybrid Cloud



Compute



Storage



Infrastructure Services



Datacenter Infrastructure





Check where the services are provided



Check where the services are provided



Products available by region

Generally Available In Preview Future Availability Not Available

Products	Non-Regional	Australia Central	Australia Central 2	Australia East	Australia Southeast
 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

Environments > Source Control Preview 1 > **Settings**

Search for a setting

▽  **Product**

Behavior, Collaboration, Features, Languages

▽  **Business**

Business closures, Calendar, Connection roles, Currencies

▽  **Users + permissions**

Application users, Business units, Column security profiles, Hierarchy security

▽  **Audit and logs**

Audit settings, Audit summary view, Entity and field audit settings, System jobs

▽  **Templates**

Access team templates, Article templates, Contract templates, Data import templates

▽  **Updates**

App update settings (Preview)

▽  **Email**

Email settings, Email tracking, Mailboxes, Server profiles

▽  **Integration**

Document management settings, Synchronization, Yammer

▽  **Data management**

Auto numbering, Automatic record creation policies, Bulk deletion, Data import wizard

▽  **Encryption**

Data encryption 

▽  **Resources**

All legacy settings, Dynamics 365 App for Outlook

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

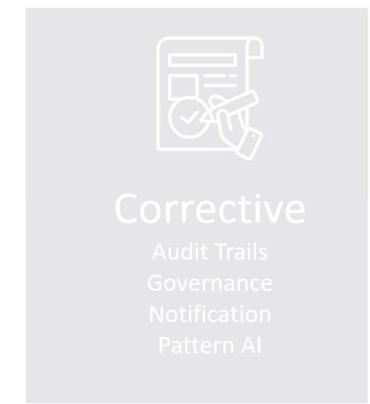
! We strongly recommend that you copy the encryption key and store it in a safe place. You may need to enter the key again to ensure that certain features keep working and the data is retrievable. For more information, see [Data Encryption](#).

! 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

Home > Enterprise applications - All applications

Enterprise applications - All applications

DXC - Azure Active Directory

Overview
Manage
All applications
Application proxy
User settings
Security
Conditional access
Activity
Sign-ins
Audit logs

Enterprise Applications			
NAME	HOME PAGE URL	OBJECT ID	APPLICATION ID
Dynamics CRM Online	http://www.microsoft.com/dynamics/crm	0f49877e-c786-457c-bc8e-6faf83f569f4	00000007-0000-0000-c000-000000000000
Microsoft Teams		eba4873a-149f-4258-8f43-bfe10df335b4	cc15fd57-2c6c-4117-a88c-00000002-0000-0ff1-ce00
Office 365 Exchange Online	http://office.microsoft.com/outlook/	3fb23654-a946-4ff8-824a-2feaaf873446	00000002-0000-0ff1-ce00-000000000000
Office 365 Management APIs		8457b204-097a-4624-9577-2ab2058828c8	c5393580-f805-4401-95e0-00000003-0000-0ff1-ce00
Office 365 SharePoint Online	http://office.microsoft.com/sharepoint/	93fb6186-9f48-41c1-a14a-a95957217342	00000003-0000-0ff1-ce00-00000005-0000-0ff1-ce00
Office 365 Yammer	https://products.office.com/yammer/	9c31c87f-dc8d-44b6-843b-6c34521f7hr9	00000005-0000-0ff1-ce00-00000006-0000-0ff1-ce00

Azure Conditional Access

The screenshot shows the Dynamics CRM Online - Conditional access page within the Azure portal. The URL in the browser bar is "Home > Dynamics CRM Online - Conditional access". The main content area is titled "Dynamics CRM Online - Conditional access" and includes a sub-header "Enterprise Application". On the left, there's a navigation sidebar with sections like Overview, Getting started, Manage (Properties, Owners, Provisioning), Security (Conditional access, Permissions), Activity (Sign-ins, Audit logs), and Troubleshooting + Support (Troubleshoot, New support request). The "Conditional access" link in the Security section is highlighted with a red box. The main content area features a "New policy" button, a "What If" button, and a note about understanding policy impact. It also includes a table showing examples of conditions and controls:

Conditions	Controls
When any user is outside the company network	They're required to sign in with multi-factor authentication
When users in the 'Managers' group sign-in	They are required be on an Intune compliant or domain-joined device

Below the table, there's a link to learn more about conditional access and a "Get started" section with a bulleted list:

- Create your first policy by clicking "+ New policy"
- Specify policy Conditions and Controls
- When you are done, don't forget to Enable policy and Create

There's also a link to interested in common scenarios?

Device Control

The screenshot shows the Dynamics CRM Online - Conditional access interface. The current screen is "Device platforms". The navigation path is: Home > Dynamics CRM Online - Conditional access > New > Conditions > Device platforms.

The "Device platforms" screen has the following configuration:

- Configure:** Yes (selected)
- Include/Exclude:** Include (selected)
- Select device platforms:** Select device platforms (radio button selected)
 - Android
 - iOS
 - Windows Phone
 - Windows
 - macOS

The "Conditions" screen is also visible in the background, showing the following conditions:

- Sign-in risk: Not configured
- Device platforms: Not configured
- Locations: Not configured
- Client apps (preview): Not configured
- Device state (preview): Not configured

The "New" screen shows the following sections:

- 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 (selected)

IP Control

Home > Dynamics CRM Online - Conditional access > New > Conditions > Locations > Select

New	Conditions	Locations	Select				
<p>Info</p> <p>* Name Example: 'Device compliance app policy'</p> <p>Assignments</p> <p>Users and groups ⓘ 0 users and groups selected</p> <p>Cloud apps ⓘ 1 app included</p> <p>Conditions ⓘ 0 conditions selected</p> <p>Access controls</p> <p>Grant ⓘ 0 controls selected</p> <p>Session ⓘ 0 controls selected</p> <p>Enable policy On Off</p>	<p>Info</p> <p>Sign-in risk ⓘ Not configured</p> <p>Device platforms ⓘ Not configured</p> <p>Locations ⓘ Not configured</p> <p>Client apps (preview) ⓘ Not configured</p> <p>Device state (preview) ⓘ Not configured</p>	<p>Control user access based on their physical location. Learn more</p> <p>Configure ⓘ</p> <p>Yes No</p> <p>Include Exclude</p> <p><input type="radio"/> Any location</p> <p><input type="radio"/> All trusted locations</p> <p><input checked="" type="radio"/> Selected locations</p> <p>Select None</p>	<p>Locations ⓘ</p> <p>Search Locations...</p> <table border="1"><thead><tr><th>NAME</th><th>TRUSTED</th></tr></thead><tbody><tr><td>MFA Trusted IPs</td><td>✓</td></tr></tbody></table>	NAME	TRUSTED	MFA Trusted IPs	✓
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 i

0 users and groups selected

Cloud apps i

1 app included

Conditions i

0 conditions selected

Access controls

Grant i

0 controls selected

Session i

0 controls selected

Enable policy

On

Off

Grant

Select the controls to be enforced.

Block access

Grant access

Require multi-factor authentication i

Require device to be marked as compliant i

Require Hybrid Azure AD joined device i

Require approved client app i
See list of approved client apps

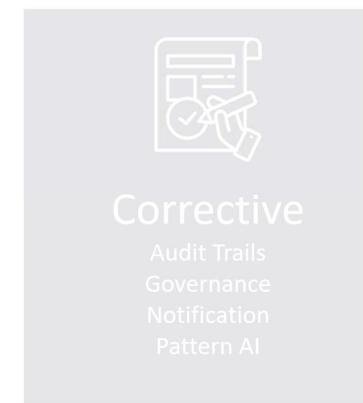
For multiple controls

Require all the selected controls

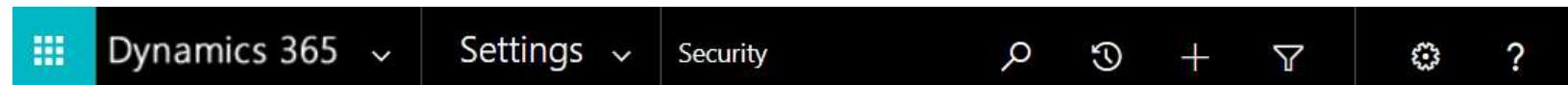
Require one of the selected controls

Preventative

Security Roles



Settings > Security



Security

Which feature would you like to work with?



