



Australian Government
Digital Transformation Agency

Litigation Hold - Standard Operating Procedure

March 2020

Contents

Document Overview	4
Background	4
Document Audience.....	4
Purpose	4
Prerequisites	4
Associated Documentation	5
Litigation Hold	5
PowerShell Litigation Hold	6
Web Interface Litigation Hold.....	7
Assign eDiscovery Permissions	8
Create eDiscovery Case	10
Manage eDiscovery Case	11
Abbreviations and Acronyms	12

Document Overview

Background

Litigation hold is to a function that can preserve a user's email account and other information that is required for investigations or enquiries such as Freedom of Information (FOI) requests. eDiscovery is used within all corporate document locations (e.g., Exchange Online mailboxes, Microsoft Teams, SharePoint Online, etc) to process and identify electronic information that could be used as evidence in legal or security cases.

Document Audience

This Standard Operating Procedure (SOP) is intended to support the ongoing operation of the Digital Transformation Agency (DTA) Blueprint. It includes the required steps that a suitably trained administrator should follow to maintain the operational state of the solution.

Purpose

The purpose of this document is to provide the necessary steps to create a litigation hold in Office 365 and manage eDiscovery within the Azure tenant.

The services and settings provided by the Blueprint should not be modified without fully understanding the security and operational consequence of the change.

Prerequisites

Before completing the procedures detailed in this document, the following prerequisites should be met:

- It is recommended that the reader/administrator performing the procedures in the document has certification and/or experience with Exchange Online and/or Office 365.
- An understanding of PowerShell in an Office 365 and/or Azure context.
- An administrative account with the required permissions, including to install the Exchange Online PowerShell Module.
- The administrator performing these steps may need to be a member of the Organization Management or Role Management roles to be able to perform the steps in the **Assign eDiscovery Permissions** section.

Associated Documentation

Table 1 identifies the documents that should be referenced and understood before administering this solution

Table 1 Associated Documentation

Name	Version	Date
DTA – Solution Overview	March	03/2020
DTA – Platform Design	March	03/2020
DTA – Workstation Design	March	03/2020
DTA – Office 365 Design	March	03/2020
DTA – Office 365 - ABAC	March	03/2020
DTA – Platform – ABAC	March	03/2020
DTA – Intune Security Baselines - ABAC	March	03/2020
DTA – Software Updates - ABAC	March	03/2020
DTA – Intune Applications – ABAC	March	03/2020
DTA – Intune Enrolment – ABAC	March	03/2020
DTA – Conditional Access Policies – ABAC	March	03/2020
DTA – Intune Compliance – ABAC	March	03/2020
DTA – Intune Configuration – ABAC	March	03/2020

Litigation Hold

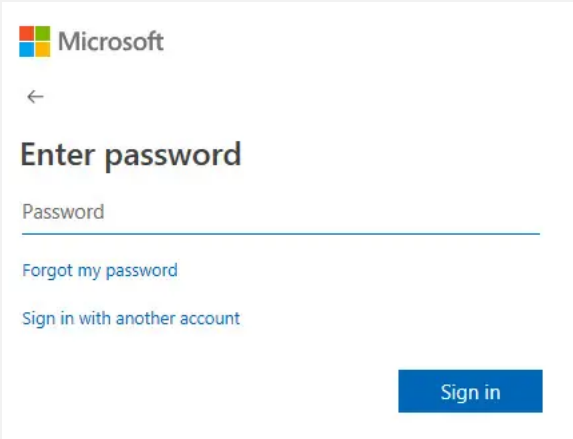
There are a number of methods that can be employed to place a mailbox on litigation hold. Two examples have been provided to show different ways of enabling litigation hold.

PowerShell Litigation Hold

This example explains how to place a single users' mailbox on litigation hold via PowerShell.

Please note that these steps require the Exchange Online PowerShell Module to be installed by an authorised administrator.

