

Integrating Microsoft Windows DFS *EventTracker Enterprise*

Abstract

The purpose of this document is to help users in monitoring Microsoft Windows DFS by deploying Windows Agent.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise version 7.x** and later, and **Microsoft Windows Server 2003** and later.

Intended audience

Administrators, who are assigned the task to monitor and manage Microsoft Windows Server 2003 and later events, using EventTracker.

The information contained in this document represents the current view of Prism Microsystems Inc. on the issues discussed as of the date of publication. Because Prism Microsystems must respond to changing market conditions, it should not be interpreted to be a commitment on the part of Prism Microsystems, and Prism Microsystems cannot guarantee the accuracy of any information presented after the date of publication.

This document is for informational purposes only. Prism Microsystems MAKES NO WARRANTIES, EXPRESS OR IMPLIED, AS TO THE INFORMATION IN THIS DOCUMENT.

Complying with all applicable copyright laws is the responsibility of the user. Without limiting the rights under copyright, this paper may be freely distributed without permission from Prism, as long as its content is unaltered, nothing is added to the content and credit to Prism is provided.

Prism Microsystems may have patents, patent applications, trademarks, copyrights, or other intellectual property rights covering subject matter in this document. Except as expressly provided in any written license agreement from Prism Microsystems, the furnishing of this document does not give you any license to these patents, trademarks, copyrights, or other intellectual property.

The example companies, organizations, products, people and events depicted herein are fictitious. No association with any real company, organization, product, person or event is intended or should be inferred.

© 2016 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.

Table of Contents

Abstract..... 1

Scope..... 1

 Intended audience 1

Pre-requisite..... 3

Enable audit local group policy for DFS..... 3

EventTracker Agent configuration 6

EventTracker Knowledge Pack (KP)..... 9

 Categories 9

 Reports..... 9

 Alerts..... 10

 Dashboards..... 10

Import knowledge pack into EventTracker 11

 To import Alerts 12

 To import Category 13

 To import Tokens 14

 To import Flex Reports 15

 To Configure Flex Dashboard..... 16

Verify knowledge pack in EventTracker 20

 Verify Alerts 20

 Verify Categories..... 21

 Verify Tokens 22

 Verify Flex Reports..... 23

Sample Reports 24

Sample Dashboards..... 25

Overview

Distributed File System (DFS) is a set of client and server services that allow an organization, using [Microsoft Windows](#) servers, to organize many distributed SMB file shares into a distributed file system.

Distributed File System is implemented as a role service of the File Services role. Distributed File System consists of two role services:

- DFS Namespaces
- DFS Replication

Pre-requisite

Prior to configuring **Windows Server 2003 and later** and **EventTracker 7.x and later**, ensure that you meet the following prerequisites:

- Administrative access on EventTracker.
- User should have Administrative rights on Microsoft Windows DFS.

Enable audit local group policy for DFS

1. Run **gpedit.msc**
2. Open the **Group Policy Editor**.
3. Expand the Computer Configuration, and go to the node **Advanced Audit Policy Configuration (Computer Configuration->Policies->Windows Settings->Security Settings->Advanced Audit Policy Configuration)**
4. Expand this node, go to **Object Access (Audit Policies->Object Access)**, then select the setting **Audit Detailed File Share Audit, Audit File Share, Audit File System**.

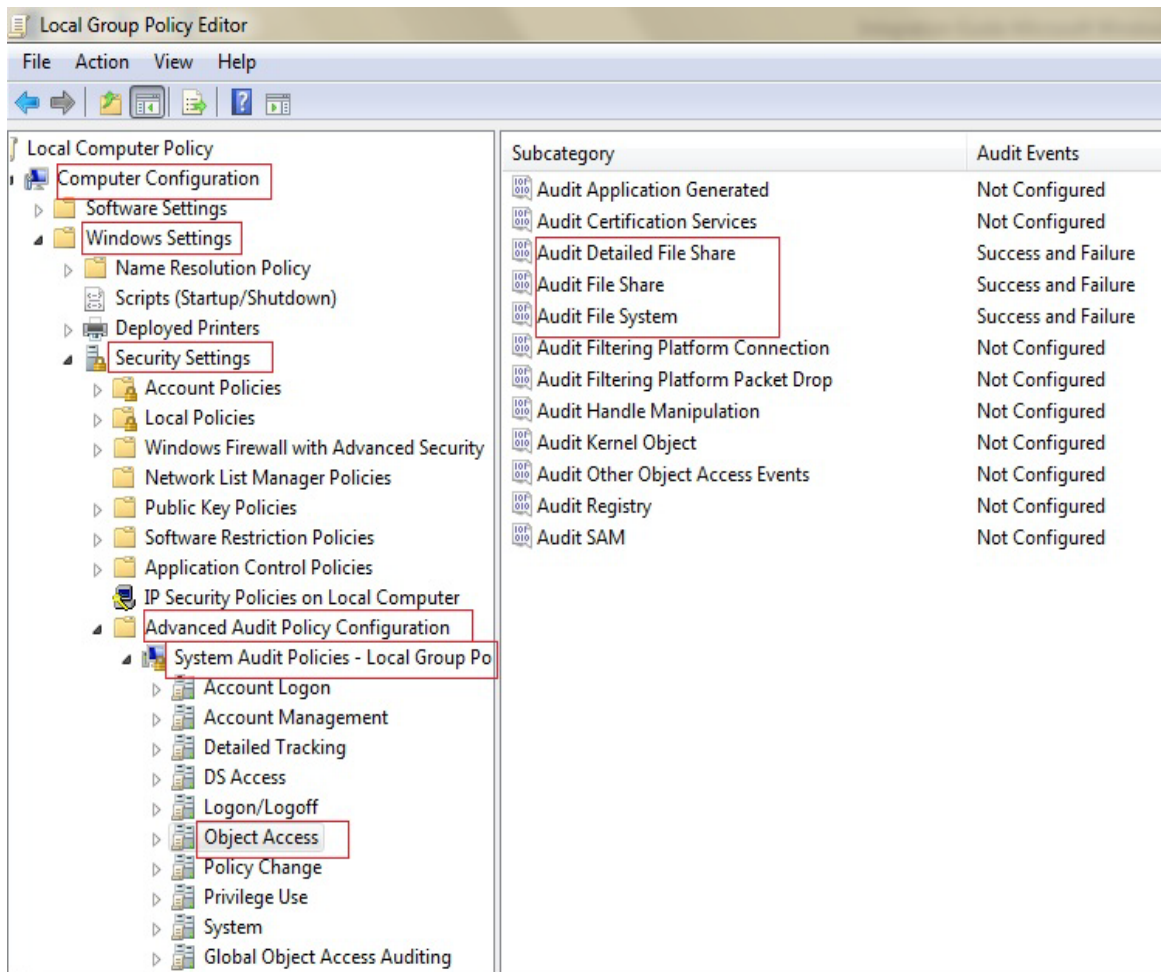


Figure 1

5. Select **Audit Detailed File Share**, right click and select **Properties**. In **Properties** console enable the check box to configure the following audit events: **Success** and **Failure**.

