

## Como crear una tarea de purga de lista de incidentes e Historial

1. Ir a “Menu > Data Protection > DLP Incident Manager > Incident Task”
2. Seleccionar “Data in-use/motion” y “Purge Incidents”
3. Click en “Actions > New Rule”

En este paso vamos a crear la tarea de purga para eliminar los incidentes de la pestaña “**Incident List**” **Tip** El mismo se utiliza comunmente como set de trabajo para facil acceso a los incidentes mas recientes. (en este ejemplo dejaremos solo 30 dias de incidentes)

The screenshot shows the McAfee DLP Incident Manager interface. The top navigation bar includes the McAfee logo and links to DLP Incident Manager, System Tree, Policy Catalog, Dashboards, Software Catalog, and Client Task Catalog. The main header indicates the current path: Data Protection > DLP Incident Manager. Below this, the 'Incident Tasks' tab is active, with a dropdown menu showing 'Data in-use/motion' selected. The left sidebar contains a 'Task Type' section with a search bar and a list of options: 'Set Reviewer', 'Automatic mail Notification', and 'Purge Incidents' (which is highlighted with an orange box). The main content area displays a table of purging rules. The first rule is 'Enabled' and sets the maximum number of Data in-use/motion incidents to 1,000,000. At the bottom, a context menu is open, showing options: 'Delete', 'New Rule' (highlighted with an orange box), 'State', and 'Actions' (highlighted with an orange box). The 'Actions' dropdown shows '1 items'.

4. Agregamos un nombre a la tarea de purga y un criterio. (mantener los ultimos 30 dias)

McAfee

DLP Incident Manager System Tree Policy Catalog Dashboards Software Catalog

Data Protection

### DLP Incident Manager

Task Rule 1 Rule Properties 2 Rule Criteria

Purge Rule

Name Regla de Purga de Incidentes

Description

State ☒ Enabled

Previous Next Save Cancel

Utilizamos el campo **UTC** y seleccionamos que “NO ESTE DENTRO DE LOS ULTIMOS” 30 dias. Esto quiere decir que todo lo superior a esos 30 dias, sera eliminado. (Guardar los cambios)

McAfee

DLP Incident Manager System Tree Policy Catalog Dashboards Software Catalog

Data Protection

### DLP Incident Manager

Task Rule 1 Rule Properties 2 Rule Criteria

Available Properties

- utc
- DLP Data In-use/motion Incidents
- Occurred (UTC)
- Capture Search Information
- Classifications
- Cloud
- Computers
- Destination User Information
- Device Information
- Device Plug UTC Time
- Device Unplugged ...
- Email
- Email - All Recipients
- Email - Matched Recipients
- Evidences
- Labels

