

Data Loss Prevention for Endpoint

1. On the Introductory Screen select the **Next** navigation button to begin the demonstration
2. Under **Admin Centers** select **Compliance**
3. Under **Solutions** select **Data Loss Prevention**
4. To the right of **overview** select **Policies**, then select **Create Policy**
5. Under **Categories** select **Financial** then select **PCI Data Security Standard (PCI DSS)**
6. The name and description of the policy template will appear, click on **Next** to continue
7. Turn on **Devices preview** by clicking on the off button to the left of **Devices(Preview)**
8. Click on **Next** to continue.
9. Click on **Edit** under **Credit Card Number** to edit the credit card number sensitivity info type
10. Under **Credit Card Number** click on **Add** to show that you can add other sensitive info types or labels. Click on **Next** to continue
11. On the protection Action page take a look at the settings then click on **Customize alert Configurations**

See Settings on the Action Page below

Protection actions

We'll automatically create detailed activity reports so you can review the content that matches this policy. What else do you want to do?

- Detect when a specific amount of sensitive info is being shared at one time**
At least or more instances of the same sensitive info type
- Send incident reports in email**
By default, you and your global admin will automatically receive the email. Incident reports are supported only for activity in Exchange, SharePoint, OneDrive, and Teams.
[Choose what to include in the report and who receives it](#)
- Send alerts if any of the DLP rules match**
By default, you and any global admins will automatically be alerted in email if a DLP rule is matched.
[Customize alert configuration](#) 
- Restrict access or encrypt the content in Microsoft 365 locations**

12. Read the Alert settings then click on **Save**. Close the Alert window.

Alert settings

Send alert every time an activity matches the rule

Send alert when the volume of matched activities reaches a threshold (applies only to activities on endpoint devices)

instances more than or equal to 5 matched activities

volumes more than or equal to 1 mb

during the last 60 minutes

13. On the Customize Access and override settings page, select **Audit only** for **Copy to a usb removable media**. You will see two options, **block, blocked with override**

- Upload to cloud services or access by unallowed browsers
- Copy to clipboard
- Copy to usb removable media
- Copy to network share
- Access by unallowed apps
- Print

14. Click on **Next** to Continue

15. On this screen I have set all of the actions to **block with override** except the first option which is set to **block**. Click on **Next** to continue

16. On the **Test or turn on the policy** screen click on **Next**.

17. Review the policy settings then click on **Submit**. Click on **Done**.