EventTracker

Actionable Security Intelligence

Integrate Microsoft Antimalware

EventTracker v8.x and above

Publication Date: September 6, 2017

Abstract

This guide provides instructions to configure **Microsoft Antimalware** to send logs to EventTracker Enterprise. Once logs are being configured to send to EventTracker Manager, alerts and reports can be configured into EventTracker.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 8.x and later, and **Microsoft Antimalware.**

Audience

Administrators who are responsible for monitoring **Microsoft Antimalware** which are running using EventTracker Manager.

Table of Contents

Overview

Microsoft Antimalware is an antivirus software (AV) product that fights malware (malicious software), including computer viruses, spyware, Trojan horses and rootkits. The software runs on Windows XP, Windows Vista and Windows 7. Built upon the same virus definitions and scanning engine as other Microsoft antivirus products, Microsoft Antimalware Service provides real-time protection, constantly monitoring activities on the computer and scanning new files as they are downloaded or created and disable detected threats.

EventTracker integrates Microsoft Antimalware and provides reports, knowledge objects and dashboards for all generated events including attacks, configuration changes etc. EventTracker will also monitor antivirus sensors and process execution statuses for all workstations in the network.

Prerequisites

- EventTracker v8.x should be installed.
- You must have a valid and active Azure subscription account to use the Microsoft antimalware for Azure features and deploy antimalware for your cloud services and or virtual machines.
- The Microsoft Antimalware solution is supported on Windows Server 2008 R2, Windows Server 2012, and Windows Server 2012 R2 operating system families.
- The VM agent is required to run the Microsoft antimalware extension on the virtual machine. Make sure VM agent is enabled on the VM.

Integration of MS Antimalware events to EventTracker server

Once you deploy the Azure portal, follow the below steps to enable the logging.

1) In the Recommendations blade, select **Enable data collection for subscriptions**. This opens the **Turn on data collection** blade.

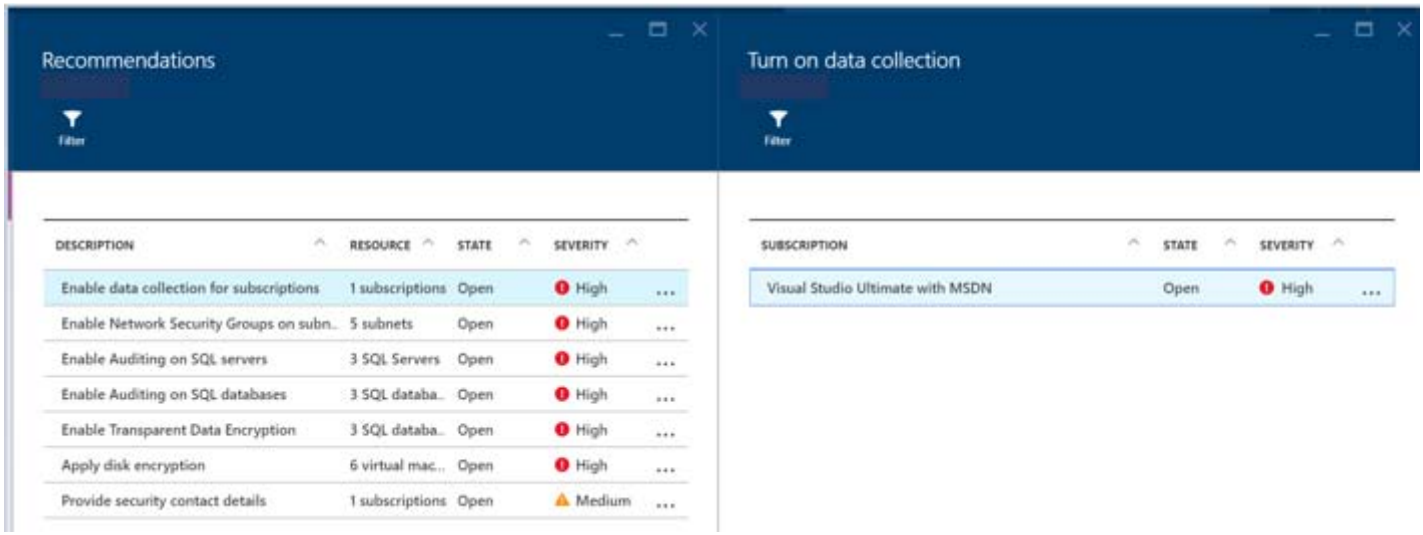


Figure 1

2) On the **Turn on data collection** blade, select your subscription. The Security policy blade for that subscription opens.
3) On the **Security policy** blade, select '**On**' under Data collection to automatically collect logs. Turning on data collection provisions the monitoring extension on all current and new supported VMs in the subscription.
4) Select **Save**.
5) Select **OK**.
6) Also, please ensure that in the VM the security extensions need to be enabled during the creation of a VM as shown below.
7) These are Virtual machine environments, so once enabled the extension, events will be shown in the Event Viewer.

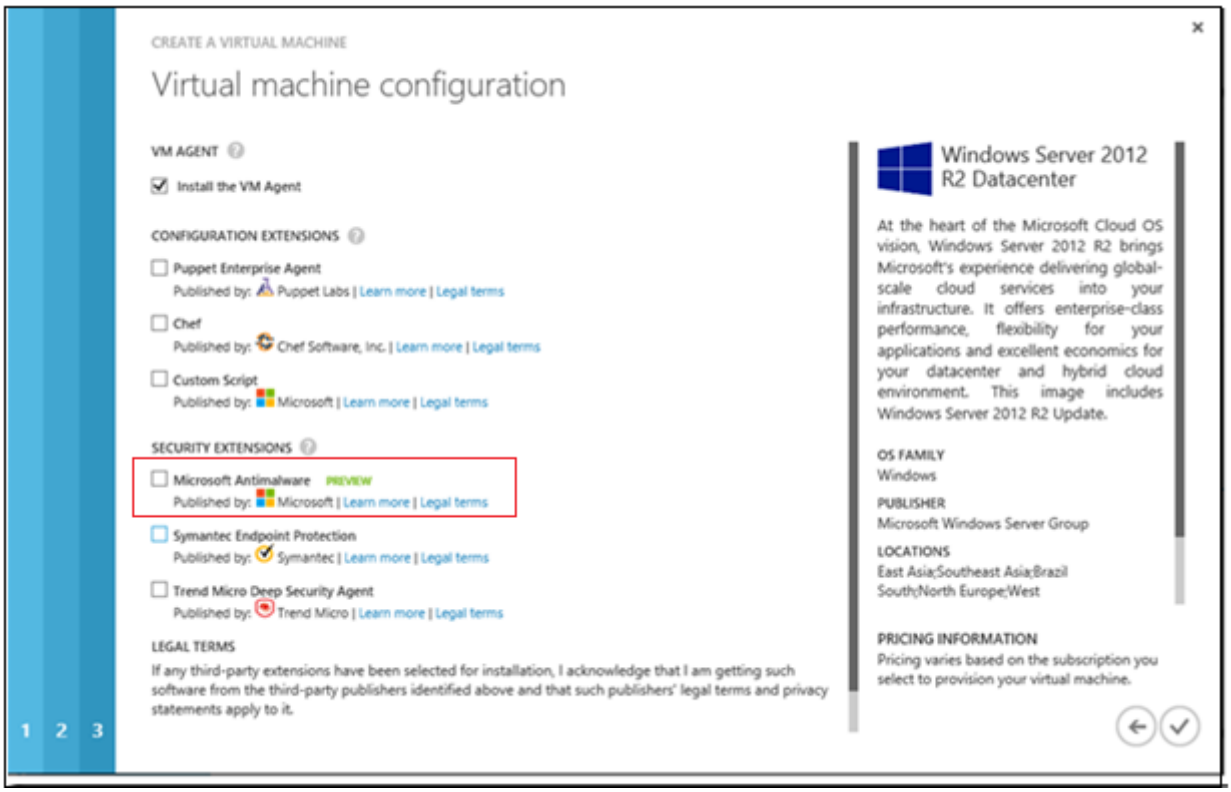


Figure 2

EventTracker Knowledge Pack

Once logs are received into EventTracker, Categories, Reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Windows.

Alerts

- **MS Antimalware-Action taken against malware activity:** This alert is generated when an action is taken against the detected malware.
- **MS Antimalware-Detected malware activity:** This alert is generated when any malware activity is detected.
- **MS Antimalware-Quarantined malware restored:** This alert is generated when a quarantined malware is restored.
- **MS Antimalware-Removed history of malware:** This alert is generated when the malware history is removed or deleted.

Flex Reports

- **MS Antimalware-Action taken against malware activity-** This report provides details about all the action taken against malware activities.

LogTime	Computer	Message	Threat Name	Severity	Threat File	Detection Source	User Name	Process Name	Action	Action Status	Error Code	Threat Description	Signature Version	Engine Version
08/10/2017 04:40:37 PM	PNPL-15-KP	Antimalware has taken action to protect this machine from malware or other potentially unwanted	PowerShell/PsAttack.A&threatid=2147722658&enterprise=1	Medium	_C:\Windows\Temp\RiZWzfMpvY.bat;file:_C:\Windows\Temp\RiZWzfMpvY.bat->[PowEncCmdFile]	Real-Time Protection	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe	Quarantine	No additional actions required	0x00000000	The operation completed successfully.	AV: 1.247.1079.0, AS: 1.247.1079.0, NIS: 117.2.0.0	AM: 1.1.13903.0, NIS: 2.1.13804.0
08/10/2017 04:40:37 PM	PNPL-15-KP	Antimalware has taken action to protect this machine from malware or other potentially unwanted software.	PowerShell/PsAttack.A&threatid=2147722658&enterprise=1	High	_C:\Windows\Temp\RiZfderty.exe->[PowEncCmdFile]	Real-Time Protection	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	Quarantine	No additional actions required	0x80508023	The program could not find the malware and other potentially unwanted software on this computer.	AV: 1.247.1079.0, AS: 1.247.1079.0, NIS: 117.2.0.0	AM: 1.1.13903.0, NIS: 2.1.13804.0
08/10/2017 04:40:37 PM	PNPL-15-KP	Antimalware has taken action to protect this machine from malware or other potentially unwanted	PowerShell/PsAttack.A&threatid=2147722658&enterprise=1	Medium	_C:\Windows\Temp\RiZWzfMpvY.bat;file:_C:\Windows\Temp\RiZWzfMpvY.bat->[PowEncCmdFile]	System	NT AUTHORITY\SYSTEM	Unknown	Quarantine	No additional actions required	0x00000000	The operation completed successfully.	AV: 1.247.1082.0, AS: 1.247.1082.0, NIS: 117.2.0.0	AM: 1.1.13903.0, NIS: 2.1.13804.0

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
8/11/2017 4:58:01 PM	1117	NTPLDTBLR38 / PNPL-1...	N/A	N/A	Microsoft Antimalware

Event Type: Information
Log Type: Application
Category Id: 0

Description:
Microsoft Antimalware has taken action to protect this machine from malware or other potentially unwanted software.
For more information please see the following:http://go.microsoft.com/fwlink/?linkid=37020&name=HackTool:PowerShell/PsAttack.A&threatid=2147722658&enterprise=1
Name: HackTool:PowerShell/PsAttack.A
ID: 2147722658
Severity: High
Category: Tool
Path: file:_C:\Windows\Temp\RiZWzfMpvY.bat->[PowEncCmdFile]
Detection Origin: Local machine
Detection Type: Concrete
Detection Source: Real-Time Protection
Process Name: C:\Windows\System32\svchost.exe
Action: Quarantine
Action Status: No additional actions required
Error Code: 0x80508023
Error description: The program could not find the malware and other potentially unwanted software on this computer.
Signature Version: AV: 1.247.1079.0, AS: 1.247.1079.0, NIS: 117.2.0.0
Engine Version: AM: 1.1.13903.0, NIS: 2.1.13804.0
<EventData><Data>%860</Data><Data>4.10.209.0</Data><Data>{6BF518FA-657A-4B23-B575-591891973519

- **MS Antimalware-Detected malware activity -** This report provides details about all the malwares that are detected by Microsoft Antimalware.

