**Lab – 17: Configure and publish the Azure Information Protection policy.**

**Objective:** The objective of this lab is –

* To configure and publish the Azure Information Protection policy.

For Azure Information Protection to work, you need to create Azure Information Protection policy as per your organization’s requirement.

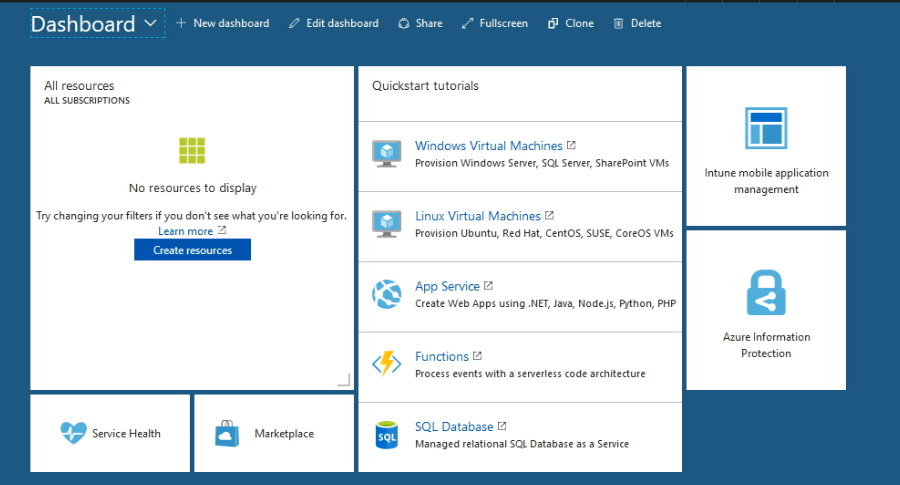
**Prerequisite:** EMS Enterprise Mobility + Security E5.

**Steps:**

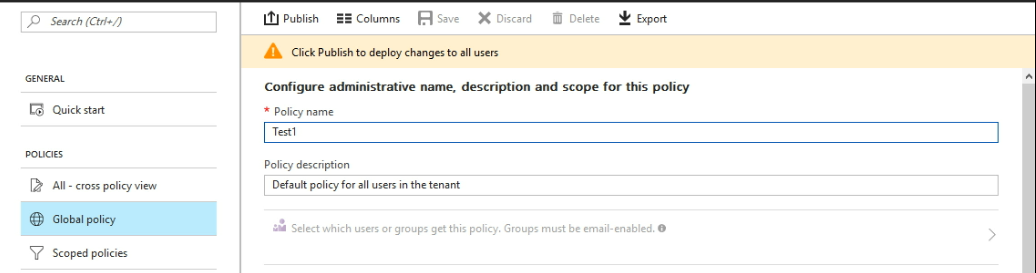
1. Sign in to your Azure Portal, by using the link - **https://portal.azure.com/**. Enter your credentials and click Sign In.



1. Microsoft Azure AD Dashboard will open.



1. Click **Azure Information Protection** from the Dashboard menu. If you are not getting this option here, then go to **New**, and then, from the **MARKETPLACE** list, select **Security + Identity.** Select **Azure Information Protection**. Then, on the Azure Information Protection blade, check **Pin to Dashboard** option and click **Create**.
2. Then in Azure Information Protection select **Global policy** to open the **Policy: Global blade**. This blade automatically opens for subsequent connections to the service and it displays the default Information Protection policy that's created for your tenant.



1. Under Configure administrative name, description and scope for this policy, you have to mention Policy Name, Policy Description.
2. Then you need to configure labels for this policy and order them by sensitivity level. Labels for classification: **Personal**, **Public**, **General**, **Confidential**, and **Highly Confidential**. The last two labels expand to show sub-labels, which provide examples of how a classification can have subcategoried.

Expand **Confidential** and check the sub-labels, **Policy** is Global and **Marking** is checked.

In the same way, Expand **Highly Confidential** and check the sub-labels, **Policy** is Global and **Marking** is checked.



1. Then you need to configure settings to display and apply on Information Protection end users.

In this we have:

Title.

Tooltip.

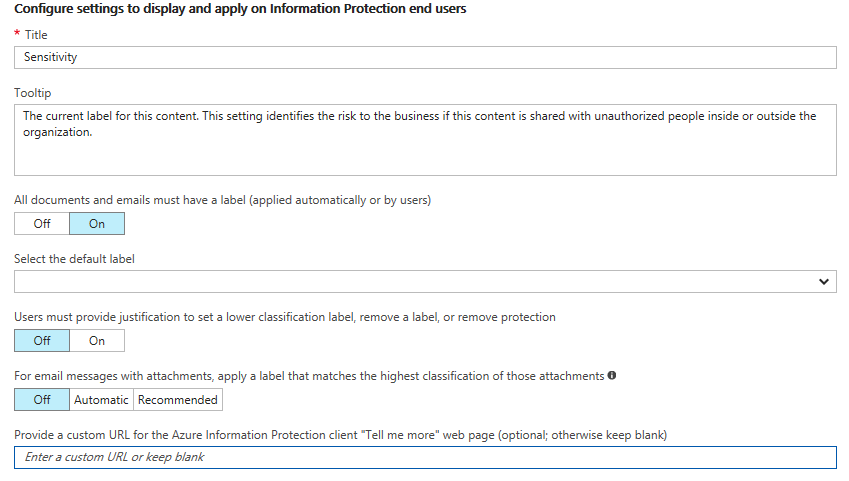
All documents and email must have a label (applied automatically or by users) : you can make it On or Off.

Select the default label.

Users must provide justification to set a lower classification label, remove a label or remove protection, it can be On or Off.

For email messages with attachments, apply a label that matches the highest classification of those attachments, it can be Off, Automatic and Recommended.

Provide a Custom URL for the Azure Information Protection client “Tell me More” web page (optional, or you can keep it blank).

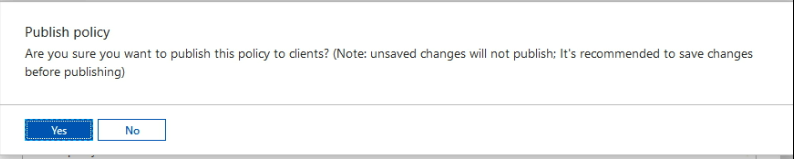


1. So, in Policy Name, type any name here Test2. Then write the description : Default policy for all users in the tenant. Then you can configure the labels as per your choice. Then here, turn Off : All documents and email must have a label (applied automatically or by users). Then select **Confidential \ All Employees** from the drop down menu of **Select the Default label**. Then ,Users must provide justification to set a lower classification label, remove a label or remove protection, Turn On or Off, as per your choice.

For email messages with attachments, apply a label that matches the highest classification of those attachments, select Off, Automatic and Recommended. And, Provide a Custom URL or keep it blank.



1. Then Click **Save**. And, click **Publish** to deploy changes to all users. A pop-up will open. If you are sure you want to publish this policy to your clients you can click **Yes**.



1. A policy was published successfully notification will open. So, in this way you can configure and publish the Azure Information Protection policy for your organization.