MS PURVIEW OVERVIEW

Microsoft Purview is a family of data governance, risk, and compliance solutions that can help your organization govern, protect, and manage your entire data estate. Microsoft Purview solutions provide integrated coverage and help address the recent increases in remote user connectivity, the fragmentation of data across organizations, and the blurring of traditional IT management roles.

This integration's purpose is to utilize Azure Information Protection part of the MS Purview (further referred to as MS Purview for simplicity) for its cataloging functionality and set up its communication with Inventa. The goal is to scan Microsoft resources like Azure DBs, OneDrive, and Exchange and build the catalog of assets scanned by Inventa with assigned corresponding labels to the data elements within and outside the MS resources.

Table 1: Use cases for Inventa integration with Purview

USE CASE	DESCRIPTION
Import sensitivity labels to Inventa	Automatically import sensitivity labels from MS Purview to Inventa. These labels will appear as sensitivity classes in Inventa , and can be mapped to data elements and document classifiers.
Use imported sensitivity labels for criticality score calculation	Use the automatically imported sensitivity labels during the **Contains over [X] data elements of [Y] sensitivity** criticality score parameter configuration.
Assign sensitivity labels to files in MS resources	Automatically assign sensitivity labels from MS Purview to files in MS resources according to the label scoring.

For details on Inventa sensitivity classes and the integration use case configuration, refer to the **Analytic Engine and Console Manager Administrator Guide**.

PREREQUISITES

1. Inventa version 3.6.0+.

2. MS Purview risk and compliance solutions.

3. MS Purview unified data governance solutions.

4. Configured and published security labels on the Microsoft Purview compliance portal, Solutions > Information protection > Labels.

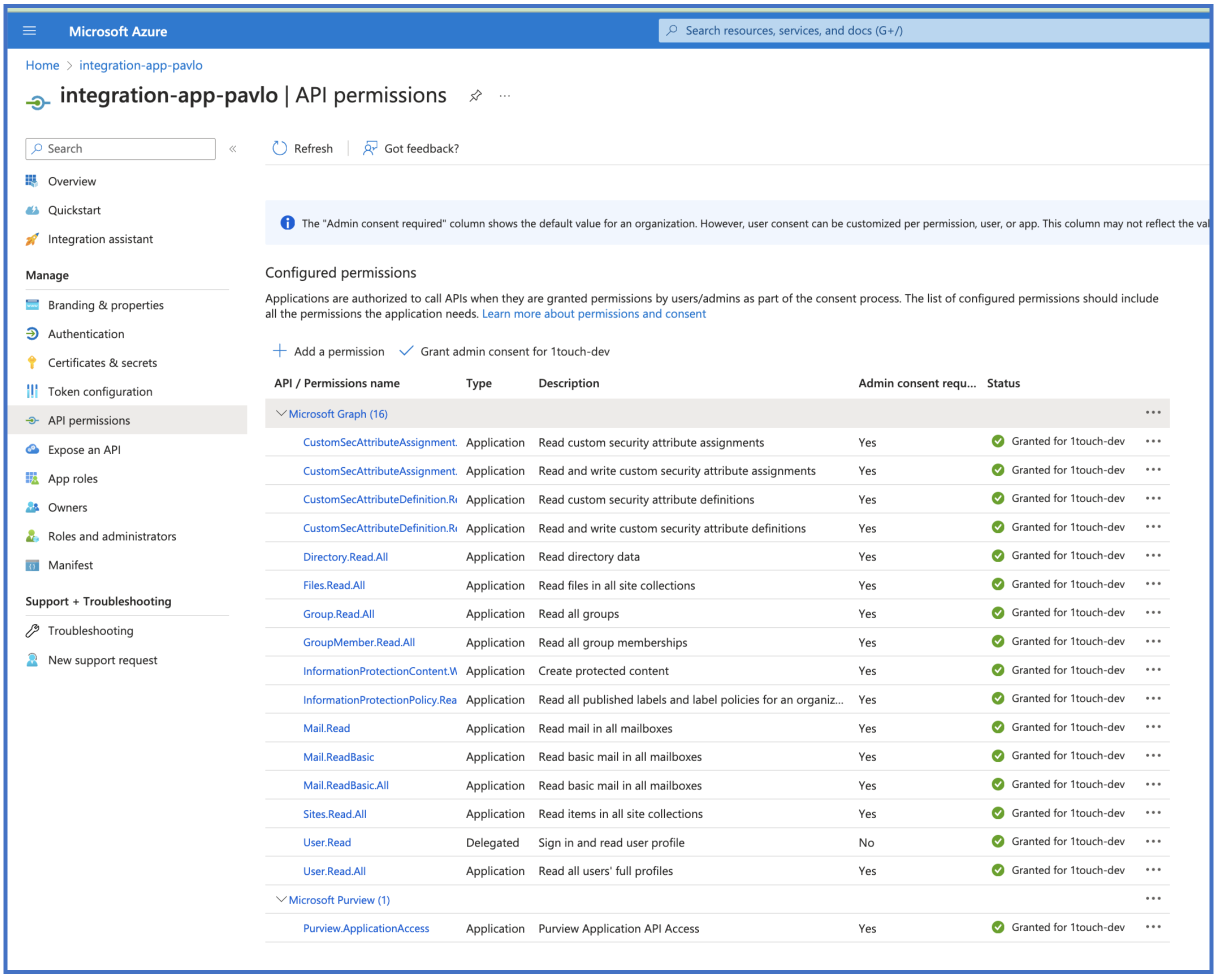
5. Register the integration app in the MS Azure portal.

