**Environment controls and data loss prevention policies**

**Exercise 1: Create and manage environments in the Power Platform Admin center**

An environment provides storage for apps, flows, data, and various other resources. When users create an app in an environment, that app can connect to any data source, including connections, gateways, and flows. How you choose to leverage environments depends on your organization and the apps you're trying to build. For more information, see Environments overview.

You can store the app/business data in a database with Common Data Service. You can create a database with Common Data Service with any environment.

**Some important considerations when creating a new environment**

* Why create an environment with a database: When you create a production environment with a Common Data Service database, you have the option to add Dynamics 365 apps such as Dynamics 365 Sales and Field Service during the creation process (by choosing Enable Dynamics 365 apps). Currently, if you don't select Enable Dynamics 365 apps at the time of database provisioning, you will not be able to make this change later.
* Why create an environment without a database: If you don't need Dynamics 365 apps or don't need to use Common Data Service, and you are creating Power Apps or Power Automate using other data sources, create the environment without the Common Data Service database.
* The Enable Dynamics 365 apps decision is not reversible: Once you create an environment, if you don't select Enable Dynamics 365 apps at the time of database provisioning, you will not be able to make this change later.
* Dynamics 365 apps and trial environments: Currently, Dynamics 365 apps cannot be enabled for trial environments.

**Create an environment with a database**

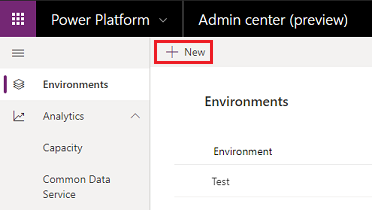
You create a database to use Common Data Service as a data store. The Common Data Service is a cloud scale database used to securely store data for business applications built on Power Apps. Common Data Service provides not just data storage, but a way to implement business logic that enforces business rules and automation against the data.

### **Prerequisites**

To create an environment with a database, you need 1GB available database capacity.

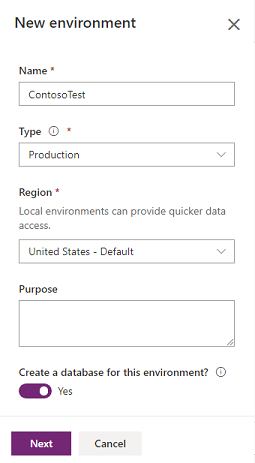
### **Steps**

1. Sign in to the Power Platform Admin center at [https://admin.powerplatform.microsoft.com](https://admin.powerplatform.microsoft.com/) as an admin (Dynamics 365 service admin, Office 365 Global admin, or Power Platform service admin).
2. In the navigation pane, select **Environments**, and then select **New**.



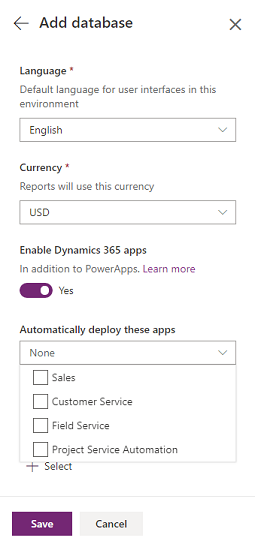
1. Enter the following, and then select **Next**.

|  |  |
| --- | --- |
| **Setting** | **Description** |
| Name | The name of your environment. |
| Type | You can choose production or trial. |
| Region | Choose a region for the environment. |
| Purpose | A description of the environment. |
| Create a database for this environment? | Select **Yes**. |



1. Enter the following, and then select **Save**.

|  |  |
| --- | --- |
| **Setting** | **Description** |
| Language | The default language for this environment. |
| Currency | The base currency used for reporting. |
| Enable Dynamics 365 apps | Select **Yes** and make a selection to automatically deploy apps such as Dynamics 365 Sales and Dynamics 365 Customer Service. |
| Deploy sample apps and data | Select **Yes** to include sample apps and data. Sample data gives you something to experiment with as you learn. You must select **No** for **Enable Dynamics 365 apps** for this setting to appear. |
| Security group | Select a security group to restrict access to this environment. |



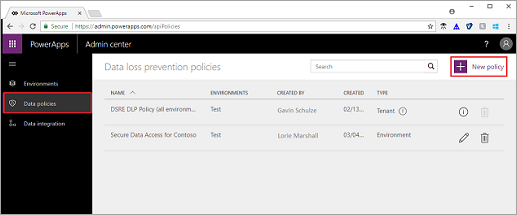
**Exercise 2: Manage data loss prevention (DLP) policies**

An organization's data is critical to its success. Its data needs to be readily available for decision-making, but it needs to be protected so that it isn't shared with audiences that shouldn't have access to it. To protect this data, Power Apps lets you create and enforce data loss prevention (DLP) policies that define which consumer connectors specific business data can be shared with. For example, an organization that uses Power Apps may not want its business data that's stored in SharePoint to be automatically published to its Twitter feed.

To create, edit, or delete DLP policies, you must have either Environment Admin or Azure Active Directory Tenant Admin permissions.

