**Configure Microsoft Dataverse (25–30%)**

**Manage the data model**

* Create or modify standard, activity, or virtual tables
* Create new tables or modify existing tables
* Determine which type of relationship to implement, including one-to-many and many-to-many
* Configure table relationships including behaviours and cascading rules
* Create new or modify existing columns, including calculated, rollup, and formula
* Configure table properties

**Manage Dataverse**

* Configure Dataverse search, and manage the search index
* Manage auditing
* Describe options for importing and exporting data
* Configure duplicate detection settings
* Configure bulk deletion

**Configure security settings**

* Manage business units
* Create and manage security roles
* Create and manage users and teams
* Create and manage column security
* Configure hierarchy security
* Configure Microsoft Entra ID group teams

## Getting Started with Dataverse

Each ***environment*** is created under a Microsoft Entra ID tenant, and only users within that tenant can access its resources. An environment (Dataverse DB and resources created in that env) is also bound to a geographic location, like the United States. Can create more than 1 env (e.g., dev and prod).

Dev env - A Power Platform **admin** can create Developer environments for other users and can restrict users from creating their own Developer environments.

Creating env - once you create an environment with Dataverse in it, you can access that Dataverse data from other environments as well. Dataverse creation with an environment reserves up to 1 GB in storage.

Dataverse

Dev env

Dev env

Dataverse

Dataverse

Prod env

Prod env

Users & Roles - After you have created an environment, users from Microsoft Entra ID that are associated with your tenant and have a selected security role are automatically added to the environment.

\*We recommend that you create Microsoft Entra ID groups and associate roles with those security groups to simplify permissions and data access.

Notes: The two Environment **roles** that are built into **every** environment are System Administrator and Environment Maker. All other roles are user security roles.

The following **operation** can be done on the **Environment**:

Change env type – prod to sandbox, sandbox to prod  
Delete env - to recover storage space and to remove personal data  
Recover env - within seven days of deletion  
Reset env – useful when we need to create new project or free up resources and personal data  
Copy env – there are two level of copy 1) Everything, and 2) Customizations and schemas only  
Restriction apply such as:  
- can only copy to an environment in the same tenant and region  
- can’t copy to prod env  
- copy and restore operations can take up to 8 hours – 24 hours

Backup and Restore

System backup – with Dynamic enabled, it stored 28 days, if not, only 7 days

Manual backup – sandbox/dev for 7 days, prod with Dynamic is 28 days

Restoring env - To restore to a production environment, you must first change its type to sandbox.

Administration mode - is useful when you want to make operational changes and not have regular users affect your work, and not have your work affect end users (non-admins).

Table

To create a table, go to <https://make.powerapps.com/>, you must be in correct environment.

Click “Table” menu item from the left menu bar. Select Create. Below are three properties:

* 1. Schema name: This is the internal name of the table created in the database
  2. Type: Standard, Activity, Virtual or Elastic.
  3. Record ownership: User or Team or Organizational

You can’t change these options once a table is created.

Table types:

1. **Standard**: A table where you can store data and add to the navigation in model-driven apps.
2. **Activity**: Store interactions with time dimensions such as phone calls, tasks, and appointments. Dataverse has a set of activity tables. These tables share the same set of columns and share security privileges. Many of the table options, including the primary column, are fixed and can't be changed. Activity tables appear in the timeline on model-driven app forms.
3. **Virtual**: Connect to data from an external data source such as Microsoft Azure SQL Database. Virtual tables appear in your app to users as regular table rows but contain data that is sourced from an external database dynamically at runtime.
4. **Elastic**: Used when your table includes a large dataset in excess of tens of millions of rows. Elastic tables are powered by Azure Cosmos DB.

Licensing Requirements for each table type

A screenshot of a computer program

Description automatically generated

Tables with complex business logic (**or Complex tables**) such as code plug-ins or real time workflows will require that users have a Power Apps or Power Automate per user license.