5. 1. Make a note of the application (client) ID, directory (tenant) ID and the client secret. These values will be used for the integration app configuration.

5.2. Grant the following permissions to the registered app:

Table 2: Required app permissions in MS Azure portal

PERMISSION	DESCRIPTION
CustomSecAttributeAssignment.Read.All	Read custom security attribute assignments
CustomSecAttributeAssignment.ReadWrite.All	Read and write custom security attribute assignments
CustomSecAttributeDefinition.Read.All	Read custom security attribute definitions
CustomSecAttributeDefinition.ReadWrite.All	Read and write custom security attribute definitions
Directory.Read.All	Read directory
Files.Read.All	Read files in all site collections
Group.Read.All	Read all groups
GroupMember.Read.All	Read all group memberships
InformationProtectionContent.Write.All	Create protected content
InformationProtectionPolicy.Read.All	Read all published labels and label policies for an organization
Mail.Read	Read mail in all mailboxes
Mail.ReadBasic	Read basic mail in all mailboxes
Mail.ReadBasic.All	Read basic mail in all mailboxes
Sites.Read.All	Read items in all site collections
User.Read	Sign in and read user profile
User.Read.All	Read all users' full profiles
Purview.ApplicationAccess	Purview Application API Access



integration-app-pavlo | API permissions

The "Admin consent required" column shows the default value for an organization. However, user consent can be customized per permission, user, or app. This column may not reflect the val

