

Your Question

Article: 00117 Question:

How to Purge Data for a Custom Filter by Creating the Scheduled Task, Filter Fields, Rules and Actions?

Net Report Answer

Introduction

This article explains how to purge data for a custom filter by creating the scheduled task, filter fields, rules and actions. Please follow the tasks below step by step:

Task 1: Creating a Scheduled Task for the Custom Filter. Task 2: Creating Fields Task 3: Creating Actions Task 4: Creating Rules

Note: this document assumes that you have already created a filter (please contact support@netreport.fr for help creating your custom filter).

Task 1: Creating a Scheduled Task for the Custom Filter

To create a scheduled task for the custom filter, in this document 'MyDevice', please follow the steps below:

Steps

- 1. Launch the Net Report Management Console, select Start> All Programs> NetReport> Management Console.
- 2. Enter your Login and Password in the Login dialog box and click OK.
- 3. Select NetReport> [localhost]> Agents> Event Scheduler in the left Console root pane.





- 4. Click The **New** in the **Tasks** tool bar to add a new Scheduled Task. The **new task** appears.
- 5. Rename the Task as appropriate, in this example MyDevice Purge. Add a **Comment** if necessary.

Console root NetReport Event Scheduler Agent Image: Server Image: Server >NetReport/localhost/Agents/Event Scheduler Image: Server Scheduler Image: Server Image: Server Image: Server Image: Server Image:	🚯 Console root\NetReport\localhost\Agents\Event Schedul	r		_ 🗆 ×
Image: Server >NetReport/localhost/Agents/Event Scheduler Image: Server >NetReport/localhost/Agents/Event Scheduler Image: Server Image: Server Image: Server	Console root -	2	Event Schedule	er Agent
Name Comment Active • Ø Event Scheduler • Ø Fortinet Fortificate UTM Consolidate, Aggregate • Ø Event Scheduler • Ø Event Scheduler Event Scheduler • Ø Event Scheduler Event Scheduler <		≝Tasks	>NetReport/localhost/Agents/Ev	ent Scheduler<
B · Ø Aventail Purge C Aventail Purge This Task schedules t ☑ B · Ø Covice This Task schedules t ☑ Image: C Device B · Ø Firewall Aggregate and Purge C Device This Task schedules t ☑ B · Ø Firewall Aggregate and Purge C Device This Task schedules t ☑ B · Ø Firewall Aggregate and Purge Firewall Aggregate and Purge This Task schedules t ☑ B · Ø Firewall Aggregate and Purge Firewall Aggregate and Purge This Task schedules t ☑ B · Ø Firewall Ageregate and Purge Firewall Aggregate and Purge This Task schedules t ☑ B · Ø Fortinet FortiGate UTM Consolidate, Aggregate and Purge Sends an event to lau ☑ Image: Imag		Name	Comment A	ctive
 D[®] Firewall Aggregate and Purge D[®] Fortinet FortiGate UTM Consolidate, Aggregate D[®] Intrusion Prevention System Purge D[®] MyDevice Purge D[®] Proxy Aggregate and Purge D[®] Fortinet FortiGate UTM Consolidate, Aggregate and Purge D[®] Sol. Firewall Alert 	System Server System System Server System Server	🥶 Aventail Purge	This Task schedules t [- 📆
B - 10 ⁰ Intrusion Prevention System Purge B - 10 ⁰ MyDevice Purge B - 10 ⁰ Proxy Aggregate and Purge B - 10 ⁰ Proxy Aggregate and Purge B - 10 ⁰ SOL Firewall Alert C Fortinet FortiGate UTM Consolidate, Aggregate and Purge C Fortinet FortiGate UTM Consolidate, Aggregate and Purge		CDevice	This Task schedules t [न् 🙀
🗄 🛷 Proxy Aggregate and Purge 🧧 Fortinet FortiGate UTM Consolidate, Aggregate and Purge Sends an event to lau 🗹 🛱		Firewall Aggregate and Purge	This Task schedules t (- 🙀
		Fortinet FortiGate UTM Consolidate, Aggregate and Purge	Sends an event to lau [- 🔂
🗈 📑 Flat File Parser 🗧 🕘 Intrusion Prevention System Purge Sends an event to lau 🗹 🛱		Intrusion Prevention System Purge	Sends an event to lau [- 🖬
		MyDevice Purge	This Task schedules t (- 🐺
🔄 Radius Proxy 🕀 🛃 Remote Microsoft WMI 🕘 Proxy Aggregate and Purge This Task schedules t 🗹 🛱		Proxy Aggregate and Purge	This Task schedules t (- 🖬
🖶 🚰 SQLServer Spyer 🔮 SQL Firewall Alert Used with SQL Alert F 🗖 🙀		SQL Firewall Alert	Used with SQL Alert F	- 🕅 .
e 🞲 Log Yault 0 Selected Tasks 🗈 🛍 🛱 🖞 🗑 👔		0 Selected Tasks	C.	6113
ii Applying Changes 💭		äApplying Changes		۲
🗄 Scheduler Status 💭		#Scheduler Status		
				<u></u>