Users

Add new users. Edit information about users and deactivate user records. Manage the teams, roles, and licenses assigned to users.



Teams

Add new teams and new members to existing teams. Modify the team description and delete members from teams.



Security Roles

Create new security roles. Manage and delete existing security roles for your organization.



Business Units

Add new business units. Edit and deactivate existing business units. Change the parent business unit.



Field Security Profiles

Manage user and team permissions to read, create, or write information in secured fields.



Hierarchy Security

Configure hierarchy security, including enabling hierarchy modeling and selecting the model. You can also specify how deep the hierarchy goes, and specify the entities to exclude from a hierarchy.



Positions

Add new Position. Modify the Position description.



Access Team Templates

Add new team templates. Modify the team template description.

■ Security Roles

 **Security Role: Sales Manager** Working on solution: Del

Entity	Create	Read	Write	Delete	Append	Append To	Assign	Share
Account	🟡	🟢	🟢	🟡	🟢	🟢	🟡	🟢
Activity	🟡	🟢	🟡	🟡	🟡	🟡	🟡	🟢
Announcement	🟢	🟢	🟢	🟢		🟢		
Application File	🔴	🟢	🔴	🔴				
Connection	🟡	🟢	🟢	🟡	🟢	🟢	🟡	🟢
Connection Role	🔴	🟢	🔴	🔴	🔴	🔴		
Contact	🟡	🟢	🟢	🟡	🟢	🟢	🟡	🟢
Customer Relationship	🔴	🔴	🔴	🔴	🔴	🔴	🔴	🔴

Key

🔴 None Selected 🟡 User 🟢 Business Unit 🟤 Parent: Child Business Units 🟩 Organization

Env > Settings > Users + permissions

Environments > Source Control Preview 1 > **Settings**

Search for a setting

▼ **Product**
Behavior, Collaboration, Features, Languages

▼ **Business**
Business closures, Calendar, Connection roles, Currencies

▲ **Users + permissions**

- Application users
- Business units
- Column security profiles
- Hierarchy security
- License to role mapping
- Mobile configuration
- Plug-ins
- Positions
- Security roles
- Teams
- Users

▼ **Audit and logs**
Audit settings, Audit summary view, Entity and field audit settings, System jobs

Security Roles

Environments > Source Control Preview 1 > Settings > Security roles > System Administrator

contact

X

^ Details

Business unit: scp1

When role is assigned to a Team

Team member gets all team privileges by default.

Team members can inherit team privileges directly based on access level. [Learn More](#)

Member's privilege inheritance

Direct User (Basic) access level and Team privileges

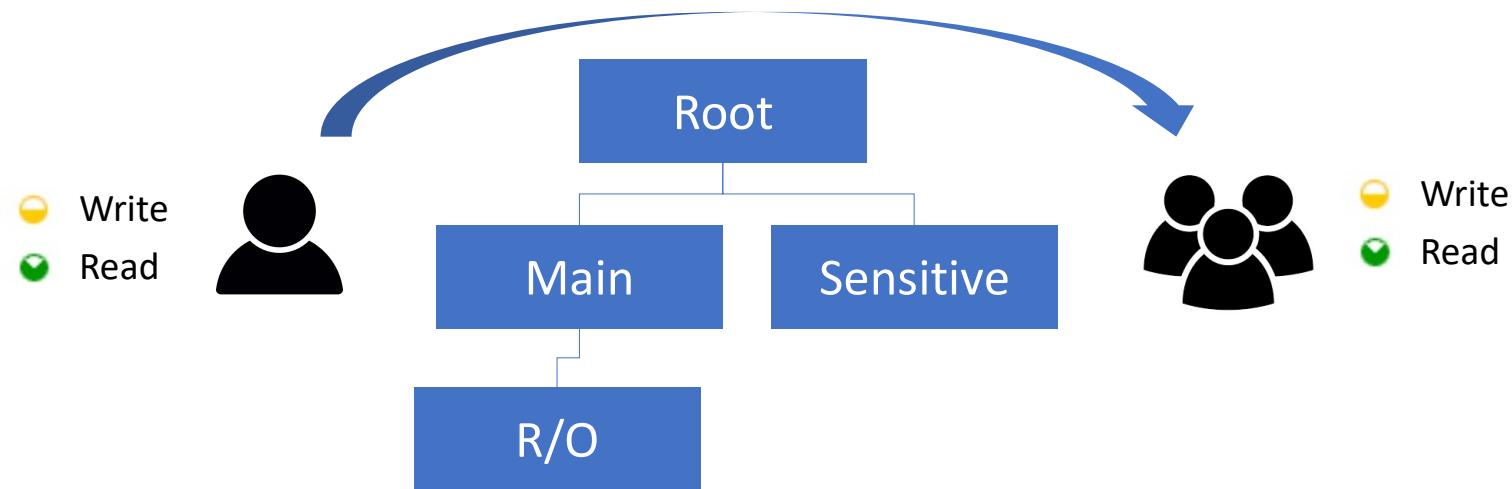
Tables Miscellaneous privileges Privacy-related privileges

Show only assigned tables

Compact Grid View On

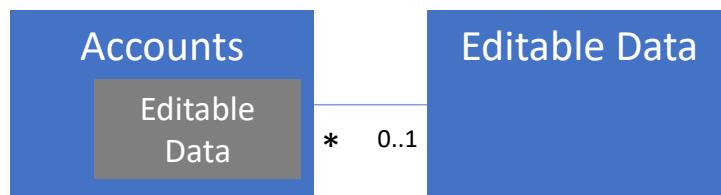
Table ↑	Name	Record ownership	Permission Settings	Create	Read	Write	Delete	Append	Append to
▼ Business Process Flows (1)									
Change Password for Portals Contact									
	adx_bpf_c2857b638fa7473d8e2f112...	Organization	Full Access	 Organization	 Organization	 Organization	 Organization	 Organization	 Organization
▼ Core Records (1)									
	Contact	... contact	User or Team	Full Access	 Organization	 Organization	 Organization	 Organization	 Organization

Business Unit and Teams

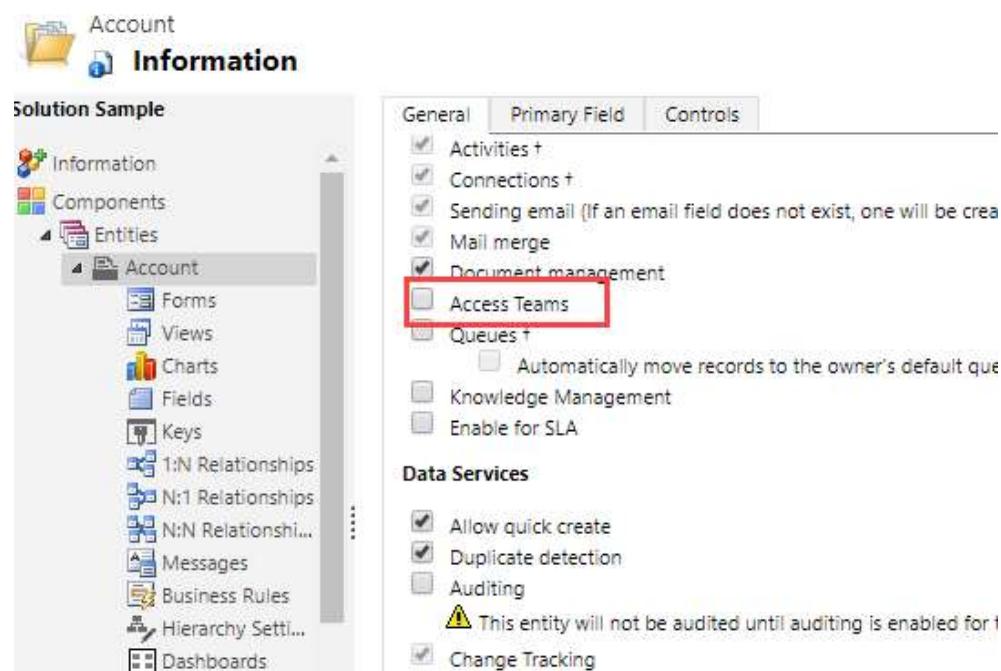


Security Requirement

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



Enable Access Teams



Access Team Template

Security

Which feature would you like to work with?