**Restricted tables** aren't standard tables within Dataverse but are included in one of the customer engagement apps in Dynamics 365 or a third-party solution. They'll require a Dynamics 365 license.

More details on Licensing Requirements for each table type are [here](https://learn.microsoft.com/en-us/power-apps/maker/data-platform/data-platform-entity-licenses).

More details on Restricted tables requiring Dynamic 365 license are [here](https://learn.microsoft.com/en-us/power-apps/maker/data-platform/data-platform-restricted-entities).

Table Ownership

1. User or team owned: Data belongs to a user or team. Actions that can be performed on these rows can be controlled at the user level.
2. Organization-owned: Data belongs to the organization. Access to the data is controlled at the organization level.

Tips: Dataverse came with many standard tables and recommended using them (by changing the column name if needed) instead of creating a new table. You can also hide the standard tables if not using them. To hide a standard table, change the security role privileges for your organization to remove the Read privilege for that table. This removes the table from most parts of the application.

A screenshot of a computer

Description automatically generated

We can customize Views and Forms for a table.

Create a Dataverse Table:

<https://learn.microsoft.com/en-us/training/modules/get-started-with-powerapps-common-data-service/3-create-a-cds-entity>

Import SharePoint list data into Dataverse Table:

<https://learn.microsoft.com/en-us/training/modules/get-started-with-powerapps-common-data-service/4-import-data-into-your-database>

Create table relationships:

<https://learn.microsoft.com/en-us/training/modules/get-started-with-powerapps-common-data-service/create-table-relationships>

Create custom table, business rule and import Excel spreadsheet data to Dataverse table

<https://learn.microsoft.com/en-us/training/modules/get-started-with-powerapps-common-data-service/4a-use-data-cds-exercise>

Dataverse Logic and Security

Reduce repetitive code in app - Tables within Dataverse can use rich server-side logic and validation to ensure data quality.

* Business rules: Business rules validate data across multiple columns in a table, and provide warning and error messages, regardless of the app that's used to create the data.
* Business process flows: Business process flows guide users to ensure they enter data consistently and follow the same steps every time. Business process flows are currently supported only for model-driven apps.
* Real-time workflows: Workflows automate business processes without requiring user interaction.
* Business logic with code: Business logic supports advanced developer scenarios that extend the application directly through code.

Business Rules

Business rules can be used for data validation, enforce requirement, set value, perform calculation, etc. Business rules depend on the scope of the rule which can be:

1. **Individual form**: The rule applies only to the specified model-driven app form.
2. **All forms**: The rule applies to all model-driven app forms.
3. **Entity**: The rule applies to all model-driven app forms and when the row is created or updated on the Dataverse table. This is the default setting.

Two main components here are Flow and Actions. Flow is the condition check and action is the tasks to perform such as showing error messages, setting field visibility or setting/clearing default value, etc.

Note: Business rules defined for a table apply to both canvas apps and model-driven apps if the table is used in the app BUT in canvas apps, show or hide, enable or disable and creating business recommendations based on business intelligence are not supported.

Dataverse Security

Standard security roles System Administrator, Environment Maker and Basic User. But should create custom security roles because standard security roles cannot be customized for your tables. You can only modify custom security roles.

You can manage security roles from the Power Platform admin center. Select your environment and select Settings, expand Users + permissions and select Security roles.

Dataverse Auditing

Three levels of auditing: Environment, Table and Column.

Dataverse auditing is supported on all custom and most customizable tables and columns. Audit logs are stored in Dataverse and **consume log storage capacity**. You can view audit logs in the Audit History tab for a single record. You can view audit logs in the Audit Summary view for all audited operations in a single environment. Audit logs can also be retrieved using the Web API or the SDK for .NET.

It's possible to refer to audit log data in a model driven app under **Audit history**.

Note that auditing won’t run if is turned off for your environment.

Dua-write vs Virtual tables/entities

Dual-write – is an out-of-box infrastructure (automated data flow) that provides near-real-time interaction between customer engagement apps and finance and operations apps. Dual-write also supports online and offline mode, and it follows the no-code/low-code principle.

