

Summary

Overview: With more and more information stored in the cloud, the ability to discover, analyze, and respond to requests for that data is more important than ever. Whether it is litigation, internal investigation, responding to a regulatory request, or policy obligation – you need to be able to find relevant content, refine that content, and prepare that content to be handed off to the requesting body in an efficient and effective way.

That's why Microsoft has added Advanced eDiscovery to the Compliance Center—to help companies quickly find relevant emails and information across large quantities of stored email and document content.

Lab steps

Compliance Center: Case Creation

What is it	Where is it and what to do
<p>The need for organizational discovery or search of electronic content, also referred to as eDiscovery is becoming more and more prevalent.</p> <p>Some eDiscovery activities may be related to legal activities; others may be as a security investigation into an employee leaking or stealing sensitive information.</p> <p>There are also a growing number of privacy related regulations related to legal compliance, such as the EU's General Data Protection Regulations (GDPR), that give individuals the right to request the information held on them. This can be a monumental task if you don't have a solution in place.</p> <p>Advanced eDiscovery in Microsoft 365 provides an effective way to manage information requests whether it is litigation, internal investigations, responding to a regulatory request or policy obligation. With Advanced eDiscovery, you can create a case, add case members, put custodians on hold, send hold notifications, cull and review content and finally export only the most relevant content when needed.</p> <p>Let's walk through the steps of creating and managing a case using the Microsoft 365 Compliance Center.</p> <p>The first step is creating a new case.</p>	<p>Navigate to https://compliance.microsoft.com/ logged in as the administrator of your given lab tenant.</p> <p>Login with the credentials you have been provided for your lab tenant</p> <ol style="list-style-type: none">1. In the left navigation pane of the Microsoft 365 compliance center, click Show all..., then click eDiscovery, then select Advanced. <p>Create a new Case</p> <ol style="list-style-type: none">2. On the Advanced eDiscovery Overview page Click on the Cases tab3. Click +Create a case4. On the New eDiscovery Case page create a new eDiscovery case as follows (Note: if this case name might already exist alter the name of this case so it is unique):<ul style="list-style-type: none">• Case name: Investigation – 0123(xx)• Case number: 01234(xx)

What is it	Where is it and what to do
	<ul style="list-style-type: none"> Do you want to configure additional settings after creating this case? No, just go to the home page. I'll use the default case settings for now New case format. <p>5. Click Save.</p>
<p>When the number of collected documents is large, it can be difficult to review them all. Advanced eDiscovery provides several tools to analyze the documents to reduce the volume of documents to be reviewed without any loss in information, and to help you organize the documents in a coherent manner.</p> <p>Now that we have created the case, we will configure case settings based on the type of case it is and the complexity expected.</p> <p>The Settings tab is used to configure search analytics within the case level. It includes settings like:</p> <p>"Near duplicates / email threading", which helps to identify duplicates and group them in your review set.</p> <p>"Themes", which helps by clustering results in a review set around themes identified in the review of the text in the document. eDiscovery users can update the document and email similarity thresholds and the maximum number of themes in Advanced eDiscovery.</p> <p>Now that we have adjusted those settings, let's look how to use custodian management and communications to help manage the eDiscovery workflow.</p>	<p><i>Settings – Analytics settings and / or basic information</i></p> <p>6. On the Investigation - 01234 page, click the Settings tab.</p> <p>7. In the Search & analytics section, click Select.</p> <p>8. Review the settings for Search & Analytics.</p> <p>9. Change the following settings:</p> <ul style="list-style-type: none"> Ensure both the Near duplicates/email threading and the Themes boxes are checked Document and email similarity threshold 70% Maximum number of themes: 10 <ol style="list-style-type: none"> Click Save. <p>10. Click Exit</p>