Users

Add new users. Edit information about users and deactivate user records. Manage the teams, roles, and licenses assigned to users.



Security Roles

Create new security roles. Manage and delete existing security roles for your organization.



Field Security Profiles

Manage user and team permissions to read, create, or write information in secured fields.



Positions

Add new Position. Modify the Position description.



Teams

Add new teams and new members to existing teams. Modify the team description and delete members from teams.



Business Units

Add new business units. Edit and deactivate existing business units. Change the parent business unit.



Hierarchy Security

Configure hierarchy security, including enabling hierarchy modeling and selecting the model. You can also specify how deep the hierarchy goes, and specify the entities to exclude from a hierarchy.



Access Team Templates

Add new team templates. Modify the team template description.

Access Team Template

Power Platform admin center Power Apps Dataverse Accelerator App New look ? RM

Home Environments Environment groups Advisor Security Analytics Billing Settings Copilot Resources Help + support Data integration Data (preview) Policies Admin centers

Environments > Source Control Preview

Search for a setting

- Product
- Business
- Users + permissions
- Audit and logs

Templates

- Access team templates
- Article templates
- Contract templates
- Data import templates
- Document templates
- Email signatures
- Email templates

Features

- Home
- Plugin monitoring
- Learn

New Team template - Unsaved

Team template · Team Templates main form

General

Name * OSS Training Entity *

Description

Access Rights

- Delete
- Append
- Append To
- Assign
- Share
- Read
- Write

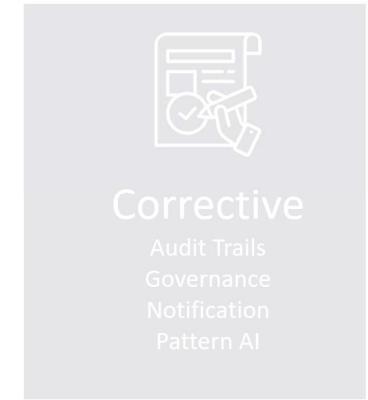
Remove their Licence - admin.microsoft.com

The screenshot shows the Microsoft 365 Admin Center interface. On the left, the navigation menu includes Home, Users (Active users selected), Guest users, Deleted users, Groups, Billing, Copilot, Setup, and Show all. The main area is titled "Active users" and shows a list of users with their email addresses. On the right, the user "Tharindu Jawardene" is selected. The "Licenses and apps" tab is active, showing a list of assigned licenses. One license, "Dynamics 365 Customer Service Enterprise vTrial", is highlighted with a red box and has a checked checkbox next to it. Other listed licenses include Microsoft Copilot Studio Viral Trial, Microsoft Fabric (free), Microsoft Power Apps Plan 2 Trial, Microsoft Power Apps for Developer, Microsoft Power Automate Free, and Power Pages vTrial for Makers.

Licenses	Description	Available Licenses
Dynamics 365 Customer Service Enterprise vTrial	9998 of 10000 licenses available	9998 of 10000 licenses available
Microsoft Copilot Studio Viral Trial	9998 of 10000 licenses available	9998 of 10000 licenses available
Microsoft Fabric (free)	Unlimited licenses available	Unlimited licenses available
Microsoft Power Apps Plan 2 Trial	9994 of 10000 licenses available	9994 of 10000 licenses available
Microsoft Power Apps for Developer	9994 of 10000 licenses available	9994 of 10000 licenses available
Microsoft Power Automate Free	9994 of 10000 licenses available	9994 of 10000 licenses available
Power Pages vTrial for Makers	9997 of 10000 licenses available	9997 of 10000 licenses available

Preventative

Entra ID Security Groups



Entra ID Security Groups

New team X

Team name *
M365 Security

Description
Add a team description

Business unit *
scp1

Administrator *
 Rami Mounla X

Team type * (i)
Select a team type

Owner

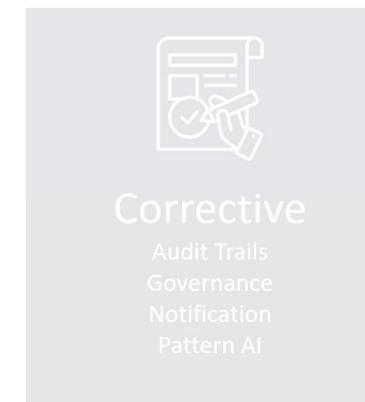
Access

Microsoft Entra ID Security Group

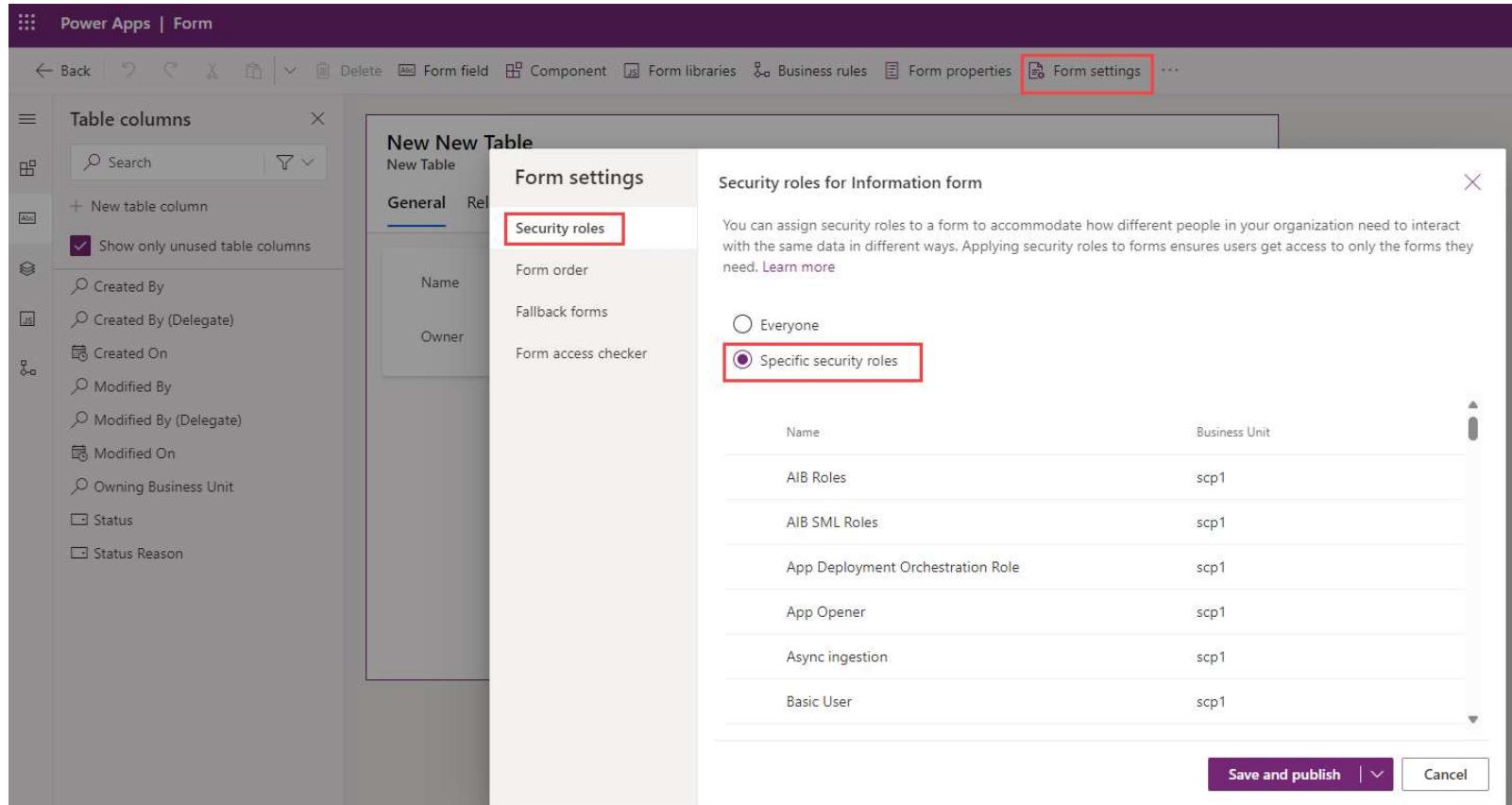
Microsoft Entra ID Office Group

Preventative

Forms and Apps Restriction



■ Restrict Access to Forms using Security Roles



Restrict Access to Business Apps with Security Roles

The screenshot shows the Power Apps portal interface. The top navigation bar has 'Power Apps' and 'First MDA' selected. The main area displays 'Published Apps (7)' and 'Apps Being Edited (0)'. A context menu is open over the 'First MDA' app card, with 'MANAGE ROLES' highlighted. A modal dialog titled 'Manage Roles - First MDA' is displayed, listing various security roles and their assigned business units. The 'Basic User' role is selected.