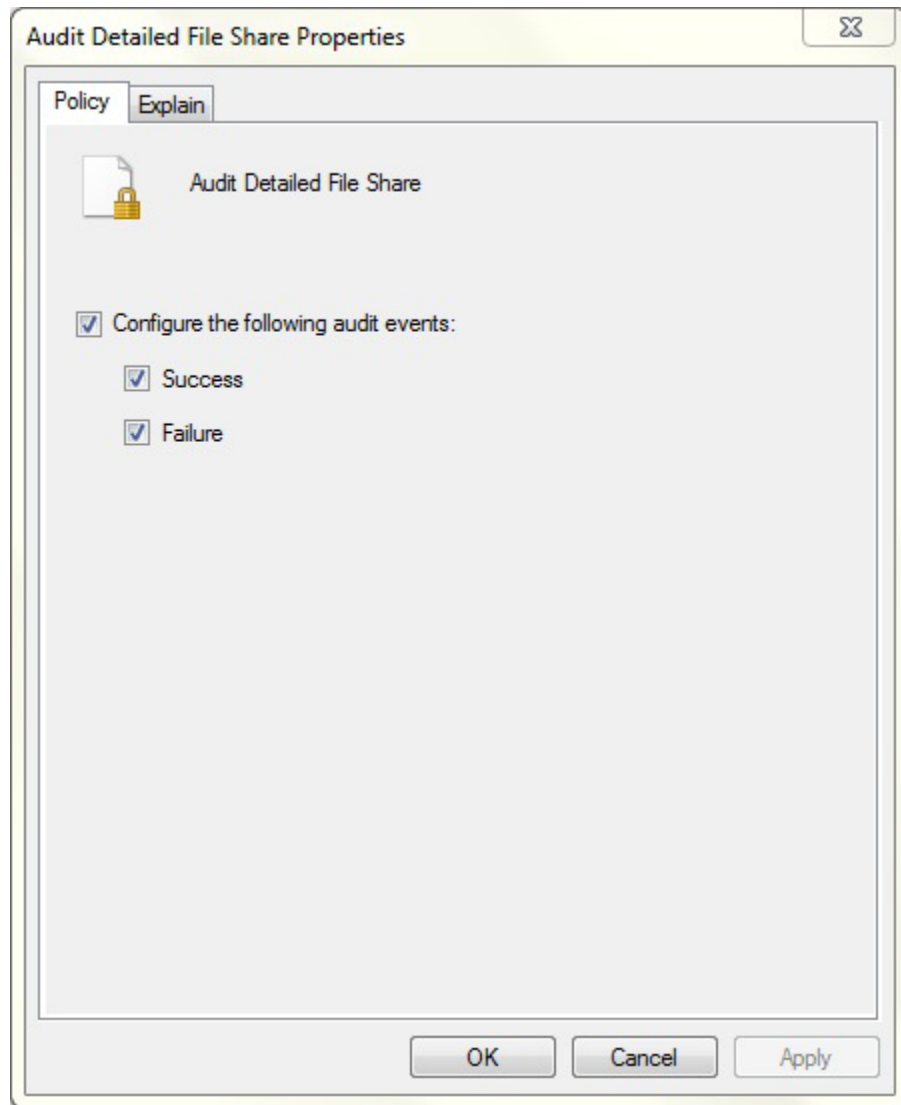


Figure 2

6. Repeat **Step 5** for **Audit File Share** and **Audit File System**.

EventTracker Agent configuration

1. Deploy EventTracker Agent in Microsoft Windows Distributed File Services Server, please follow the steps mentioned in [How to Install EventTracker and Change Audit](#).
2. Select the **Start >All Programs>Prism Microsystems> EventTracker**.
3. In **EventTracker Control Panel**, and select **EventTracker Agent Configuration**.
4. Select **Event Filters** tab, and then click the **Filter Exception** button.

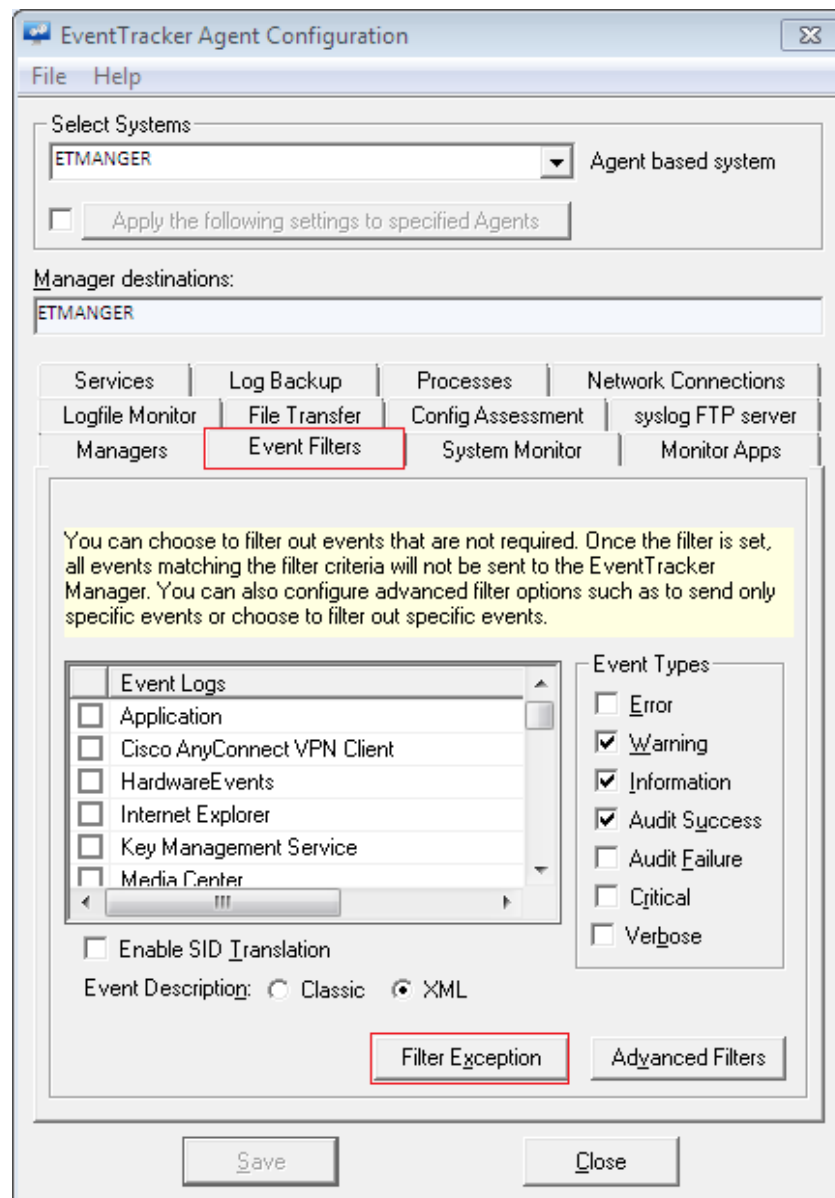


Figure 3

Filter Exception window displays.

- Click the **New** button.

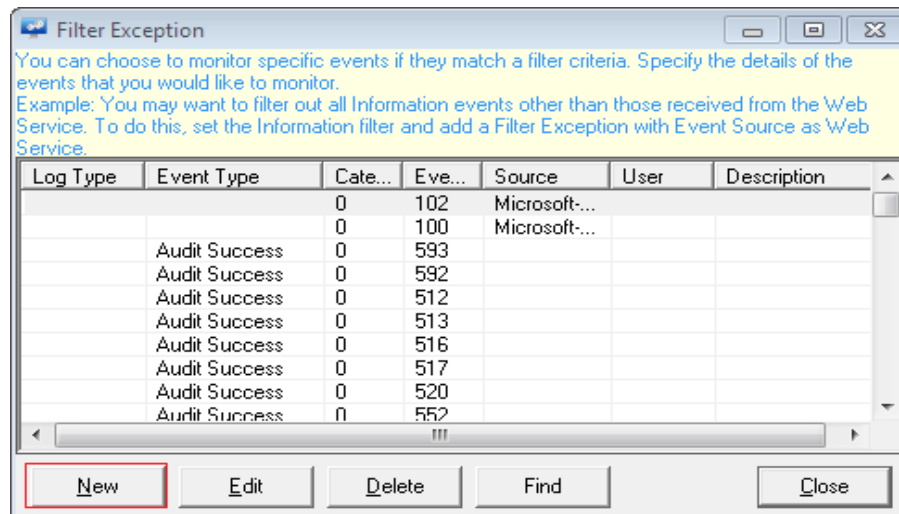


Figure 4

Event Details window displays.

- In **Match in Source:** box, enter 'Microsoft-Windows-Security-Auditing' and specify **Event ID:** 5140.