Configured permissions

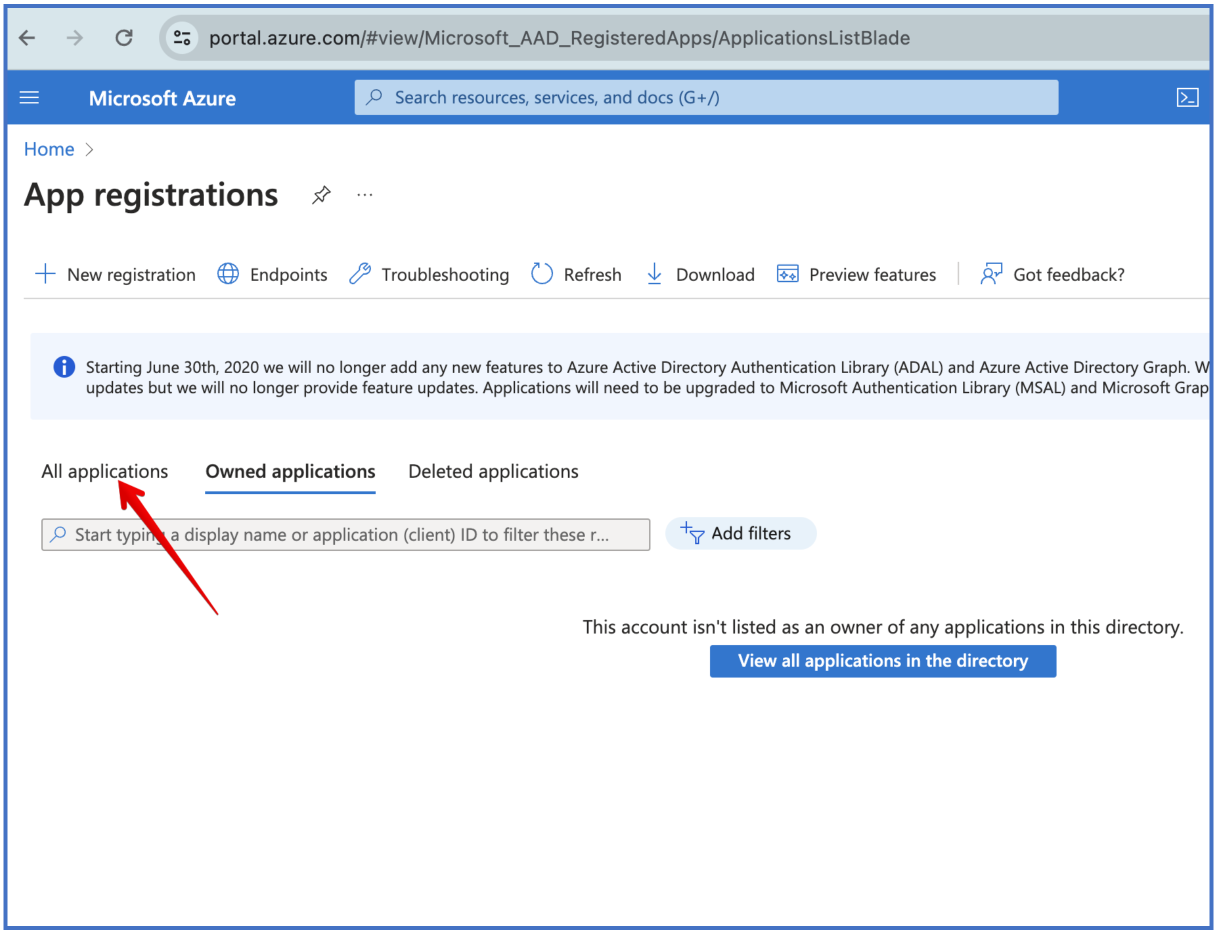
Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (16)				
CustomSecAttributeAssignment.	Application	Read custom security attribute assignments	Yes	✓ Granted for 1touch-dev
CustomSecAttributeAssignment.	Application	Read and write custom security attribute assignments	Yes	✓ Granted for 1touch-dev
CustomSecAttributeDefinition.R	Application	Read custom security attribute definitions	Yes	✓ Granted for 1touch-dev
CustomSecAttributeDefinition.R	Application	Read and write custom security attribute definitions	Yes	✓ Granted for 1touch-dev
Directory.Read.All	Application	Read directory data	Yes	✓ Granted for 1touch-dev
Files.Read.All	Application	Read files in all site collections	Yes	✓ Granted for 1touch-dev
Group.Read.All	Application	Read all groups	Yes	✓ Granted for 1touch-dev
GroupMember.Read.All	Application	Read all group memberships	Yes	✓ Granted for 1touch-dev
InformationProtectionContent.W	Application	Create protected content	Yes	✓ Granted for 1touch-dev
InformationProtectionPolicy.Rea	Application	Read all published labels and label policies for an organiz...	Yes	✓ Granted for 1touch-dev
Mail.Read	Application	Read mail in all mailboxes	Yes	✓ Granted for 1touch-dev
Mail.ReadBasic	Application	Read basic mail in all mailboxes	Yes	✓ Granted for 1touch-dev
Mail.ReadBasic.All	Application	Read basic mail in all mailboxes	Yes	✓ Granted for 1touch-dev
Sites.Read.All	Application	Read items in all site collections	Yes	✓ Granted for 1touch-dev
User.Read	Delegated	Sign in and read user profile	No	✓ Granted for 1touch-dev
User.Read.All	Application	Read all users' full profiles	Yes	✓ Granted for 1touch-dev
Microsoft Purview (1)				
Purview.ApplicationAccess	Application	Purview Application API Access	Yes	✓ Granted for 1touch-dev