Name	Business Unit
AIB Roles	sqp1
AIB SML Roles	sqp1
App Deployment Orchestrator	sqp1
App Opener	sqp1
Async Ingestion	sqp1
Basic User	sqp1
BizQAAApp	sqp1
Bot Author	sqp1
Bot Contributor	sqp1
Bot Transcript Viewer	sqp1
Bulk Archival Role	sqp1
BusinessApplicationPlatformR...	sqp1
Cards Basic Role	sqp1
Cards Role	sqp1

Environment Security Groups

Power Platform admin center

Open Resources Settings Convert to production Backup & Restore Copy Reset

Environments > Power Pages

Details

Environment URL
pagesdxc1.crm6.dynamics.com

State
Ready

Region
Australia

Refresh cadence
Frequent

Type
Sandbox

Security group
Not assigned

Organization ID
8d740331-ff7e-4d86-bd9d-1fe9e460f460

Environment ID
389f06de-6131-e1b9-bf73-22c6edb437cd

See all

Edit

Auditing

Manage

Edit security group

Power Pages

Restrict environment access to members of a security group or select None to opt for open access across your tenant. [Learn more](#)

Search security groups by display names or emails that start with this



rami's



Name ↑

- Restricted access

Rami's Team

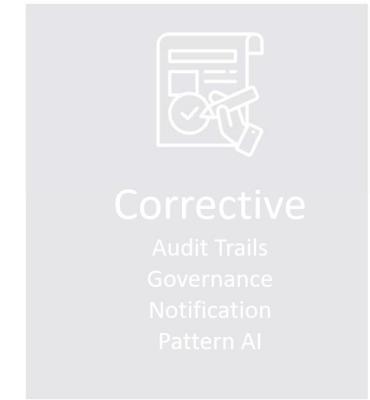
RamisTeam@CSCPortal.onmicrosoft.com

Done

Cancel

Preventative

Credential Management



Creating a Web/API account

The screenshot shows the Azure Active Directory App registrations page. On the left, there's a navigation bar with various services like All services, Dashboard, and Azure Active Directory. The Azure Active Directory item is highlighted with a red box. The main area shows a list of applications with columns for DISPLAY NAME, APPLICATION TYPE, and APPLICATION ID. A message at the top says, "The preview experience for App registrations is available. Click this banner to launch the preview experience." Below it, there's a search bar and a "View all applications" button. On the right, a "Create" dialog is open, prompting for the application's name, type (set to "Web app / API"), and sign-on URL. The "New application registration" button is also highlighted with a red box.

Create Secret Key

The screenshot shows three windows from the Microsoft Azure portal:

- API Application User**: Shows basic application details like Display name (API Application User), Application type (Web app / API), and Home page (https://localhost). The **Settings** tab is selected.
- Settings**: Shows application settings under GENERAL, API ACCESS, and TROUBLESHOOTING + SUPPORT sections. The **Keys** section is highlighted with a red box.
- Keys**: Shows a list of existing keys. A new key named "FirstKey" is being created, with its value set to "12/31/2299". The "Key description" and "Duration" fields are also visible.

The screenshot shows the Power Platform admin center interface. On the left, there's a sidebar with various navigation options like Home, Environments, Advisor, Security, Analytics, Billing, Settings, Copilot, Resources, Help + support, Data integration, Data (preview), and Policies. The 'Environments' option is selected. In the main area, a breadcrumb path shows 'Environments > Source Control Preview 1 > Settings > Application users'. A red box highlights the 'New app user' button. Below it, a table lists application users with columns for Name and App ID. Another red box highlights the 'Source Control Preview 1' environment name in the breadcrumb.

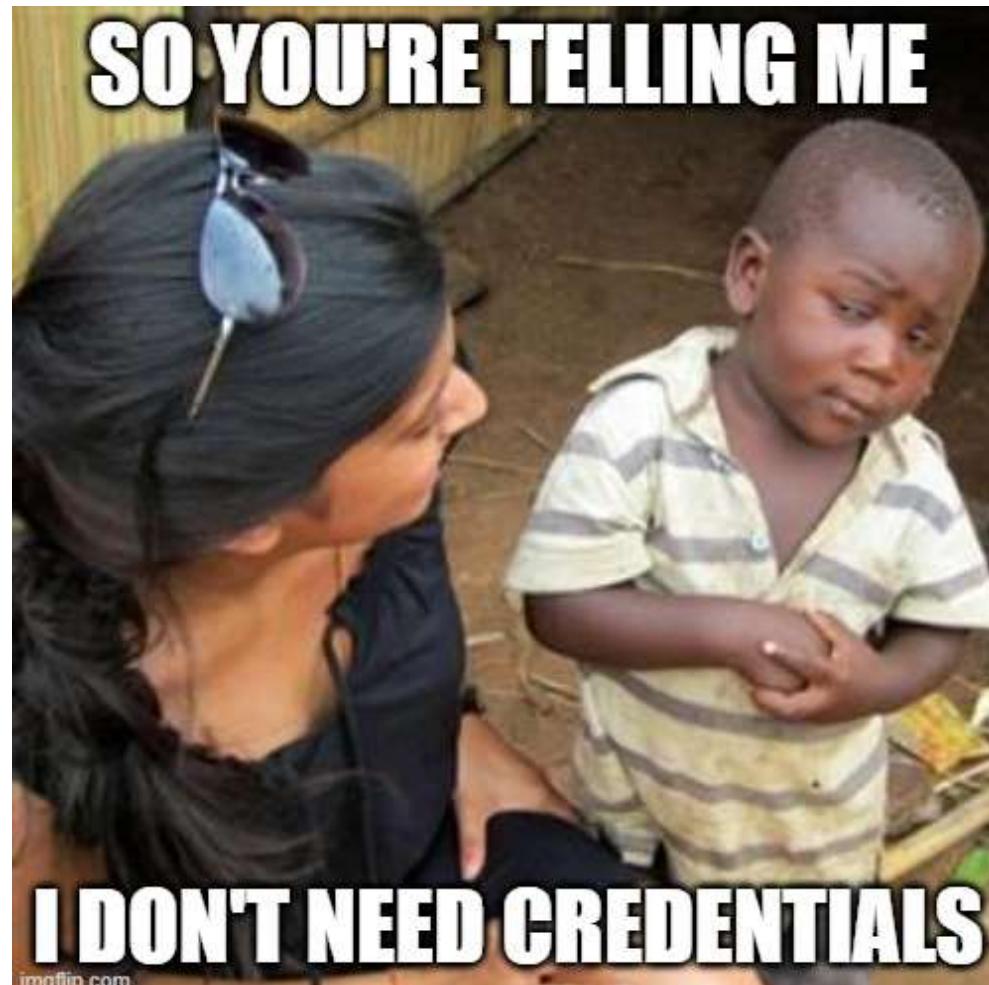
Add an app from Microsoft Entra ID

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



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

Home > Managed Identities >

Create User Assigned Managed Identity

Basics Tags Review + create

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * ⓘ Visual Studio Enterprise Subscription

Resource group * ⓘ Create new

Instance details

Region * ⓘ East US

Name * ⓘ

Create managed identity 2/3

Edit Federated Credential ...

Configure an identity from an external OpenID Connect Provider to get tokens as this managed identity to access Microsoft Entra ID protected services.

Federated credential scenario * ⓘ

Configure an identity managed by an external OpenID Connect Provider to access Azure resourc... ▾

Connect your account

Enter the details of the account that you want to connect with Microsoft Entra ID. These values will be used by Microsoft Entra ID to validate the connection.