LogTime	Computer	Message	Threat Name	Severity	Threat File	Detection Type	Detection Source	User Name	Process Name	Signature Version	Engine Version
08/10/2017 03:28:44 PM	PNPL-15-KP	Antimalware has detected malware or other potentially unwanted software.	PowerShell/PsAttack.A&threatid=2147722658&enterprise=1	Medium	_C:\Windows\Temp\RiZWzfMpvY.bat;file:_C:\Windows\Temp\RiZWzfMpvY.bat->[PowEncCmdFile]	Concrete	Real-Time Protection	NT AUTHORITY\SYSTEM	C:\Windows\System32\cmd.exe	AV: 1.247.1079.0, AS: 1.247.1079.0, NIS: 117.2.0.0	AM: 1.1.13903.0, NIS: 2.1.13804.0
08/10/2017 03:28:44 PM	PNPL-15-KP	Antimalware has detected malware or other potentially unwanted software.	PowerShell/PsAttack.A&threatid=2147722658&enterprise=1	Medium	_C:\Windows\Temp\RiZWzfMpvY.bat->[PowEncCmdFile]	Concrete	Real-Time Protection	NT AUTHORITY\SYSTEM	C:\Windows\System32\svchost.exe	AV: 1.247.1079.0, AS: 1.247.1079.0, NIS: 117.2.0.0	AM: 1.1.13903.0, NIS: 2.1.13804.0
08/10/2017 03:28:44 PM	PNPL-15-KP	Antimalware has detected malware or other potentially unwanted software.	PowerShell/PsAttack.A&threatid=2147722658&enterprise=1	Medium	_C:\Windows\Temp\RiZWzfMpvY.bat;file:_C:\Windows\Temp\RiZWzfMpvY.bat->[PowEncCmdFile]	Concrete	System	NT AUTHORITY\SYSTEM	Unknown	AV: 1.247.1082.0, AS: 1.247.1082.0, NIS: 117.2.0.0	AM: 1.1.13903.0, NIS: 2.1.13804.0

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
8/11/2017 5:05:43 PM	1116	NTPLDTBLR38 / PNPL-1...	N/A	N/A	Microsoft Antimalware

Event Type: Information
Log Type: Application
Category Id: 0

Description:
Microsoft Antimalware has detected malware or other potentially unwanted software.
For more information please see the following: http://go.microsoft.com/fwlink/?linkid=37020&name=HackTool:PowerShell/PsAttack.A&threatid=2147722658&enterprise=1
Name: HackTool:PowerShell/PsAttack.A
ID: 2147722658
Severity: Medium
Category: Tool
Path: file:_C:\Windows\Temp\RiZWzfMpvY.bat->[PowEncCmdFile]
Detection Origin: Local machine
Detection Type: Concrete
Detection Source: Real-Time Protection
User: NT AUTHORITY\SYSTEM
Process Name: C:\Windows\System32\cmd.exe
Signature Version: AV: 1.247.1079.0, AS: 1.247.1079.0, NIS: 117.2.0.0
Engine Version: AM: 1.1.13903.0, NIS: 2.1.13804.0
<EventData><Data>%860</Data><Data>4.10.209.0</Data><Data>{B06F123B-0AA1-487A-B3D2-875D681E2FF8}</Data><Data>2017-07-19T15:58:48.879Z</Data><Data></Data><Data></Data><Data>2147722658</Data><Data>HackTool:PowerShell/PsAttack.A</Data><Data>2</Data><Data>Medium</Data><Data>34</Data><Data>Tool</Data><Data>http://go.microsoft.com/fwlink/?lin

- **MS Antimalware-Quarantined malware restored-** This report provides details on all the quarantined malwares that were restored.

LogTime	Computer	Message	Threat Name	Severity	Threat File	User Name	Signature Version	Engine Version	Malware Details
08/10/2017 05:32:53 PM	PNPL-15-KP	Antimalware has restored an item from quarantine.	PowerShell/PsAttack.A&threatid=2147722658&enterprise=1	Medium	_C:\Windows\Temp\RiZWzfMpvY.bat	CORP\dagnerdl00	AV: 1.249.20.0, AS: 1.249.20.0	1.1.14003.0	http://go.microsoft.com/fwlink/?linkid=37020&name=HackTool:PowerShell/PsAttack.A&threatid=2147722658&enterprise=1

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
8/11/2017 4:22:30 PM	1009	NTPLDTBLR38 / PNPL-1...	N/A	N/A	Microsoft Antimalware

Event Type: Information
Log Type: Application
Category Id: 0

Description:
Microsoft Antimalware has restored an item from quarantine.
For more information please see the following:http://go.microsoft.com/fwlink/?linkid=37020&name=HackTool:PowerShell/PsAttack.A&threatid=2147722658&enterprise=1
Name: HackTool:PowerShell/PsAttack.A
ID: 2147722658
Severity: Medium
Category: Tool
Path: file:_C:\Windows\Temp\RiZWzfMpvY.bat
User: CORP\dagnerdl00
Signature Version: AV: 1.249.20.0, AS: 1.249.20.0
Engine Version: 1.1.14003.0
<EventData><Data>%860</Data><Data>4.10.209.0</Data><Data></Data><Data></Data><Data></Data><Data></Data><Data></Data><Data>CORP</Data><Data>dagnerdl00</Data><Data>S-1-5-21-525170056-763419254-2745571669-8216</Data><Data>HackTool:PowerShell/PsAttack.A</Data><Data>2147722658</Data><Data>2</Data><Data>34</Data><Data>http://go.microsoft.com/fwlink/?linkid=37020&name=HackTool:PowerShell/PsAttack.A&threatid=2147722658&enterprise=1</Data><Data>file:_C:\Windows\Temp\RiZWzfMpvY.bat</Data><Data></Data><Data></Data><Data></Data><Data></Data><Data></Data><Data>

- **MS Antimalware-Removed history of malware-** This report provides details about the malware history that was removed.

LogTime	Computer	Message	User Name
08/10/2017 06:26:08 PM	PNPL-15-KP	Antimalware has removed history of malware and other potentially unwanted software.	NT AUTHORITY\SYSTEM

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
8/11/2017 4:22:32 PM	1013	NTPLDTBLR38 / PNPL-1...	N/A	N/A	Microsoft Antimalware

Event Type: Information
Log Type: Application
Category Id: 0

Description:
Microsoft Antimalware has removed history of malware and other potentially unwanted software.
Time: ?7/?18/?2017 10:17:11 AM
User: NT AUTHORITY\SYSTEM
<EventData><Data>%860</Data><Data>4.10.209.0</Data><Data>?7/?18/?2017 10:17:11 AM</Data><Data></Data><Data></Data><Data></Data><Data></Data><Data>NT AUTHORITY</Data><Data>SYSTEM</Data><Data>S-1-5-18</Data></EventData>

- **MS Antimalware-Service stopped:** This report provides details about all the services that are stopped.

LogTime	Computer	Message	Scan ID	Scan Type	Scan Parameters	User Name
08/10/2017 05:49:45 PM	PNPL-15-KP	Antimalware scan has been stopped before completion.	0EFCCCCA-BFE2-4E3B-A504-3D018A7853DB	Antimalware	Quick Scan	NT AUTHORITY\NETWORK SERVICE
08/10/2017 05:49:45 PM	PNPL-15-KP	Antimalware scan has been stopped before completion.	16AEED5D-A570-4B9A-88BC-0E15659538D4	Antimalware	Full Scan	NT AUTHORITY\NETWORK SERVICE

Logs Considered:

LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
8/11/2017 4:22:31 PM	1002	NTPLDTBLR38 / PNPL-1...	N/A	N/A	Microsoft Antimalware

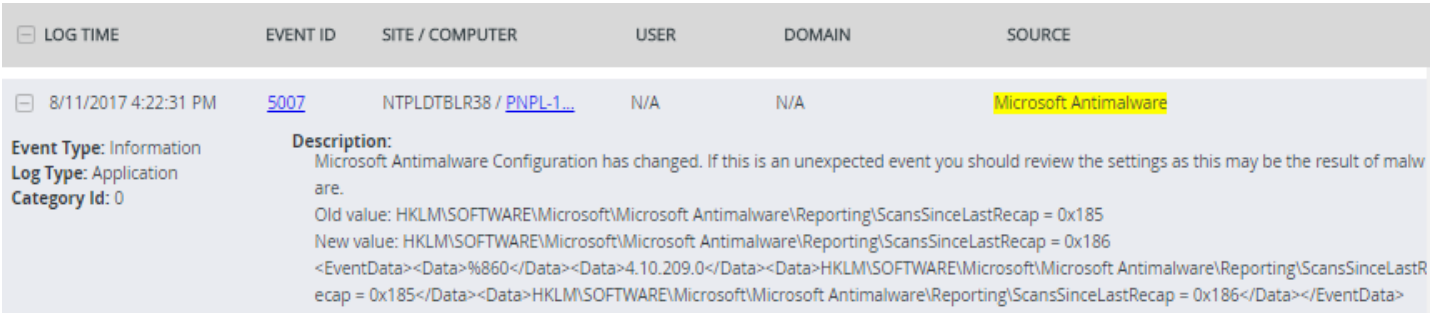
Event Type: Information
Log Type: Application
Category Id: 0

Description:
Microsoft Antimalware scan has been stopped before completion.
Scan ID: {16AEED5D-A570-4B9A-88BC-0E15659538D4}
Scan Type: Antimalware
Scan Parameters: Full Scan
User: NT AUTHORITY\NETWORK SERVICE
<EventData><Data>%860</Data><Data>4.10.209.0</Data><Data>{16AEED5D-A570-4B9A-88BC-0E15659538D4}</Data><Data>2</Data><Data>%802</Data><Data>2</Data><Data>%805</Data><Data>NT AUTHORITY</Data><Data>NETWORK SERVICE</Data><Data>NT AUTHORITY\NETWORK SERVICE </Data></EventData>

- **MS Antimalware-Configuration changes-** This report provides details about all the configuration changes that are done.

LogTime	Computer	Message	Old value	New value
08/10/2017 06:07:43 PM	PNPL-15-KP	Antimalware Configuration has changed. If this is an unexpected event you should review the settings as this may be the result of malware.	HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Reporting\ScansSinceLastRecap = 0x185	HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Reporting\ScansSinceLastRecap = 0x186
08/10/2017 06:07:43 PM	PNPL-15-KP	Antimalware Configuration has changed. If this is an unexpected event you should review the settings as this may be the result of malware.	HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Reporting\ScansSinceLastRecap = 0x186	HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Reporting\ScansSinceLastRecap = 0x187

Logs Considered:



LOG TIME	EVENT ID	SITE / COMPUTER	USER	DOMAIN	SOURCE
8/11/2017 4:22:31 PM	5007	NTPLDTBLR38 / PNPL-1...	N/A	N/A	Microsoft Antimalware

Event Type: Information
Log Type: Application
Category Id: 0

Description:
Microsoft Antimalware Configuration has changed. If this is an unexpected event you should review the settings as this may be the result of malware.
Old value: HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Reporting\ScansSinceLastRecap = 0x185
New value: HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Reporting\ScansSinceLastRecap = 0x186
<EventData><Data>%860</Data><Data>4.10.209.0</Data><Data>HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Reporting\ScansSinceLastRecap = 0x185</Data><Data>HKLM\SOFTWARE\Microsoft\Microsoft Antimalware\Reporting\ScansSinceLastRecap = 0x186</Data></EventData>

Import MS Antimalware knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Knowledge Objects
- Alerts
- Flex Reports
- Parsing Rule

NOTE: Export knowledge pack items in the following sequence:

- Knowledge Objects
- Alerts
- Flex Reports
- Parsing rule

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.

