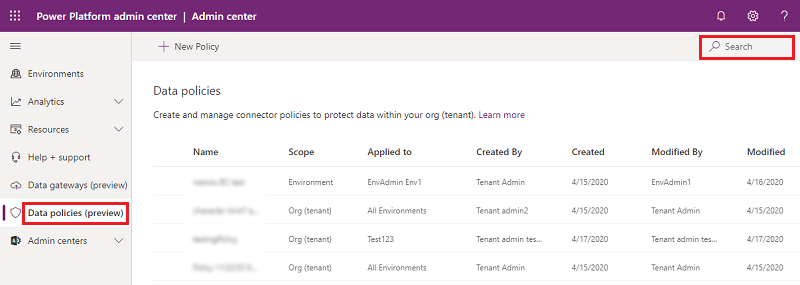
**Manage data loss prevention (DLP) policies**

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 Power Platform service admin permissions

## **Find and view DLP policies**

1. Sign into the Power Platform admin center.
2. In the navigation pane, select **Data policies**. If you have a long list of policies, use the **Search** box to find specific DLP policies.

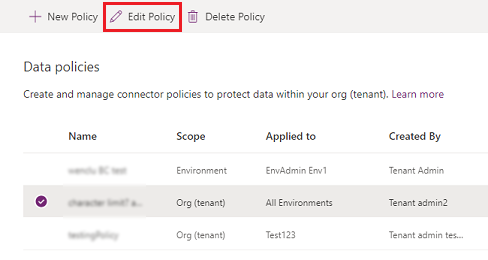


The list view shows the following attributes:

|  |  |
| --- | --- |
| **Attribute** | **Description** |
| Name | The name of the policy. |
| Scope | Type of the policy such as environment-level policy or tenant-level |
| Applied to | Environment scope associated with the policy. For an environment-level policy, this will be a specific (single) environment name associated with the policy. For a tenant-level policy, this can be one of the following values:   * + All environments   + All environments, except (n)   + (n) environments   + Single environment name |
| Created by | User who created the policy. |
| Created (On) | Date on which the policy was created. |
| Modified by | User who modified the policy. |
| Modified (On) | Date on which the policy was modified. |

## **Edit a DLP policy**

1. Sign into the Power Platform admin center.
2. In the list of data loss prevention policies, select an environment and then select **Edit Policy**. If you have a long list of policies, use the **Search** box to find specific environments.



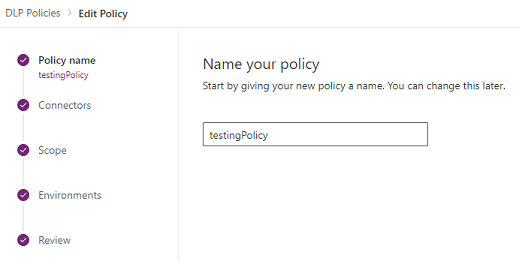
**Note**

Environment Admins can't edit environments created by the tenant admin.

1. Proceed through the Edit policy steps (see [Create a DLP policy](https://docs.microsoft.com/en-us/power-platform/admin/create-dlp-policy)), and then select **Update Policy**.

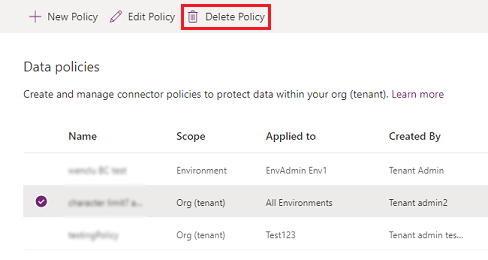
**Note**

Environment DLP policies cannot override tenant-wide DLP policies.



## **Delete a DLP policy**

1. Sign into the Power Platform admin center.
2. In the list of data loss prevention policies, select an environment and then select **Delete Policy**. If you have a long list of policies, use the **Search** box to find specific environments.



**Note**

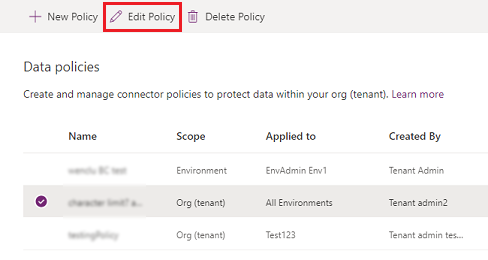
Environment Admins can't delete environments created by the tenant admin.

1. In the confirmation dialog box, select **Delete**.

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

## Change the default data group

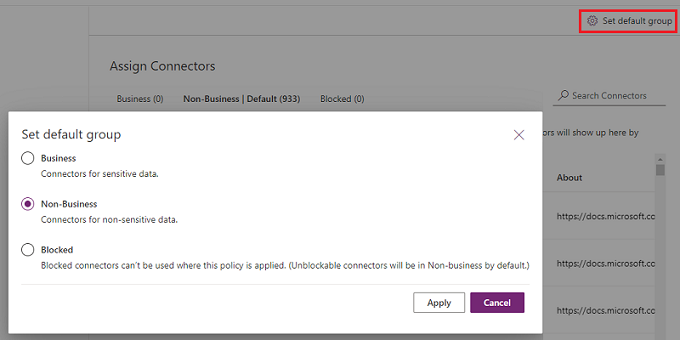
1. Sign in to the Power Platform admin center.
2. In the list of data loss prevention policies, select an environment and then select **Edit Policy**. If you have a long list of policies, use the **Search** box to find specific environments.



**Note**

Environment Admins can't edit environments created by the tenant admin.

1. Select the **Connectors** step in the **Edit Policy** process.
2. In the upper-right, select **Set default group**.



1. Choose a default group, and then select **Apply**. See [Connector classification](https://docs.microsoft.com/en-us/power-platform/admin/wp-data-loss-prevention#connector-classification) and [Default data group for new connectors](https://docs.microsoft.com/en-us/power-platform/admin/wp-data-loss-prevention#default-data-group-for-new-connectors).
2. Select **Next** as needed to close the **Edit Policy** process.

The data group you chose will be the default group to auto classify any new connectors added to Power Platform after your policy has been created.

PowerShell

<https://docs.microsoft.com/en-us/power-platform/admin/powerapps-powershell#data-loss-prevention-dlp-policy-commands>