



# Microsoft Defender Advanced Threat Protection

## Tutorial

Automated data classification

March 2019

## Copyright

This document is provided "as-is." Information and views expressed in this document, including URL and other internet website references, may change without notice.

Some examples depicted herein are provided for illustration only and are fictitious. No real association or connection is intended or should be inferred.

This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.

© 2019 Microsoft. All rights reserved.

Please refer to [Microsoft Trademarks](#) for a list of trademarked products.

All other trademarks are property of their respective owners.



## Introduction: AIP integration & data classification

---

Microsoft Defender ATP integrates with Azure Information Protection (AIP) enabling discovery, automated classification and protection of sensitive data stored on customers devices.

This scenario provides step-by-step instructions to run on your selected test machine to store, classify, and gain visibility on sensitive data stored on devices so you can explore and understand how Microsoft Defender ATP enables sensitive data classification.

### The test machine required for this simulation must:

- Onboard to Microsoft Defender ATP
- Manage [sensitivity labels](#) in [Office 365 Security & Compliance Center \(SCC\)](#)
  - Note: If you're using AIP to manage sensitivity labels please follow the [label migration process](#)
- Run the latest [Windows Insider build](#)
- Optional
  - Onboard to [AIP analytics preview](#)
  - [Enable AIP integration](#) in Microsoft Defender Security Center

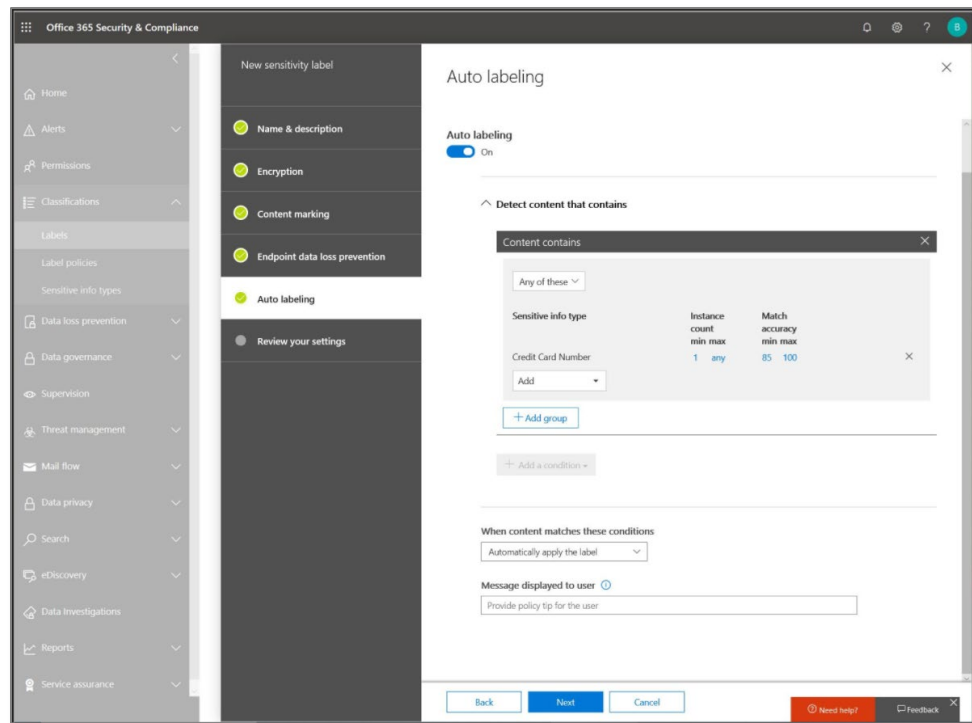
For onboarding instructions, [read to the product guide](#). We recommend running the local onboarding script to onboard the test machine.