6. Click Modify Task to the right of the new Scheduled Task in this example MyDevice Purge. The [MyDevice Purge] Task page appears in the right pane.

- 7. Select the [MyDevice] Target Filter.
- 8. Click **New** three times and add the following three **Destination Fields**:

Destination field	Value
keeplastDetails	The number of days of data you wish to keep before its is purged. In this
	example 61 days.
maxDetails	The maximum size of data you want to keep before the data is purged. In this
	example -1 means that there is no limit.
deviceType	The device concerned by the purge task, in this example MyDevice.

Console root\NetReport\localhost\Agents\Event Schedule	er\MyDevice Purge		
Console root	B		MyDevice Purge Task ▲
Agents	[∥] Record	>Ne	tReport/localhost/Agents/Event Scheduler/MyDevice Purge<
CiteCk Point (Kean Inne) CiteCk Point (Kean Inne) CiteCk Point (Kean Inne) CiteCk Point (Kean Inne) CiteCk Point (Kean Inne)	Target Filter : Destination Field	MyDevice	2
 	keeplastDetails maxDetails	61	
⊕ ⊕	deviceType	MyDevice	
⊕-	Erequenc	v	
Metroport communication Ping	This tasks starts on 200	7/11/11 and runs at 00:00 a	every day.
	·		



 Select Console root> NetReport> [localhost]> Agents> Event Scheduler> [MyDevice Purge]> Frequency in the left Console root pane. The Frequency configuration for [MyDevice Purge] page appears in the right pane.

🚯 Console root\NetReport\localhost\Agents\Event Schedul	er\MyDevice Purge\Frequency	
Console root	Frequency configuration for I	WyDevice Purge
- III Packages Server B → ULA - → Agents R → III Check Point (Real Time)	>NetReport/localhost/Agents/Event Scheduler/ # S c h e d u l e	MyDevice Purge/Frequency<
Event Scheduler Aventail Purge Gov CDevice Gov CDevice Gov Firewall Aggregate and Purge Gov Fortinet FortiGate UTM Consolidate, Aggre	Schedule Type : Deily Begin Date/Time : 11 novembre 2007, 00:00 End Date : 10 novembre 2007	
MyDevice Purge MyDevice	Day interval : 1 This tasks starts on 2007/11/11 and runs at 00:00 every day.	2
Hor Har Value	Repeat Task Repeat the task Interval : Duration t	
SQLServer Spyer	This task is not repeated.	

- 10. Select the frequency with which you wish the scheduled purge task to be performed.
- 11. Select Console root> NetReport> [localhost]> Agents> Event Scheduler in the left Console root pane.