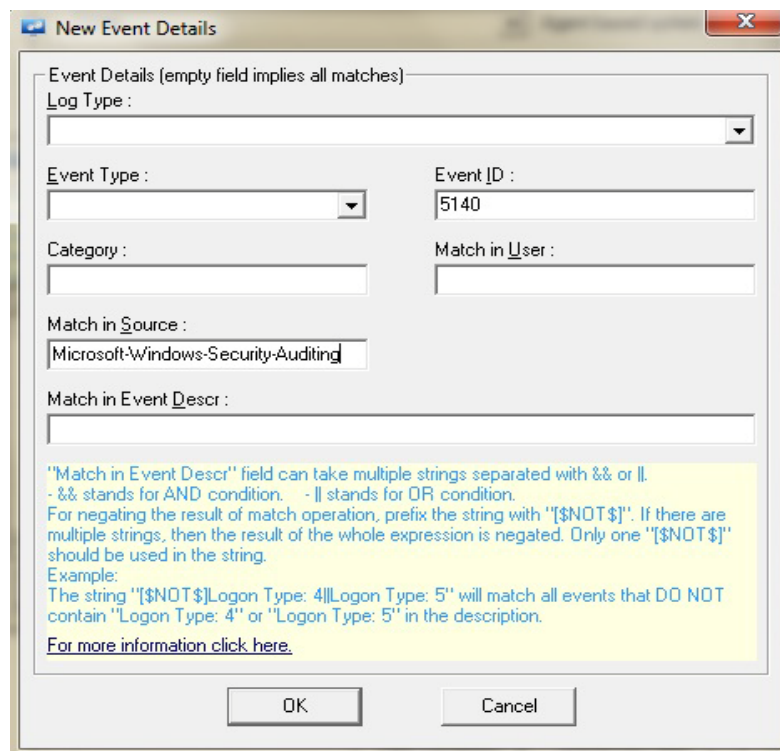


Figure 5

7. Click the **OK** button.
8. **Save** the configuration and **Close** the EventTracker Agent Configuration window.

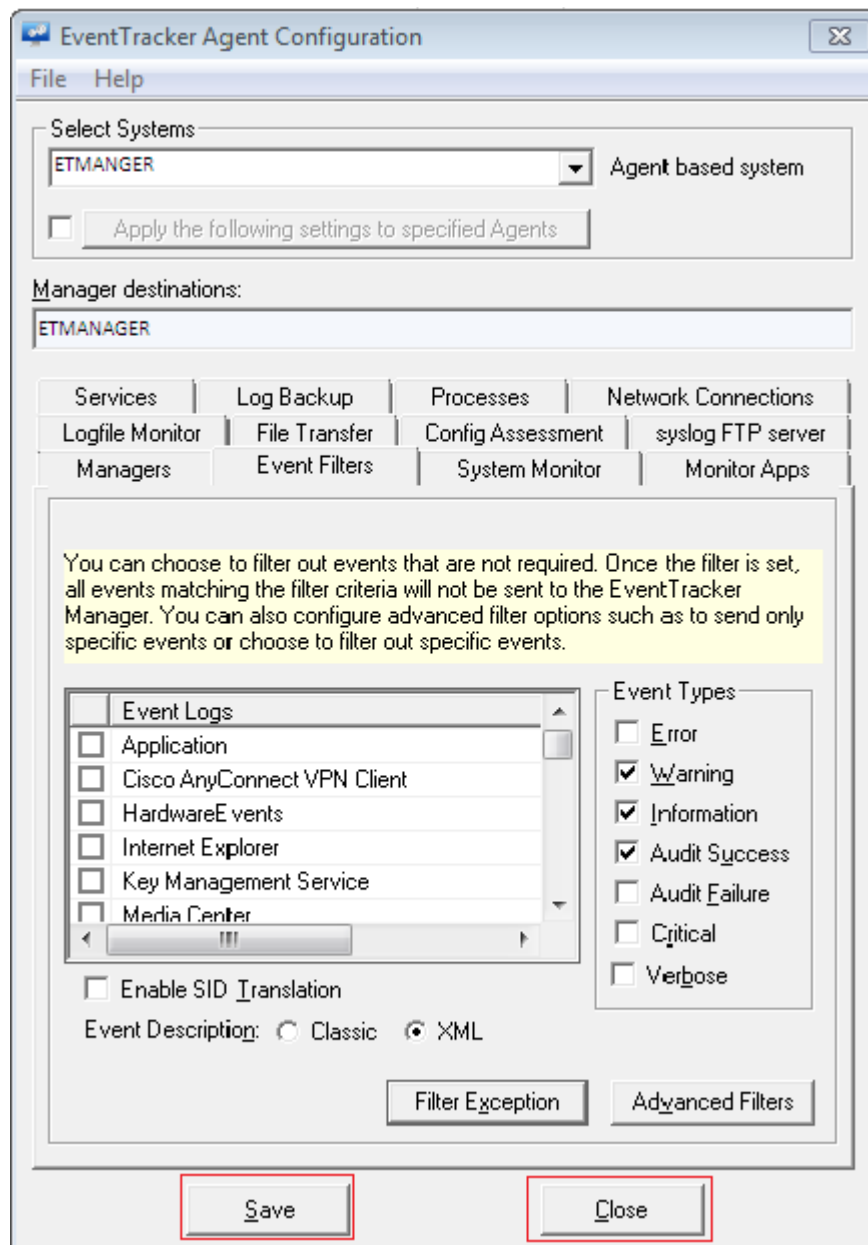


Figure 6

EventTracker Knowledge Pack (KP)

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

The following Knowledge Packs are available in EventTracker Enterprise to support Distributed File System.

Categories

- **Microsoft Windows DFS: User logon** - This category based report provides information related to users whose account was successfully logged on.
- **Microsoft Windows DFS: Network share object accessed** - This category based report provides information related to account details, network information , shared path details and related accesses.
- **Microsoft Windows DFS: Auditing setting changed** - This category based report provides information related to when admin change the audit SACL of an object, such as file or folder auditing settings on object were changed.
- **Microsoft Windows DFS: Client desired access** - This category based report provides information related to a network share object that was checked to see whether client can be granted desired access or not granted.
- **Microsoft Windows DFS: Namespace activity** – This category based report provides information related to whether DFS has connected to active directory or facing any issues while connecting and also whether server has finished initialization of building namespaces.
- **Microsoft Windows DFS: Replication activity** – This category based report provides information related to replication initialization, replicated folder information and replicated folder violation details.

Reports

- **Microsoft Windows DFS: User logon** - This report provides information related to DFS login which includes columns such as account name, account domain, login type, source address, source port and workstation name.

- **Microsoft Windows DFS: Network share object accessed** - This report provides information related to network share object accessed which includes columns such as account name, account domain, object type, source address, source port, share name, share path and accesses.
- **Microsoft Windows DFS: Auditing setting changed** - This report provides information related to auditing setting changed which includes columns such as account name, account domain, object server, object type, object name and new security descriptor details.
- **Microsoft Windows DFS: Client desired access** - This report provides information related to client desired access which includes columns such as account name, account domain, object type, source address, source port, share name, share path, relative target name, access request information and access check results and whether desired access is granted or not granted.
- **Microsoft Windows DFS: Namespace activity** - This report provides information related to namespace activity which includes shared folder details located at dfsroots.
- **Microsoft Windows DFS: Replication activity** – This report provides information related replication activity which includes replicated folder root, file path, replicated folder name and replicated group name.

Alerts

- **Microsoft Windows DFS: Namespace active directory issues** - This alert is generated when DFS server fails to contact domain controller, active directory and unable to access private data from active directory.
- **Microsoft Windows DFS: Replication stopped** - This alert is generated when DFS replication service stops replication on the replicated folder.

Dashboards

- **Microsoft Windows DFS: User logon** – This dashboard give us the information about users, whose account was successfully logged on.

Import knowledge pack into EventTracker

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

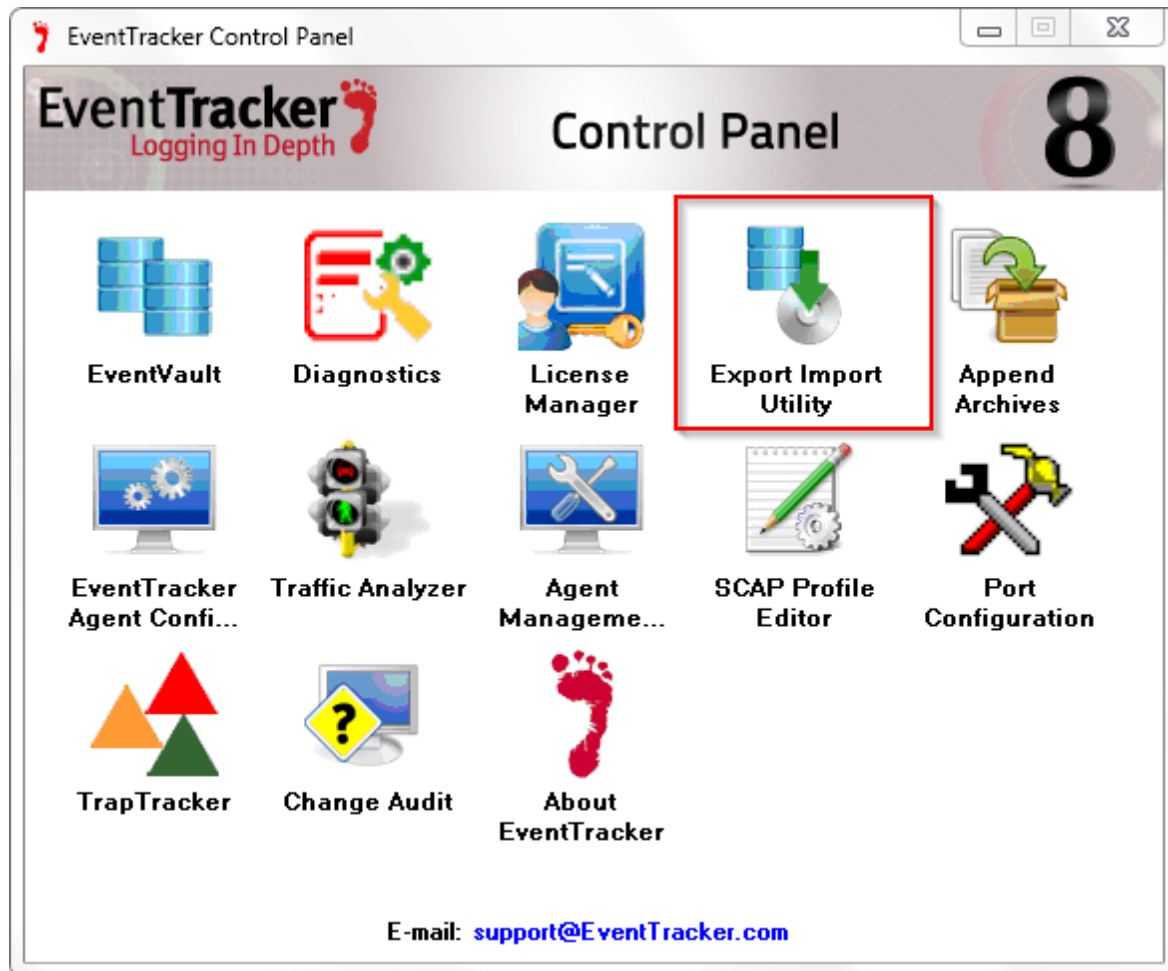



Figure 7

Import **Alerts/Category/Tokens/ Flex Reports** as given below.