## Run the simulation

---

### Configure classification and protection policy in Office 365 Security & Compliance Center

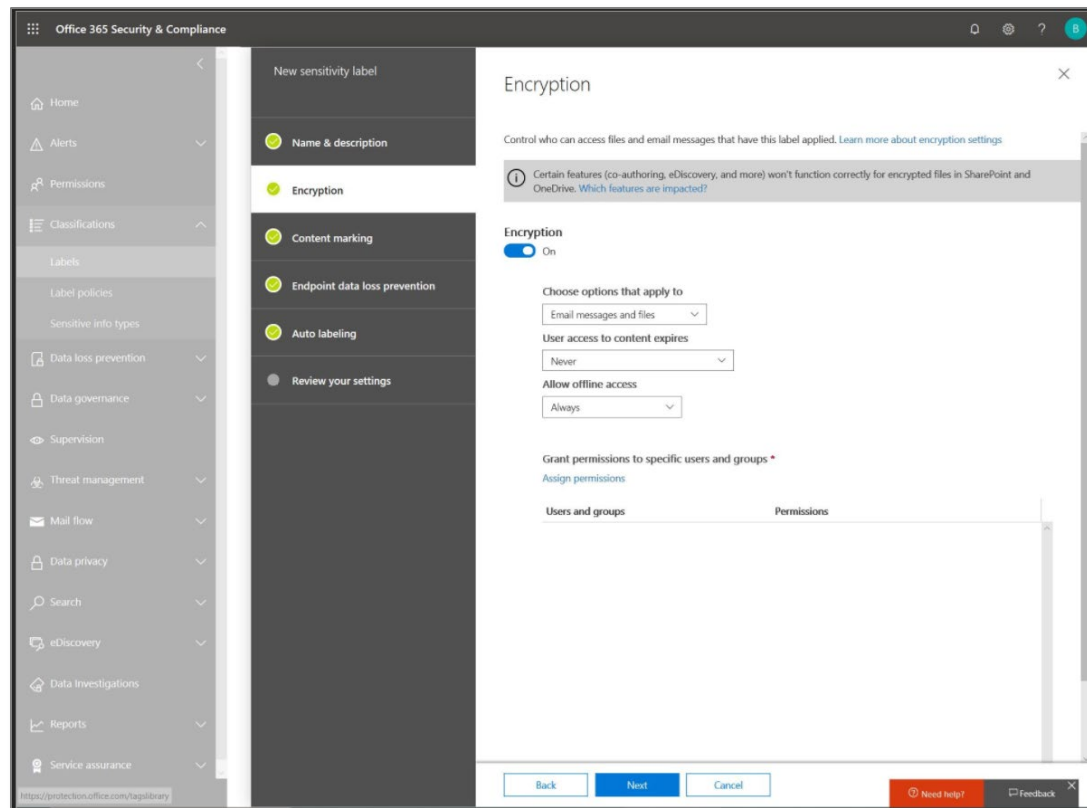
1. Create a new or select an existing sensitive info type label.  
NOTE: We recommend that you create a new label to avoid impacting existing labels or policies.
2. Click on **Edit label** to open the label settings.
3. Set a policy for Data classification.
  - a. Go to *'Auto labeling'*
  - b. Skip the Wizard steps until you reach the Auto labeling page.
  - c. In the Auto labeling page, Switch *'Auto labeling'* on.
  - d. Add a new auto-labeling rule that matches a *'Credit Card Number'* with a minimum instance count of **1**.
  - e. Validate that *'When content matches these conditions'* setting is set to *'Automatically apply the label'*



*Auto labeling page in the security & compliance center*

#### 4. (Optional) Set an 'Endpoint Protection Policy'.

- a. [Microsoft Defender ATP integrates with WIP](#), using this integration customers can protect sensitive data based on labels.
- b. To enable protection, go to 'Endpoint data loss prevention' and switch it **on**



*Endpoint protection policy in the security & compliance center*

## Create simulation sensitive data on test devices

1. On the test device/s that's onboarded to Microsoft Defender ATP, copy the attached 'DLP\_Test\_Sensitive\_File" test file.