## Create a DLP policy

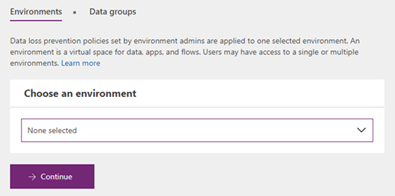
1. In the navigation pane, click or tap **Data policies**, and then click or tap **New policy**.



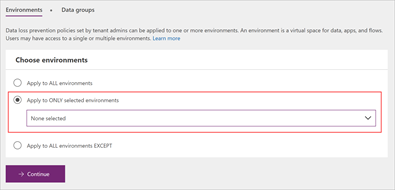
1. The **Data Policy Name** field auto-populates with a name based on the time and date the policy is created. Replace this with **Secure Data Access for Contoso**.



1. The options on the **Environments** tab differ depending on whether you're an Environment admin or a Tenant admin. If you're an Environment admin, select an environment from the drop-down list, and then click or tap **Continue**.

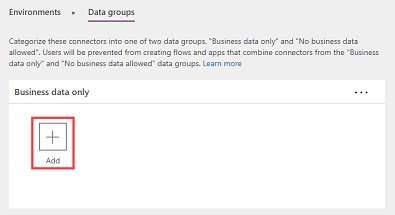


If you're a Tenant admin, you can create DLP policies that apply to one or more environments, or to all environments within the tenant (including those created using a trial license). For this topic, click or tap **Apply to ONLY selected environments**, select an environment from the drop-down list, and then click or tap **Continue**.

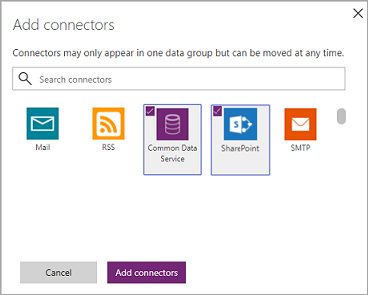


Note that environment DLP policies cannot override tenant-wide DLP policies.

1. On the **Data groups** tab, under **Business data only**, click or tap **Add**.

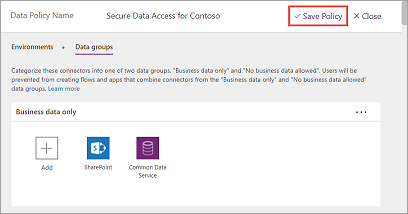


1. In the **Add connectors** window, select **Common Data Service** and **SharePoint** (you may have to scroll down or search to find them), and then click or tap **Add connectors** to add them to the **Business data only** data group.



Connectors can reside in only one data group at a time and are added to the **No business data allowed** group by default. By moving Common Data Service and SharePoint to the **Business data only** group, you're preventing users from creating flows and apps that combine these two connectors with any of the connectors in the **No business data allowed** group.

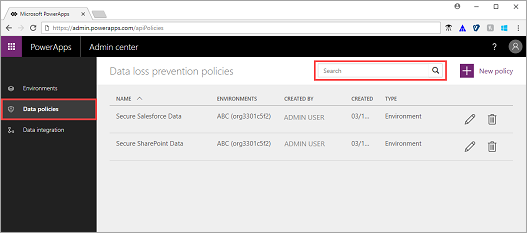
1. Click **Save policy**.



The Secure Data Access for Contoso policy is created and appears in the list of data loss prevention policies. Since the Twitter connector resides in the **No business data allowed** data group, this policy ensures that the Common Data Service and SharePoint do not share their data with Twitter.

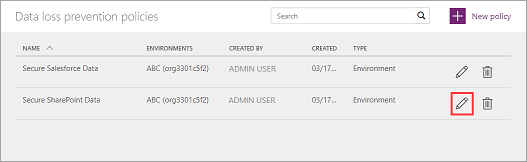
## **Find a DLP policy**

1. Sign into the Admin center at [https://admin.powerapps.com](https://admin.powerapps.com/).
2. In the navigation pane, click or tap **Data policies**. If you have a long list of policies, use the **Search** box to find specific DLP policies.



## **Edit a DLP policy**

1. In the list of data loss prevention policies, click or tap the pencil icon next to the policy you want to edit.



1. Make your changes, and then click or tap **Save Policy**.

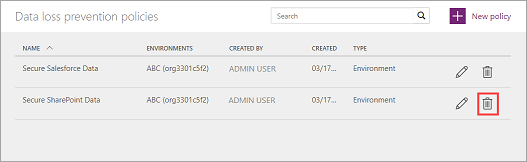
**Note**

Environment DLP policies cannot override tenant wide DLP policies.

To review the changes, find the DLP policy in the list of data loss prevention policies and click or tap it to review its properties.

## **Delete a DLP policy**

1. In the list of data loss prevention policies, click or tap the trash can icon next to the policy you want to delete.



1. In the confirmation dialog box, click or tap **Delete**.

The policy is deleted and no longer appears in the list of data loss prevention policies.