To import Alerts

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

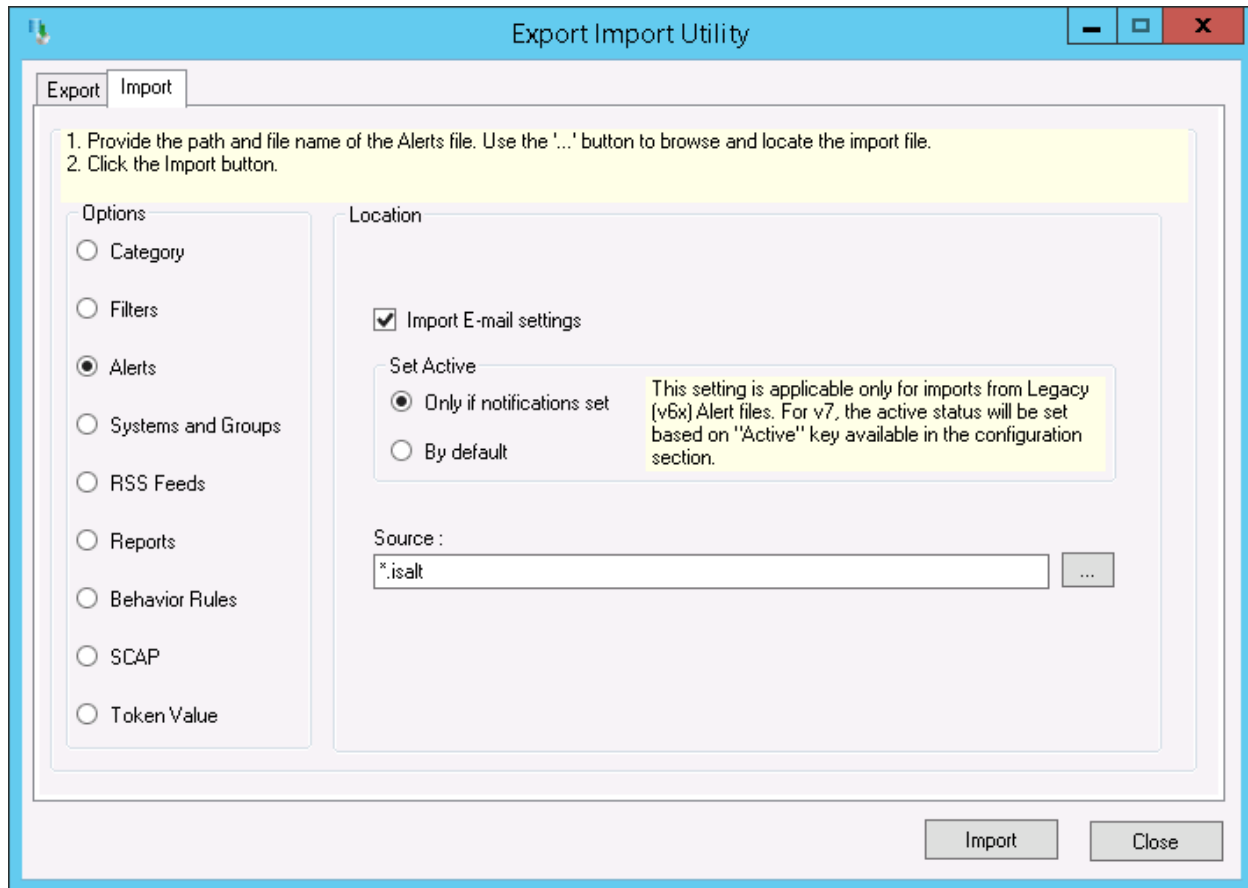


Figure 8

2. Locate **Microsoft Windows DFS.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

EventTracker displays success message.

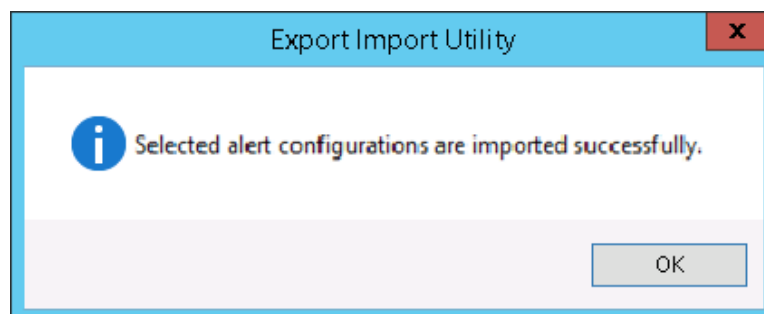


Figure 9

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

To import Category

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

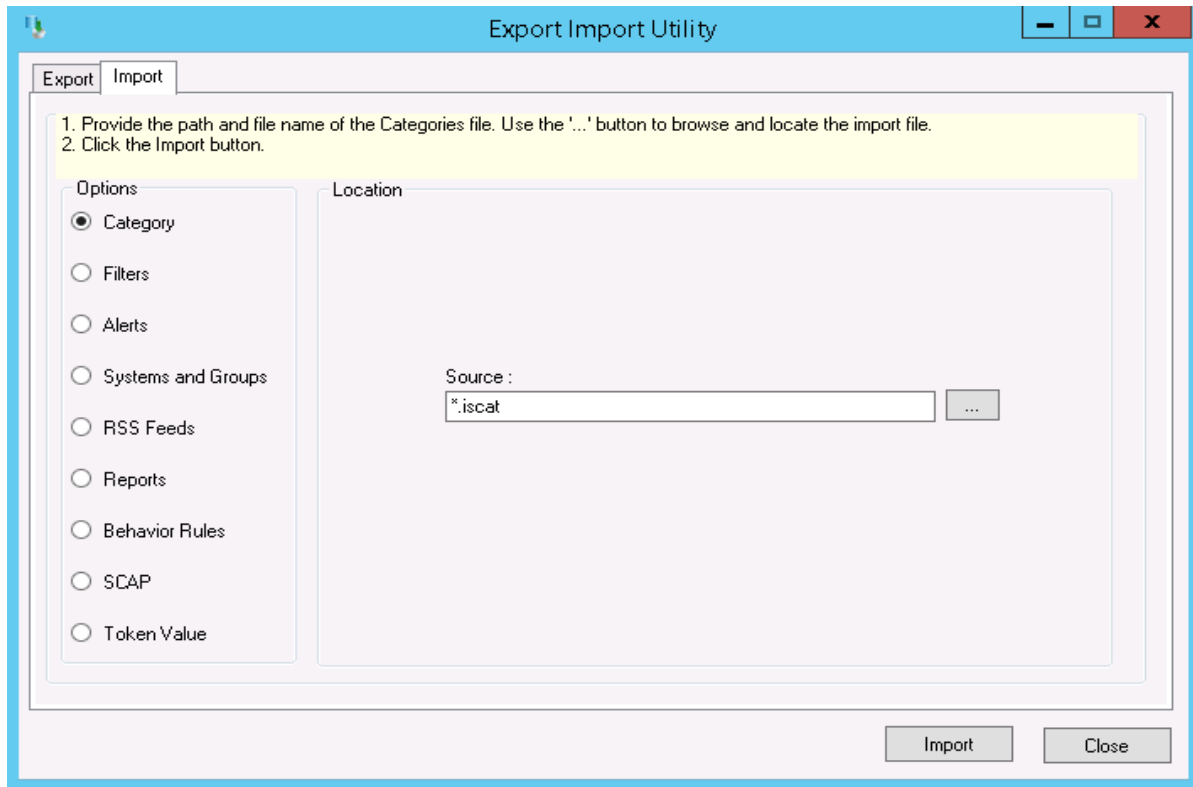


Figure 10

2. Locate Microsoft Windows DFS.**iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.

EventTracker displays success message.