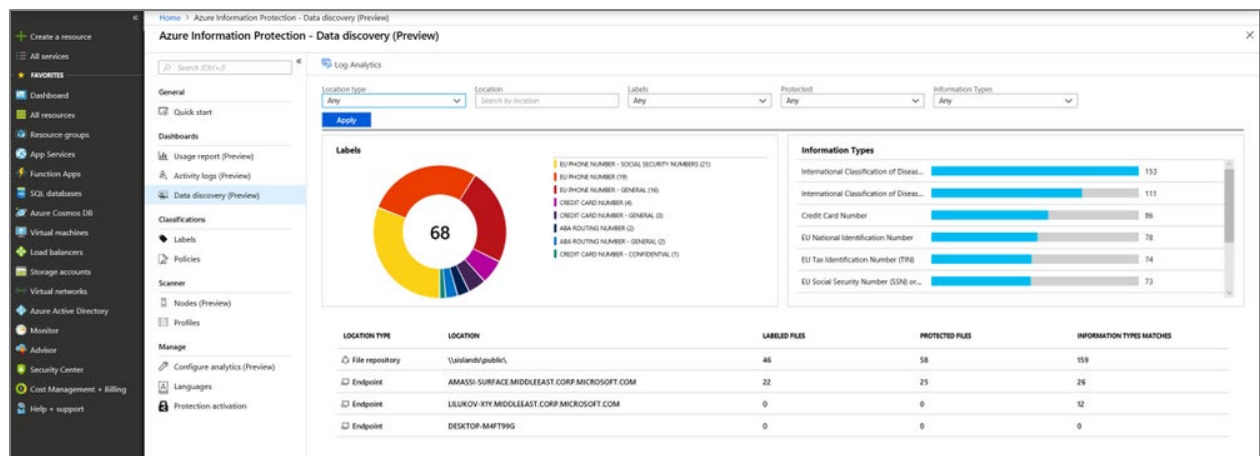


DLP\_Test\_SensitiveFile.csv

2. Microsoft Defender ATP will automatically detect the files containing sensitive data based on the classification policy created in the previous step.

## Discover files automatically classified on devices

1. Open [AIP Data Discovery dashboard](#).



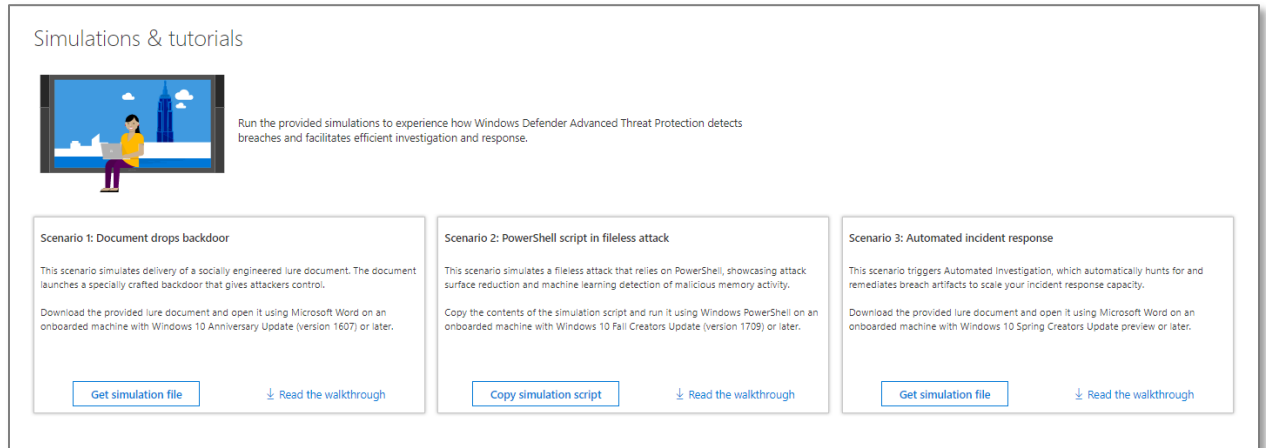
2. See the discovery report.
  - a. On the data discovery tab , find the test device that was used in the previous scenario
  - b. Click on the device , and view a list of files observed on this device, with their sensitivity labels and information types

*Note: Please allow approximately 15-20 minutes for the AIP Dashboard Discovery to show the file you created.*

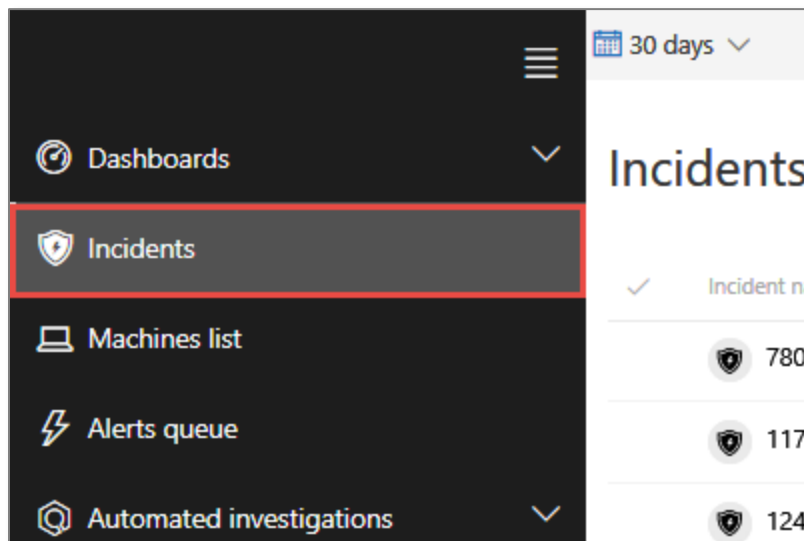


## Use sensitivity labels to prioritize & investigate security incidents

1. Log in to the Microsoft Defender ATP portal and go to **Help (?) > Simulations & tutorials**.



2. Run one of the attack simulation scenarios (Scenarios 1-3) on the test devices used for the automated classification simulation.
3. After 15-30 minutes of the simulated attack, you should find new incidents in the Microsoft Defender Security Center dashboard.
4. Open the the incidents queue.