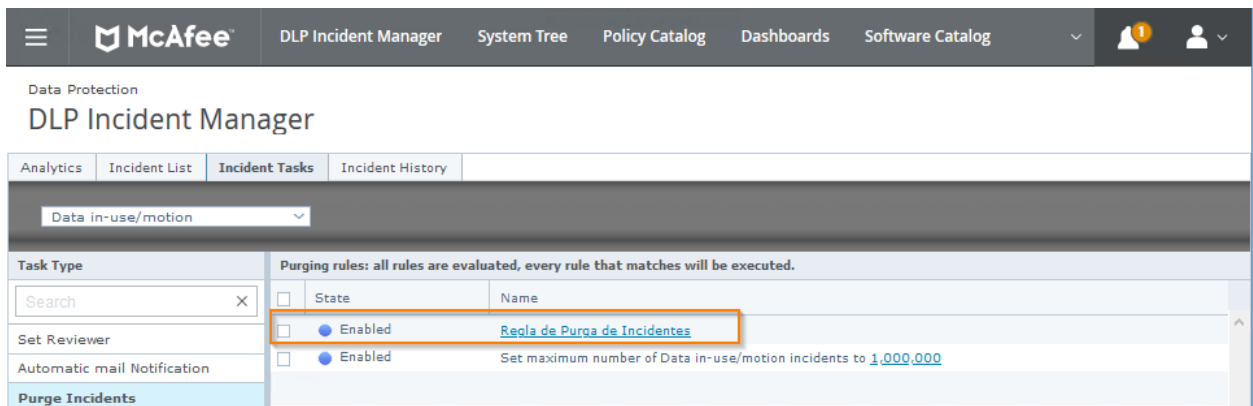
Property Comparison Value

DLP Data In-use/motion Incidents

Occurred (UTC) Is not within the last 30 Days

Previous Next Save Cancel

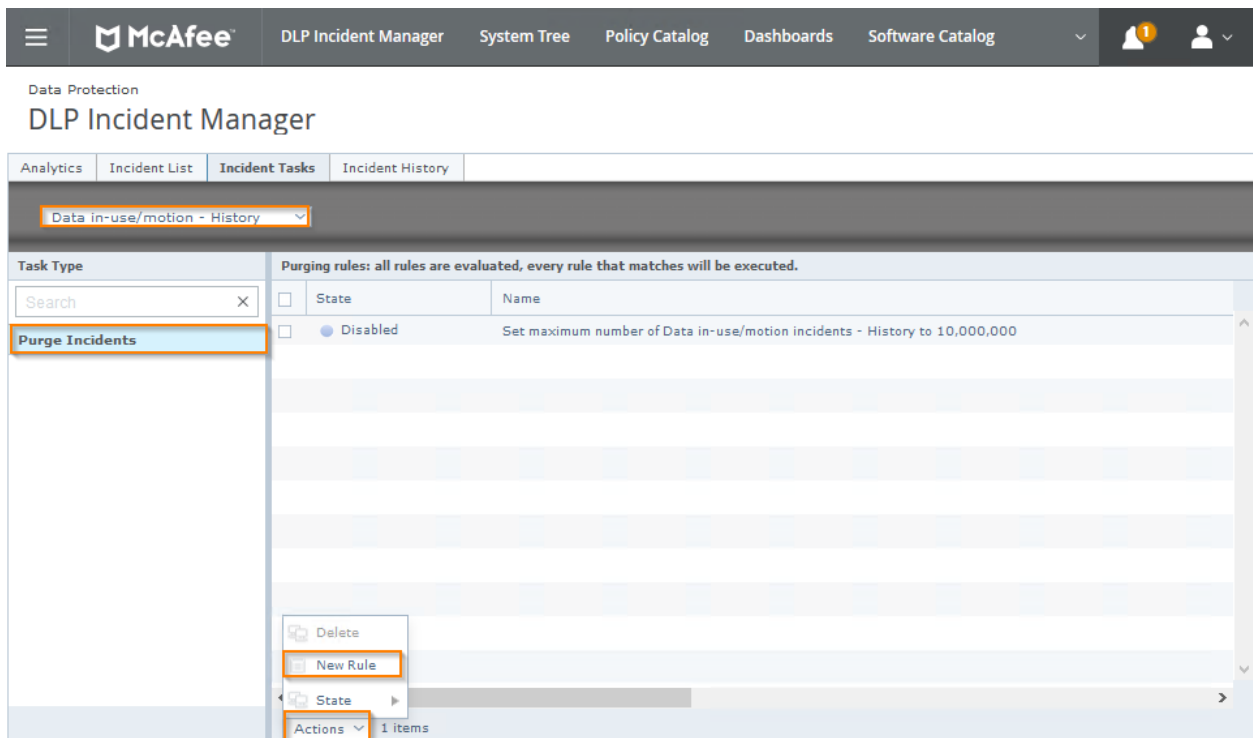
La misma se ve asi:



- Ahora Vamos por la de Historial. Cabe aclarar que la misma es la que se encarga Tambien de eliminar de manera definitiva las evidencias fisicas guardadas en el servidor definido para tal proposito.