Table 2 PowerShell Litigation Hold

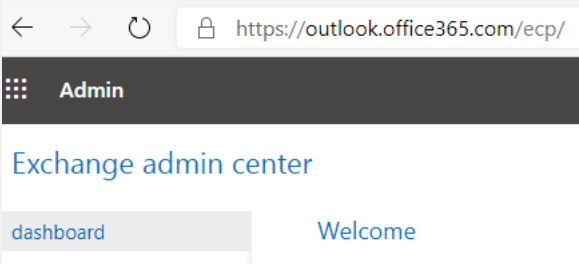
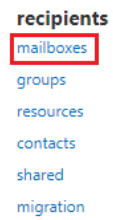
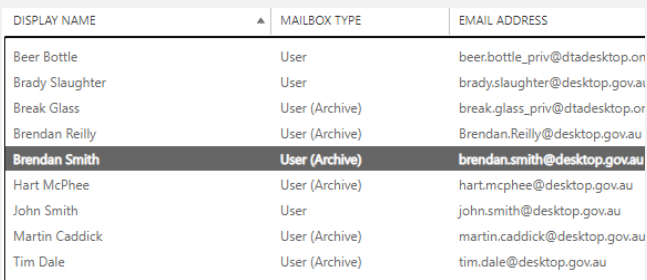
Step	Instruction	Screenshot
1.	Launch the Microsoft Exchange Online PowerShell module	No screenshot required
2.	Connect to the tenant using the following command: Connect-EXOPSSession - UserPrincipalName your.name@desktop.gov.au	No screenshot required
3.	A pop-up window will appear asking for your password, enter it and press Sign in . You will also be requested for a MFA challenge response, accept it, the pop-up window will close when authentication is successful.	
4.	Run the following command to place a mailbox on litigation hold: Set-Mailbox user.name@desktop.gov.au -LitigationHoldEnabled \$true - LitigationHoldDuration 365	No screenshot required

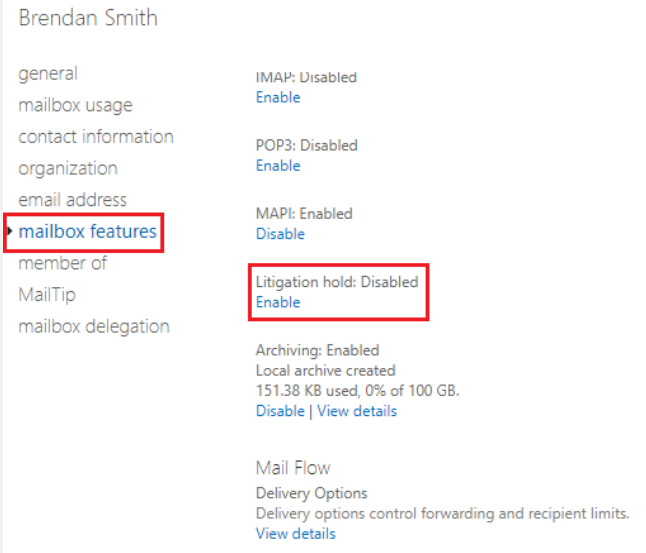
Step	Instruction	Screenshot
5.	Run the following command to put all mailboxes in the tenant in litigation mode: <code>Get-Mailbox -ResultSize Unlimited -Filter {RecipientTypeDetails -eq "UserMailbox"} Set-Mailbox -LitigationHoldEnabled \$true -LitigationHoldDuration 365</code>	No screenshot required
6.	When complete, close your session with the following command: <code>Remove-PSSession</code>	No screenshot required

Web Interface Litigation Hold

This example explains how to place a single users' mailbox on litigation hold via the Exchange Admin Center (EAC) web interface.