Figure 3: Registered app permissions in MS Azure portal

GETTING A SECRET KEY FOR MS AIP

1. Log in into your Microsoft accout in Azure portal. Go to App registrations > All applications.



portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationsListBlade

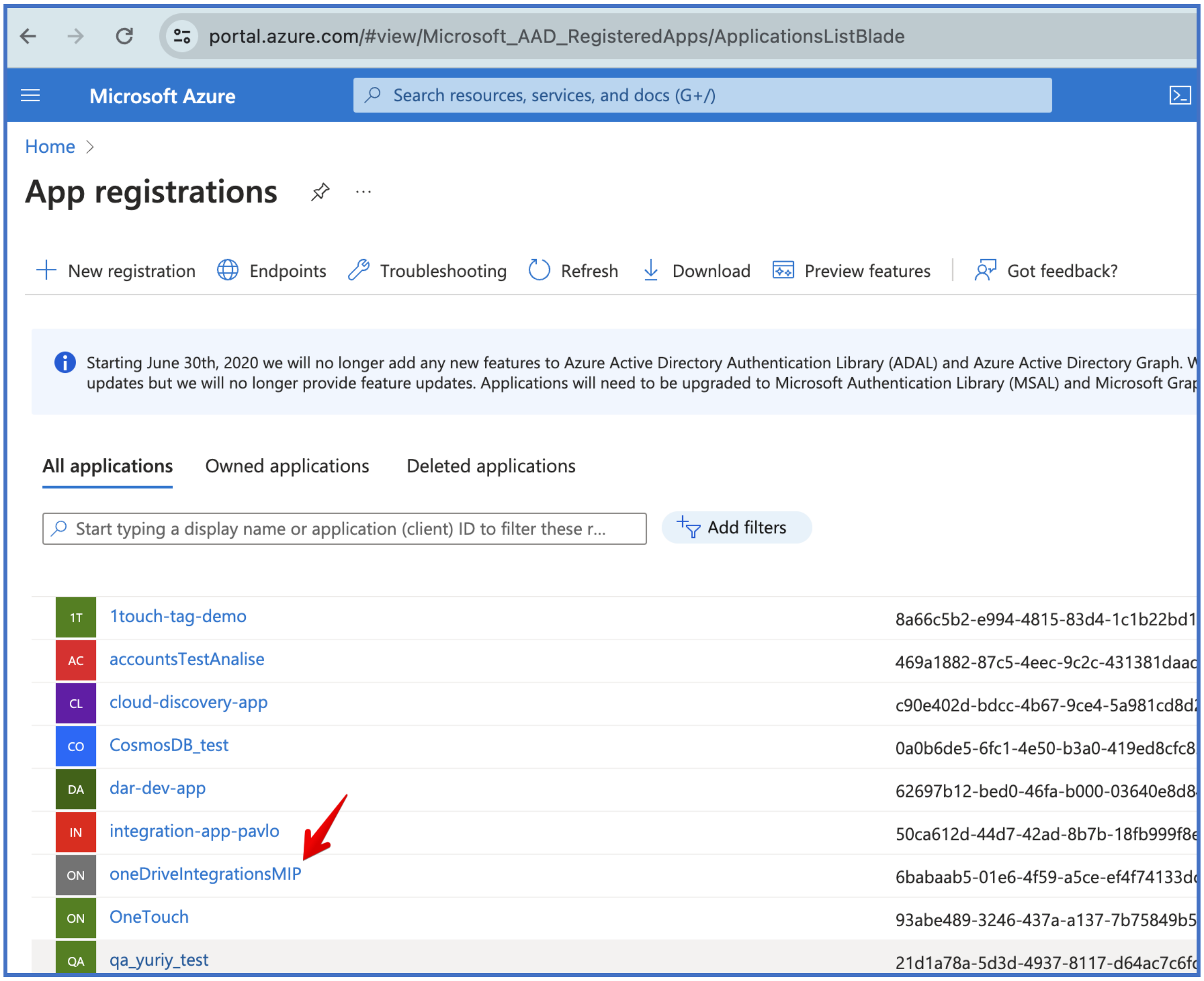
Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. W updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Grap

All applications
Owned applications
Deleted applications
Start typing a display name or application (client) ID to filter these r...
Add filters

This account isn't listed as an owner of any applications in this directory.

Figure 4: All applications in Azure portal

2. From the list of applications, select the dedicated integration with Inventa.


portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationsListBlade
Microsoft Azure
Search resources, services, and docs (G+/)
Home >
New registration
Endpoints
Troubleshooting
Refresh
Download
Preview features
Got feedback?
All applications
Owned applications
Deleted applications
Start typing a display name or application (client) ID to filter these r...
Add filters

