

## Como encontrar la ubicacion fisica de las evidencias guardadas en el servidor

1. Ir a Menu > Data Protection > DLP Incident Manager > Incident List
2. Seleccionar e ingresar al incidente deseado

McAfee										
DLP Incident Manager										
Data Protection										
DLP Incident Manager										
Analytics Incident List Incident Tasks Incident History										
Present: Data in-use/motion View: Default Edit Delete Save Time: (no time filter) Filter: (no custom filter) Edit Delete Save No Filter										
Group By: None										
Search X										
Incident ID	Reporting Product	Occurred (UTC)	Severity	Incident Type	User Principal Nam...	User Logon Name (...)	Computer Name	Actual Action	Rules	
458	DLP for Windows	September 28, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Whatsapp application...	
457	DLP for Windows	September 28, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	No Action	Whatsapp application...	
456	DLP for Windows	September 28, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	No Action	Whatsapp application...	
455	DLP for Windows	September 28, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	No Action	Whatsapp application...	
454	DLP for Windows	September 28, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	No Action	Whatsapp application...	
453	DLP for Windows	September 28, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	No Action	Whatsapp application...	
452	DLP for Windows	September 28, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Whatsapp application...	
451	DLP for Windows	September 28, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	No Action	Whatsapp application...	
450	DLP for Windows	September 28, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	No Action	Whatsapp application...	
449	DLP for Windows	September 28, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Whatsapp application...	
448	DLP for Windows	September 28, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Whatsapp application...	
447	DLP for Windows	September 28, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Whatsapp application...	
446	DLP for Windows	September 16, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Whatsapp application...	
445	DLP for Windows	September 16, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Whatsapp application...	
444	DLP for Windows	September 16, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Whatsapp application...	
443	DLP for Windows	September 16, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Whatsapp application...	
442	DLP for Windows	September 16, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Whatsapp application...	
441	DLP for Windows	September 16, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Whatsapp application...	
440	DLP for Windows	September 16, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Whatsapp application...	
439	DLP for Windows	September 16, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Whatsapp application...	
438	DLP for Windows	September 16, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Whatsapp application...	
437	DLP for Windows	September 16, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Whatsapp application...	
436	DLP for Windows	September 16, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Whatsapp application...	
435	DLP for Windows	September 16, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Whatsapp application...	
434	DLP for Windows	September 16, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Whatsapp application...	
433	DLP for Windows	September 16, 2020...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Whatsapp application...	
432	DLP for Windows	May 27, 2020 8:01...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Whatsapp application...	
431	DLP for Windows	May 21, 2020 7:59...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Web Protection Rule ...	
430	DLP for Windows	May 21, 2020 7:41...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Web Protection Rule ...	
429	DLP for Windows	May 21, 2020 7:41...	Warning (1)	Web Protection	Administrator@TEST...	TEST\Administrator	WIN10	Block	Web Protection Rule ...	

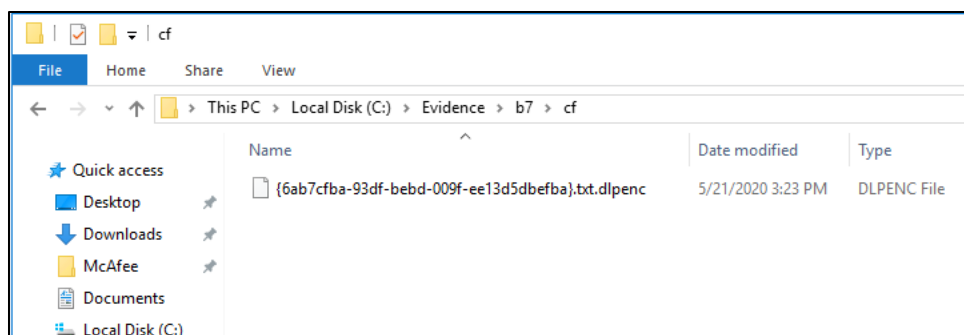
The screenshot shows the McAfee ePolicy Orchestrator 5.10.0 interface. The main window is titled "DLP Incident Manager" and displays details for incident 432. The incident occurred on May 27, 2020, at 7:59:55 PM. The incident type is "Web Protection" and the actual action is "Block". The severity is set to "Warning" and the status is "New". The resolution is "None" and the reviewer is "Unassigned". The endpoint details show the computer name as "WIN10", IP as "192.168.2.100", and user principal name as "Administrator@TEST.LAB". The source application is "firefox.exe". The reporting product is "DLP for Windows", product version is "11.3.0.17", and policy name is "DLP Policy Firefox Test (13)". The total match count is 1 and the total content size is 0.25 KB. The evidence table shows a single entry for "HTTP Request Payload.txt" with a match count of 1. The evidence name is "HTTP Request Payload.txt", item type is "HTTP Payload", file size is 1 KB, and the match count is 1. The unique match string is "...me\"Block file key word bluetaco 2.txt\",size\";4425\";item...". The unique match string is "bluetaco" and the classification is "Classification by Bluetacoword (1)".

Cuando pase el mouse sobre el archive cera como en la parte inferior vera un link extenso que dice lo siguiente (puede copiarlo y pegarlo en un editor de texto)

**javascript:openEvidence("\\\\epo\\evidence\\','HTTP Request Payload.txt','B7\\CF\\{6AB7CFBA-93DF-BEBD-009F-EE13D5DBEFBA}.txt.dlpenc');**

En el, puede ver el nombre del archivo de evidencia generado y los nombres de la carpeta con su formato encriptado.

El mismo es lo mismo que verlo aqui:



**Recuerde que solo desde ePO podra acceder al archivo original (de haber) o a los archivos generados como evidencia segun la regla disparada y la naturaleza de los datos.**