Table 3 Web Interface Litigation Hold

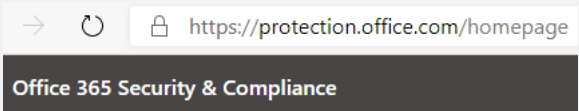
Step	Instruction	Screenshot																														
1.	Log into the Exchange Admin center at https://outlook.office365.com/																															
2.	On the Dashboard , click on mailboxes under the recipients heading																															
3.	Within the mailboxes screen, identify the mailbox to be placed on litigation hold then double click it.	 <table border="1"> <thead> <tr> <th>DISPLAY NAME</th><th>MAILBOX TYPE</th><th>EMAIL ADDRESS</th></tr> </thead> <tbody> <tr> <td>Beer Bottle</td><td>User</td><td>beer.bottle_priv@dtadesktop.on</td></tr> <tr> <td>Brady Slaughter</td><td>User</td><td>brady.slaughter@desktop.gov.au</td></tr> <tr> <td>Break Glass</td><td>User (Archive)</td><td>break.glass_priv@dtadesktop.or</td></tr> <tr> <td>Brendan Reilly</td><td>User (Archive)</td><td>Brendan.Reilly@desktop.gov.au</td></tr> <tr> <td>Brendan Smith</td><td>User (Archive)</td><td>brendan.smith@desktop.gov.au</td></tr> <tr> <td>Hart McPhee</td><td>User (Archive)</td><td>hart.mcphee@desktop.gov.au</td></tr> <tr> <td>John Smith</td><td>User</td><td>john.smith@desktop.gov.au</td></tr> <tr> <td>Martin Caddick</td><td>User (Archive)</td><td>martin.caddick@desktop.gov.au</td></tr> <tr> <td>Tim Dale</td><td>User (Archive)</td><td>tim.dale@desktop.gov.au</td></tr> </tbody> </table>	DISPLAY NAME	MAILBOX TYPE	EMAIL ADDRESS	Beer Bottle	User	beer.bottle_priv@dtadesktop.on	Brady Slaughter	User	brady.slaughter@desktop.gov.au	Break Glass	User (Archive)	break.glass_priv@dtadesktop.or	Brendan Reilly	User (Archive)	Brendan.Reilly@desktop.gov.au	Brendan Smith	User (Archive)	brendan.smith@desktop.gov.au	Hart McPhee	User (Archive)	hart.mcphee@desktop.gov.au	John Smith	User	john.smith@desktop.gov.au	Martin Caddick	User (Archive)	martin.caddick@desktop.gov.au	Tim Dale	User (Archive)	tim.dale@desktop.gov.au
DISPLAY NAME	MAILBOX TYPE	EMAIL ADDRESS																														
Beer Bottle	User	beer.bottle_priv@dtadesktop.on																														
Brady Slaughter	User	brady.slaughter@desktop.gov.au																														
Break Glass	User (Archive)	break.glass_priv@dtadesktop.or																														
Brendan Reilly	User (Archive)	Brendan.Reilly@desktop.gov.au																														
Brendan Smith	User (Archive)	brendan.smith@desktop.gov.au																														
Hart McPhee	User (Archive)	hart.mcphee@desktop.gov.au																														
John Smith	User	john.smith@desktop.gov.au																														
Martin Caddick	User (Archive)	martin.caddick@desktop.gov.au																														
Tim Dale	User (Archive)	tim.dale@desktop.gov.au																														

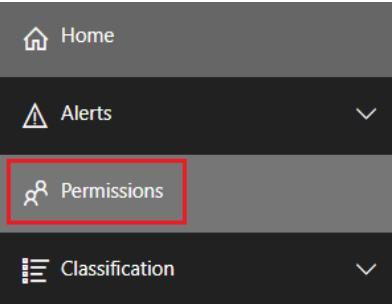
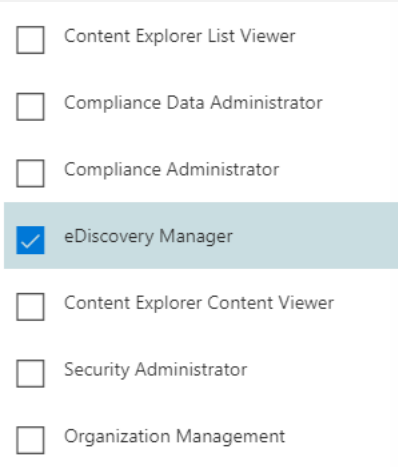
Step	Instruction	Screenshot
4.	A pop-up window will appear, when it does, select mailbox features from the left-hand pane	No screenshot required
5.	Within mailbox features , scroll down until you see the Litigation hold section and enable/disable as required	
6.	<p>If enabling litigation hold, please note that you will be prompted to enter the following:</p> <ul style="list-style-type: none"> - Litigation hold duration (days) - A note/description for the hold - A URL to direct users to for further information 	No screenshot required

Assign eDiscovery Permissions

The following table describes the steps required to modify **eDiscovery Manager** permissions within the tenant.