Issuer URL * ⓘ

<https://cf5:b62a78ae.e4.enviorment.api.powerplatform.com/sts>

Subject identifier * ⓘ

component:pluginassembly.thumbprint:99CA466C22EFB9642029FE6F90,environe...

Credential details

Enter and review the details for this credential. The credential name cannot be edited after creation.

Name * ⓘ

FIC

Audience * ⓘ

<api://AzureADTokenExchange>

[Edit \(optional\)](#)

Create managed identity 2/3

Edit Federated Credential ...

Configure an identity from an external OpenID Connect Provider to get tokens as this managed identity to access Microsoft Entra ID protected services.

Federated credential scenario * ⓘ

Configure an identity managed by an external OpenID Connect Pr

Connect your account

Enter the details of the account that you want to connect with Microsoft Entra ID. These values will be used by the connection.

Issuer URL * ⓘ

https://cf5...:b62a78ae.e4.environment.api.pov

Subject identifier * ⓘ

component:pluginassembly.thumbprint:99CA466C22EFB9E

Credential details

Enter and review the details for this credential. The credential name cannot be edited after creation.

Name * ⓘ

FIC

Audience * ⓘ

api://AzureADTokenExchange

Edit (optional)

8. Enter the following information:

- **Issuer:** The URL of the token issuer. Format similar to this: `https://[environment ID prefix].[environment ID suffix].environment.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.

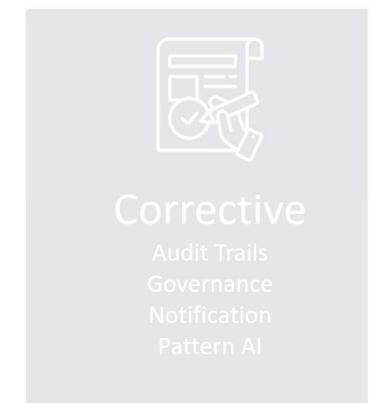
Sample Copy

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

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

Preventative

Data Policies



Data Policies

The screenshot shows the Power Platform admin center interface for creating a new DLP Policy. On the left, the navigation menu includes options like Home, Environments, Advisor, Security, Analytics, Billing, Settings, Copilot, Resources, Help + support, Data integration, Data (preview), Policies, Tenant isolation, Customer Lockbox, Enterprise policies, Billing policies, and Admin centers.

The main area displays the 'DLP Policies > New Policy' screen. It shows a 'Policy name' field with 'Salesforce' selected, and a 'Prebuilt connectors' section where 'Custom connectors' is chosen. Below this is the 'Assign connectors' section, which includes tabs for Business (0), Non-business (1255), Default, and Blocked (1). The 'Blocked' tab is selected, showing a list of connectors: 'Salesforce' (selected and highlighted with a red border), 'SharePoint', and 'OneDrive'. A note states: 'Blocked connectors can't be used where this policy is applied.'

A modal window titled 'Connector actions' is open, specifically for the 'Salesforce' connector. It lists various actions with their 'Allowed' status:

Action	Info	Allowed
Create record	(i)	<input checked="" type="checkbox"/> Yes
Execute SOSL search query	(i)	<input checked="" type="checkbox"/> Yes
Get records	(i)	<input checked="" type="checkbox"/> Yes
Close or abort a job	(i)	<input checked="" type="checkbox"/> Yes
Create a job (V2)	(i)	<input checked="" type="checkbox"/> Yes
Delete a job	(i)	<input checked="" type="checkbox"/> Yes
Delete record	(i)	<input checked="" type="checkbox"/> Yes
Execute a SOQL query	(i)	<input checked="" type="checkbox"/> Yes
Get a Record by External ID	(i)	<input checked="" type="checkbox"/> Yes
Get all jobs	(i)	<input checked="" type="checkbox"/> Yes
Get job info	(i)	<input checked="" type="checkbox"/> Yes

At the bottom of the modal, there are 'Default connector action settings' with radio buttons for 'Allow new connector actions' (selected) and 'Block new connector actions'. There are also 'Feedback', 'Save', and 'Cancel' buttons.

Environment Group

The screenshot shows the Power Platform admin center interface. The left sidebar has a navigation menu with items: Home, Environments, Environment groups (which is highlighted with a red box), Advisor, Security, and Analytics. The main content area title is "Environment groups". It includes a sub-instruction: "Organize your environments into groups and govern them in bulk by applying rules. [Learn more](#)". At the top right of the main area, there are buttons for "New group" (highlighted with a red box), "Environment Routing", "Refresh", and a search bar labeled "Search groups". Below the title, there is a table with columns: Name ↑, Environments, Rules, Created on, and Created by. One row is visible, showing "Develop..." under Name, "0" under Environments, "0" under Rules, "Mon, 16 Sept 2024, 10:54 pm GM..." under Created on, and "Rami Mounla" under Created by.

Name ↑	Environments	Rules	Created on	Created by
Develop...	0	0	Mon, 16 Sept 2024, 10:54 pm GM...	Rami Mounla

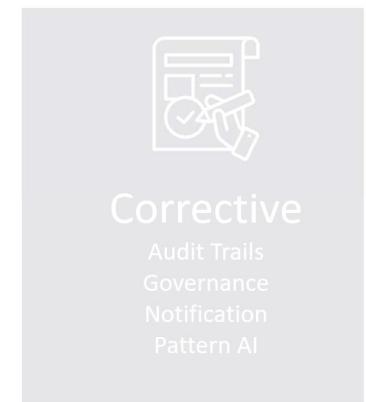
Environment Group

The screenshot shows the 'Development' environment group settings. The left sidebar includes 'Home', 'Environments', 'Environment groups' (selected), 'Advisor', 'Security', 'Analytics', 'Billing', 'Settings', 'Copilot', 'Resources', 'Help + support', 'Data integration', 'Data (preview)', and 'Policies'. The main area has a 'Publish rules' button and an 'Edit' button. A yellow banner says: 'New or edited rules are marked with *'. Click the publish button to apply them to the environments in this group. The 'Development environments' section shows 'Environments (0)' and 'Rules (6)'. A note says: 'Apply a unique set of rules to all environments in your group.' Below is a table:

Name	Description	Status
Sharing controls for Canvas apps	Limit how broadly your resources can be shared.	Not published
* Usage insights	Stay informed about what's happening in your environments.	Configured
Maker welcome content	Provide customized welcome content to help makers get started...	Not published
Solution checker enforcement	Automatically verify solution checker results for security and reli...	Not published
Backup retention	Configure environment backup retention period	Not published
Enable AI-generated description...	Automatically generate descriptions for Power Apps	Not published

Preventative

Masking Sensitive Data





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.