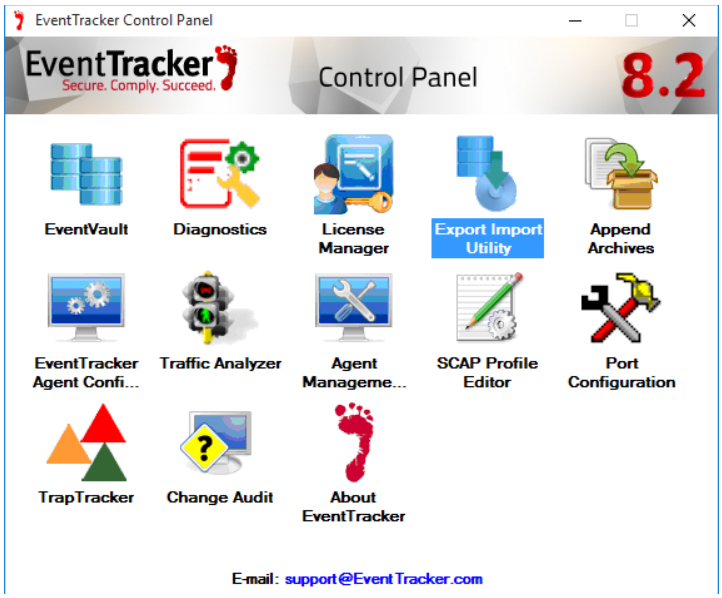


Figure 3

3. Click the **Import** tab.

Alerts

1. Click **Alerts** option, and then click the browse  button.
2. Locate the **MS Antimalware alerts.isalt** file, and then click the **Open** button.

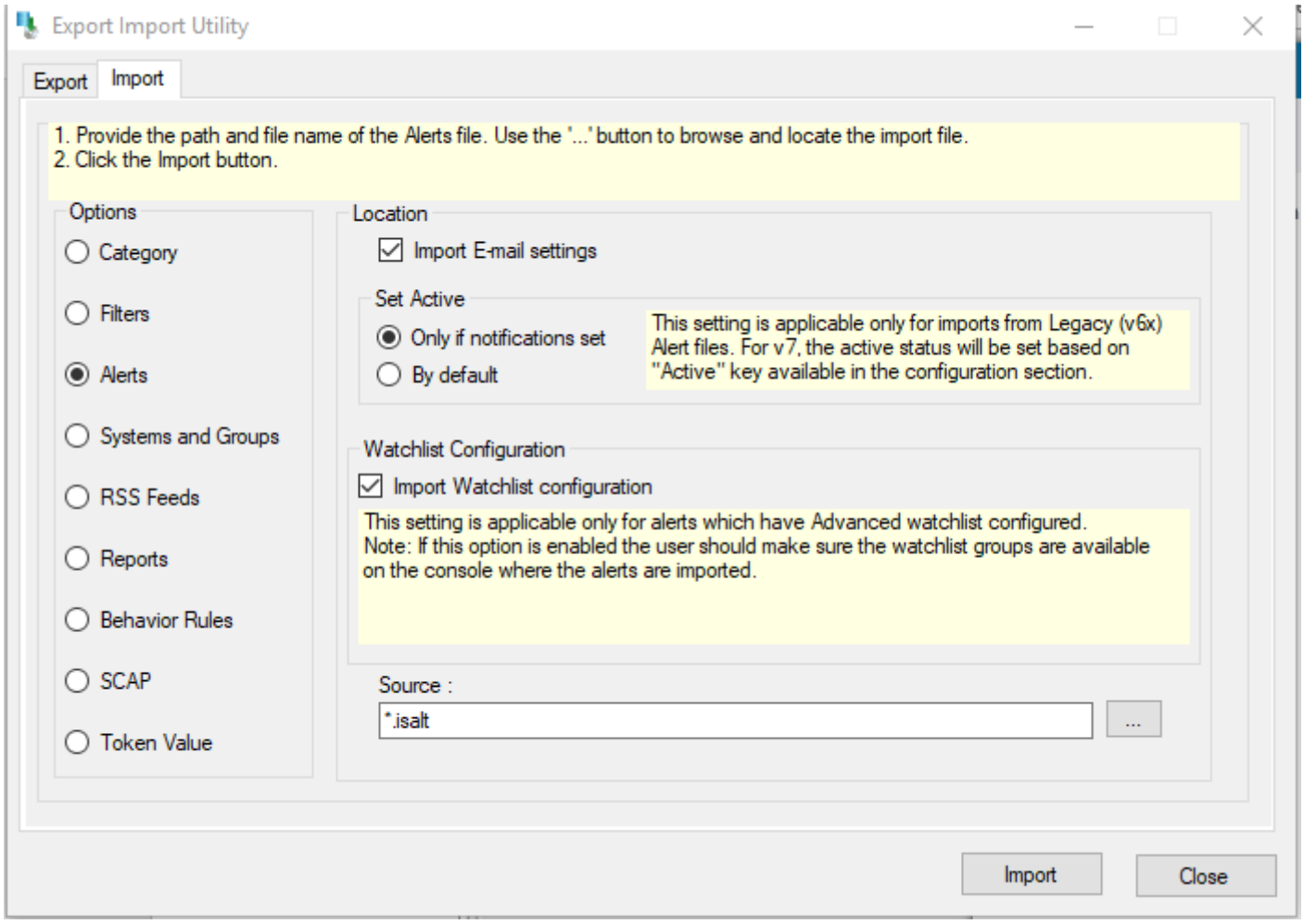


Figure 4

2. To import alerts, click the **Import** button.

   EventTracker displays success message.