Virtual Entities – tables dose not reside in Dataverse. Instead, it continues to reside in the app where it belongs but support CRUD operations. The entities must be made available as virtual entities in Dataverse to support CRUD.

Together, virtual entities and dual write are part of the shared data layer for the convergence of finance and operations apps and the Dataverse platform. They're complementary technologies that are intended to work **together**.

When you must have access to your data offline, consider Dual write. If data is for read-only then consider virtual entities which also save the storage space in Dataverse.

**Primary Column** – a way to identify a record in a table and is not a unique identifier (NOT a Primary Key). The Unique identifier column is a GUID (autogenerated). To make the primary column unique, then create an alternate key (with unique value) and assign the Primary Name column to the new key. You can create up to five keys for each table. All values in the key are unique.

**Choice Column** – Two options: Local Choice vs Global Choice.

Local choices can only be used by the table and column that they're created against and can't be reused on other tables. A global choice is a separate component and can be reused for multiple columns on multiple tables. The list of choices is shared for the table columns that reference the global choice.

**Dataverse Data Export Options** – Beside exporting Excel format, offer both Power Automate and Azure Synapse Link.

Power Automate – use cloud flows with the Dataverse connector to query table rows and generate output files. Power Automate can extract exactly the information that you require in the format that you need.

Azure Synapse Link – after enabling the Azure Synapse Link for Dataverse in the Power Apps maker portal, you choose the tables in Dataverse and Dataverse will perform a continuous replication of data to Azure to either an Azure Data Lake storage Gen2 account or an Azure Synapse Analytics workspace.

Using Dataflow to import data into Dataverse

Create dataflow with destination storage and schedule data refresh. This can be done in Power App Portal under “Dataflows” (may need to click on …More menu option).

Importing data using dataflow link is [here](https://learn.microsoft.com/en-us/training/modules/load-export-data-create-data-views/5a-import).

**Action-based Data Source (Service Name or Action Connectors)**

Differ from the more popular tabular data sources. You use functions to interact with the data source instead of just reading and writing data. But it cannot be used with **Forms Control**. Most action-based data sources provide functions for updating the data as appropriate. An action-based data source can also be for things like sending emails or other notifications, not necessarily only for reading and writing data. Power App supports both tables and action-based data sources.

More on how to work with action-based data source is [here](https://learn.microsoft.com/en-us/training/modules/connect-to-other-data-in-powerapps-canvas-app/2-work-with-action-based-data-sources).

**Power Automate is a companion of Power App**

Power Automate helps you to pull data from many different tables and action connectors, so it's a valuable companion for Power Apps. Power Automate is a connector to Power App.

Use case: Send email when someone submit form – this can be done using Power App, but

Use case: Start approval process after sending email – this is where Power Automate comes in

Explanation: You can have Power Apps trigger a Power Automate flow when the user submits the data. Power Automate can then look up who the user's manager is and send the manager an approval request. Power Automate will then help get a response from the manager, update the data source with the status based on their response, and send the original submitter an update.

User case: Consuming third-party API that return complex JSON data and need to purify before storing it to our table. Power Automate can do that and store data to table and then Power App will take care of displaying or working with those data further.

Power App  
is a Trigger Point

Trigger (with params)

Power Automate  
take those params and perform action on the flow

More use cases can be found [here](https://learn.microsoft.com/en-us/training/modules/connect-to-other-data-in-powerapps-canvas-app/3-flow-and-powerapps).

## Manage permissions and administration for Dataverse

More on Environment - Each environment can have zero or one instance of a Dataverse database, and it serves as a collection of objects such as tables, flows, apps, connections, and security roles. Typically, an organization might use multiple environments to support different groups of users simultaneously. This setup allows you to limit who can access specific data, apps, and workflows in each environment. One common practice is to create separate environments for different stages of application lifecycle management (ALM), such as development, testing, and production. In production environment, you configure permissions to allow access to the data, apps from Microsoft Power Apps, and Microsoft Power Automate workflows.