5. Scroll to the right and observe a new 'Data Sensitivity' column.

Classification	Status	Data sensitivity ⓘ
Not set	Active	
Not set	Active	Highly Confidential
Not set	Active	
Not set	Active	
Not set	Active	
Not set	Active	Highly Confidential

This column reflects sensitivity labels that have been observed on machines related to the incidents providing SecOps with an indication of whether sensitive files may be impacted by the incident as they prioritize incident investigation & response issues.

6. Open the incident page to further investigate. Note that the data sensitive attribution carries over into the incident page.



Incidents > 69837


  
69837
  
Data sensitivity: Highly Confidential

Status  
Active

Assigned to  
Unassigned

7. Click on the machines tab to identify machine storing files with sensitivity labels.





Alerts	Machines	Investigations (0)	Evidence	Graph	beta
Customize columns 30 items per page 1-19					
Machine name	Risk level	Related alerts	First activity	Last activity	Data sensitivity
 [redacted]	Low	1 / 1	12/23/18, 1:18 PM	2/24/19, 7:30 AM	Confidential
 [redacted]	Low	1 / 1	12/23/18, 12:12 PM	2/11/19, 4:55 AM	Highly Confidential

- Click on the machines that store sensitive data and search through the timeline to identify which files may be impacted.

30 days

confidential

Customize columns

Event time	Event	Behaviors	User
Mar 31, 2019, 2:47:57.740 ...	 OUTLOOK.EXE created file [redacted]	Highly Confidential...	 [redacted]
Mar 29, 2019, 11:22:39.83...	 OUTLOOK.EXE created file [redacted]	Highly Confidential...	 [redacted]

Note: The event side pane now provides additional insight to the WIP and AIP protection status.

OUTLOOK.EXE created file Feb 27 - [REDACTED]

**Event info**

Event	OUTLOOK.EXE created file Feb 27 [REDACTED]
Event time	Mar 10, 2019, 1:00:21.834 PM
Action type	FileCreated
Behaviors	Confidential \ Any User (No Protection)
User	[REDACTED]
Entities	explorer.exe > OUTLOOK.EXE > [REDACTED]

**Event entities graph**

explorer.exe

OUTLOOK.EXE

Process name	OUTLOOK.EXE
Execution time	Mar 5, 2019, 9:54:04.995 AM
Path	c:\program files (x86)\microsoft office\root\office16\outlook.exe
Integrity level	Medium
Access privileges (UAC)	Restricted
Process ID	14960
Command line	"OUTLOOK.EXE" /restore
SHA1	14b2a7891d40abaf9b09feb2008d35069b1f5783

**created file**

Feb 27 - NHS bi-weekly status (002).pptx

File name	[REDACTED]
Folder path	C:\Users\[REDACTED]\Local\Microsoft\Windows\NetCache\Content.Outlook\LUUQAEMX
SHA1	f1464fe4de9dd874d93f9473595065f53e274ea4
SHA256	78d774515fe63dcb552719e590f76c9c1824e561be8e205c4
Data sensitivity	Confidential \ Any User (No Protection)
WIP Protected	No
AIP Protected	No

- These data points are also exposed through the 'FileCreationEvents' in advanced hunting, allowing advanced queries and schedule detection to take into account sensitivity labels and file protection status.

ReportId
AppGuardContainerId
SensitivityLabel
SensitivitySubLabel
IsWindowsInfoProtectionApplied
IsAzureInfoProtectionApplied

## Conclusion

---

We've simulated how to use AIP labels and auto classification in order to automatically classify sensitive data stored on devices, and walked through how compliance officers can view the information via AIP discovery, and how security analysts can utilize this information to better prioritize and respond to security incidents.

We hope you enjoyed this simulation and are now encouraged to explore other features and capabilities. For more information, [read the product guide at docs.microsoft.com](https://docs.microsoft.com).

Click the feedback icon on the Microsoft Defender ATP portal to let us know how you feel about this simulation or any other aspects of the product. We would love to hear your ideas about additional simulations and tutorials. Thank you!