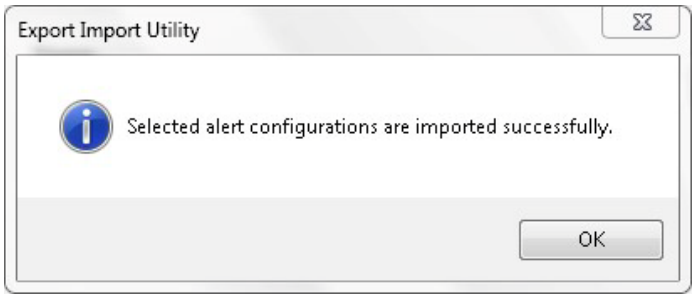


Figure 5

3. Click **OK**, and then click the **Close** button.

Knowledge Objects

1. Click **Knowledge objects** under Admin option in the EventTracker manager page.

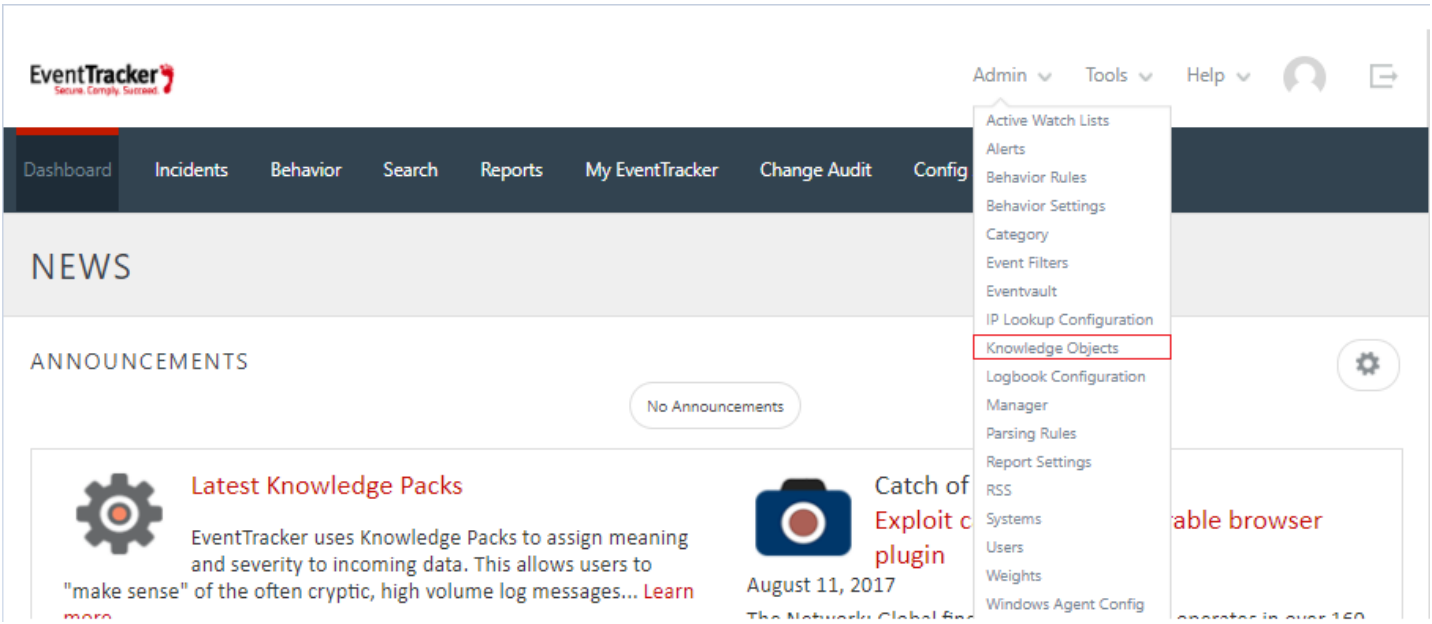


Figure 6

2. Locate the **MS Antimalware knowledge objects.etko**, and then click **Import** button

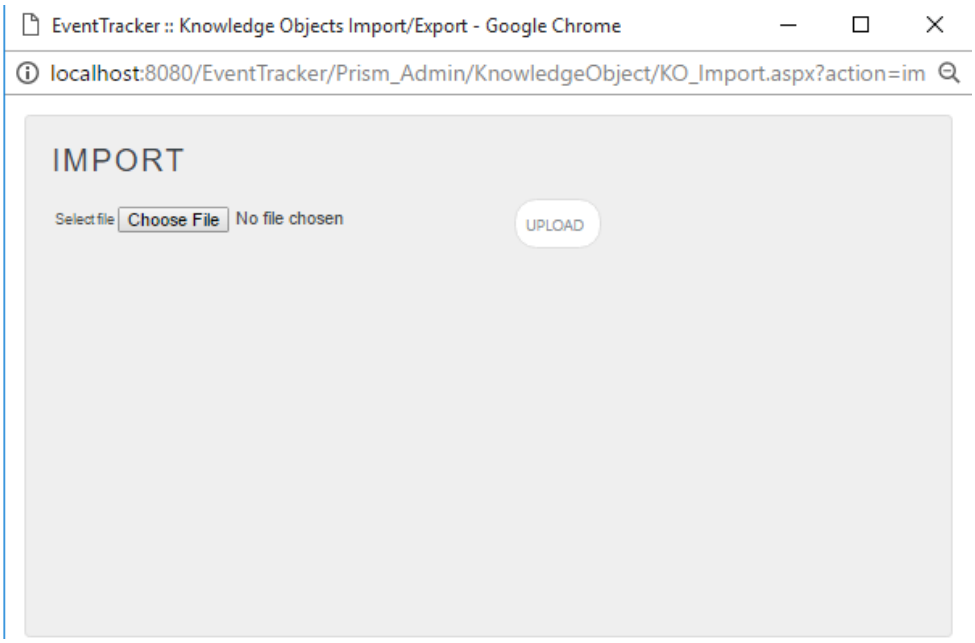


Figure 7

3. Choose the Knowledge objects that needs to be imported and click on **upload**.

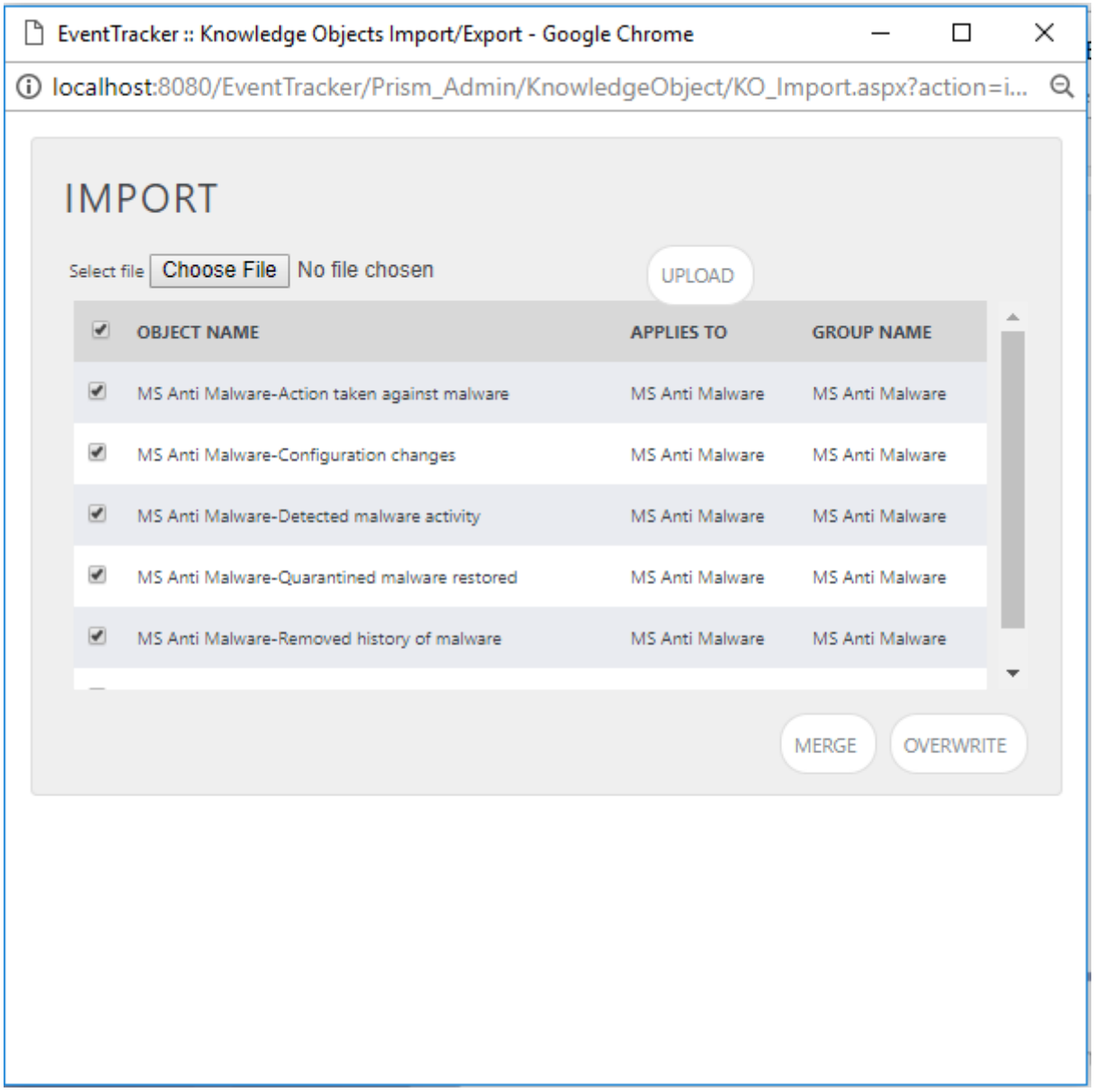


Figure 8

4. Knowledge objects are now imported successfully.

Figure 9

Flex Reports

1. Click **Reports** option, and then click the browse ... button.
2. Locate the **MS Antimalware reports.etcrx** file, and then click the **Open** button.