🔂 Console root\NetReport\localhost\Agents\Event Schedule	er*	
Console root ⊡- ♦ NetReport ⊡- ↓ localhost ■ □ ↓ Docalhost	2	Event Scheduler Agent
I Packages Server	,	>NetReport/localhost/Agents/Event Scheduler<
E-∲ Agents B-S Check Point (Real Time)	≣ Tasks	
	Name	Comment Active
	Aventail Purge	This Task schedules t 💌 📆
Joy Firewall Aggregate and Purge Joy Fortinet FortiGate UTM Consolidate, Aggregal	CDevice	This Task schedules t 🗷 🚮
Intrusion Prevention System Purge MyDevice Purge	Firewall Aggregate and Purge	This Task schedules t 🗹 🛛 👔
OF Proxy Aggregate and Purge OF SQL Firewall Alert Of SQL	Fortinet FortiGate UTM Consolidate, Aggregate and Purge	Sends an event to lau 🗹 🚮
	Intrusion Prevention System Purge	Sends an event to lau 🔽 🚮
	MyDevice Purge	This Task schedules t 🔽 🙀
	Proxy Aggregate and Purge	This Task schedules t 🔽 🛛 🗗
€ 😚 SQLServer Spyer	SQL Firewall Alert	Used with SQL Alert F 🗖 🛛 🛱
⊕-@ Log Vault ⊕-© Backups	0 Selected Tasks	Þa 🛱 🗋 🖬 🙎
	[∦] Applying Changes	
	Click here to save all your o All the changes you have made locally will t	changes. be sent to the scheduler.
	Apply Changes	2
	₿Scheduler Status	
	Stop Running Event Scheduler is running.	\$

12. Click **Apply Changes** to save the changes you have just made. Note the asterisk next to **the Event Scheduler** branch in the left **Console root** pane disappears indicating that your changes have been saved.



Task 2: Creating Fields

ET REPORT

To add the following fields for the [MyDevice] filter, please follow the steps below:

- Bad_Record
- deviceType
- keeplastDetails
- MaxDetails

Steps

1. Select Console root> [localhost]> ULA> Filters> [MyDevice]> Fields in the left Console root pane.

🕸 netreport - [Console rootWe	tReport\localhost\ULA*\Filters\WyDev	ice\Fields]			
🚯 File Action View Favorites	Window Help				_ & ×
← → 🗈 📧 😫					
Console root - NetReport - Iocalhost					Fields
⊡ 🚸 ULA*			>NetReport/loc	alhost/ULA/Filters/M	yDevice/Fields<
⊡ ∳ Settings	‼Fields				
🛨 🚟 Cisco PIX	Name 🔺	Туре	Expression	Comment	
EngineEvent	0 Selected Fields			Ę	e 🛱 🗋 🗊 💈
MyDevice MyDevice Actions Actions Rules Fields Dictionary Agents Galaxy Backupc					

2. Click \square New four times to add four new fields.

🕸 netreport - [Console root\Ne	tReport\localhost\ULA*\Filters\MyDev	rice\Fields]			
🚯 Eile <u>A</u> ction <u>V</u> iew Fav <u>o</u> rites	<u>W</u> indow <u>H</u> elp				_ & ×
← → 🗈 📧 😫					
Console root					Fields
			>NetReport/I	localhost/ULA/Filters/MyD	evice/Fields<
	[∦] Fields				
E Cisco PIX	Name 🔺	Туре	Expression	Comment	
EngineEvent	_New Field	String -	Record("afield")		🖊 Edit
	_New Field1	String	Record("afield")		/ Edit
Rules Fields	_New Field2	String	Record("afield")		/ Edit
Dictionary	_New Field3	String -	Record("afield")		/ Edit
E Agencs	0 Selected Fields			Ba (£ 1 t 👔 🖉
⊞…©р васкиря					
< · · · >					-



3. Edit the fields as follows:

Name	Туре	Expression
Bad_Record	String	Record("BadRecord")
deviceType	String	Record("deviceType")
keeplastDetails	String	Record("keeplastDetails")
MaxDetails	String	Record("MaxDetails")



Task 3: Creating Actions

NET REPORT

We are now going to add four default actions and then customize them (renaming them and parameterizing them for our specific needs.

Default Action Name	Rename Default Action to:
Stop Group	Do not Perform the Rules Below
Execute an SQL Statement	Purge[MyDevice]
Write to Winlog	[MyDevice] Purge has started
Write to Winlog	[MyDevice] Purge has ended

To do so, please follow the steps below:

Steps

1. Select Console root> NetReport> [localhost]> ULA> Filters> [MyDevic]e> Actions in the left Console root pane.

5		A	ctions
	1:	>NetReport/localhost/ULA/Filters/Te	st/Actions<
# A c t i o n s			
Name		Comment	. 🔺
🗧 Message Box		Display the XML Record	
StopAll			STOP
StopGroup			
0 Selected Actions	Correlate and Alert	- - -	1 🗋 🗊 🔗