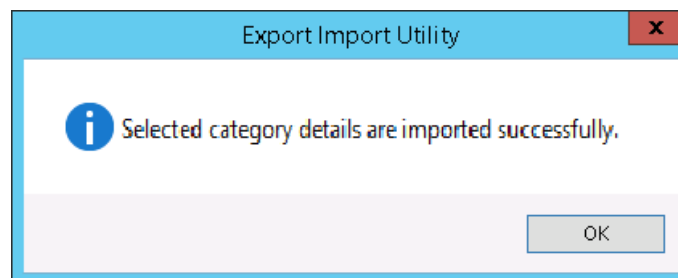



Figure 11

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

To import Tokens

- Click **Token value** option, and then click the browse  button.

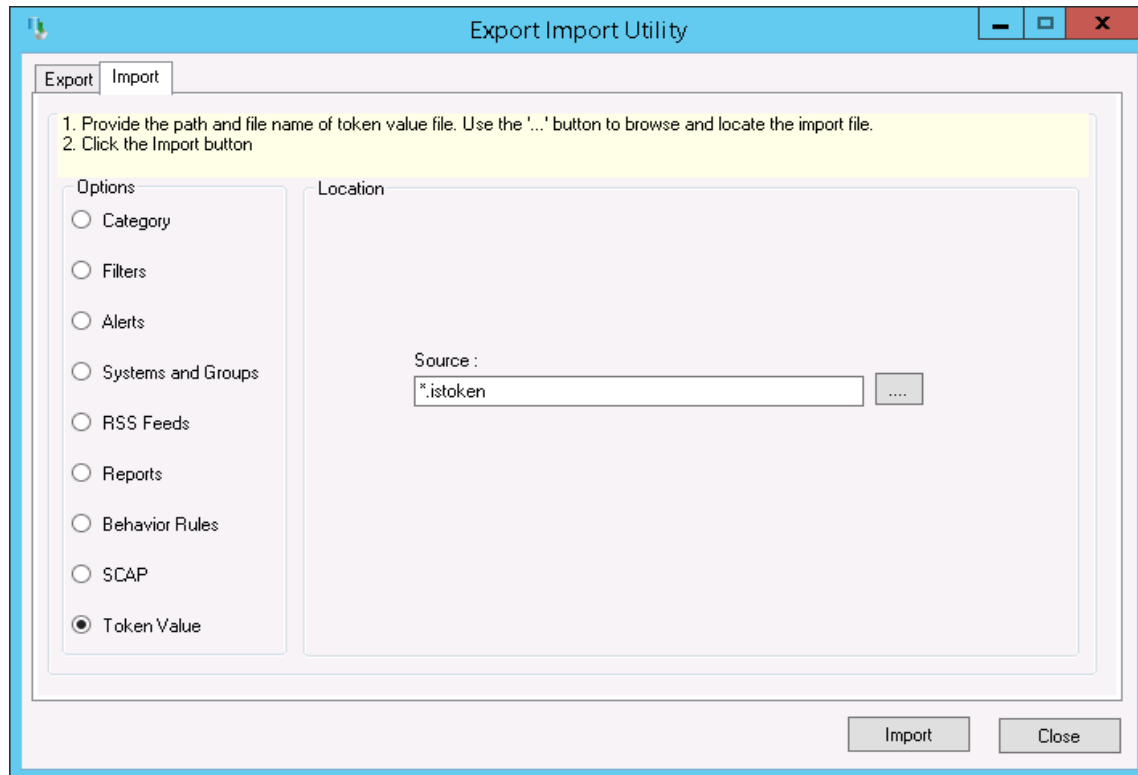


Figure 12

- Locate the **Microsoft Windows DFS.istoken** file, and then click the **Open** button.
- To import tokens, click the **Import** button.

EventTracker displays success message.

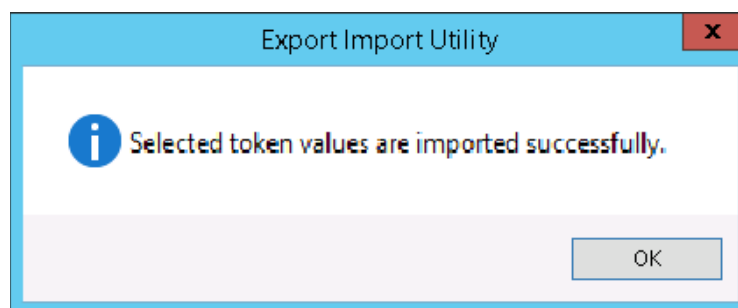



Figure 13

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

To import Flex Reports

- Click **Report** option, and then click the browse  button.

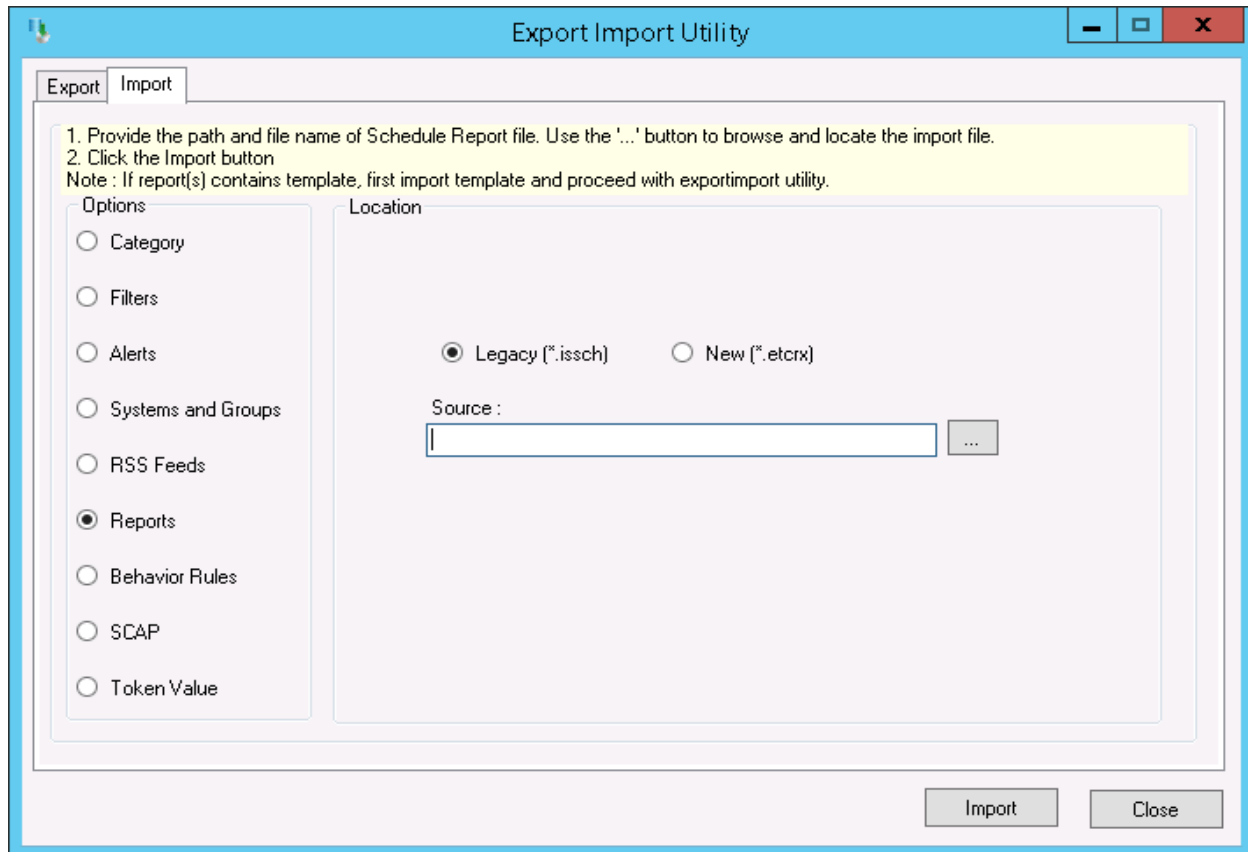


Figure 14

- Locate the **Microsoft Windows DFS.issch** file, and then click the **Open** button.
- Click the **Import** button to import the scheduled reports.

EventTracker displays success message.