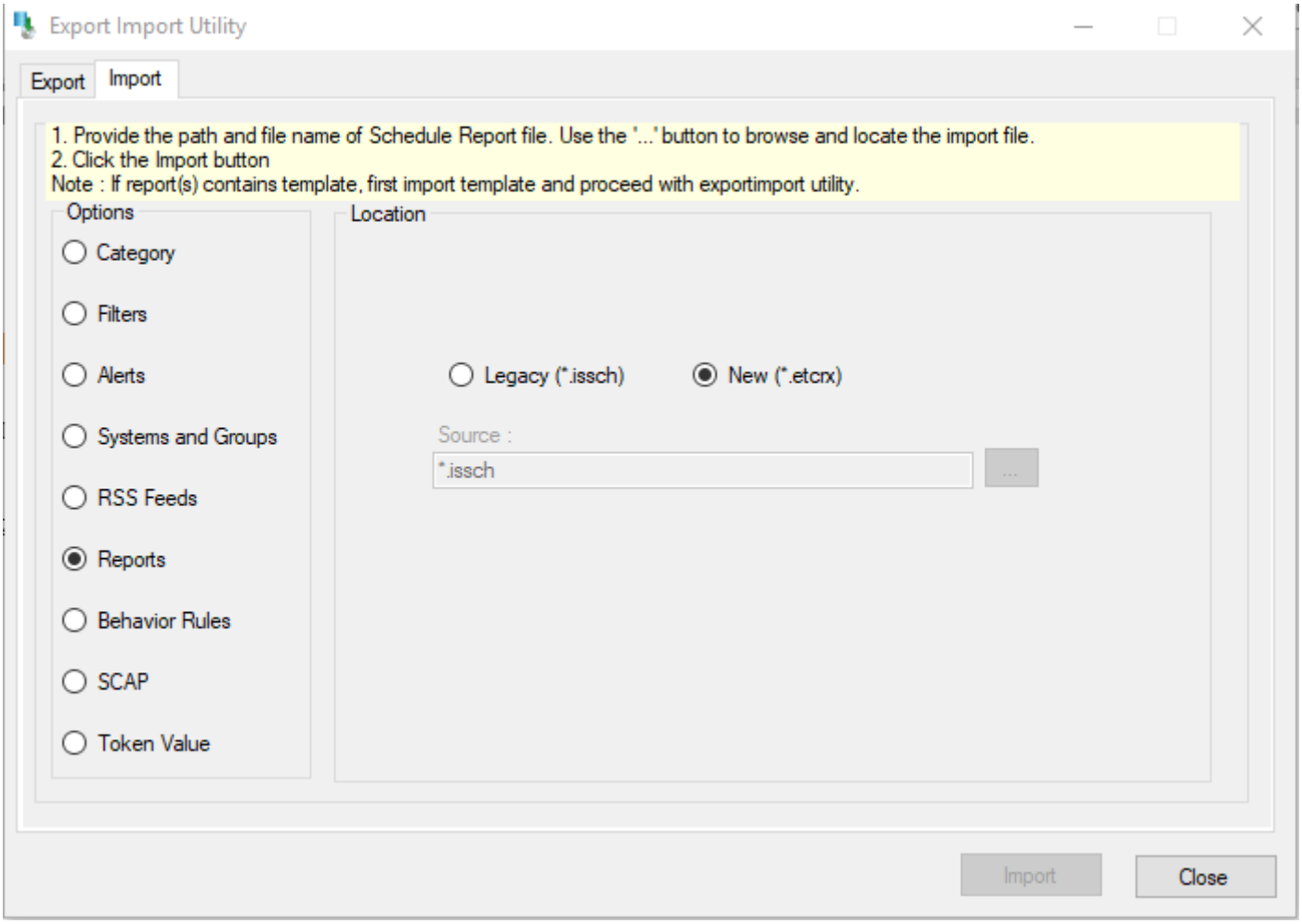


Figure 10

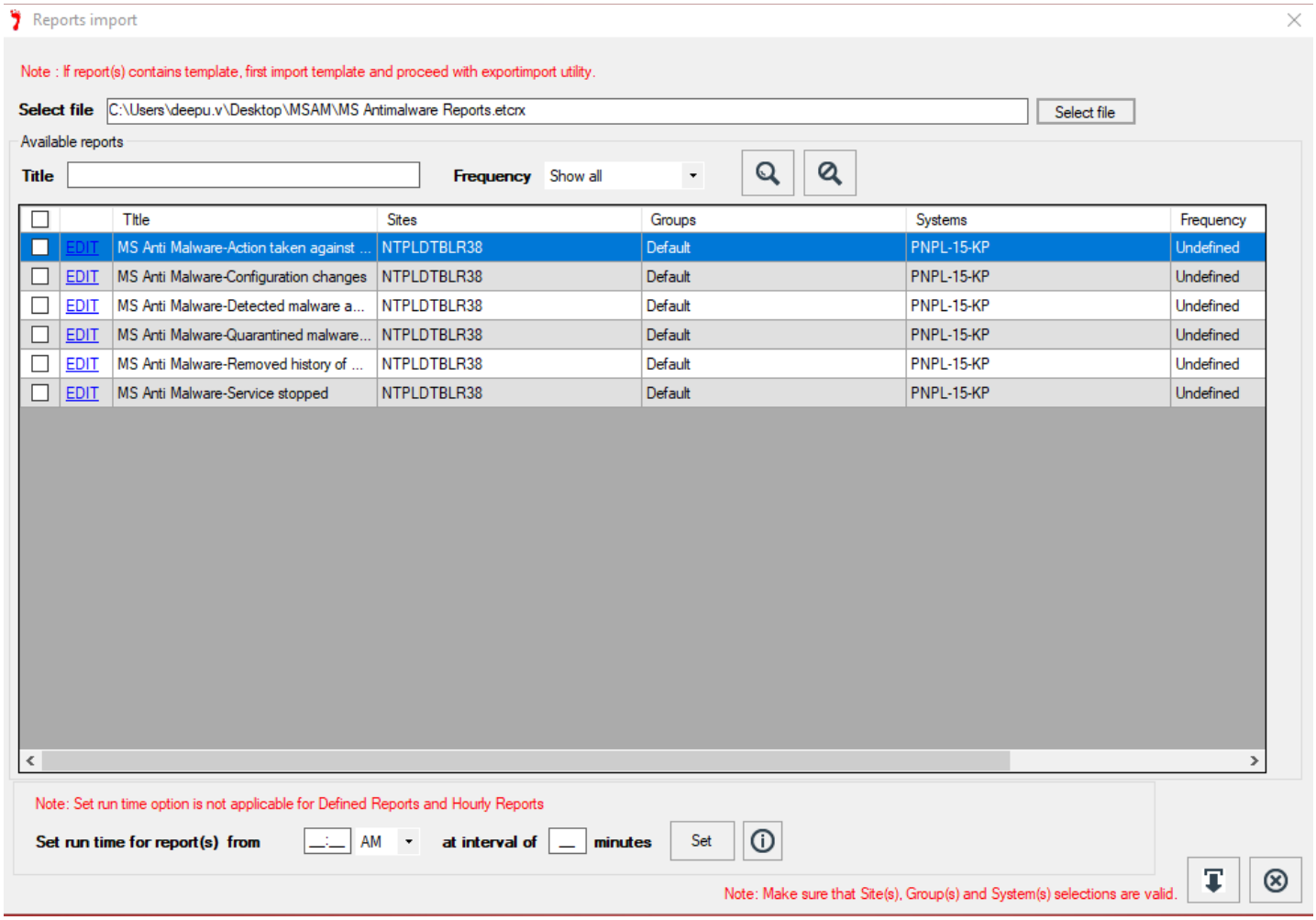


Figure 11

3. Click the **Import** button to import the **scheduled** reports. EventTracker displays success message.

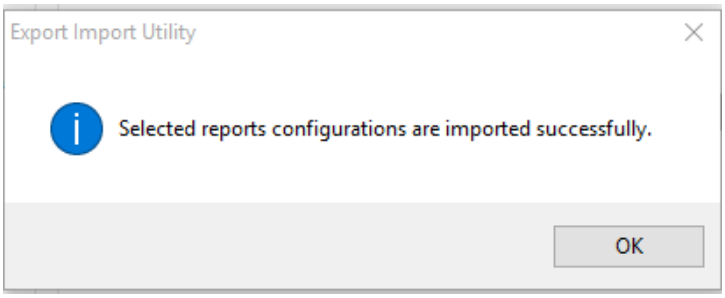


Figure 12

Parsing Rule

1. Click **Token Value** option, and then click the browse ... button.

2. Locate the **MS Antimalware Token Value.istoken** file, and then click the **Open** button.

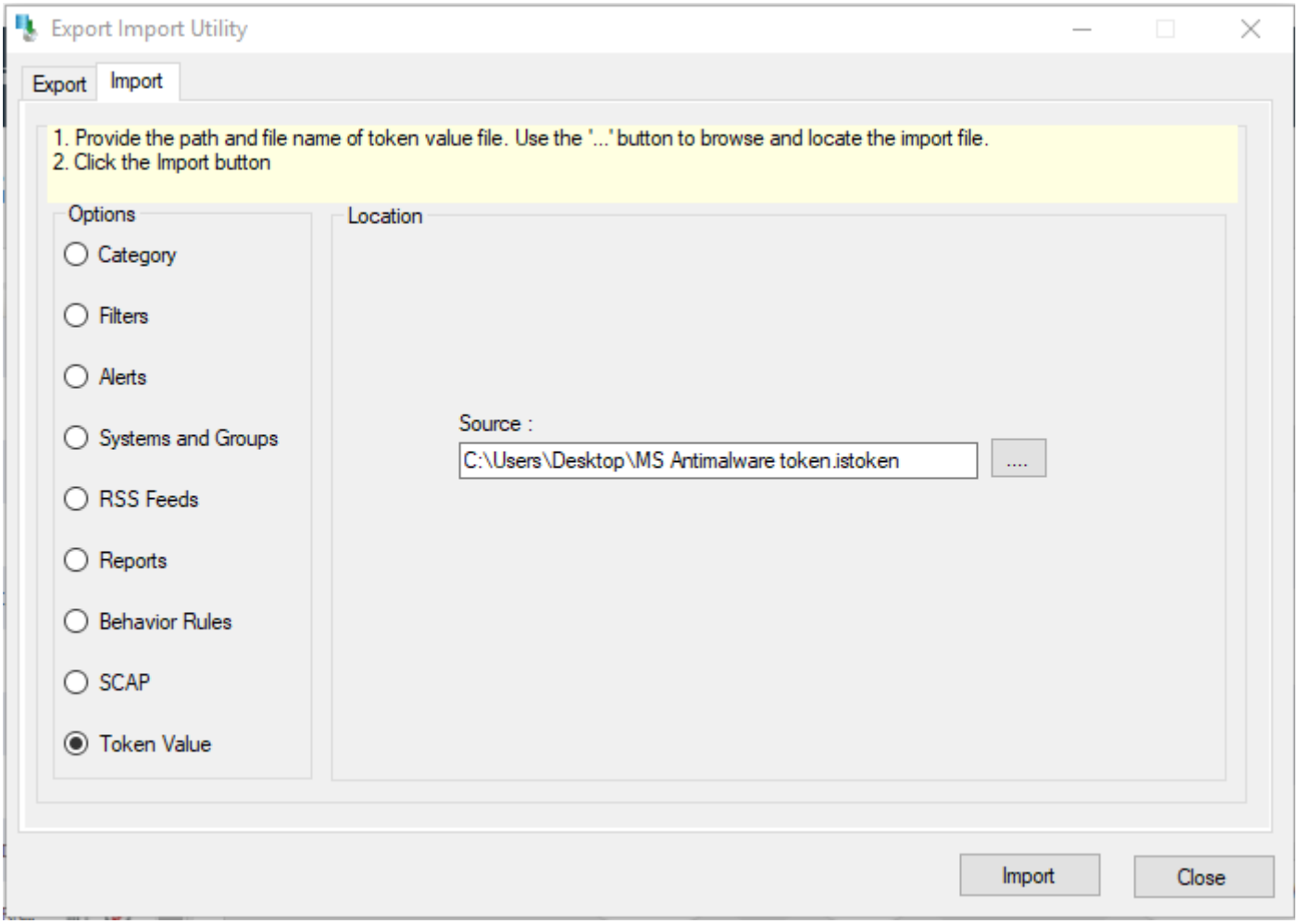


Figure 13

4. Click the **Import** button to import the tokens. EventTracker displays success message.

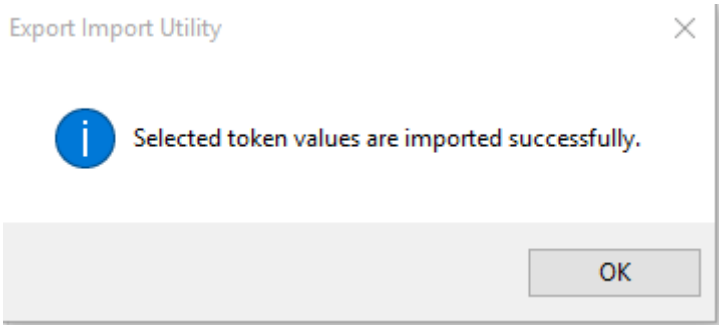


Figure 14

Verify MS Antimalware knowledge pack in EventTracker

Alerts

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Alerts**.
2. In the **Search** field, type **MS Antimalware**, and then click **Go** button.
3. Alert Management page will display the imported **MS Antimalware** alert.

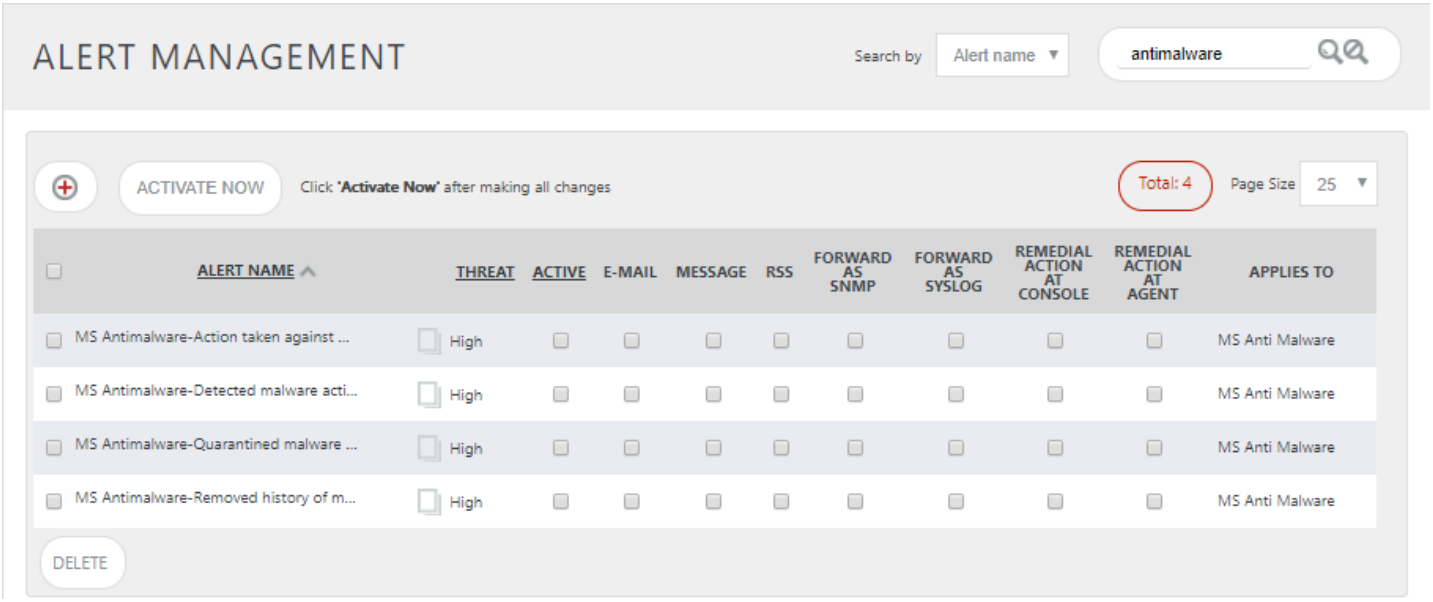


Figure 15

4. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

Figure 16

5. Click the **OK** button, and then click the **Activate now** button.

NOTE: You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.

Flex Reports

1. In the **EventTracker Enterprise** web interface, click the **Reports** menu, and then select **Configuration**.
2. In **Reports Configuration** pane, select **Defined** option.
3. In search box enter '**MS Antimalware**, and then click the **Search** button.
   EventTracker displays Flex reports of '**MS Antimalware**

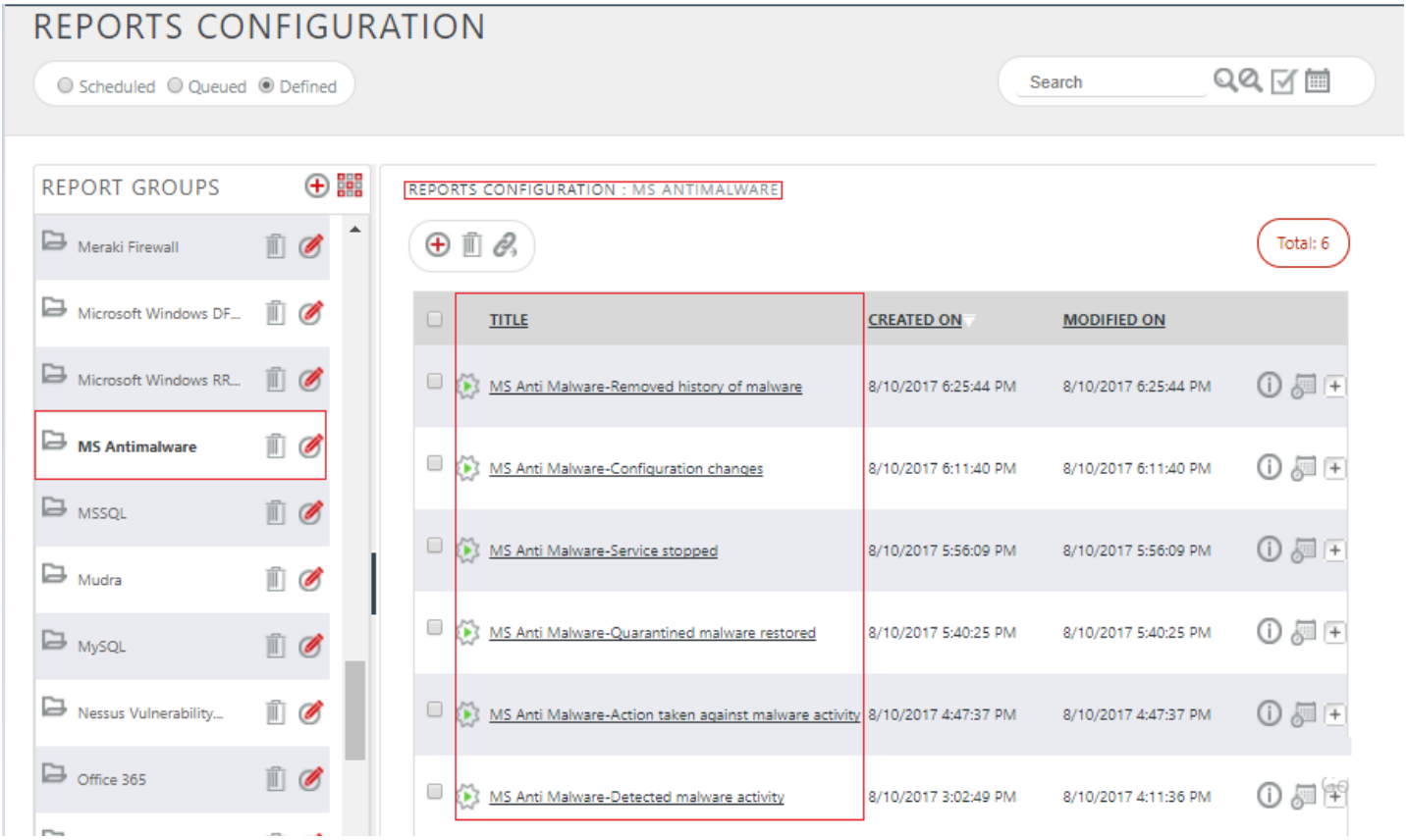


Figure 17

Parsing Rule

1. Logon to **EventTracker Enterprise** web interface.
2. Click the **Admin** menu, and then click **Parsing Rules.**
3. Click on **MS Antimalware** group option.