2. Select the **StopGroup** action.

				Actions
		>Ne	tReport/localhost/ULA/Filte	ers/Test/Actions<
₿ A c t				
Name			Comment	
🔋 Messag	e Box		Display the XML Record	
🔋 StopAll				STOP
StopGro	up			
0 Selected	Actions	Correlate and Alert		ta 🛍 🗋 🧋



3. Rename Stop Group to Do not Perform the Rules Below.

			Actio	ns
_		>Ne	tReport/localhost/ULA/Filters/Test/Act	tions<
	Actions		(
	Name		Comment	. 🔺
8	Message Box		Display the XML Record	
8	StopAll			STOP
8	Do not Perform the Rules Below			
0 3	Selected Actions	Correlate and Alert	🖬 🛱 🖬 (Ì 💈

4. Select Execute an SQL Statement from the drop-down list.

Correlate and Alert	•
Correlate and Alert	٠
Custom action	
Execute an SQL Statement	
Generate Dashboard	
Go to a rules group	
Go to next rules group	
Insert to Database	
Insert To Database with aggregation functions	
Kill a process on a computer	
Modify the value of a Performance Counter	
Run an action when a threshold is raised	•

5. Click **New** in the tool bar. The **Execute an SQL Statement** action appears.

∥ A c	tions			
Nan	ne		Comment	. 🔺
🛢 Mes	sage Box		Display the XML Record	-
🛢 Exec	cute an SQL Statement		comment	
🛢 Stop	All			STOP
🛢 Do n	ot Perform the Rules Below			
0 Select	ted Actions	Correlate and Alert	🔽 🛱 🛍 🖌	Ū 🔗



6. Rename Execute an SQL Statement action to Purge [MyDevice].

11		A	ctions
	>	NetReport/localhost/ULA/Filters/Te	est/Actions<
∥ Actions			
Name		Comment	. 🔺
🔵 Message Box		Display the XML Record	
Purge MyDevice		comment	
StopAll			STOP
Do not Perform the Rules Below			
0 Selected Actions	Correlate and Alert	- Pa (ð 🗋 🗴 🔗

7. Click the appears.

modify action icon to the right of Purge MyDevice. The Purge [MyDevice] page

.		Purge MyDevice
		>NetReport/localhost/ULA/Filters/Test/Actions/Purge MyDevice<
II Configu		
Connection:	Database Connection	×
SQL Statement :		
DELETE FROM My	Table WHERE id=0	
	

8. Replace the SQL Statement with the following statement:

```
EXEC NR_Lock 'MyDevice Purge'
EXEC nr_purge_table 'MyDevice_rawdata', '[MyDeviceDateFieldName]',
<field>keeplastDetails</field>, <field>MaxDetails</field>
EXEC NR_Unlock 'MyDevice Purge'
```

Note: 'MyDevice_rawdata' refers to the table containing the raw data for the device in question. Alternatively you could replace 'MyDevice_rawdata' by the name of another data table, as long as it includes a date column in order to purge records according to the value of the keeplastDetails field.

Note: [MyDeviceDateFieldName] refers to the name of the date field for the device log data in question, this is the reference date to be used to purge data.



🚯 Console root\NetReport	localhost\ULA*\Filters\MyDev	vice\Actions\Purge MyDevice
Average State	:	Purge MyDevice
E Setting:		>NetReport/localhost/ULA/Filters/MyDevice/Actions/Purge MyDevice<
Filters	E Configurat	ion 💌
🗄 🔡 Dat	Connection:	Database Connection
🕀 📑 🕅 Dat	SQL Statement :	
Den Den Forl Mt Forl Mt Forl	EXEC NR_Lock 'HyDev: EXEC nr_purge_table EXEC NR_Unlock 'Aven	ice Purge' 'MyDevice_rawdata', '[MyDeviceDateField]', <field>keeplastDetails</field> , <field>MaxDetails</field> atail Purge'

9. Go back to the **Actions** branch.

NET REPORT

10. Select Write to Winlog from the drop-down list.

Actio		
	>NetReport/localhost/ULA	/Filters/Test/Actions<
# Actions		
Name	Comment	. 🔺
💿 Message Box	Display the XML Record	
Purge MyDevice	comment	
🛢 StopAll		STOP
😑 Do not Perform the Rules Below		
Write to Winlog	comment	
0 Selected Actions	Correlate and Alert	💽 🖻 🛍 🛍 🕯 💈