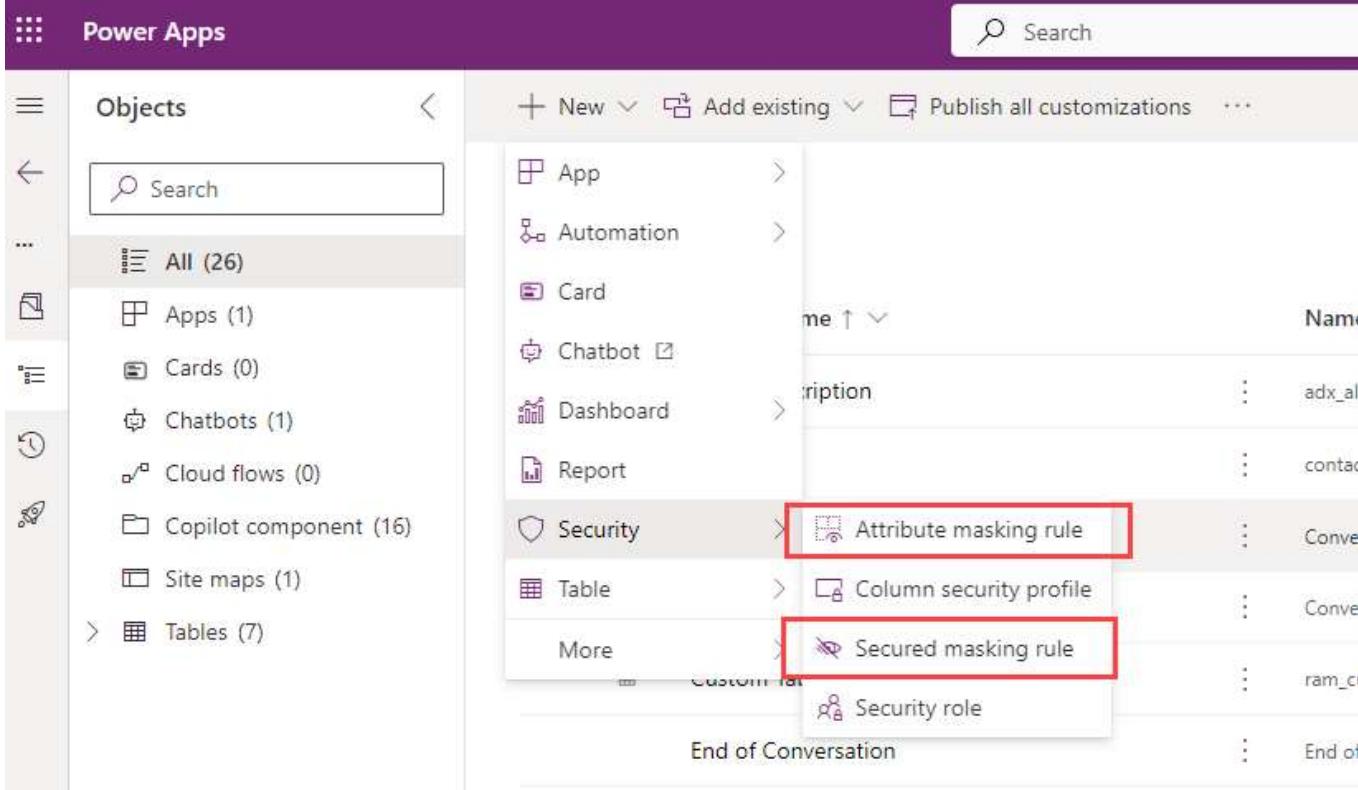
However, in July, the United States Federal Commission said in a press release that hashing was not adequate protection.

"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



The screenshot shows the Microsoft Power Apps interface, specifically the 'Objects' section. On the left, there's a navigation bar with icons for Home, Recent, My apps, and Power Automate. Below it is a search bar and a 'Search' button. The main area is titled 'Objects' with a back arrow and a search bar. At the top right are buttons for '+ New', 'Add existing', 'Publish all customizations', and three dots. The left sidebar lists various object types: 'All (26)' (selected), 'Apps (1)', 'Cards (0)', 'Chatbots (1)', 'Cloud flows (0)', 'Copilot component (16)', 'Site maps (1)', and 'Tables (7)'. The main content area shows a list of objects: 'App', 'Automation', 'Card', 'Chatbot', 'Dashboard', 'Report', 'Security' (selected), 'Table', 'More', and 'End of Conversation'. Under 'Security', two items are highlighted with red boxes: 'Attribute masking rule' and 'Secured masking rule'. There are also three dots next to each of these items.

Masking Sensitive Data

ram_maskemail - Saved

Secured Masking Rule

Summary Related ▾

Name *

Display Name *

Description *

Regular Expression - Learn *
more at
<https://go.microsoft.com/fwlink/p/?linkid=2259742>

Masked Character *

Enter Plain Text Test Data

Enter Rich Text Test Data

Masked Plain Text Test Data

Masked Rich Text Test Data

Masking Sensitive Data

Data type * ⓘ

Single line of text

Format *

Text

Required ⓘ

Optional

Searchable ⓘ

Advanced options ^

Schema name * ⓘ

ram_sampletext

General

Enable column security ⓘ

Masking Sensitive Data

ram_EmailMasking - Saved

Secured Masking Column

Summary Related ▾

UniqueName * ram_EmailMasking

Attribute * ram_sampletext

Entity * New Table

Secured Masking Rule *  ram_maskemail

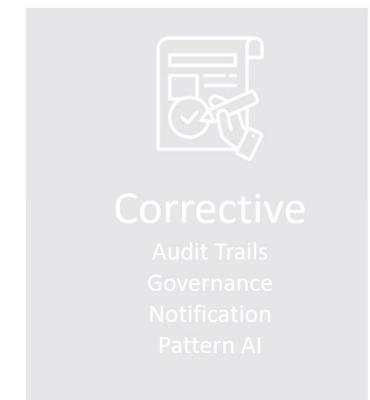
Masking Sensitive Data

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

```
1 {
2     "@odata.context": "https://scp1.crm.dynamics.com/api/data/v9.2/$metadata#ram_newtables",
3     "value": [
4         {
5             "@odata.etag": "W/\"3499795\"",
6             "createdon": "2024-09-17T04:41:20Z",
7             "_ownerid_value": "ff685a4c-db10-ef11-9f89-0022480c1f28",
8             "utcconversiontimezonecode": null,
9             "_createdby_value": "ff685a4c-db10-ef11-9f89-0022480c1f28",
10            "overriddencreatedon": null,
11            "statecode": 0,
12            "modifiedon": "2024-09-17T04:41:20Z",
13            "statuscode": 1,
14            "importsequencenumber": null,
15            "_createdonbehalfby_value": null,
16            "ram_name": "Hello",
17            "timezoneruleversionnumber": null,
18            "_modifiedby_value": "ff685a4c-db10-ef11-9f89-0022480c1f28",
19            "ram_newtableid": "87d0090f-af74-ef11-ac20-000d3a32e15c",
20            "versionnumber": 3499795,
21            "_owningbusinessunit_value": "0d625a4c-db10-ef11-9f89-0022480c1f28",
22            "_modifiedonbehalfby_value": null,
23            "ram_samplertext": "*",
24            "_owningteam_value": null,
25            "_owninguser_value": "ff685a4c-db10-ef11-9f89-0022480c1f28"
26        }
27    ]
28 }
```

Preventative

Other areas to secure



Power Pages

The screenshot shows the Microsoft Power Pages security settings interface. On the left, under the 'Pages' tab, the 'Security' section is selected. A red box highlights the 'Table permissions' link. In the center, a modal window titled 'New table permission' is open. The 'Basic' tab is selected. The 'Name *' field is empty and has a red border, with the error message 'Name is required'. The 'Table *' field is also empty. The 'Access type *' dropdown is set to 'Global access', which is highlighted with a red box. Below it, other options are listed: 'Global access' (description: 'Show all rows in the table to users in the selected roles.'), 'Contact access' (description: 'Show rows in the table associated to the signed-in user (contact)'), 'Account access' (description: 'Show rows in the table associated to the signed-in user's account details.'), and 'Self access' (description: 'Users can make changes to 'Contact' row. For example, change to the contact details on the profile page.'). At the bottom right of the modal are 'Save' and 'Cancel' buttons.

CoPilot Studio

The screenshot shows the Microsoft Copilot Studio interface. At the top, there's a decorative header with a pattern of colored squares (purple, blue, black). The main navigation bar includes 'Copilot Studio' (selected), 'Copilots' (selected), and 'Settings'. On the left sidebar, under 'Copilots', several custom copilots are listed: 'Paws Haven bot', 'Copilot in Power Apps' (selected), 'PermitApplication 1 bot' (highlighted with a red box), 'Dairy Effluent Storage Calculator', 'Pet Adoption bot', 'Adopt-a-Pet bot', 'MyFirstCopilot', 'Water Park bot', and 'Car Rental Site bot'. Under 'Microsoft', there's 'Copilot for Microsoft 365'. A section labeled 'Coming soon' is also present. The 'Settings' tab is active, showing the 'Security' section. The 'Authentication' sub-section is highlighted with a red box. It contains instructions: 'Verify a user's identity during a conversation. The copilot receives secure access to the user's data and is able to take actions on their behalf, resulting in a more personalized experience.' Below this is a 'Choose an option' section with three radio buttons: 'No authentication' (publicly available in any channel), 'Authenticate with Microsoft' (Entra ID authentication in Teams and Power App), and 'Authenticate manually' (selected, with a red box around it; it says 'Set up authentication for any channel' and has a 'Require users to sign in' toggle switch). Other settings include a 'Redirect URL' field with the value 'https://token.botframework.com/.auth/web/re' (also highlighted with a red box) and 'Copy' button, and dropdowns for 'Service provider' (set to 'Generic OAuth 2') and 'Client ID' (placeholder). The 'Client secret' field contains '.....'.