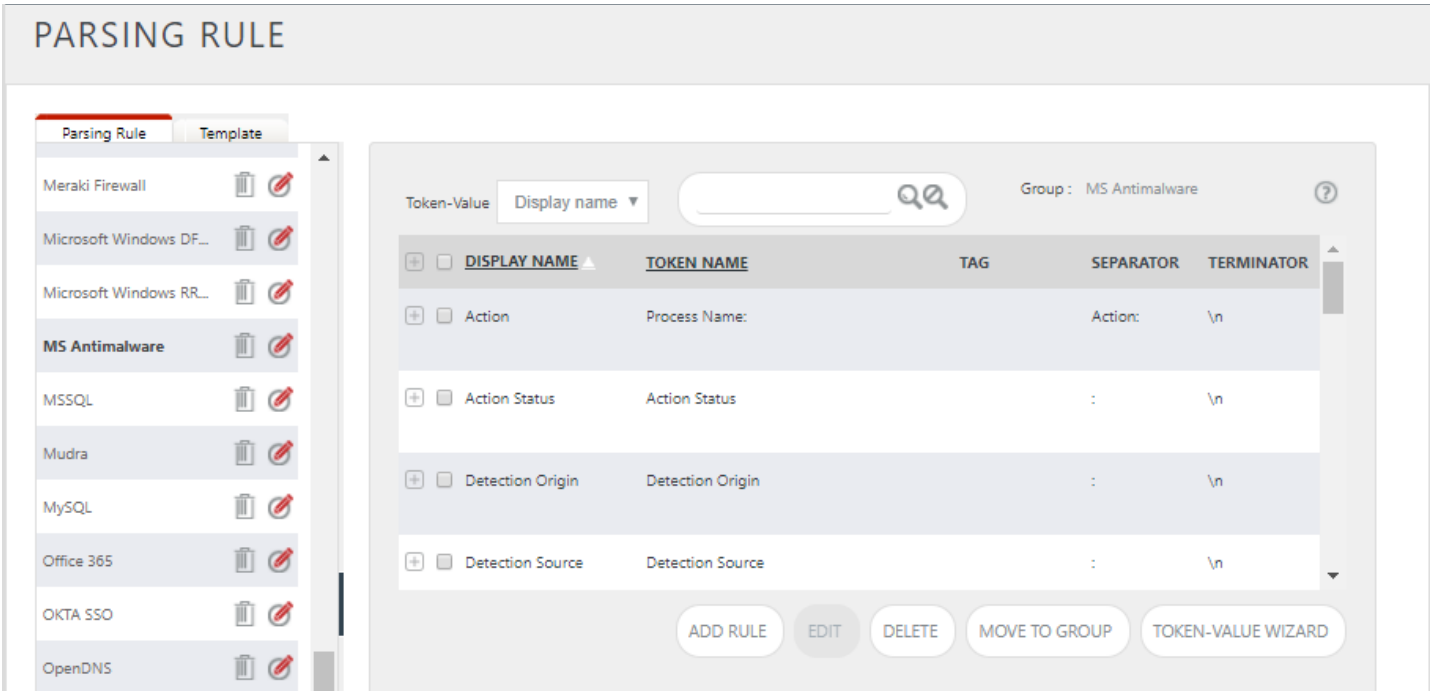


Figure 18

Create Flex Dashboards in EventTracker

NOTE: To configure the flex dashboards, schedule and generate the reports. Flex dashboard feature is available from EventTracker Enterprise v8.0.

Schedule Reports

1. Open **EventTracker** in browser and logon.

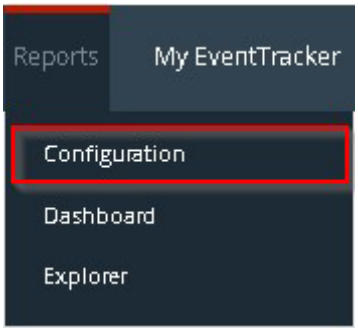


Figure 19

2. Navigate to **Reports>Configuration**.
3. Select **MS Antimalware** in report groups. Check **Defined** dialog box.

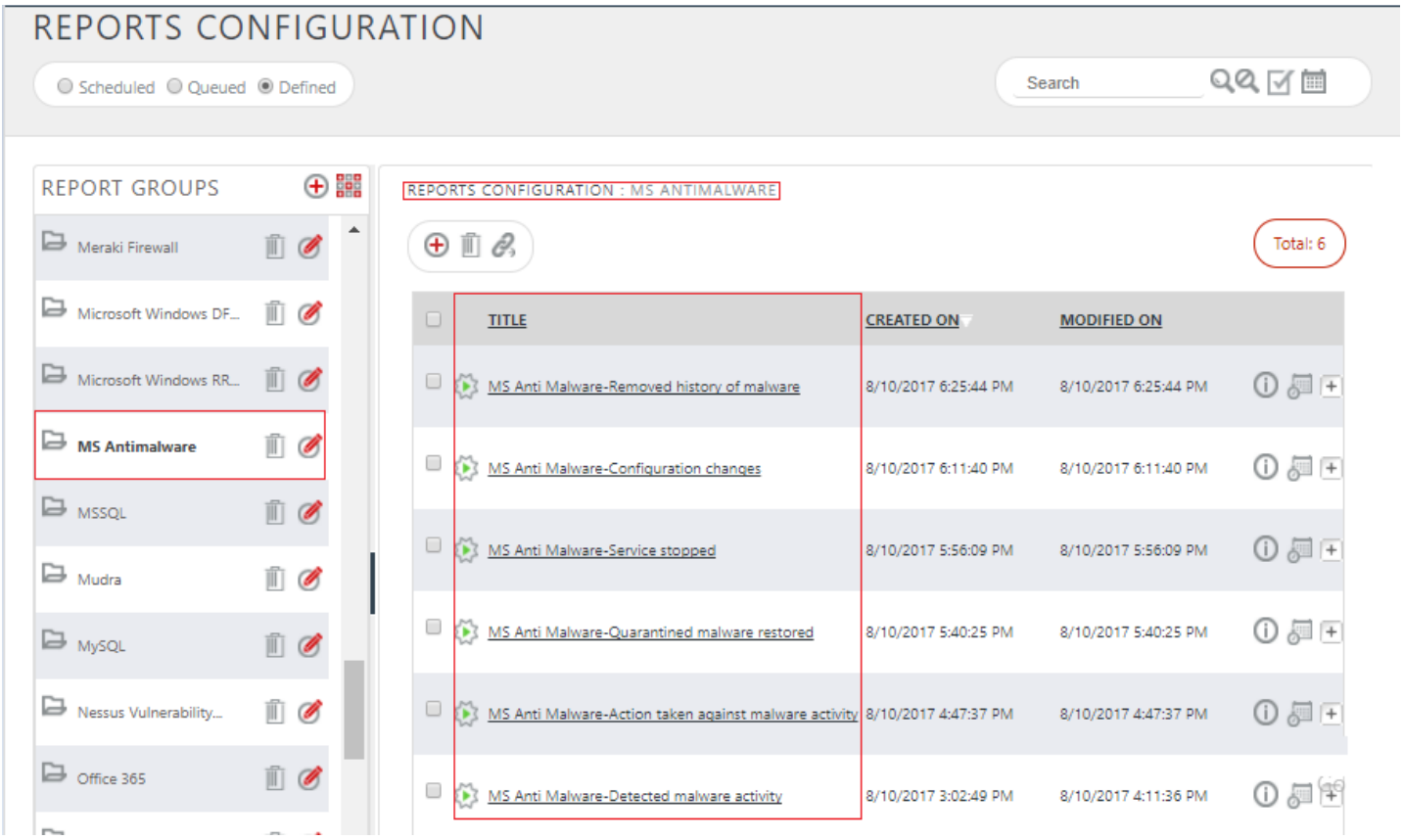


Figure 20

4. Click on '**schedule**'  to plan a report for later execution.
5. Click **Next** button to proceed.
6. In review page, check **Persist data in EventVault Explorer** option.