11. Rename the Write to Winlog action as follows: [MyDevice] Purge has Started.

Action Action		
	>NetReport/localhost/ULA/F	ilters/Test/Actions<
# Actions		
Name	Comment	. *
📮 Message Box	Display the XML Record	
Purge MyDevice	comment	
StopAll		STOP
Do not Perform the Rules Below		
MyDevice Purge has Started	comment	🦀
0 Selected Actions	Correlate and Alert	- Ba 🛱 🗋 🗴 👔



- 13. Select the Information Event Type.
- 14. Select the **NRAgent** and **NRAgentTime** records and click **Delete** to remove them.
- 15. Enter the following message:

[MyDevice] Purge has Started.



10 Copyright © 2007 Net Report. All rights reserved. <u>http://www.net-report.net</u>



16. Select Write to Winlog from the drop-down list.

*		Actions
	>NetReport/localhost/UL	A/Filters/Test/Actions<
# Actions		
Name	Comment	
🧧 Message Box	Display the XML Record	
🧧 Purge MyDevice	comment	1
🧧 StopAll		STOP
🧧 Do not Perform the Rules Below		
MyDevice Purge has Started	comment	
Write to Winlog	comment	
0 Selected Actions	Correlate and Alert	💽 🏝 🛍 🛍 🗊 🔗

17. Rename the Write to Winlog action as follows: [MyDevice] Purge has Ended.

*		Actions
	>NetReport/localhost/ULA/	/Filters/Test/Actions<
# Actions		
Name	Comment	. 🔺
🥶 Message Box	Display the XML Record	
Purge MyDevice	comment	1
🔮 StopAll		STOP
Do not Perform the Rules Below		
🥶 MyDevice Purge has Started	comment	🦀
MyDevice Purge has Ended	comment	
0 Selected Actions	Correlate and Alert	💽 🛍 🛍 🛍 😵



- 19. Select the Information Event Type.
- 20. Select the **NRAgent** and **NRAgentTime** records and click **Delete** to remove them.
- 21. Enter the following message: [MyDevice] Purge has Ended



12 Copyright © 2007 Net Report. All rights reserved. <u>http://www.net-report.net</u>



Task 4: Creating Rules

NET REPORT

We are now going to add the following rules

Steps

1. Select Console root> NetReport> [localhost]> ULA> Filters> [MyDevice]> Rules in the left Console root pane.

Console root\NetReport\localhost\ULA*\Filters\MyDevic	ce\Rules		
Console root ⊡ ♦ NetReport ⊡ ↓ localhost	4	Rules Grou	ps for MyDevice
Ackages Server		>NetReport/localhost/	ULA/Filters/MyDevice/Rules<
Gettings Filters	≣Rules Groups		
Aventail Filter	Name	Comment	#
Database Management - Firewall and Prox Database Management - IPS	😅 New rules group	Comments on ne	ew rules group 🛛 🔹
Database Management - UTM Demo	0 Selected Actions		↑ ↓ ☜ @ ᠿ 前 🖇
EngineEvent			
Actions			
Rules ▼			▼
	7		

2. Rename the New rules group to Purge Data.

🖸 Console root\NetReport\localhost\ULA*\Filters\MyDevice\Rules				
NetReport Iocalhost Modeses Server	4	Rules Groups for MyDevio	ce	
	∦Rules Groups	>NetReport/localhost/ULA/Filters/MyDevice/Re	ules<	
Protection Heat P	Name Purge Data	Comment Comments on new rules group	#	
 B Database Management - UTM C Demo C Demo<td>0 Selected Actions</td><td>A A 🕫 🛱 🗍 🕯</td><td>12</td>	0 Selected Actions	A A 🕫 🛱 🗍 🕯	12	
MyDevice				
	l			

3. Select the **Purge Data** node of the **Rules** branch in the left **Console root** pane.

				Purge Data
				>NetReport/localhost/ULA/Filters/Device/Rules/Purge Data<
#	Action	Active	Critical	Custom criteria
				A 🗸 🗋 👘 😵



4. Click **A New** to add a new rule.

Purge Dat				
>NetReport/localhost/ULA/Filters/Device/Rules/Purge Da				
Custom criteria	Critical	Active	Action	ŧ
	no	yes	Stop	