Table 4 eDiscovery permissions

Step	Instruction	Screenshot
1.	Navigate to the Office 365 Security & compliance Center (https://protection.office.com/)	

Step	Instruction	Screenshot
2.	In the left-hand pane, click on Permissions	
3.	Within the Permissions window, tick the eDiscovery Manager checkbox	
4.	Within the eDiscovery Manager pane that appears, make any changes that are required. Within this pane, you are able to assign an eDiscovery Manager , and eDiscovery Administrator , modify the existing assigned roles	No screenshot required

Create eDiscovery Case

The following table describes how to create a new eDiscovery case within the Microsoft 365 Compliance Center.

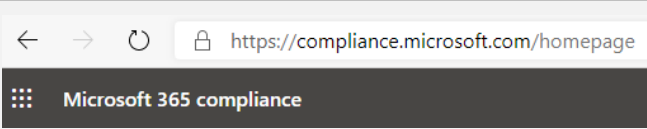
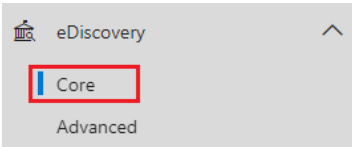
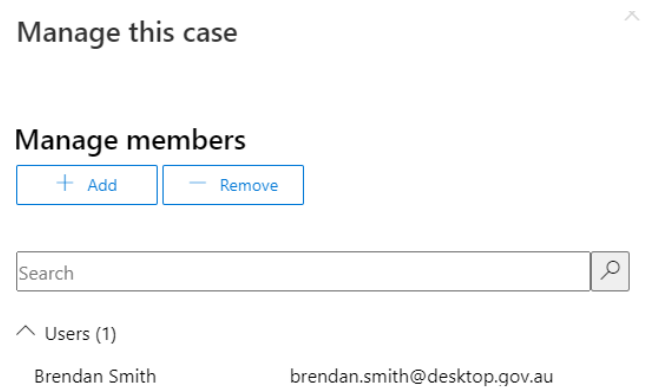
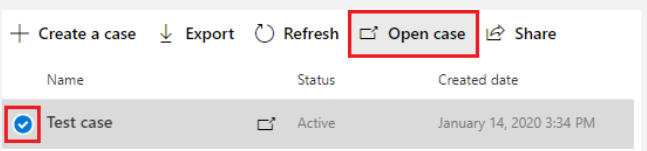
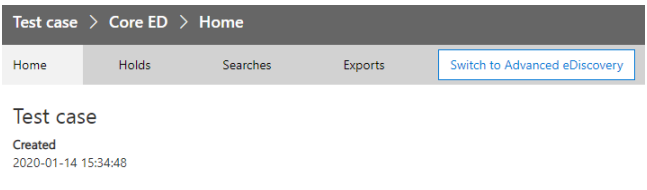
Table 5 Create eDiscovery Case

Step	Instruction	Screenshot
1.	Navigate to the Microsoft 365 Compliance Center (https://compliance.microsoft.com/)	
2.	In the left-hand pane, select eDiscovery , then click on Core	
3.	Within the Core eDiscovery screen click the Create a case button	
4.	In the pane that appears on the right of the window, enter a Case name and Case description then press Save	<div><h3>New case</h3><p>Enter a name and description</p><p>Give this case a friendly name so you can easily find it again later.</p><p>*Case name</p><input type="text" value="Test case"/> <p>Case description</p><input type="text" value="Test description."/></div> <div><div>Save</div><div>Cancel</div></div>

Manage eDiscovery Case

The following table describes how to manage an existing eDiscovery case within the Microsoft 365 Compliance Center.

Table 6 Manage eDiscovery Case

Step	Instruction	Screenshot
1.	Navigate to the Microsoft 365 Compliance Center (https://compliance.microsoft.com/)	
2.	In the left-hand pane, select eDiscovery , then click on Core	
3.	Within the Core eDiscovery window, identify your case, then click on it	No screenshot required
4.	The Manage this case window will appear, within it you can manage members, role groups, and the case status. You can also close or delete the case. When these changes have been made, press either Save or Close	
5.	Back in the Core eDiscovery screen, check the radio tick box for your case then press Open case	
6.	A new browser tab will open, within it you can view holds, perform searches, and perform exports.	

Abbreviations and Acronyms

Table 7 details the abbreviations and acronyms used throughout this document.

Table 7 Abbreviations and Acronyms

Acronym	Meaning
DTA	Digital Transformation Agency
EAC	Exchange Admin Center
FOI	Freedom of Information
SOP	Standard Operating Procedure