Custodian Management & Communications

What is it	Where is it and what to do
<p>Using custodian management and communications you can manage the eDiscovery workflow around identifying, collecting, and preserving potentially relevant information.</p> <p>The first step is to add custodians, or non-custodian data, to the case. ("Custodians" are the individuals who have administrative control of a document or electronic file that may be relevant to your eDiscovery case.)</p> <p>A workflow will guide you through the process adding custodians to the case, configure the data sources associated with the person that are important to monitor and place a hold on the custodians.</p> <p>Let's review how this is done...</p> <p>Not only can you choose the custodial locations such as Nestor's email inbox and OneDrive for Business, but you can also quickly locate the shared locations Nestor has access to, such as Teams or Sites.</p> <p>For example, if Nestor was part of a Business Development team you could add that shared location to this case to capture that Teams content for review.</p>	<p>Add Custodians to a Case</p> <ol style="list-style-type: none">11. Click the Data sources tab.12. On the Data sources page, click Add data source and select Add new custodians13. On the Select custodian page, add the following users to the case:<ul style="list-style-type: none">• Nestor Wilke• Isaiah Langer• Christie Cline14. Click Next15. On the Hold settings page, verify Hold is selected for the custodians, and then click Next.16. On the Review your custodians step, click Submit17. Click Done

What is it	Where is it and what to do
<p>Organizations are often required to inform custodians that they are on legal hold and need to be able to track when the custodians have been notified about the legal hold. Organizations can now manage their legal workflow around custodian communications from within Advanced eDiscovery in the Compliance Center.</p> <p>Admins can send, collect, and track legal hold notifications. You can customize the hold notification workflows and content to meet your organization's needs.</p> <p>You can use templates to build out commonly used communications, escalate with reminders and manage notifications. While creating these notifications, you can add links to ensure that custodians acknowledge receiving this information.</p> <p>A rich text editor is provided to create the Hold Notice and variables are available that can be used to create the notice.</p> <p>The admin can define settings for notifications for a new issuance, re-issue or release of hold communications and define the content within the hold as well as utilize common variables such as display name, acknowledgement link and more.</p>	<p>Create and send hold notification</p> <ol style="list-style-type: none"> 18. Click the Communications tab and select + New Communication. 19. On the Name Communication step enter Hold Notification under Name 20. Select the tenant admin user from the Issuing officer dropdown 21. Click Next. <p>Note: All custodial notifications will be sent on behalf of the Issuing Officer.</p> <ol style="list-style-type: none"> 22. Create the Hold Notice by using the rich-text editor and merge fields. There is sample Hold Notice content you can copy and paste at the end of this document in the Portal Content section. 23. In the text editor at the bottom of the sample letter, highlight the line Replace with ACKNOWLEDGEMENT LINK and click the Acknowledgement Link button to insert the merge field. 24. Click Next. 25. On the Set Notifications – Required page, click the Edit button next to the Issuance notification and enter the following information and <ul style="list-style-type: none"> Subject: Issuance of Hold Notification Body:

What is it	Where is it and what to do
	<p>TO: {{DisplayName}}</p> <p>This is the issuance of the hold notification. The hold notification is attached.</p> <p>{{IssuingOfficerEmail}}</p> <p>26. Click Save</p> <p>27. Click the Edit button next to the Reissue notification</p> <p>Subject: Reissue of Hold Notification</p> <p>Body:</p> <p>TO: {{DisplayName}}</p> <p>This is the reissue of the hold notification. The hold notification is attached.</p> <p>{{IssuingOfficerEmail}}</p> <p>28. Click Save</p> <p>29. Click the Edit button next to the Release notification</p> <p>Subject: Release of Hold Notification</p> <p>Body:</p> <p>TO: {{DisplayName}}</p> <p>This is the reissue of the hold notification. The hold notification is attached.</p> <p>{{IssuingOfficerEmail}}</p> <p>30. Click Save.</p> <p>31. After the required set notifications are created, click Next.</p> <p>32. On the Set Notifications – Optional page, click Next.</p>


What is it	Where is it and what to do
	<p>33. On the Choose the custodians you want to notify page, click + Select custodians</p> <p>34. On the Select custodians flyout menu, check the box next to each custodian and click Add</p> <p>35. On the Choose the custodians you want to notify page, click Next</p> <p>36. On the Review your settings page, verify the settings and click Submit</p> <p>37. Click Done</p> <p>38. In the left navigation menu under eDiscovery click on Advanced to return to the Advanced eDiscovery overview</p>
<p>Using the Data sources tab, users can view a custodian's activity. This can be used to search and identify a custodian's activity over time. Let's review a case that was created.</p> <p>This custodial activity view helps you understand a bit more about the custodian in the case and their activities. This view helps search the Office 365 audit log for activities during certain timeframes as related to email, groups, documents, permissions, directory services, and more.</p>	<p><i>View custodian audit activity</i></p> <p>39. On the Advanced eDiscovery page, On your Investigation – xxxx</p> <p>40. On Investigation – xxxx page, click the Data Sources tab</p> <p>41. Select Nestor Wilke</p> <p>42. On the Nestor Wilke details page, Click View activity</p> <p>43. Specify a date range and select Search to view recent custodian activity data (this lab might not have any relevant info at the moment, if blank skip to 44.)</p> <p>44. Click the X in the upper right corner to close the View Activity page.</p> <p>45. Click the X in the upper right corner to close Nestor Wilke detail page</p>