5. Right-click on the new rule. The context menu appears.

						Purge Data
_					>NetR	Report/localhost/ULA/Filters/MyDevice/Rules/Purge Data<
#	Action	Active	Critical	Custom criteria		
	Inser	yes 	NO		Delete Insert New Field	
		1	1	1		♠ ↓ 🗅 🖮 😵

6. Click New Field, the New Field dialog box appears.

New Field		×
Bad_Record	•	OK)
		Cancel



7. Select Bad_Record from the drop-down list.

					Purge Data
					>NetReport/localhost/ULA/Filters/MyDevice/Rules/Purge Data<
#	Action	Active	Critical	Custom criteria	
1	Inser	yes	no		
	w Field Bad_Record Bad_Record ReviceType ReeplastDet MaxDetails	d J ails			OK Cancel
	1	1	1	1	↑ ↓ 🗅 🖮 😵

- 8. Click OK.
- 9. Note the Bad_Record column is added to the Purge Data table.

						Purge Data
						>NetReport/localhost/ULA/Filters/MyDevice/Rules/Purge Data<
#	Action	Active	Critical	<	Bad_Record	Custom criteria
1	Insert to Database	yes	no			
						A 🔶 🗋 👘 😵

- 10. Right-click again on the new rule. The context menu appears.
- 11. Select deviceType from the drop-down list.

ew Field	>
deviceType	OK
deviceType	Canaal
MaxDetails	Lancel

12. Click OK.



13. Note the deviceType column is added to the Purge Data table.

NET REPORT

								Purge Data
						>Ne	etReport/local	host/ULA/Filters/MyDevice/Rules/Purge Data<
#	Action	Active	Critical	<	Bad_Record		deviceType	Custom criteria
1	Insert to Database	yes	no					
								1 🕈 🔶 🗇 👔

14. We are now going to edit the rule we added and add the following four rules with the following values:

#	Action	Active	Critical	<	Bad_Record	<	deviceType
1	Do not Perform the Rules Below	yes	no			Ŷ	MyDevice
2	Purge MyDevice	yes	no	IS NULL		=	MyDevice
3	MyDevice Purge has Started Event	yes	no	IS NULL		=	MyDevice
4	MyDevice Purge has Ended Event	yes	no	IS NULL		=	MyDevice

Console root\NetReport\localhost\ULA*\Filters\MyDevic	e\Rules\	Purge Data								
Average Server									Purge Data	1
⊡ - 😽 ULA* ⊕ - 📴 Settings		1			1	>NetReport/lo	calho	st/ULA/Filters/	MyDevice/Rules/Purge Data<	<
E 🔷 Filters	Ŧ	Action	Active	Critical	 <	Bad_Record	<	device lype	Custom criteria	
🕀 🔷 Aventail Filter	1	Do not Perform the Rules Below	yes	no			\diamond	MyDevice		
🕀 🥵 Database Management - Firewall and Prox	2	Purge MyDevice	yes	no	IS NULL		=	MyDevice		
Database Management - IPS	3	MyDevice Purge Started Event	yes	no	IS NULL		=	MyDevice		
Database Management - UTM	4	MyDevice Purge Ended Event	yes	no	IS NULL		=	MyDevice		
Engliedvent										
Actions										
E Rules										-
Purge Data										-
Dictionary										
Agents										
E Log Vault										-
Him So Backups										4
									🏫 🗅 🔶 🔨	
	,									_



15. To select an action, double-click the cell in question in the **Action** column and select the action from the drop-down list.

A NetReport A NetRep							Pures Data
				>NetReport/lo	calhoe	t/III A/Filtore/	
Gettings	Active	Critical	<	Bad_Record	<	deviceType	Custom criteria
Aventail Filter Do not Perform the Rules Below Do not Perform the Rules D	yes yes yes yes	no no no no	IS NULL IS NULL IS NULL		<>	MyDevice MyDevice MyDevice MyDevice	↑ ↓ @ ::::::::::::::::::::::::::::::::::

16. To specify the rule's field value double-click the cell in question and select the value from the drop-down list.



- 17. To apply the changes you have made once you have added all the rules, select **Console root> NetReport>** [localhost]> ULA.
- 18. Click Apply Changes.