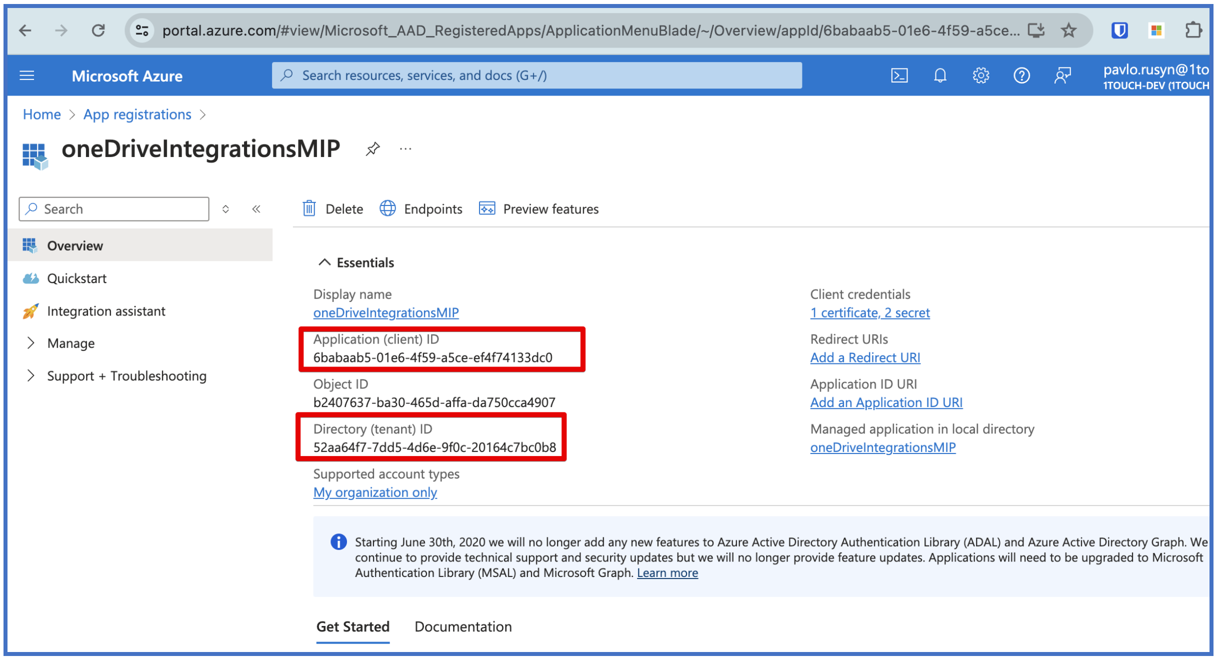
App registrations

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. W
updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Grap

1T	1touch-tag-demo	8a66c5b2-e994-4815-83d4-1c1b22bd1
AC	accountsTestAnalise	469a1882-87c5-4eec-9c2c-431381daac
CL	cloud-discovery-app	c90e402d-bdcc-4b67-9ce4-5a981cd8d
CO	CosmosDB_test	0a0b6de5-6fc1-4e50-b3a0-419ed8cfc8
DA	dar-dev-app	62697b12-bed0-46fa-b000-03640e8d8
IN	integration-app-pavlo	50ca612d-44d7-42ad-8b7b-18fb999f8e
ON	oneDriveIntegrationsMIP	6babaab5-01e6-4f59-a5ce-ef4f74133d
ON	OneTouch	93abe489-3246-437a-a137-7b75849b5
QA	qa_yuriy_test	21d1a78a-5d3d-4937-8117-d64ac7c6f

Figure 5: Selecting the integration app

3. On the application page, make a note of the application (client ID) and directory (tenant) ID.


portal.azure.com/#view/Microsoft_AAD_RegisteredApps/ApplicationMenuBlade/~/Overview/appId/6babaab5-01e6-4f59-a5ce...
Microsoft Azure
Search resources, services, and docs (G+/)
pavlo.rusyn@1to
1TOUCH-DEV (1TOUCH
Home > App registrations >
oneDriveIntegrationsMIP
Search
Overview
Quickstart
Integration assistant
Manage
Support + Troubleshooting
Delete
Endpoints
Preview features
Essentials
Get Started
Documentation

Display name
oneDriveIntegrationsMIP

Application (client) ID
6babaab5-01e6-4f59-a5ce-ef4f74133dc0

Object ID
b2407637-ba30-465d-affa-da750cca4907

Directory (tenant) ID
52aa64f7-7dd5-4d6e-9f0c-20164c7bc0b8

Supported account types
My organization only

Client credentials
1 certificate, 2 secret

Redirect URIs
Add a Redirect URI

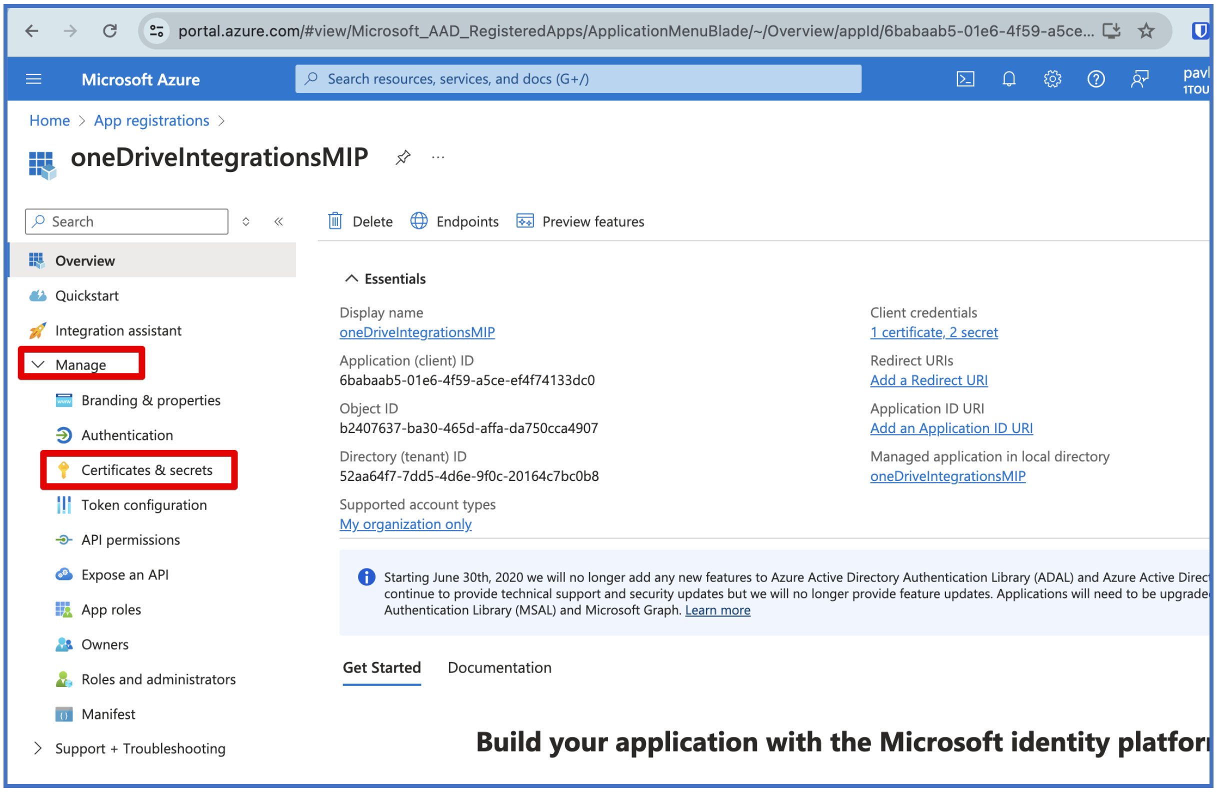
Application ID URI
Add an Application ID URI