Link to Synapse

The screenshot shows the Microsoft Power Platform canvas interface. On the left, there's a navigation bar with various icons: Home, Create, Learn, Apps, Tables, Flows, Solutions, Azure Synapse Link (which is highlighted with a red box), Chatbots, Websites, More, and Power Platform. The main area displays a list of tables from an Azure Synapse Link for Dataverse connection. The 'Tables' tab is selected, showing a list of entities: Account, Appointment, Contact, Email, Fax, Letter, and Task. Above this list are buttons for Refresh, Manage tables (which is also highlighted with a red box), Unlink, and Go to Azure. To the right, a modal window titled 'Manage tables' is open, showing a list of tables under the 'Dataverse' section. There are 7 of 217 selected. A search bar at the top of the modal contains the text 'contact'. Below the search bar, the table list includes: Adx_invitation_invitecontacts, Adx_invitation_redeemedcontacts, Contact (which is checked), and Powerpagecomponent_mspp_webrole_contact.

Table ↑	Name	Sync stat
Account	account	Active
Appointment	appointment	Active
Contact	contact	Active
Email	email	Active
Fax	fax	Active
Letter	letter	Active
Task	task	Active

Manage tables		
Dataverse		
7 of 217 selected ⓘ		
Advanced		
contact		
Table ↑	Name	
Adx_invitation_invitecontacts	adx_invitation_invitecontacts	
Adx_invitation_redeemedcontacts	adx_invitation_redeemedcontacts	
Contact	contact	<input checked="" type="checkbox"/>
Powerpagecomponent_mspp_webrole_contact	powerpagecomponent_mspp_webrole_contact	

Azure Back Bone – Secure Network

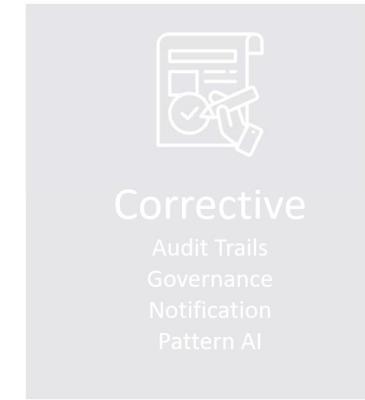
The screenshot displays the Azure Security (Preview) dashboard. On the left, a navigation sidebar includes Home, Environments, Environment groups, Advisor, Security (selected), Analytics, Billing, Settings, and Copilot. The main content area is titled "Security (Preview)" and contains the following sections:

- Score**: Understand how secure is your organization. A gauge meter shows the score as "Standard".

The summarized security posture status is derived from the active system recommendations. Follow the recommended actions to improve the security posture of your organization.
- Address remaining recommendations to improve security posture**:
 - 13 recommendation(s) for 9 of 13 environments
 - 1 recommendation(s) for securing your tenant
- Readiness**: Microsoft Power Platform security and governance documentation and Power Platform Trust Center.
- Environment security groups**:
 - Description**: Control which users have access to environments using Entra security groups. [Learn more](#)
 - Impact**: High
 - Recommended action**: No recommendations
 - Completion status**: 100%
 - Refreshed**: 7:16 PM, 09/15/2024
- Manage environment security group**
- Environments Azure vNet**:
 - Description**: Protect traffic between resources inside your virtual network without exposing them over the public internet. [Learn more](#)
 - Impact**: High
 - Recommended action**: Coming soon
 - Completion status**: No data
 - Refreshed**: -
- Manage Azure vNet**
- Audit**:
 - Description**: Enable Dataverse audit to comply with your security policy and monitor user activity and access logs. [Learn more](#)
 - Impact**: Medium
 - Recommended action**: No recommendations
 - Completion status**: No data
 - Refreshed**: -
- Customer Lockbox**:
 - Description**: Manage Microsoft attempts to access customer data for troubleshooting and diagnostics. [Learn more](#)
 - Impact**: Low
 - Recommended action**: [Enable Managed Environments](#)
 - Completion status**: 0%

Preventative

Power Platform Admin Center



Learn more about [Privacy + Security](#) ↗

Privacy preference

Show privacy statement link for this organization



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;cp;crf;csh;dll;exe;fx;hlp;hta;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;mb;md;mda;mdt;mdw;mdz;msc;msh;msh1;msh1xml;msh2;msh2xml;mshxml;msi;msp;mst;ops;pcd;pif;prf;prg;printer;pst;reg;rem;scf;scr;scrt;shb;shs;shtm;shtml;soap;stm;tmp;url;vb;vbe;vbs;vsmacros;vss;vst;vsw;ws;wsc;ws;f;wsh
```

Blocked Mime Types

Block upload of these mime types

Session Expiration

Set custom session timeout



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



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.



[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;ash;asmx;asp;bas;bat;cdccer;chm;class;cmd;com;con  
fig;cpl;crtsch;dll;exe;fpx;hlp;http;httr;htw;ida;idc;idq;infins;isp;its;jar;jse  
;js;shl;ink;madm;maf;mag;mann;mq;marmas;matmaur;mvn;mw;md;md  
;bmde;mdt;mdw;mdz;mscm;sh1;msh1xml;msh2;msh2xml;mshxml  
;msi;msp;mstop;pcd;pif;prf;prg;printer;pstregrem;scf;scrct;shb;shs;  
htm;html;soap;stml;tmp;url;vb;vbe;vbs;vsmacros;vss;vst;vsw;ws;wsc;ws  
;fwsh
```

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;ash;asmx;asp;bas;bat;cdx;cer;chm;class;cmd;com;con  
fig;cpl;crts;csd;dll;exe;fxphlp;hta;htc;htw;ida;idc;idq;inf;ini;is;its;jar;jse  
;ksh;lnk;mad;maf;mag;mann;mq;mar;mas;mat;maur;max;mw;mda;md  
;bmde;mdt;mdw;mdz;mscmsh;mhsh1;msh1xml;msh2;msh2xml;msxml  
;ims;imsip;mstop;pcd;pif;prg;printer;pstreg;rem;scf;scrsct;shb;shs;  
htm;html;soap;stm;tmp;urlvb;vbevb;vs;macros;vss;vst;vsw;ws;wscws  
;fwsh
```

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;con  
fig;cpl;crts;csd;dll;exe;fxphlp;hta;htc;htw;ida;idc;idq;inf;ini;is;its;jar;jse  
jsh;lnk;mad;maf;mag;mann;maq;marmas;matr;maur;mauv;maw;mda;md  
bmde;mdt;mdw;mdz;mscmsh;mhsh1;msh1xml;msh2;msh2xml;mshxml  
ims;imsip;msstop;pcd;pif;prg;printer;pstreg;rem;scf;ser;ct;shb;shs;  
htm;html;soap;stm;tmp;urlvb;vbevb;vs;macros;vss;vst;vsw;ws;wscws  
fwsh
```

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](#)

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

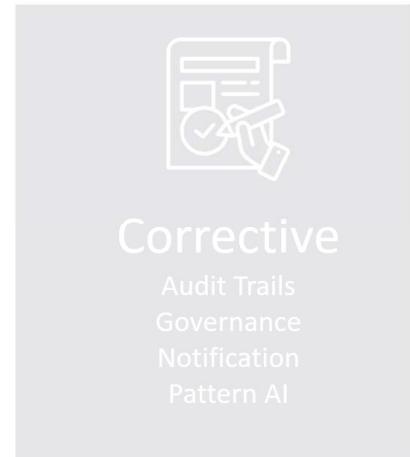
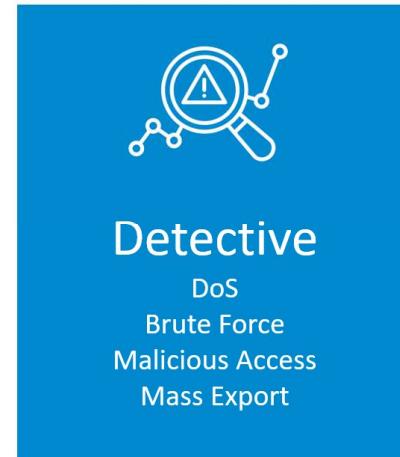
No IP SAS restriction set. [Learn more](#)