Searches

What is it	Where is it and what to do
<p>After creating the case and adding the custodian data sources, the next step is to search for relevant content to start to build out case related content.</p> <p>Let's look at an example of how you can quickly do this by creating a new collection.</p> <p>First you will name the collection you want to build.</p> <p>Next, you will define the search criteria by adding conditions. Conditions are granular parameters such as dates, authors or even email recipients.</p> <p>You can also add related custodians to the search, and additional shared data locations if necessary.</p> <p>If we wanted to create this review set, we could review the details before completing the process, but for this lab we will just click Cancel to discard the review set.</p> <p>A review set helps improve performance and stability of working with your content after you have validated the initial search results.</p>	<p>Create a Collection</p> <p>46. On the Investigation - xxxx page, click the Collections tab, then click + New collection</p> <p>47. On the Name and description page, in the Name field, type Search for Dummy Data and click Next</p> <p>48. On the Choose custodial data source page, click the Select all switch to turn it on</p> <p>49. Click Next</p> <p>50. On the Choose non-custodial data sources step, click Next</p> <p>51. On the Additional locations step, click Next</p> <p>52. Under Define your collection conditions click Add condition as follows:</p> <ul style="list-style-type: none"> Size (in bytes): Greater than > 1 <p>53. Click Next.</p> <p>54. Check the box next to Collect items and add to review set</p> <p>55. Ensure that Add to new review set is selected</p> <p>56. Under Review set name, type Dummy Data</p> <p>57. Click Next</p> <p>58.in the bottom right corner of the screen click Cancel</p> <p>59. Click Yes</p>


What is it	Where is it and what to do
<p>With the review set, organizations can take an early pass at reducing content with queries and conditions, reviewing content in place, and tagging content with a customizable coding panel.</p>	
<p>After creating a collection, you can use Search Statistics and Review options to verify the search you created is collecting the type of data you need. Let's look at the Search for Custodian Data collection that was created earlier to review some of its collection results.</p> <p>Statistics can provide a quick view of collection estimates showing the estimated items by each location, the estimated number of hits per location and the data volume by location. You are able to download a condition report and review a list of top locations in the collection.</p> <p>You can also review a sample of the content collected. If your search returns more than million records, sampling will show a preview of the content collected.</p>	<p><i>Preview results and search stats</i></p> <p>60. On the Investigation - Lighthouse page, on the Collections tab, select the Search for Dummy data collection and then click Search Statistics</p> <p>61. On the Search Statistics page, on the drop-down list, expand the Collection Estimates, Condition report, and Top locations</p> <p>62. To review a sampled set of results, click Review Sample</p> <p>63. Click on one of the items to see the source of the data sample and what it contains.</p> <p>64. Click the X in the upper right corner</p> <p>65. Click Close</p>

Working Set Management

What is it	Where is it and what to do
<p>We can start creating a review set before the Collection has been created. Before a collection can be added to a review set, the following will occur:</p> <ul style="list-style-type: none"> • Advanced eDiscovery is going to collect all the content from your search results, • It will process all that content by extracting the metadata, • The results will be placed in a centralized index. • These results can then be searched through one interface <p>If you want to add data from a source other than Microsoft 365 into your search, a process is provided to add that data after you complete your initial search.</p> <p>A review set has already been created for this lab, so we will click cancel here.</p>	<p>Create a Review set</p> <p>66. On the Investigation - Lighthouse page, click the Review Sets tab</p> <p>67. Click + Add review set</p> <p>68. On the New review set page, under Name, enter Additional Custodial Data, and click Cancel</p>
<p>As part of the working set, you can configure a customizable tagging panel for early review activities, including custom tags for further triage of the data included in the working set.</p> <p>This helps reviewers with early classification and culling of data to get to only the most responsive and relevant set of data.</p> <p>After they are not needed any longer, tags can also be easily deleted to keep the tag list focused. When a tag is deleted, it is</p>	<p>Review tag panel</p> <p>69. Click the Search for Dummy Data review set</p> <p>70. On the Dummy Data page, click the Manage drop down</p> <p></p> <p>71. Click Tags</p> <p>72. Hover over the Preview section to draw attention to the different types of tags available</p> <p>73. Click + Add Section</p>