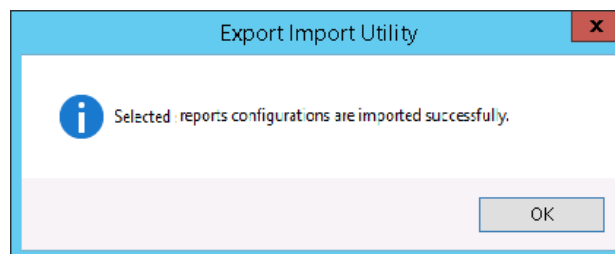


Figure 15

4. Click the **OK** button. Click the **Close** button.

To Configure Flex Dashboard

1. Schedule flex reports (Microsoft Windows DFS: User logon) after importing them.
2. During scheduling, please check **Persist data In EventVault Explorer** and select all the columns to persist.

The screenshot shows the 'REPORT WIZARD' interface, specifically 'Step 8 of 10'. The title is 'MICROSOFT WINDOWS DFS-USER LOGON LOGS'. The main section is 'DISK COST ANALYSIS'. It displays the following information:

- Estimated time for completion: 00:01:08(HH:MM:SS)
- Number of cab(s) to be processed: 19
- Available disk space: 261 GB
- Required disk space: 50 MB

Below this information are three radio button options for delivery:

- ☐ Enable publishing option (Configure SMTP Server in manager configuration screen to use this option)
- ☒ Deliver results via E-mail
- ☐ Notify results via E-mail

There is a text input field for 'To E-mail' with a placeholder text: '[Use comma(,) to separate multiple e-mail recipients]'. Below this is a dropdown menu for 'Update status via RSS' with the selected option 'Select Feed'. Another dropdown menu for 'Show in' has the selected option 'none'. At the bottom, there is a checkbox labeled 'Persist data In Eventvault Explorer' which is checked.

Figure 16

REPORT WIZARD

TITLE: MICROSOFT WINDOWS DFS-USER LOGON
DATA PERSIST DETAIL

CANCEL < BACK NEXT >

Select columns to persist

Step 9 of 10

RETENTION SETTING


Retention period: days ⓘ

☐ Persist in database only *[Reports will not be published and will only be stored in the respective database]*

SELECT COLUMNS TO PERSIST

COLUMN NAME	PERSIST
Computer	<input checked="" type="checkbox"/>
Account Name	<input checked="" type="checkbox"/>
Account Domain	<input checked="" type="checkbox"/>
Source Computer	<input checked="" type="checkbox"/>
Source Address	<input checked="" type="checkbox"/>
Source Port	<input checked="" type="checkbox"/>

Figure 17

- Now, wait for report to run as per schedule time or run it manually.
- After generating report, click on **Dashboard > Flex**.
- Click on **Add Dashboard**  button and fill **Title** and **Description** box and save it.

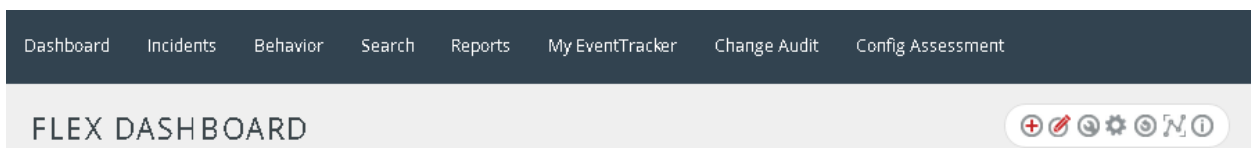
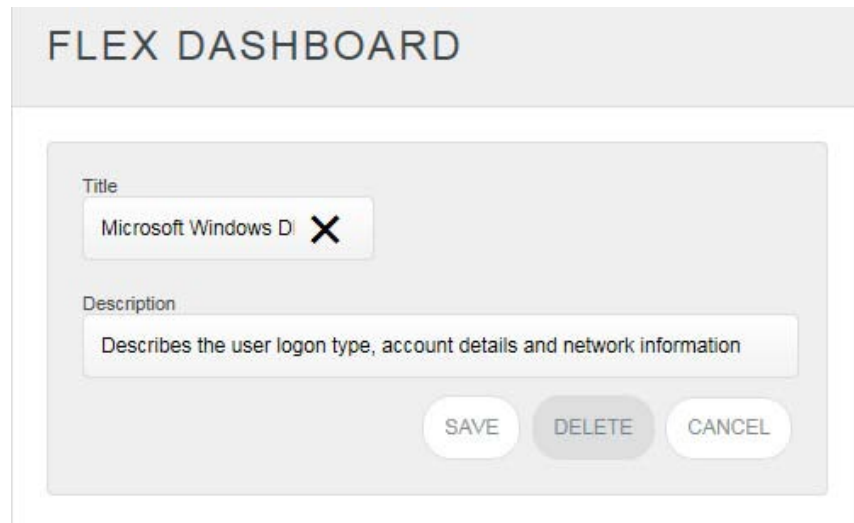


Figure 18




FLEX DASHBOARD

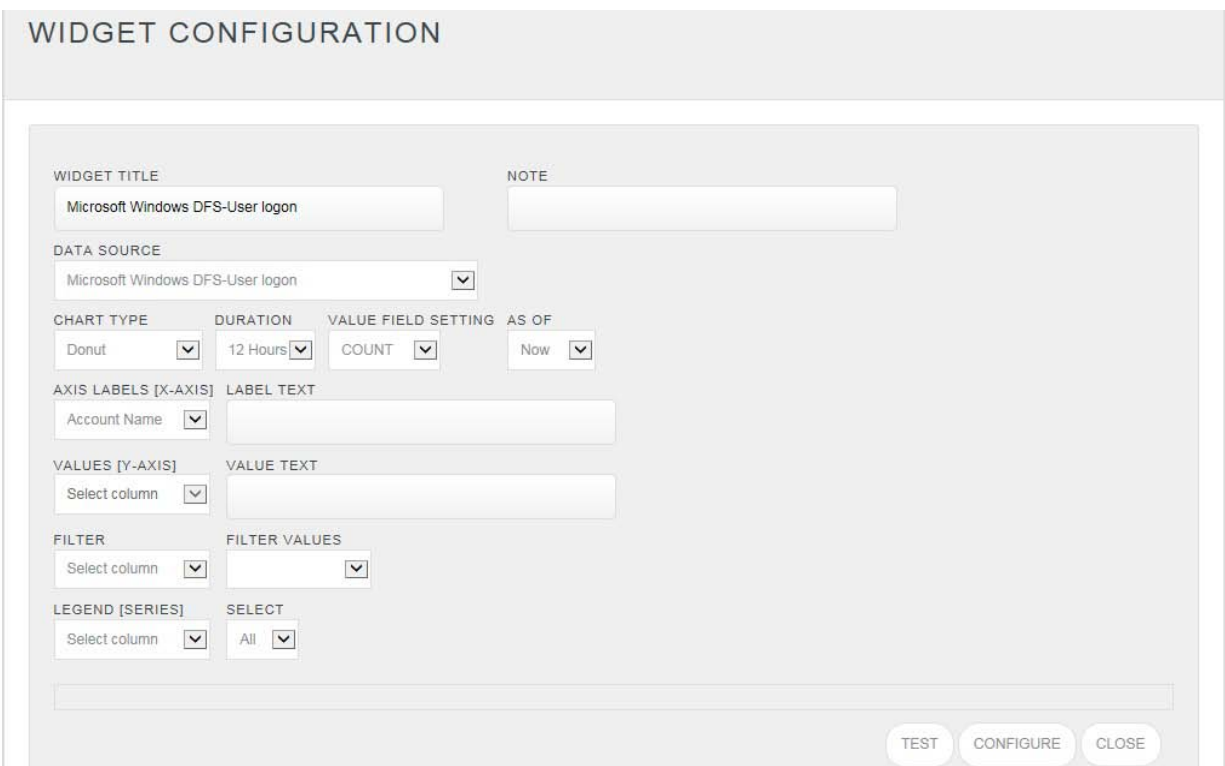
Title
Microsoft Windows D X

Description
Describes the user logon type, account details and network information

SAVE DELETE CANCEL

Figure 19

- Now, create Dashlet for Microsoft DNS (Top URL usage) by clicking on **Configure flex dashlet** .
- Fill **WIDGET TITLE** (Top URL usage), select **DATA SOURCE** (Microsoft DNS-Name resolution successfully), select **CHART TYPE** and select **AXIS LABELS [X-AXIS]**.



WIDGET CONFIGURATION

WIDGET TITLE
Microsoft Windows DFS-User logon

NOTE

DATA SOURCE
Microsoft Windows DFS-User logon

CHART TYPE
Donut

DURATION
12 Hours

VALUE FIELD SETTING
COUNT

AS OF
Now

AXIS LABELS [X-AXIS]
Account Name

LABEL TEXT

VALUES [Y-AXIS]
Select column

VALUE TEXT

FILTER
Select column

FILTER VALUES

LEGEND [SERIES]
Select column

SELECT
All

TEST CONFIGURE CLOSE

Figure 20

- After selecting and filling all the options, click on the **TEST** button to check the Dashlet. If data are coming properly, then click on **CONFIGURE** button.