Managed application in local directory
oneDriveIntegrationsMIP

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Directory Graph. We continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgraded to Microsoft Authentication Library (MSAL) and Microsoft Graph. Learn more

Figure 6: Application (client ID) and directory (tenant) ID

4. Go to Manage > Certificates & Secrets.



Display name
oneDriveIntegrationsMIP

Application (client) ID
6babaab5-01e6-4f59-a5ce-ef4f74133dc0

Object ID
b2407637-ba30-465d-affa-da750cca4907

Directory (tenant) ID
52aa64f7-7dd5-4d6e-9f0c-20164c7bc0b8

Supported account types
My organization only

Client credentials
1 certificate, 2 secret

Redirect URIs
Add a Redirect URI

Application ID URI
Add an Application ID URI

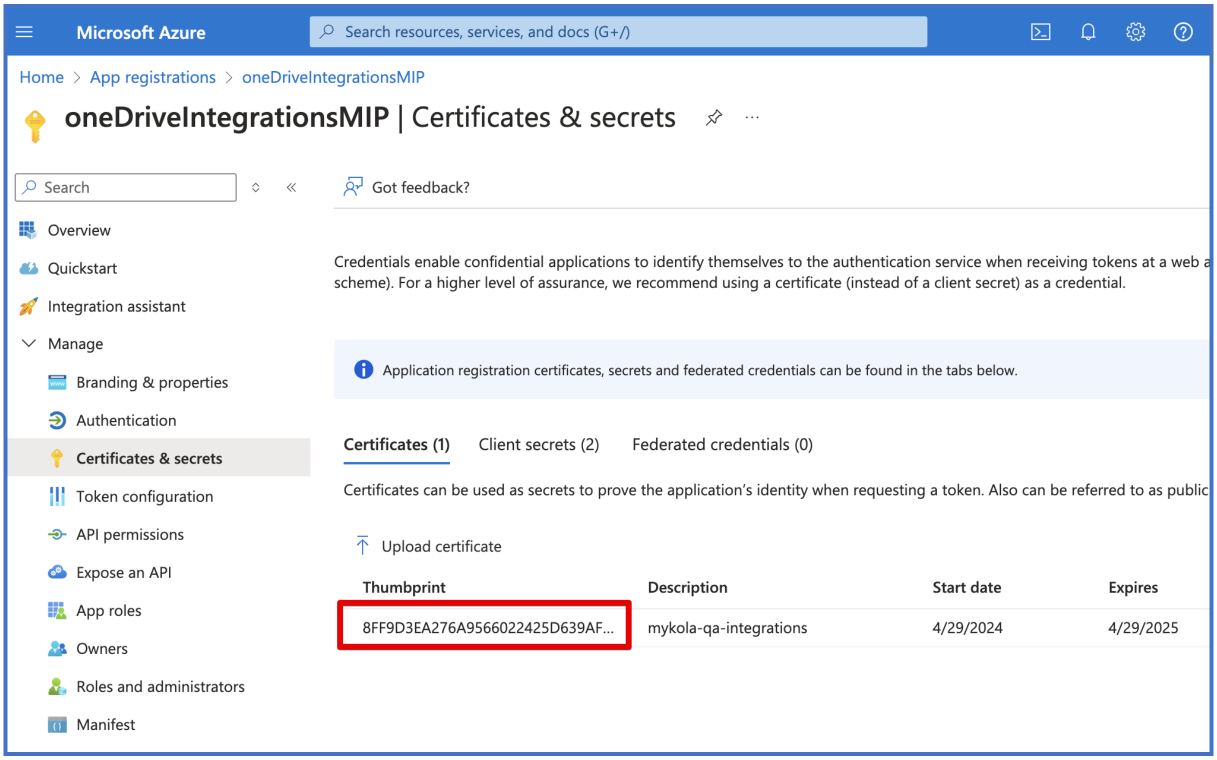
Managed application in local directory
oneDriveIntegrationsMIP