*En este paso vamos a crear la tarea de purga para eliminar los incidentes de la pestaña “Incident History” **Tip** El mismo se utiliza comunmente como set de trabajo Hitorico, para buscar evidencias antiguas o en casos de evidencia para Aditorias. (En este ejemplo dejaremos 90 dias de incidentes) **Dato:** La evidencia se elimina de manera efectiva posterior a los 60 dias de mercado como evidencia a eliminar. Luego de esos 60 dias se elimina de manera automatica.*

- Ir a “Menu > Data Protection > DLP Incident Manager > Incident Task”
- Seleccionar “Data in-use/motion History” y “Purge Incidents”
- Click en “Actions > New Rule”



- Agregamos un nombre a la tarea de purga y un criterio. (mantener los ultimos 90 dias)

McAfee™

DLP Incident Manager
System Tree
Policy Catalog
Dashboards
Software Catalog

1

Data Protection

DLP Incident Manager

Task Rule

1 Rule Properties

2 Rule Criteria

Purge Rule

Name	Regla de Purga de Incidentes Historicos
Description	Purga de incidentes y evidencia mayor a 90 dias.
State	<input checked="" type="radio"/> Enabled

Previous
Next
Save
Cancel

Utilizamos el campo **UTC** y seleccionamos que “NO ESTE DENTRO DE LOS ULTIMOS” 90 dias. Esto quiere decir que todo lo superior a esos 90 dias, sera eliminado. (Guardar los cambios)

McAfee™

DLP Incident Manager
System Tree
Policy Catalog
Dashboards
Software Catalog

1

Data Protection

DLP Incident Manager

Task Rule

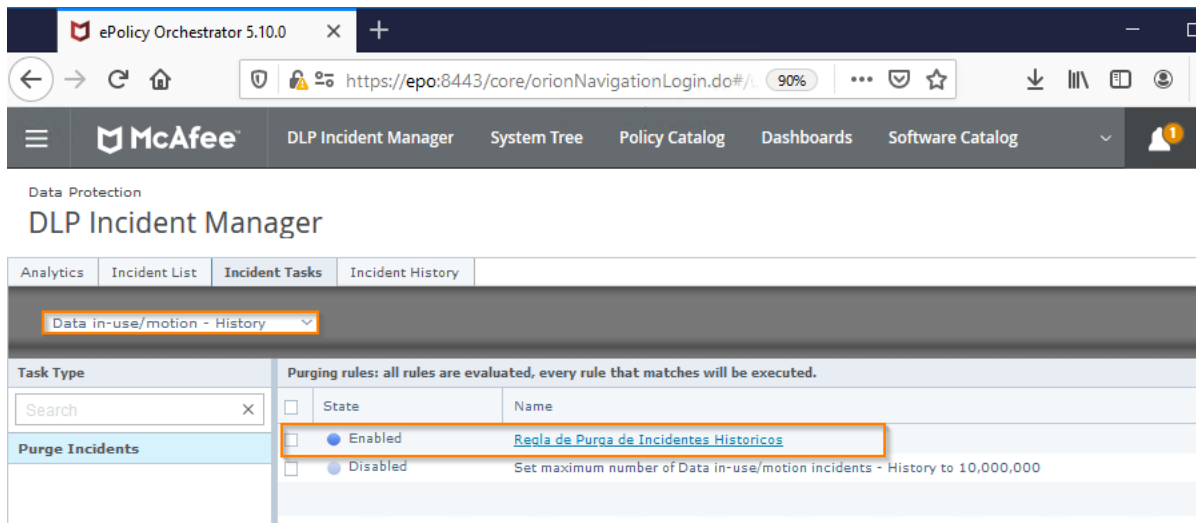
1 Rule Properties

2 Rule Criteria

Available Properties	Property	Comparison	Value
<div>utc</div> <div> DLP Data In-use/motio... </div> <div> Occurred (UTC) </div> <div> Capture Search Informa... </div> <div> Classifications </div> <div> Cloud </div> <div> Computers </div> <div> Destination User Inform... </div> <div> Device Information </div> <div> Device Plug UTC Ti... </div> <div> Device Unplugged ... </div> <div> Email </div> <div> Email - Matched Recipie... </div> <div> Email - Matched Recipie... </div> <div> Evidences </div> <div> Labels </div>	DLP Data In-use/motion Incidents History	Is not within the last	90 Days