Enable SAS Logging in Purview

Off

Detective

Customer Lockbox



Lockbox

Power Platform admin center



Home

Environments

Environment groups

Adviser

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

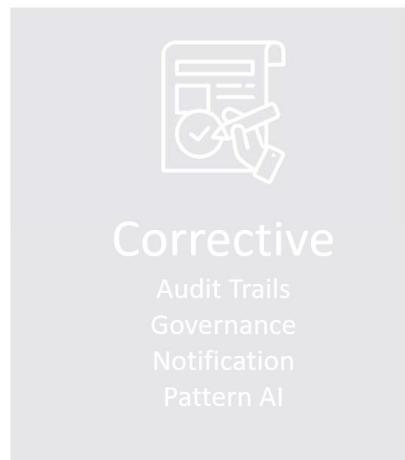
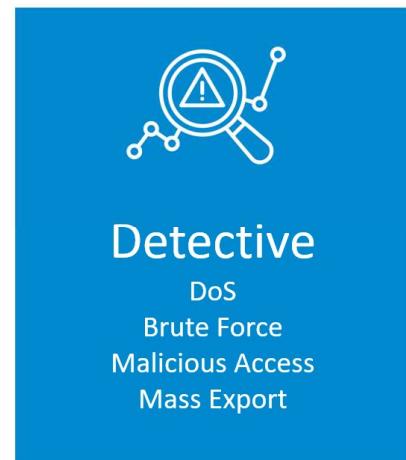
The screenshot shows the Power Platform admin center interface. The left sidebar includes options like Home, Environments, Analytics, Resources, Help + support, Data integration, Data (preview), Policies (with Data policies), and Customer Lockbox. The main content area is titled "Configure Customer Lockbox" and contains two buttons: "Approve" and "Deny", which are highlighted with a red box. Below this is a section titled "Customer Lockbox" with the sub-instruction "View and manage your lockbox requests. Access period and expiration are approximate." It shows two tabs: "Pending" (selected) and "Recent". A table lists one pending request:

Support request ID	Applies to	Name	Status
1	Environment with dat...	LockboxEnabled	ApprovalActionReque...

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

Detective

Sentinel





Get It Now

Pricing information
Cost of deployed template components

Categories
Security
Compute

Support
Support

Legal
Under Microsoft Standard
Contract
Privacy Policy

Microsoft Sentinel Solution for Dynamics 365 CE Apps (Preview)

Microsoft Corporation

[Overview](#) [Plans](#) [Ratings + reviews](#)

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

<input type="checkbox"/> Severity ↑↓	↑↓ Name ↑↓	Rule type ↑↓	Status ↑↓	Tactics
<input type="checkbox"/>	High D365 - Audit log data deletion	Scheduled	Enabled	
<input type="checkbox"/>	High D365 - Login by a sensitive privileged user	Scheduled	Disabled	
<input type="checkbox"/>	High D365 - Login from IP in the block list	Scheduled	Disabled	
<input type="checkbox"/>	High D365 - Login from IP not in the allow list	Scheduled	Disabled	
<input type="checkbox"/>	Medium D365 - Audit log configuration change	Scheduled	Enabled	
<input type="checkbox"/>	Medium D365 - Dormant admin or previously non-admin user conduc...	Scheduled	Enabled	
<input type="checkbox"/>	Medium D365 - Encryption settings changed	Scheduled	Enabled	
<input type="checkbox"/>	Medium D365 - Mass deletion of records	Scheduled	Enabled	
<input type="checkbox"/>	Medium D365 - Mass export of records to Excel	Scheduled	Enabled	
<input type="checkbox"/>	Medium D365 - Monitored Security configuration changed	Scheduled	Enabled	
<input type="checkbox"/>	Medium D365 - Monitored User configuration changed	Scheduled	Enabled	
<input type="checkbox"/>	Medium D365 - Sign-in from an unauthorized domain	Scheduled	Enabled	
<input type="checkbox"/>	Medium D365 - User bulk retrieval outside normal activity	Scheduled	Enabled	
<input type="checkbox"/>	Low D365 - New Office user agent detected	Scheduled	Enabled	
<input type="checkbox"/>	Low D365 - New user agent detected	Scheduled	Enabled	
<input type="checkbox"/>	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



Admin centre security

≡

- Home
- Environments
- Environment groups
- Advisor
- Security**
- Analytics
- Dataverse
- Power Automate
- Power Apps
- Billing
- Settings
- Copilot
- Resources
- Capacity
- Catalogs
- Dynamics 365 apps
- Power Pages sites
- Help + support
- Data integration

Security (Preview)

Evaluate the security of your organization. Review recommendations and take action to improve your security posture.

Score
Understand how secure is your organization

The summarized security posture status is derived from the active system recommendations. Follow the recommended actions to improve the security posture of your organization.



Address remaining recommendations to improve security posture

13 recommendation(s) for 9 of 13 environments

1 recommendation(s) for securing your tenant

Readiness

Microsoft Power Platform security and governance documentation

Power Platform Trust Center

IP firewall

Description: Restrict access to Dataverse on Managed Environments. Recommendations for this feature are only provided for environments that have activity in the past 30 days. [Learn more](#)

Impact: High

Recommended action: [Enable IP firewall](#)

Completion status:  0%

Refreshed: 6:14 PM, 09/14/2024

[Manage IP firewall](#)

Tenant Isolation

Description: Restrict to/from cross tenant connections established via Power Platform applications and flows. [Learn more](#)

Impact: High

Recommended action: [Enable tenant isolation](#)

Completion status:  0%

Refreshed: 6:14 PM, 09/14/2024

[Manage tenant isolation](#)

Audit

Description: Enable Dataverse audit to comply with your security policy and monitor user activity and access logs. [Learn more](#)

Impact: Medium

Recommended action: No recommendations

Completion status: No data

Refreshed: -

Customer Lockbox

Description: Manage Microsoft attempts to access customer data for troubleshooting and diagnostics. [Learn more](#)

Impact: Low

Recommended action: [Enable Managed Environments](#)

Completion status:  0%

Refreshed: 9:53 PM, 09/14/2024

Read Audit Logs

The screenshot shows the Microsoft 365 Admin Center interface. On the left, a navigation sidebar lists various admin centers like Home, Users, Groups, Roles, Billing, Copilot, Support, Settings, Setup, Reports, and Health. A red box highlights the 'Security' link under Admin centers. A large purple arrow points from the bottom-left towards the main content area. The main content area is titled 'Microsoft Defender' and shows the 'Audit' section. The URL in the browser bar is <https://security.microsoft.com/auditlogsearch?viewid=Async%20Search&tid=c960ab06-df2f-4bee-83ac-1efdd4a01c30>. The audit search interface includes fields for Date and time range (UTC), Keyword Search, Admin Units, and various filter options. The 'Audit' link in the left sidebar is also highlighted with a red box.



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/>



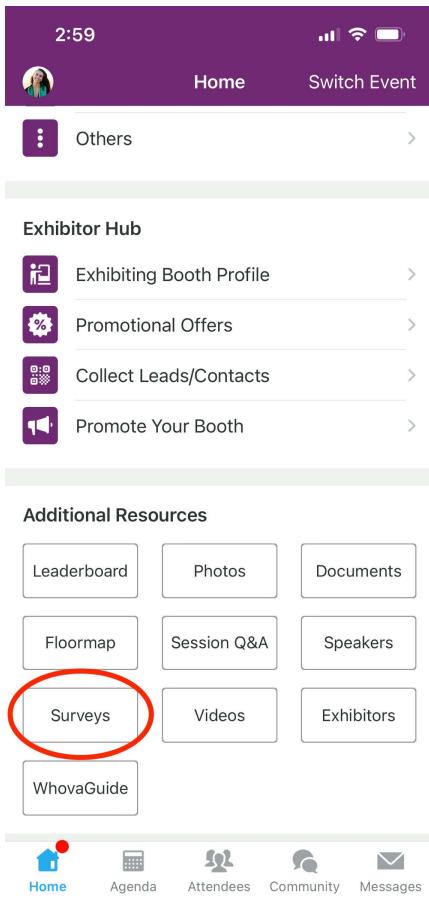
<https://mvp.microsoft.com/en-US/MVP/profile/845a3682-b20f-e511-aa77-6c3be5a8e164>



<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!