Starting June 30th, 2020 we will no longer add any new features to Azure Active Directory Authentication Library (ADAL) and Azure Active Direc continue to provide technical support and security updates but we will no longer provide feature updates. Applications will need to be upgrade Authentication Library (MSAL) and Microsoft Graph. Learn more

Build your application with the Microsoft identity platfor

Figure 7: Managing certificates & secrets

5. Make a copy of the thumbprint.



Credentials enable confidential applications to identify themselves to the authentication service when receiving tokens at a web a scheme). For a higher level of assurance, we recommend using a certificate (instead of a client secret) as a credential.

Application registration certificates, secrets and federated credentials can be found in the tabs below.

Certificates can be used as secrets to prove the application's identity when requesting a token. Also can be referred to as public

Thumbprint	Description	Start date	Expires
8FF9D3EA276A9566022425D639AF...	mykola-qa-integrations	4/29/2024	4/29/2025

Figure 8: Application certificates & secrets

IMPLEMENTATION

1. The integration app imports the sensitivity labels data from MS Purview so Inventa is then able to use it for labeling the data elements both within the Microsoft resources (in Azure DBs, OneDrive, Exchange, etc.) and outside of them .

2. Labels can then be managed in MS Purview after letting Purview know what type of data should be classified.

3. The sensitivity labels are then used to build a catalog of items detected by Inventa and mark their relations to various data assets.

MS PURVIEW APP INSTALLATION & REMOVAL

INSTALLATION

The integration package is provided on demand. It can be installed on your VM, local machine, or cluster node. To deploy the project, perform the following steps:

1. Start the stack using command below:

```
docker-compose up -d --build
```

2. The application upgrade procedure is the same as for installation. The docker volumes removal may be required, only if specified explicitly.

REMOVAL

1. To delete the application, stop the containers from the directory with deployment files:

```
docker-compose down
```

2. Remove the docker volumes created for the project. Volumes can be listed using command:

```
docker volume ls
docker volume rm <s-now related volumes>
```

MS PURVIEW APP USAGE

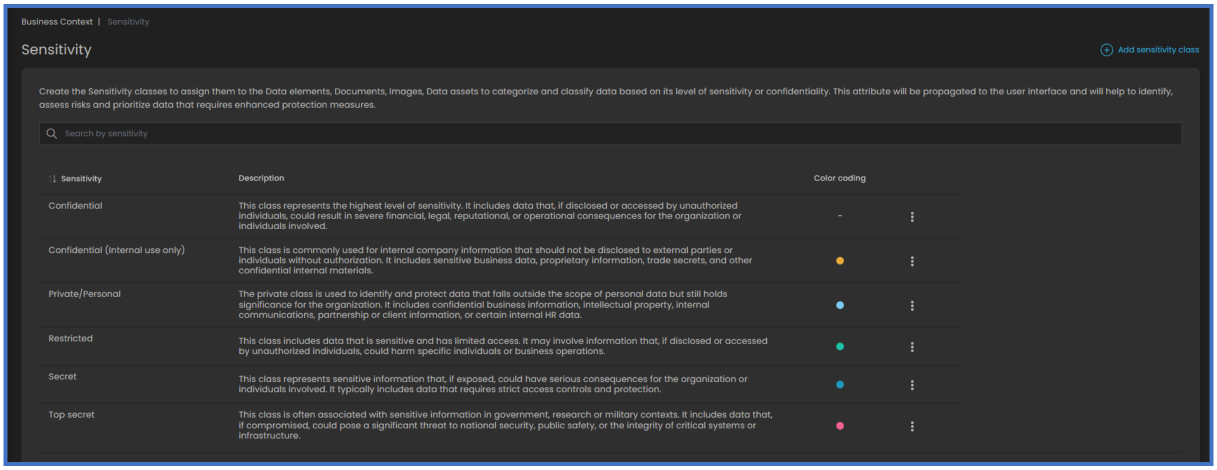
IMPORTING THE SENSITIVITY LABELS AND USING THEM FOR CATALOGING

Create a set of sensitivity labels in MS Purview and communicate with Inventa in order to import the list and use it for cataloging in Inventa.

For example, an organization configures a set of sensitivity labels: General, Confidential/All Employees, Confidential/Executive Employees, Highly Confidential. Based on an organization's data security policies, all data containing credit card information should be categorized as General, Confidential/All Employees.

The integration app imports the General, Confidential/All Employees, Confidential/Executive Employees, Highly Confidential labels from MS Purview and into Inventa. These labels appear as sensitivity classes in Inventa platform > Business context > Sensitivity.