What is it	Where is it and what to do
<p>also removed from all documents that have been tagged. We will now proceed to delete this tag.</p>	<p>74. In the Enter section title type Demo Tag</p> <p>75. Click Save</p> <p>76. Click on the vertical ellipses </p> <p>77. Hover over but do not select the Add option button and the Add check box</p> <p>78. In the Enter selection label box, type This is for a demo</p> <p>79. Click on the vertical ellipses next to Demo tag and click Delete</p> <p>80. Click Yes, delete this option</p> <p>81. Click Close</p>
<p>In many cases, organizations will need to include data from sources other than Office 365. To do that, Advanced eDiscovery provides a process for uploading that content.</p> <p>You can quickly create a container for non-Office 365 data and upload data into that container for inclusion in the case.</p>	<p>Load non-Office 365 data</p> <p>82. On the Dummy Data page, under Manage drop-down , in the Non-Office 365 data box, click View uploads.</p> <p>83. On the Non-Office 365 data page, click Upload files.</p> <p>84. Click Next: Upload files.</p> <p>85. On the Upload files page, verify the path to the non-Office 365 files and the path to azcopy.exe, this is where we could Copy to clipboard and use the tools to upload a copy of the data to the review set.</p> <p>86. As we don't have any information in the lab to upload, lets click Cancel for now.</p>

Review and Tagging

What is it	Where is it and what to do
<p>You can analyze, review, and organize the content within a review set. You will run analysis first to minimize the number of documents you need to review, and query within a working set to find the set of documents you want to review.</p> <p>Hopefully, the analytics has already been run for you, so you can view the reports within the review set.</p> <p>After running the document and email analytics for this review set, we can see the detailed graphs that help us visualize the data under review. On the Analytics page, you will be able to view metrics on the types and sources of documents contained in the review set</p>	<p>Run eDiscovery analytics</p> <p>87. Click the Analytics dropdown </p> <p>88. Click Show reports and review the report</p> <p>NOTE: If presented with “This working set is being analyzed; please check back when the analysis is complete. Please click the refresh button to check its latest state” click Refresh.</p> <p>89. When finished reviewing the report, click the X in the upper right-hand corner of the screen</p>
<p>The review experience includes a native, text and annotate view to provide options to support the various ways your team assess content.</p> <p>You can view the content in a viewer in the document’s native format. While viewing the document, you can redact content, allowing you to export the content with some of the information redacted.</p>	<p>Annotate a document</p> <p>90. In the Search for Dummy Data review set list, click on an email</p> <p>NOTE: Not all content will be viewable. If presented with “Sorry! File not supported. You can download the file and process it offline” select another item from the content list.</p> <p>91. In the native view window, click Annotate</p> <p>92. Click the Drawing drop-down menu, then click Area redaction</p>

What is it	Where is it and what to do
	<p>93. Click, then drag the mouse over a few sentences to create a selection area</p> <p>NOTE: The redaction will automatically fill the selected area.</p> <p>94. To the right of the Drawing drop-down menu, click the square Toggle Annotation Transparency icon, to view the redacted content</p>

Jobs

What is it	Where is it and what to do
Any process in Advanced eDiscovery that takes more than a few seconds is created as a job. The Jobs tab tracks the status of jobs that are running or have been completed.	<p>Overview of jobs</p> <p>95. On the Investigation – Lighthouse page, click the Jobs tab.</p> <p>96. Click the Filter button to display which filters are selected</p> <p>97. Click Cancel</p> <p>98. On the Jobs page, under the Type column, click on an item to expose its details pane</p> <p>99. In the details pane point to Job type, Job status, and Progress</p> <p>100. At top right, click the icon to close the panel</p>