Security Roles – Go to environment -> Settings -> Security Roles.

After you define a security role in the environment, you can:

* Associate it directly with users.
* Associate it with Dataverse business units and teams.

Individually assigning security roles to users can be a tedious process for groups of users. Instead, you can associate a security role with a team and then add all users to the team. After you assign a user to the team, they receive the security role's privileges. Often, organizations use this approach to accelerate the assignment of security roles to groups of users. A key concept of Dataverse security is that privileges are accumulative across all assigned security roles, with the highest privilege access winning.

List of actions can perform are: Create, Read, Write, Delete, Append, Append To, Assign, Share. These actions make up the ***privileges*** of a security role.

Business Units - Go to environment -> Settings -> Business Units.

Business units provide security and structure for grouping users. Often, you would use business units to mimic an organization’s departmental structure (but they don't need to). Business units are hierarchical, and every Dataverse instance has a single root business unit. Beneath the root business unit, you can create child business units to further segment and secure your data.

Important: If you move a user to a different business unit, you need to reassign their security roles. Each user is a member of only one business unit, but a team can have user members from multiple business units.

Access Level – Each privilege (Create, Read, etc.) can be granted different access levels.

* None – No access
* User – access to record owned by users, shared with them or their teams
* Business Unit – access to records in user’s business unit. Because this access level gives access to information throughout the business unit, it should be restricted to match the organization's data security plan. For managers with authority over the business unit.
* Parent: Child Business Unit – access to records in users’ business units or all subordinate units. This level gives access to information throughout the business unit and subordinate business units. For managers with authority over the business units.
* Organization – access to all records in the organization regardless of the business unit hierarchical level they belong to. For managers with authority over the organization.

**Tips: Together the privileges and access levels make up role-based access control in Dataverse.**

Teams – important security building blocks. Business units own teams. Every business unit has a default team that the system automatically creates when you create the business unit. Dataverse manages members of the default team, which contains all users who are associated with that business unit. You can’t add or remove members from the default team manually. Instead, the system dynamically adjusts the members as you add new users to or remove them from business units.

Tips: Users can be members of multiple teams, which allows for a powerful way of granting permissions to users without micromanaging access at the individual user level.

Hierarchy Security – In addition to business units, you can help secure Dataverse by using one of the out-of-the-box hierarchical security models. The hierarchy security model extends Dataverse security. Two security models that you can use for hierarchies are:

* Manager hierarchy - To access data the subordinate's data, a user must be in the same business unit as the subordinate or in the parent business unit of the subordinate’s business unit. You can establish the manager and subordinate relationship by using the Manager field on the User table.
* Position hierarchy - Allows data access across business units. With position hierarchy security, you can define various job positions in the organization and arrange them in a hierarchy by using the Position table. Then, you can add users to any given position by using the Position lookup column on the User record.

To configure “Hierarchy Security”, Go to environment -> Settings -> Users + permissions -> Hierarchy security. Then select “Enable Manager hierarchy Model” option or “Enable Position hierarchy Model”, you may click “Configure” hyperlink next to it to configure one of the selected hierarchy models.

Tips: For performance, avoid creating many business units. Instead, create fewer business units and add hierarchy security.

Table/record ownership – Dataverse supports two types of record ownership: organization owned, and user or team owned. Record ownership is a choice that happens when you create the table, and you can't change it afterward.

For organization-owned records, the only access level choices are that the user can do the operation, or they can’t. For user and team-owned records, the access level choices for most privileges are: (1) Organizational, (2) Business unit, (3) Business unit and child business unit, (4) Only the user’s own records.

Record-level security in Dataverse – A user's access to a record is the combination of all their security roles, the business unit that they're associated with, the teams that they're members of, and the records that are shared with them. All access in Dataverse is accumulative across all of those concepts in the scope of a Dataverse database environment. These entitlements are only granted in a single database and are individually tracked in each Dataverse database, requiring a user to have an appropriate license to access Dataverse.