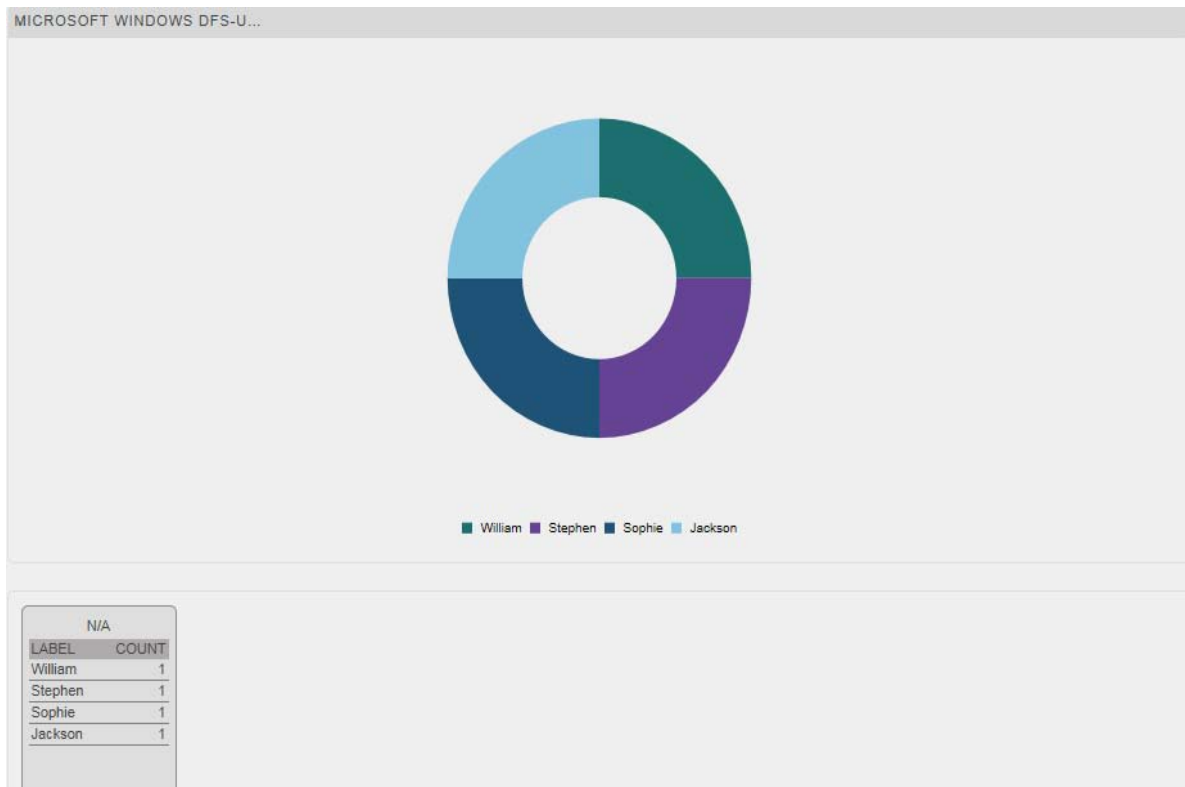


Figure 21



- After creation of Dashlet for Microsoft Windows DFS User login, click on **Customize flex dashlet** .
- Select Microsoft Windows DFS User login: Top URL usage dashlet and click on **ADD** button .



Figure 22

11. Now, you can see the Dashlet on Dashboard.

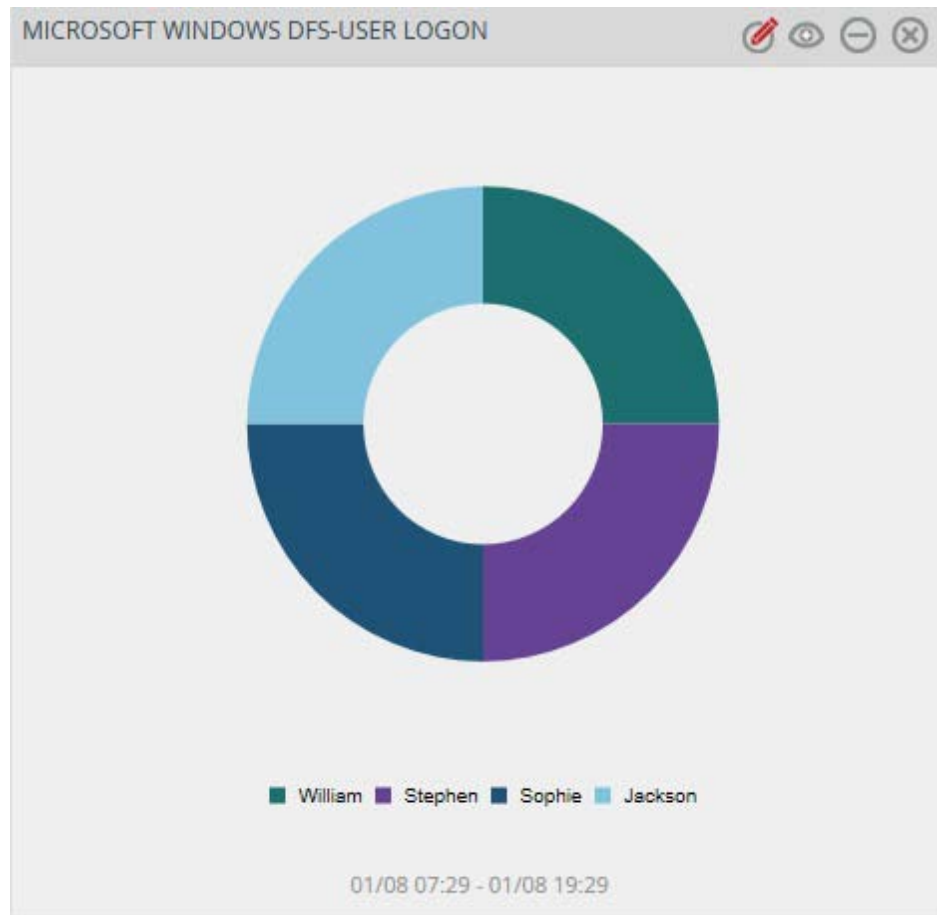


Figure 23

Verify knowledge pack in EventTracker

Verify Alerts

1. Logon to **EventTracker Enterprise**.
2. Click **Admin** dropdown, and then click **Alert**
3. In **Search** field, type '**Microsoft Windows DFS**', and then click the **Go** button.

Alert Management page will display all the imported Microsoft Windows DFS alerts.

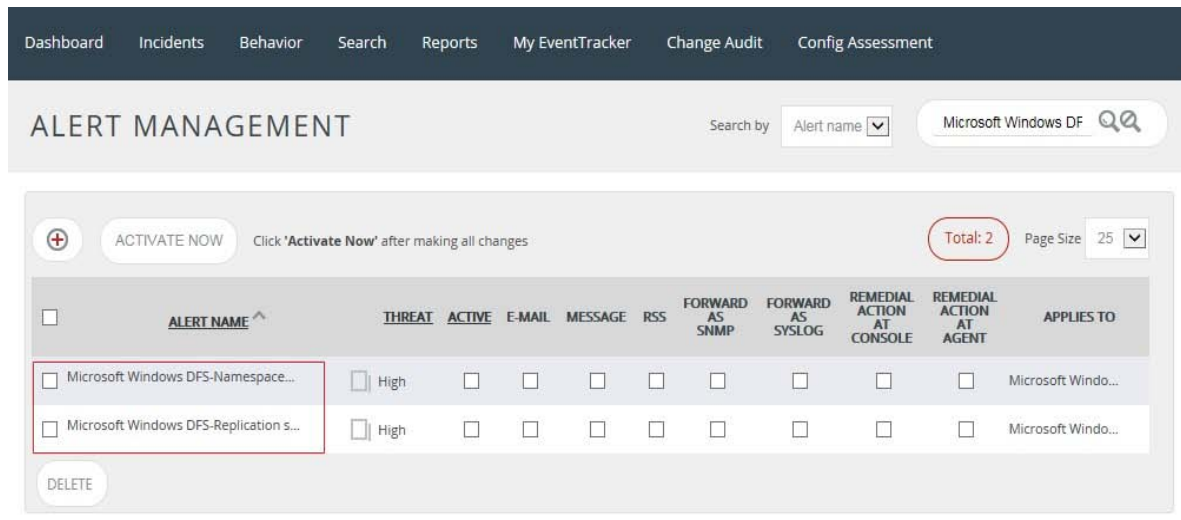


Figure 24

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

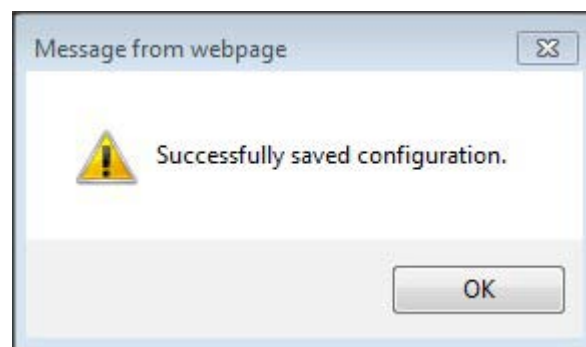


Figure 25

- Click **OK**, 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.