Errors

What is it	Where is it and what to do
<p>Sometimes, Office 365 services are unable to fully index a file. A common example of this is when a file is password protected. Error remediation allows you to fix errors and add the corrected files back into the system so the files can be processed as if the problem never occurred. In some cases, it's not necessary to remediate errors but it's important to simply report the errors that were encountered.</p> <p>The errors tab lists all errors that were encountered and further breaks down the errors by file count and includes the number of items and the size.</p> <p>Because creating a new error remediation takes some time, we are not going to complete that step during this demo and will now cancel this wizard.</p>	<p>Error reporting</p> <p>101. On the Investigation - Lighthouse page, click the Processing tab</p> <p>102. Click the View drop-down, and then click Errors</p> <p>103. Click the Scope drop-down, and then click Custodial Data</p> <p>104. Click the box next to the left of File is protected to select it, then click + New error remediation</p> <p>NOTE: Preparation may take a few minutes.</p> <p>105. Review the remediation steps in the New remediation wizard, click Cancel, and then click Yes</p>

Export

What is it	Where is it and what to do
<p>In some cases, a lawyer or another third party may just need to download a few documents from a case for a specific deposition which can be facilitated using the download option.</p>	<p>Download query results</p> <p>106. On the Investigation - Lighthouse page, click the Review Sets tab, and then click on the Custodial Data review set.</p> <p>107. In the Review Set, select multiple documents by clicking the single select radio button to the left of the document.</p>

What is it	Where is it and what to do
	108. Click the Actions drop-down menu, then click Download to download these items to your local downloads folder
For bigger volumes, you can use the export option. You have several options for how to export the content, choose the one that makes the most sense in your context and export the relevant content to enable the next steps of your process.	<p><i>Export query results to Microsoft provided Azure Blob</i></p> <p>109. On the Saved filter queries, click on one of the queries.</p> <p>110. Select multiple emails and/or documents by clicking the single select radio button to the left of the document.</p> <p>111. Click Action (right arrow icon) and click Export.</p> <p>112. Complete Export Options as follows:</p> <ul style="list-style-type: none"> • Export Name: Custodial Data Export • Export These Documents: Selected documents only • Output options: Condensed directory structure <p>113. Click Export.</p> <p>114. In the A job has been created! dialog, click OK</p>

Conclusion

What is it	Where is it and what to do
<p>DEMO CONCLUSION</p> <p>As you can see, Microsoft Advanced eDiscovery enables companies to quickly find relevant emails and information across large quantities of stored email and document content. Even if stored in the cloud, Advanced eDiscovery streamlines discovery and analysis processes, allowing organizations to respond to requests in a timely manner. Whether it is litigation, internal investigation, responding to a regulatory request or policy obligation – you'll be able to find relevant content, refine</p>	No Click steps

What is it	Where is it and what to do
that content, and prepare that content to be handed off to the requesting body in an efficient and effective way.	

Portal Content

You can copy the letter as follows and update the fields for the hold notice on the portal content:

Hold Order
Confidential

To: {{DisplayName}}

From: Office of General Counsel

Date: {{IssuingDate}}

The company has received a subpoena from SEC which will require the collection and production of certain company documents in connection with an investigation of insider trading. We intend to comply fully with the subpoena and to cooperate with the SEC investigation. A description of the documents covered by the subpoena is attached.

To fully comply with the SEC subpoena, it is vital that all documents described in the attachment (including hard copy documents as well as electronic data and documents) be preserved, and all routine destruction or discarding of any such documents or data, whether pursuant to formal company policies or otherwise, be suspended until further notice. This includes turning off any "autodelete" functions and ensuring that back-up tapes are preserved and not overwritten or deleted. If you have a question about whether something needs to be preserved, err on the side of preserving it until advised otherwise by legal counsel.

This policy applies to all such documents whether kept at the office, at off-site storage facilities, or at your home. It includes not only formal company documents, but also materials such as handwritten notes, drafts, calendars, and the like. In addition, if anyone under your supervision has custody or control of such documents or data and it is not listed as a recipient of this memorandum, please forward it to them immediately. If you know of others who should receive this memorandum, or if you know of documents beyond our control that should be preserved, please notify {{IssuingOfficerEmail}} immediately.

Detailed instructions regarding the procedures for collection of documents will follow shortly and will be designed to minimize disruption of your daily business activities. Until such instructions are provided, all documents and files should be maintained as they are kept in the ordinary course of business.

The subpoena should not be discussed outside of any discussions necessary for document preservation and compliance, or in communications with company counsel. There should be no discussions with third parties.

We require that you acknowledge this notice by clicking the link below.

Replace with ACKNOWLEDGEMENT LINK

If you have any questions concerning this notice, please contact {{IssuingOfficerEmail}}