The Inventa user assigns the General, Confidential/All Employees sensitivity classes to the Credit Card Number data element.



Sensitivity

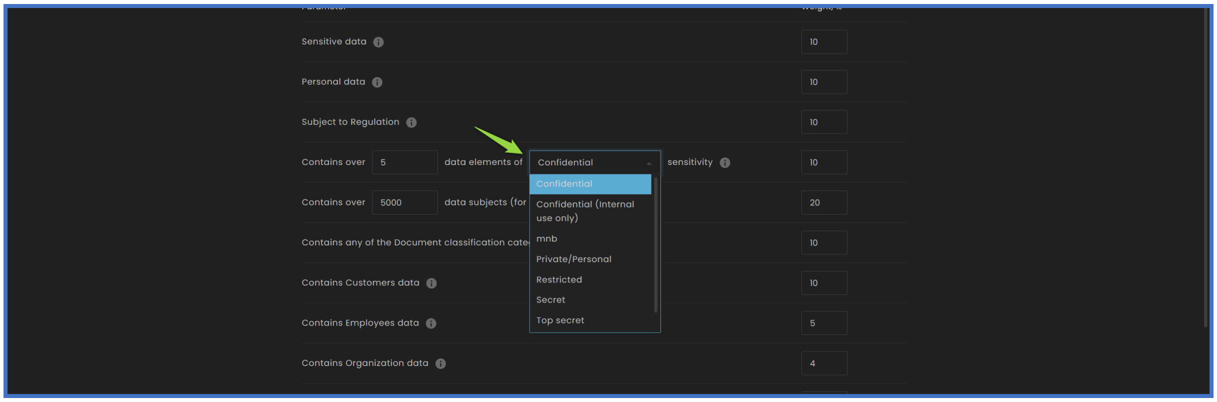
Create the Sensitivity classes to assign them to the Data elements, Documents, Images, Data assets to categorize and classify data based on its level of sensitivity or confidentiality. This attribute will be propagated to the user interface and will help to identify, assess risks and prioritize data that requires enhanced protection measures.

Sensitivity	Description	Color coding	
Confidential	This class represents the highest level of sensitivity. It includes data that, if disclosed or accessed by unauthorized individuals, could result in severe financial, legal, reputational, or operational consequences for the organization or individuals involved.	-	⋮
Confidential (Internal use only)	This class is commonly used for internal company information that should not be disclosed to external parties or individuals without authorization. It includes sensitive business data, proprietary information, trade secrets, and other confidential internal materials.	●	⋮
Private/Personal	The private class is used to identify and protect data that falls outside the scope of personal data but still holds significance for the organization. It includes confidential business information, intellectual property, internal communications, partnership or client information, or certain internal HR data.	●	⋮
Restricted	This class includes data that is sensitive and has limited access. It may involve information that, if disclosed or accessed by unauthorized individuals, could harm specific individuals or business operations.	●	⋮
Secret	This class represents sensitive information that, if exposed, could have serious consequences for the organization or individuals involved. It typically includes data that requires strict access controls and protection.	●	⋮
Top secret	This class is often associated with sensitive information in government, research or military contexts. It includes data that, if compromised, could pose a significant threat to national security, public safety, or the integrity of critical systems or infrastructure.	●	⋮

Figure 1: Sensitivity classes in Inventa

USE IMPORTED SENSITIVITY LABELS FOR CRITICALITY SCORE CALCULATION CONFIGURATION

Automatically imported sensitivity labels can be used in the configuration process of how Inventa calculates criticality score for data sources and files. The labels imported from MS Purview will be available for the **Contains over [X] data elements of [Y] sensitivity** parameter in the sensitivity selection dropdown menu on the **Criticality score configuration** page.



Sensitive data	10
Personal data	10
Subject to Regulation	10
Contains over 5 data elements of Confidential sensitivity	10
Contains over 5000 data subjects (for	20
Contains any of the Document classification cate	10
Contains Customers data	10
Contains Employees data	5
Contains Organization data	4

Figure 2: Sensitivity class dropdown

ASSIGN THE INVENTA SENSITIVITY LABELS TO FILES

Import a set of sensitivity labels from MS Purview to Inventa and use them for labeling in Microsoft resources like OneDrive, Exchange Online, etc.

> Microsoft allows assigning only one label per file. The integration app will assign the label with the highest scoring configured in Inventa platform › Business Context › Sensitivity.

For example, you import a set of sensitivity labels and configure there scoring: General (scoring 10), Confidential/All Employees (scoring 25), Confidential/Executive Employees (scoring 35), Highly Confidential (scoring 70) in Inventa.

Inventa classifies a file in OneDrive that matches the General and Highly Confidential sensitivity classes. The integration will assign the Highly Confidential label to this file because of a higher scoring.