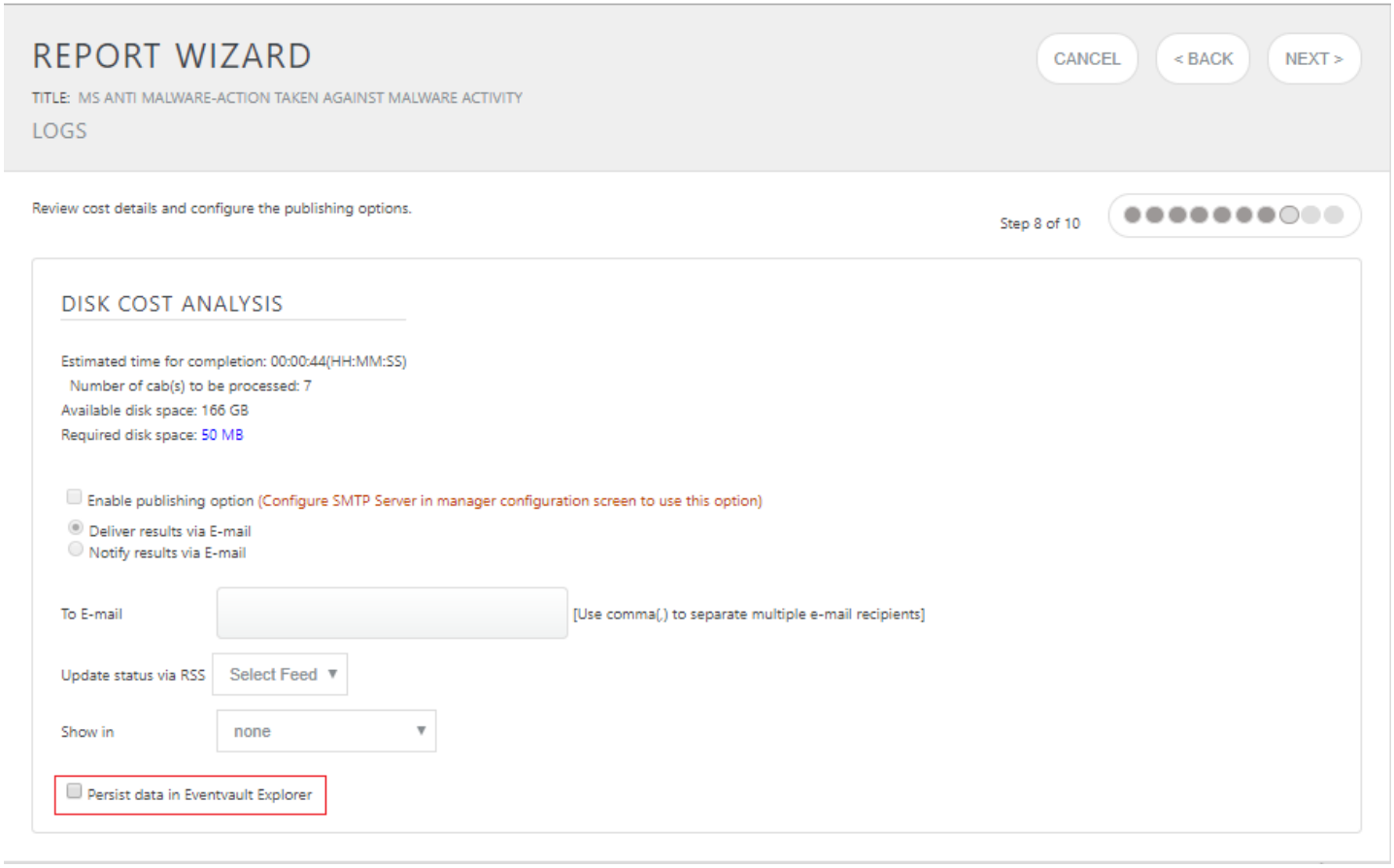


Figure 21

7. In next page, check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.

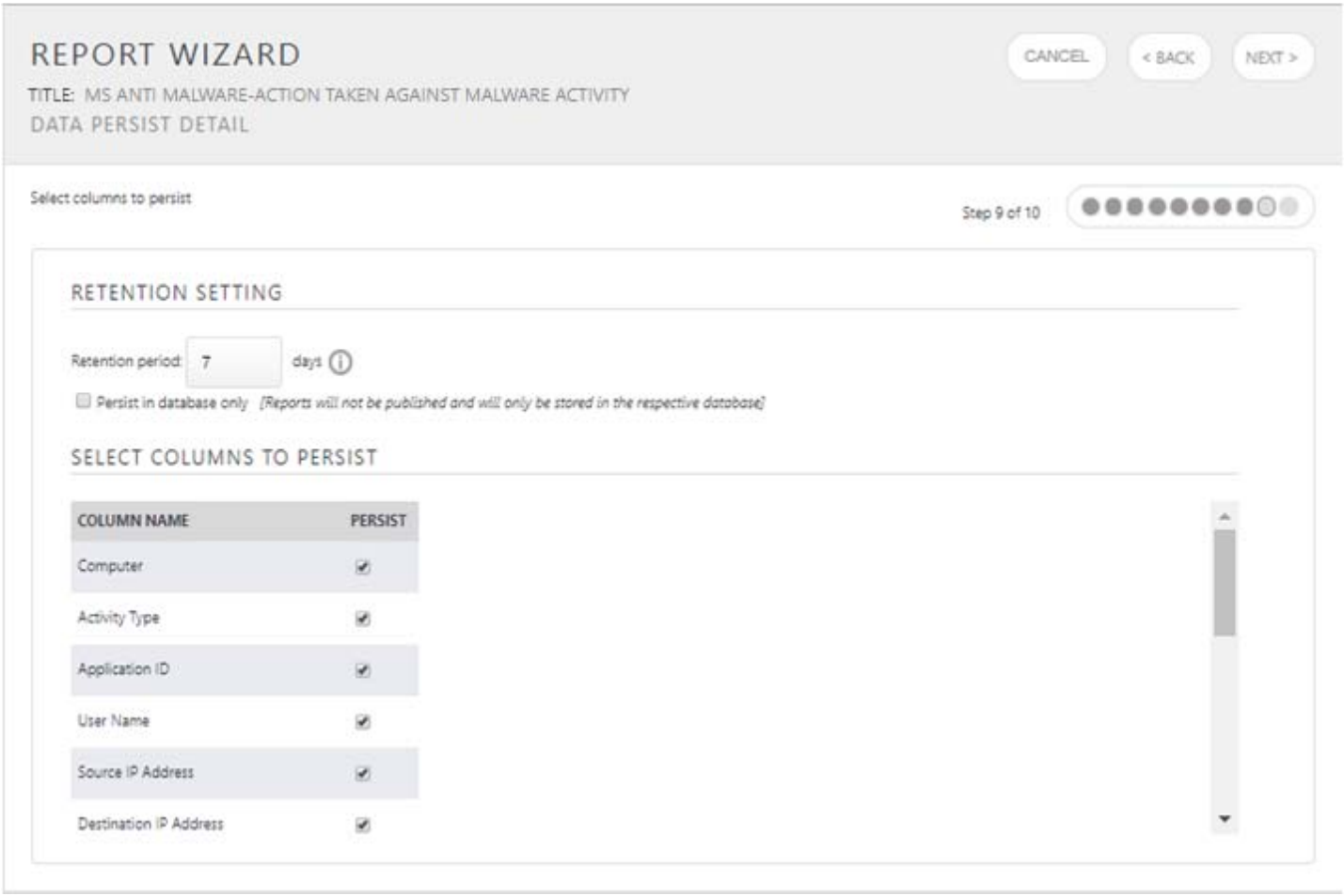


Figure 22

8. Proceed to next step and click **Schedule** button.
9. Wait till the reports get generated.

Create Dashlets

1. Open **EventTracker Enterprise** in browser and logon.

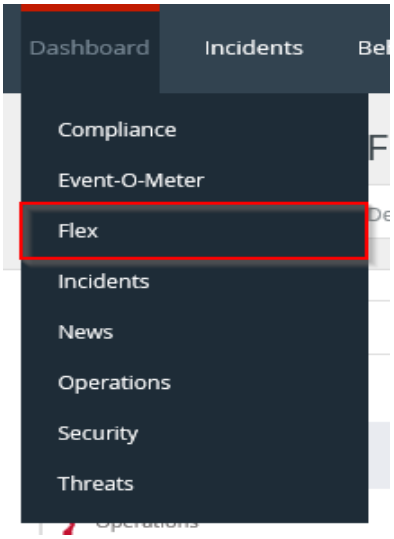


Figure 23

2. Navigate to **Dashboard>Flex**.
   Flex Dashboard pane is shown.

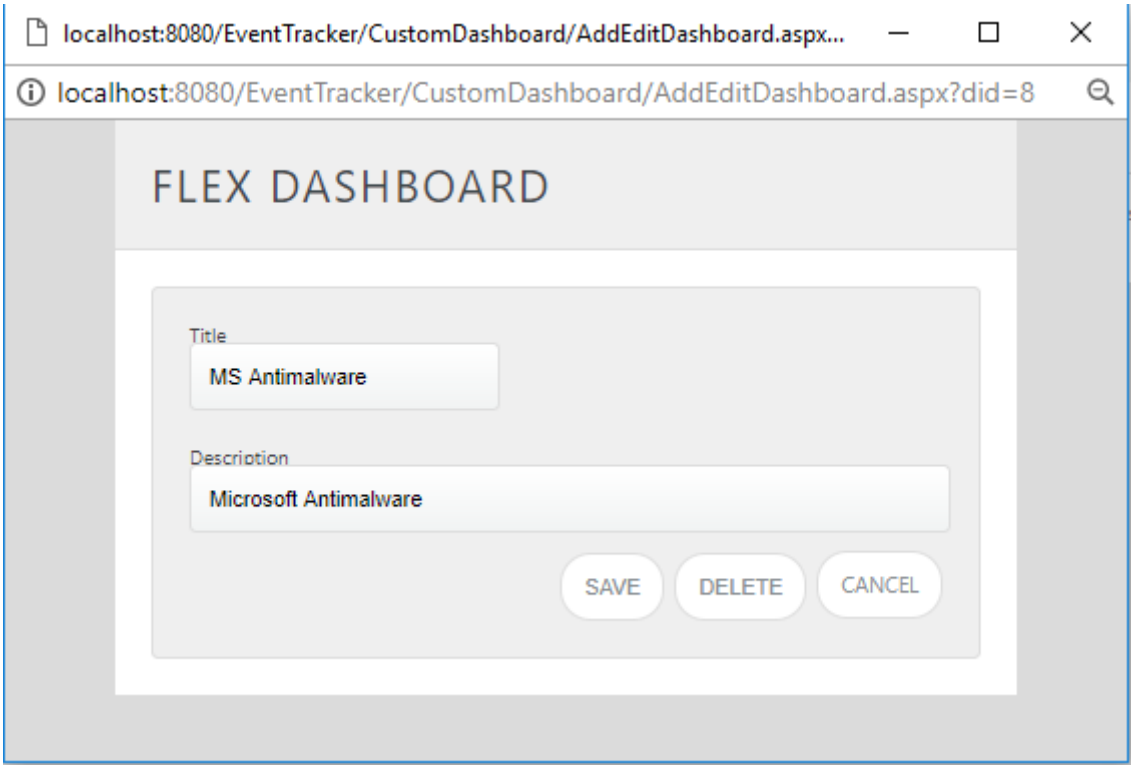


Figure 24

3. Fill suitable title and description and click **Save** button.
4. Click ⚙ to configure a new flex dashlet. Widget configuration pane is shown.

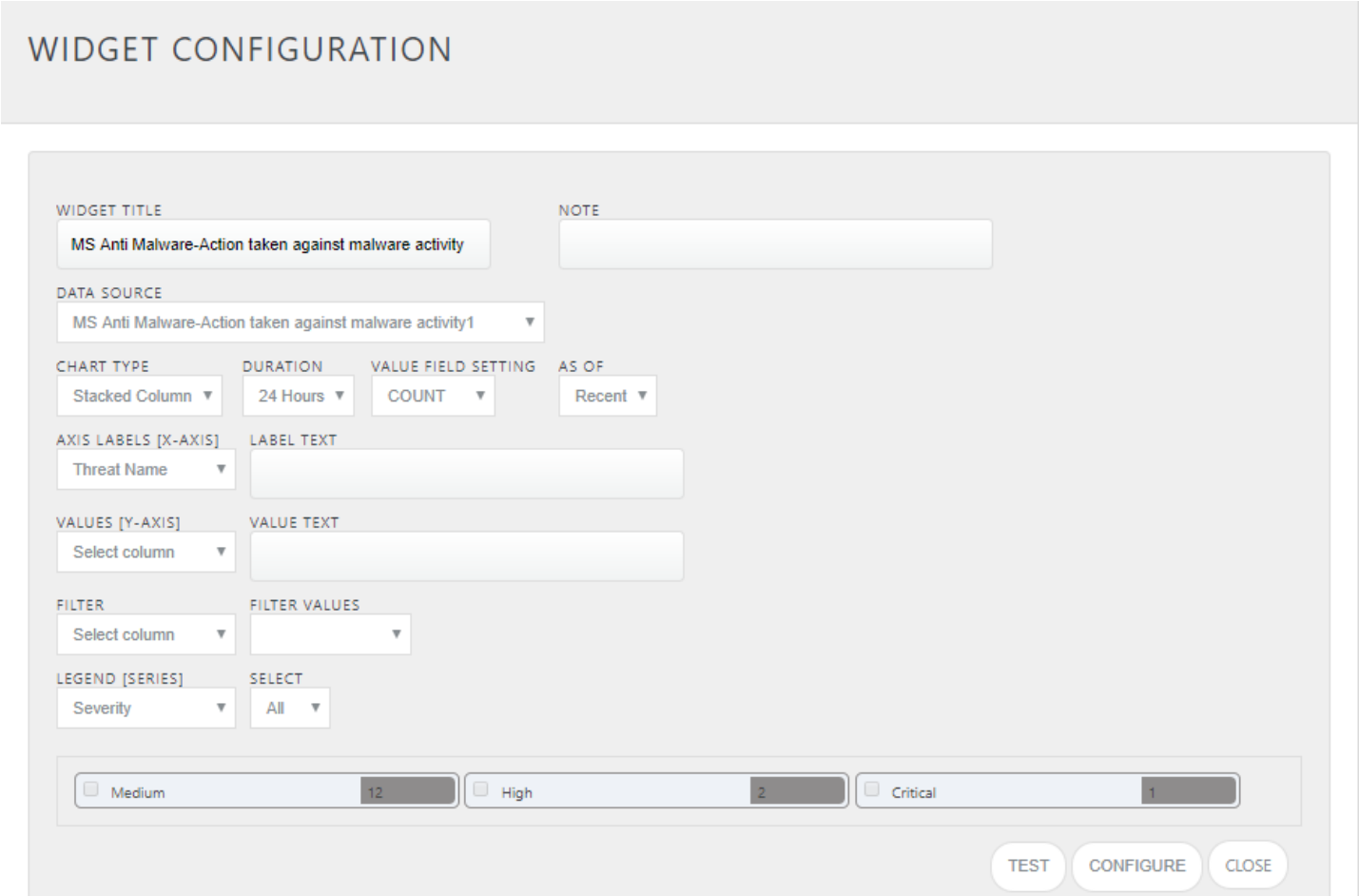


Figure 25

5. Locate earlier scheduled report in **Data Source** dropdown.
6. Select **Chart Type** from dropdown.
7. Select extent of data to be displayed in **Duration** dropdown.
8. Select computation type in **Value Field Setting** dropdown.
9. Select evaluation duration in **As Of** dropdown.
10. Select comparable values in **X Axis** with suitable label.
11. Select numeric values in **Y Axis** with suitable label.
12. Select comparable sequence in **Legend**.
13. Click **Test** button to evaluate. Evaluated chart is shown.