Column-level security to control access - You can turn on column-level security on a column-by-column basis. Then, you can manage access by creating a Column Security Profile. The profile contains all columns that have column-level security turned on and the access granted by that specific profile. You can control each column in the profile for Create, Update, and Read access. Then, you would associate Column Security Profiles with a user or teams to grant users with those privileges to the records that they already have access to.

Important: A user must already have access to the record (row-level) for the Column Security Profile to grant them access to the columns.

Configure user’s environment security - After you create roles, teams, and business units in an environment, you can assign users with their security configurations.

1. When you create a user, associate the user with a business unit. By default, this business unit is the root business unit in the organization. The system also adds the user to the default team of that business unit.
2. Assign security roles that the user needs and/or add them as members of certain teams. Remember, teams can also have security roles, and the effective rights of the user is the combination of directly assigned security roles with those of any teams that the user is a member of.

Additionally, if you use column-level security, you need to associate the user, or a team of the user, to a Column Security Profile that you created.

## Get started with security roles in Dataverse

A security role has certain privileges associated with it, and you can associate a user with one or many security roles.

Environment roles – Environments have two predefined roles that provide access to permissions within an environment.

* Environment admin - Before a Dataverse database is added to the environment, the Environment Admin role can perform all administrative actions on an environment.
* Environment Maker - can create resources within an environment including apps, connections, custom connectors, gateways, and flows using Power Automate.

The following rules apply to members of the ***Environment Maker*** role:

* Environment Makers can distribute the apps that they build in an environment to other users within an organization. They share the app with individual users, security groups, or all users in the organization.
* Users or groups that are assigned to these environment roles aren't automatically given access to the environment's database (if it exists). They must be given access separately by a Database owner.
* Whenever a new user signs up for Power Apps, they're automatically added to the Maker role of the default environment.

You assign users to one of these two roles when considering what permissions, you want to give to a user in an environment. However, if the environment has a Dataverse database, more roles are added, and the permissions options broaden.

Environments with a Dataverse datastore - When an environment has a Dataverse datastore, users must be assigned the System Administrator role instead of the Environment Admin role for full admin privileges.

Important: Users who make apps that connect to Dataverse and need to create or update table and security roles need to be assigned the System Customizer role in addition to the Environment Maker role. This is necessary because the Environment Maker role doesn't have privileges on the environment's data.

Refer following table for summary of resources available for predefined security roles.

A screenshot of a computer

Description automatically generated

Permission Settings - Configuration of table permissions can also be done with predefined groups of permissions. Select a table, and then select Permission Settings in the command bar or select More Actions (…) > Permission Settings.

A screenshot of a computer

Description automatically generated

Beside permission settings on a table, “Miscellaneous privileges” (such as Bulk Edit, Merge, etc.) and “Privacy related privileges” (such as Export to Excel), can also be configured.

Tips: Privacy related privileges only use the None or Organization access levels. Most miscellaneous privileges only use the None or Organization access levels but there are some miscellaneous privileges that can have all access levels set.

Configure Dataverse team for security - Using Microsoft Dataverse teams is optional. However, teams provide an easy way to share business objects and let you collaborate with other people across business units. Although a team belongs to one business unit, it can include users from other business units. You can associate a user with more than one team.

Team Types - can be one of the following: Owner, Access, Microsoft Entra ID Security group, or Microsoft Entra ID Office group. Go to environment -> Settings -> Users + permissions -> Teams.

* Owner team: an owner team owns records and has security roles assigned to the team. A user's privileges can come from their individual security roles, those of the teams that they're part of or the ones they inherit. Team members are added manually to the owner team.
* Access team: an access team doesn't own records and doesn't have security roles assigned to the team. The team members have privileges defined by their individual security roles and by roles from the teams they're members of.
* Microsoft Entra ID group team: Like owner teams, a Microsoft Entra ID group team can own records and can have security roles assigned to the team. Security and Office are two group team types, and they correspond directly to Microsoft Entra ID group types. Team members are dynamically derived (added and removed) when they access an environment based on their Microsoft Entra ID group membership.