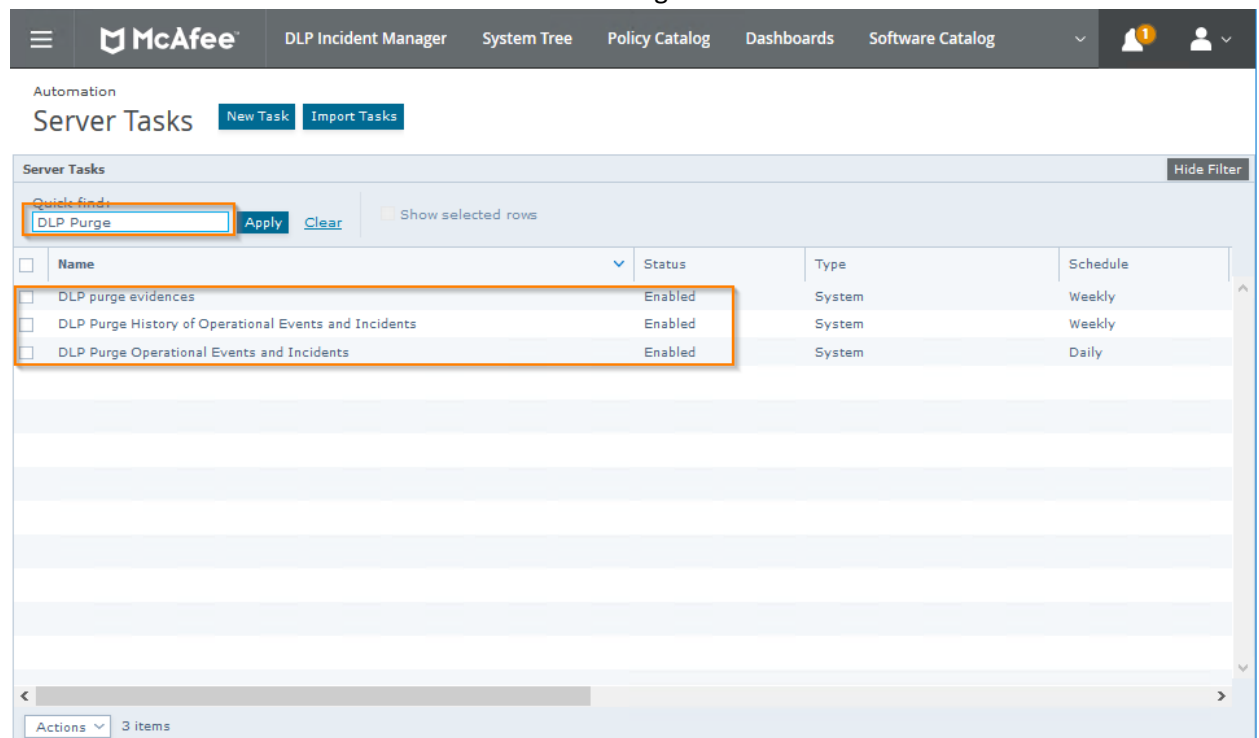
Previous
Next
Save
Cancel

La misma debe verse así:



10. Por ultimo, solo debe revisarse que las tareas de Servidor que ejecutan estas Tareas de DLP esten Activas. Las mismas se encuentran en el siguiente Menu.

**Menu > Automation > Server Tasks > “buscar DLP Purge”**



Si es de su agrado, puede revisar las mismas y modificarlas segun crea necesario su ejecucion.

**McAfee Technical Support Team**