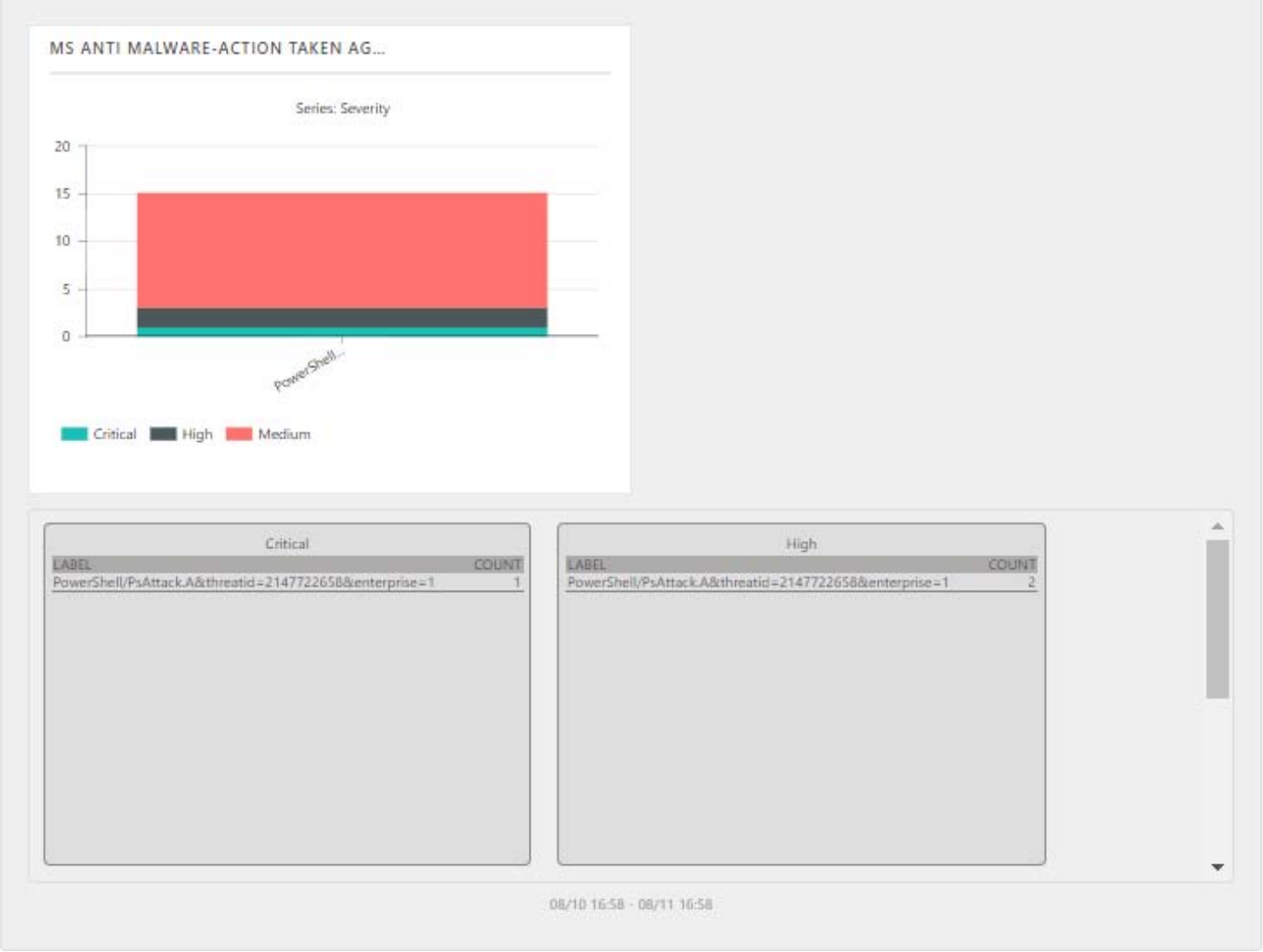


Figure 26

14. If satisfied, click **Configure** button.

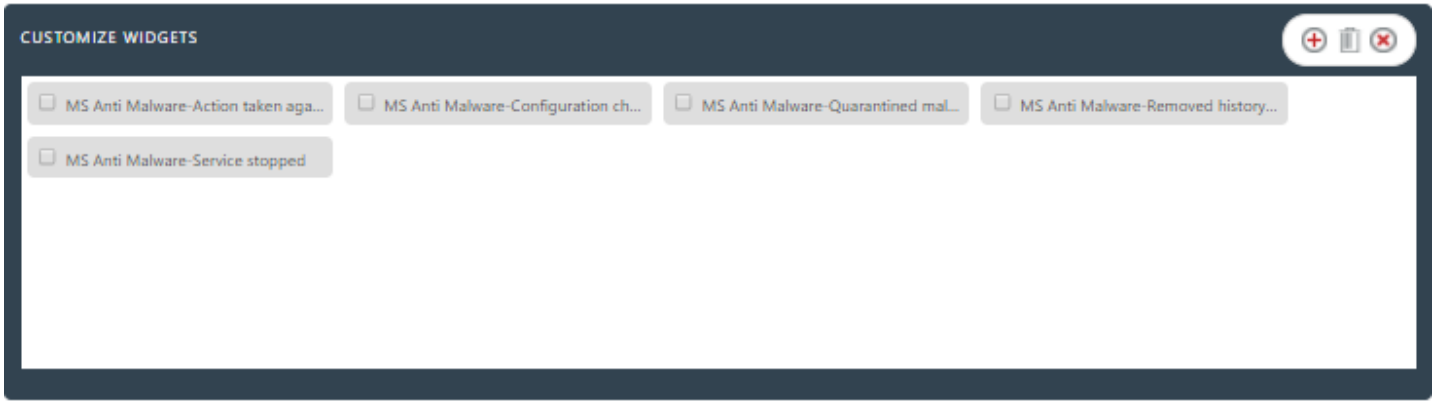
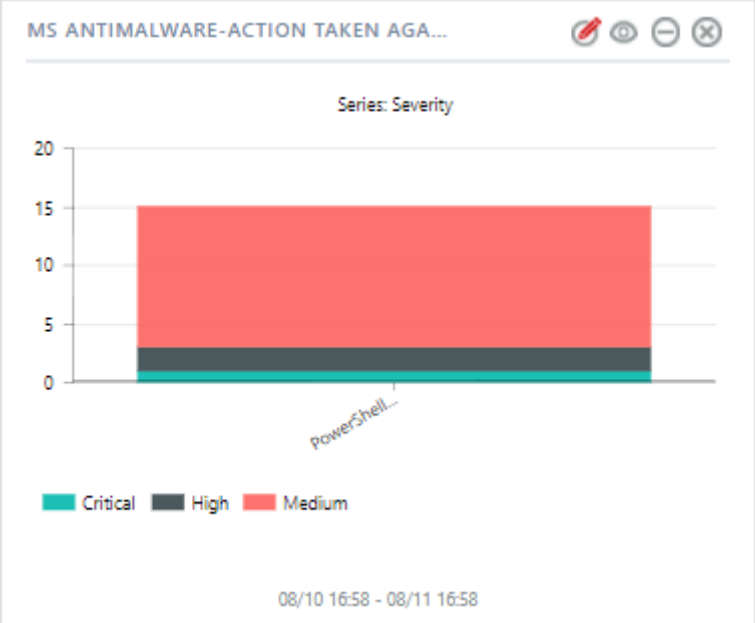


Figure 27

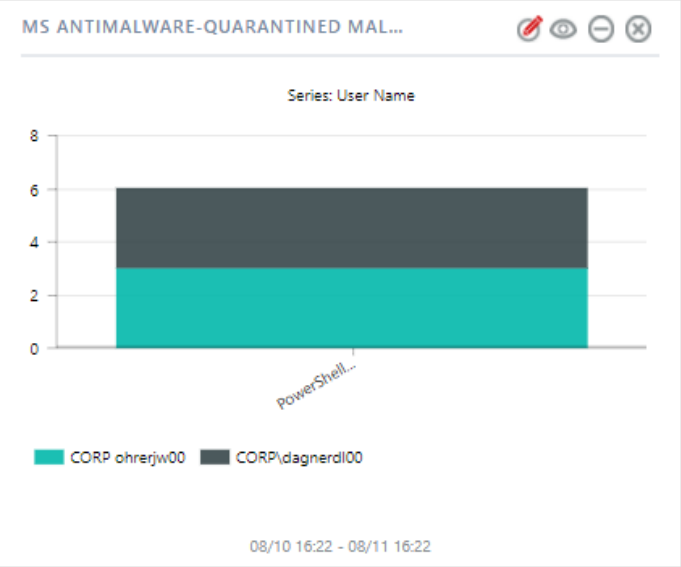
15. Click 'customize' to locate and choose created dashlet.
16. Click to add dashlet to earlier created dashboard.

Sample Flex Dashboards

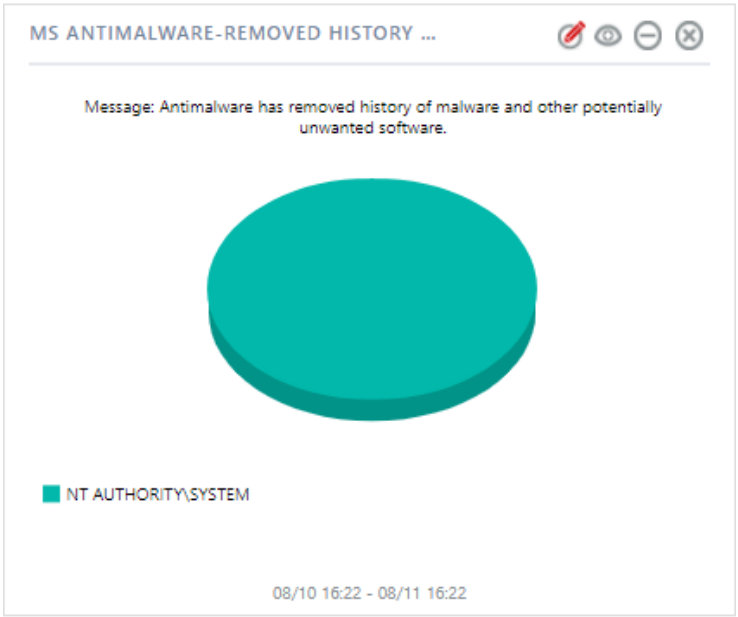
- **REPORT: MS Antimalware-Action taken against malware activity**
  WIDGET TITLE: MS Antimalware-Action taken against malware activity
  CHART TYPE: Stacked Column
  AXIS LABELS [X-AXIS]: Threat Name
  LEGEND [SERIES]: Severity



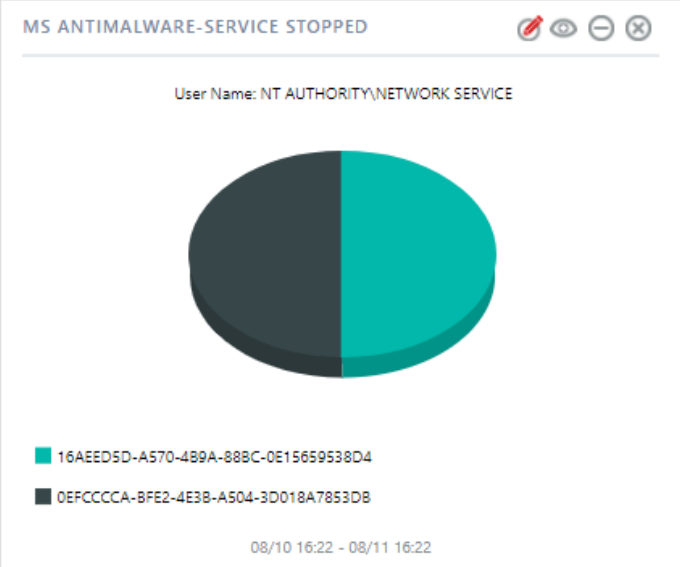
- **REPORT: MS Antimalware-Quarantined malware restored**
  WIDGET TITLE: MS Antimalware-Quarantined malware restored
  CHART TYPE: Stacked Column
  AXIS LABELS [X-AXIS]: Threat Name
  LEGEND [SERIES]: User Name



- **REPORT: MS Antimalware-Removed history of malware**
  WIDGET TITLE: MS Antimalware-Removed history of malware
  CHART TYPE: Donut
  AXIS LABELS [X-AXIS]: User Name
  LEGEND [SERIES]: Message



- **REPORT: MS Antimalware-Service stopped**
  WIDGET TITLE: MS Antimalware-Service stopped
  CHART TYPE: Pie
  AXIS LABELS [X-AXIS]: Scan Id
  LEGEND [SERIES]: User Name



- **REPORT: MS Antimalware-Configuration changes**
  WIDGET TITLE: MS Antimalware-Configuration changes
  CHART TYPE: Stacked Column
  AXIS LABELS [X-AXIS]: Old Value
  LEGEND: New Value