The administrator can create Microsoft Entra ID group teams that are associated to the Microsoft Entra ID groups in each of the Dataverse environments. Then they can assign a security role to these group teams. For each Microsoft Entra ID group, the administrator can create group teams based on the Microsoft Entra ID group Members, and/or Owners, or Guests, and assign a respective security role to each of these teams. When members of these group teams access these environments, their access rights are automatically granted based on the group team's security role.

Provision and deprovision users - Once the group team and its security role are established in an environment, user access to the environment is based on the user membership of the Microsoft Entra ID groups. When a new user is created in the tenant, all the administrator needs to do is assign the user to the appropriate Microsoft Entra ID group, and assign Dataverse licenses. The user can immediately access the environment without the need to wait for the administrator to assign a security role.

When users are deleted or disabled in Microsoft Entra ID or removed from the Microsoft Entra ID groups, they lose their group membership. These users won't be able to access the environment when they try to sign in.

Important: The memberships for the user's Microsoft Entra ID groups and Dataverse group teams are synchronized, and the user's access rights are dynamically derived at run time.

## Use administration options for Dataverse

Tenant Storage Capacity - Dataverse storage is broken into three sources:

* **Database:** Refers to the data that is being stored in tables in your Dataverse database. This includes item like out-of-the-box tables, custom tables, and more.
* **Log:** Refers to log files and that are being used to capture information such as audit logs, or plug-in trace logs.
* **File:** Refers to images or files that are being stored in your Dataverse environment such as a customer’s picture stored on their contact record.

Dataverse Search - delivers fast and comprehensive search results in a single list, sorted by relevance. With Dataverse search enabled, a search box is always available at the top of every page in all the model-driven apps in the environment.

Search Index - The search index defines which tables appear in search results. You can manage search index from the **Overview** tab within a solution.

Auditing - Data change auditing, is configured at the Dataverse environment, table, and column level. Enabling and disabling of auditing can only be done by someone in the System Administrator or System Customizer role.

Auditing settings for tables and columns are solution aware and will be transported with the schema as the solution is installed in another environment. However, each environment must have auditing enabled at the environment level for these settings to perform as expected.

Tips: If auditing is disabled at the environment level, no auditing data is captured, even if auditing is configured for tables and columns in the environment.

Go to environment -> Settings -> Audit & Logs -> Audit settings

Enabling auditing on tables and columns - By default, new Dataverse tables that are created have auditing disabled. You can enable or disable auditing for tables using the classic solution explorer. When auditing is enabled for a table, auditing is enabled for all eligible columns of that table. When editing a column, you can find the auditing switch under the advanced options section on the column properties.

Important: After changing any of the column audit configurations to enable or disable, you must publish changes for the table or publish all changes.

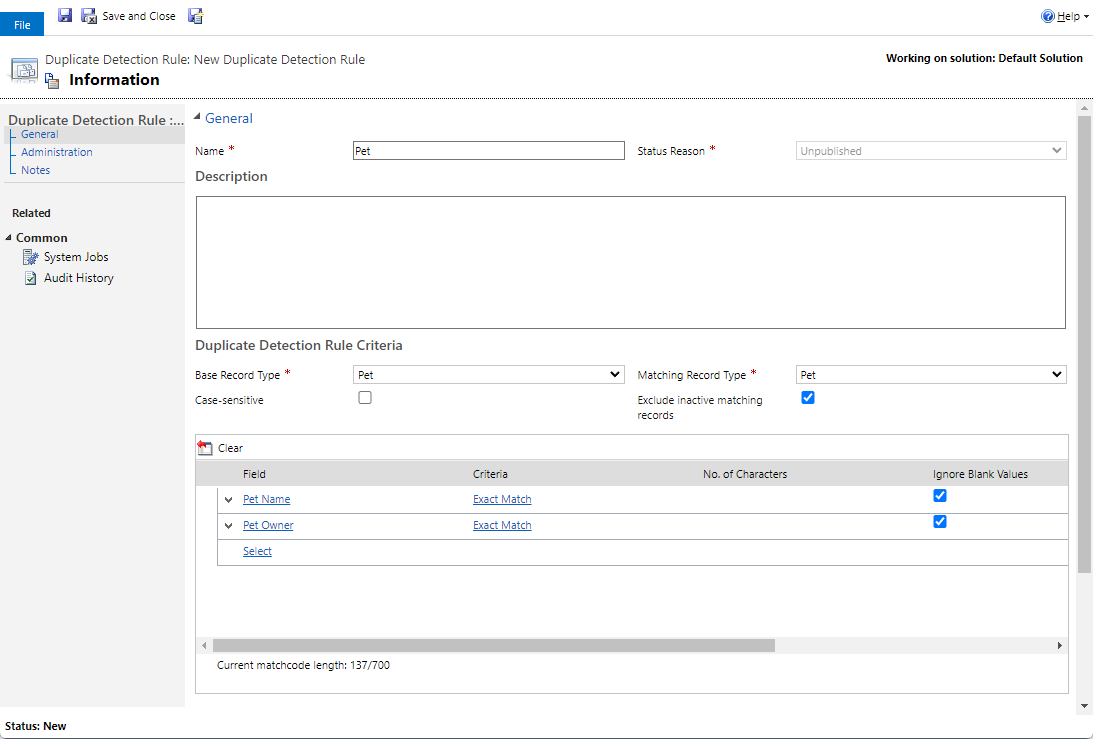
Duplicate Detection - Microsoft Dataverse includes basic duplicate detection functionality. Duplicate detection must be enabled in the environment's settings in the Power Platform admin centre under the **Data management** section.

Important: To detect duplicates for a table's rows, you must first edit the table's properties in the Power Apps maker portal and enable the Apply duplicate detection rules option.

Configure duplication detection rules - To detect duplicates, you need to define rules to determine potential duplicate data. You can only create duplicate detection rules for tables that have been enabled for duplicate detection. Duplicate detection rules are managed in the environment's settings in the Power Platform admin center under the Data management section.

To create a duplicate detection rule: Select the base and matching tables. The matching table defaults to the selected base table but can be changed. Select column and then Select matching criteria.

The matching criteria you can select is simple.



Tips: You should select **Exclude inactive matching records** to prevent duplicates being found for deactivated rows and you should select **Ignore blank values** to prevent multiple blank to blank duplicates being detected.

Duplicate detection jobs **-** Duplicate detection jobs run as scheduled background jobs to find duplicates on a table. Duplicate detection jobs are managed in the environment's settings in the Power Platform admin center under the **Data management** section. Duplicate detection jobs are created by using a wizard.

Bulk Delete - Bulk delete is managed in the environment's settings in the Power Platform admin center under the Data management section. Dataverse has many bulk delete jobs to clean up its own data.

Long term data retention - capability of Microsoft Dataverse that enables you to transfer your data from a Dataverse datastore to a managed data lake and securely retain unlimited data long term in a cost-efficient way. Dataverse long term data retention requires a **Managed** environment. Once data is retained as long term (inactive) data, it can't be moved back to the active data store. Set up retention policies by defining criteria for a given data table. The retained data is never moved out of Dataverse, it's stored in a Dataverse managed data lake. The data is always secured with Dataverse security backed by Microsoft Entra ID. Enable long term data retention in a table's properties in the Power Apps maker portal. Then you can create a data retention policy in the Power Apps maker portal. When creating a data retention policy, select a table, choose an existing table view, and then define the schedule as Daily, Weekly, Monthly, or Yearly. To view retained data you require organizational access level read privilege on the table.