Verify Categories

- Ligon to **EventTracker Enterprise**.
- Click **Admin** dropdown, and then click **Categories**.

3. In **Category Tree**, to view imported categories, scroll down and expand Microsoft Windows DFS group folder to view the imported categories.

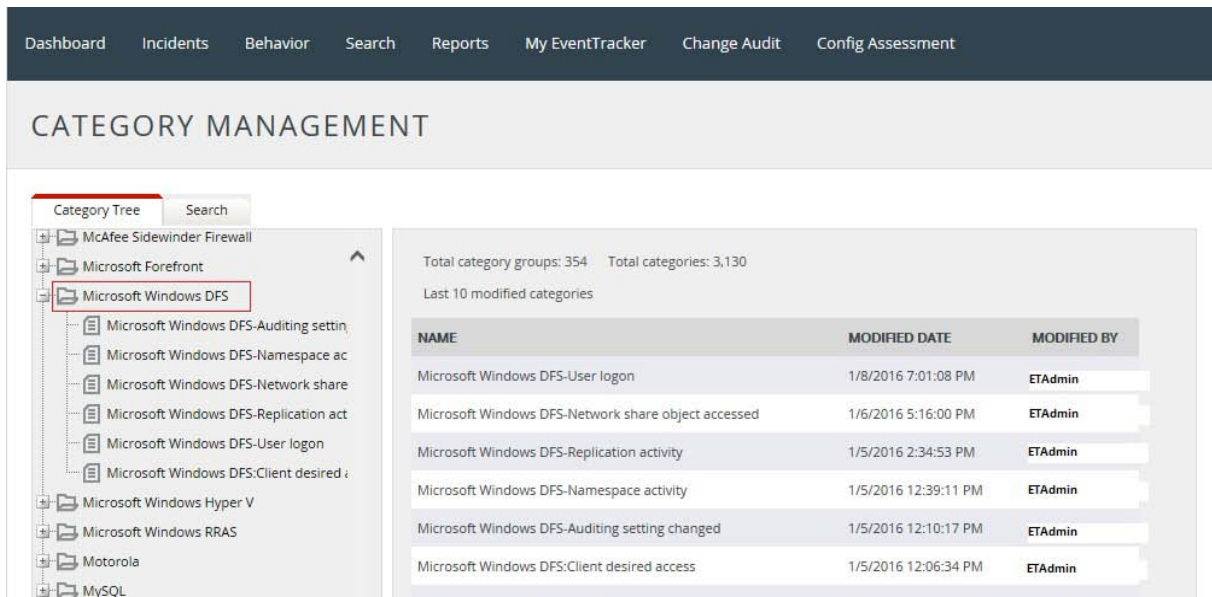


Figure 26

Verify Tokens

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** dropdown, and then click **Parsing rule**.

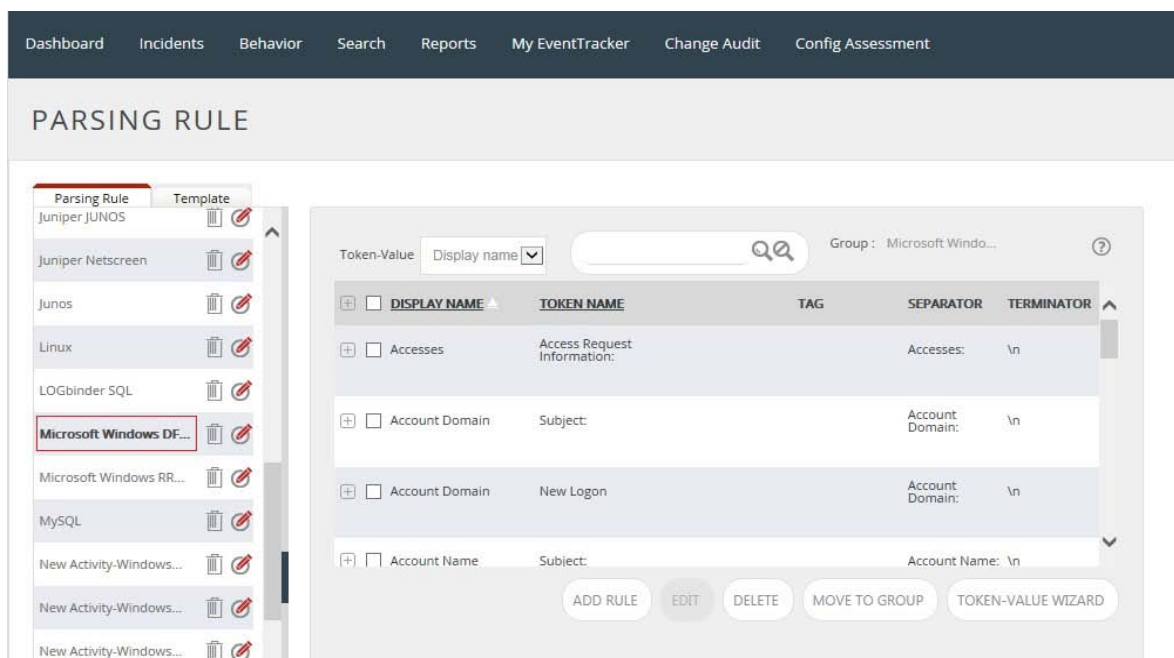


Figure 27

Verify Flex Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports**.
3. Select the **Configuration**.
4. In the **Reports Configuration**, select **Defined** radio button.

EventTracker displays **Defined** page.

5. In search box enter **Microsoft Windows DFS**.

EventTracker displays flex reports of Microsoft Windows DFS.

The screenshot shows the EventTracker Reports Configuration page. The top navigation bar includes links for Dashboard, Incidents, Behavior, Search, Reports, My EventTracker, Change Audit, and Config Assessment. The main heading is 'REPORTS CONFIGURATION'. Below this, there are three radio buttons: 'Scheduled', 'Queued', and 'Defined' (which is selected). To the right of the radio buttons is a search bar containing 'Microsoft Windows DF' and icons for search, filter, and calendar. On the left side, under 'REPORT GROUPS', there is a list of report groups: 'Microsoft Windows DF...', 'Microsoft Windows RR...', 'New Activity-Windows...', 'Office 365', 'OKTA SSO', 'OpenDNS', 'Palo Alto Firewall', and 'Persistent'. The 'Microsoft Windows DF...' group is highlighted. On the right side, under 'REPORTS CONFIGURATION : ALL', there is a table with columns 'TITLE', 'CREATED ON', and 'MODIFIED ON'. The table contains five rows of data, each with a checkbox, a gear icon, a title, and two dates. A 'Total: 5' badge is visible in the top right corner of the table area.

	TITLE	CREATED ON	MODIFIED ON	
<input type="checkbox"/>	Microsoft Windows DFS-User login	1/6/2016 4:27:54 PM	1/8/2016 6:55:49 PM	
<input type="checkbox"/>	Microsoft Windows DFS-Network share object acces...	1/5/2016 6:23:08 PM	1/5/2016 6:38:56 PM	
<input type="checkbox"/>	Microsoft Windows DFS-Replication activity	1/4/2016 6:48:38 PM	1/5/2016 11:37:38 AM	
<input type="checkbox"/>	Microsoft Windows DFS-Namespace activity	1/4/2016 6:42:36 PM	1/4/2016 6:42:36 PM	
<input type="checkbox"/>	Microsoft Windows DFS-Client desired access	1/4/2016 12:46:10 PM	1/4/2016 3:42:39 PM	

Figure 28

Sample Reports

1) Microsoft Windows DFS: User logon

Microsoft Windows DFS-User logon							
LogTime	Computer	Account Name	Account Domain	Source Computer	Source Address	Source Port	Logon Type
01/08/2016 07:14:52 PM	DFS-SERVER	Jackson	Contoso	mercury	192.168.11.72	40459	3
01/08/2016 07:15:40 PM	DFS-SERVER	Stephen	Contoso	venus	192.168.11.96	51258	3
01/08/2016 07:16:43 PM	DFS-SERVER	William	Contoso	bageera	192.168.11.83	41630	3
01/08/2016 07:17:36 PM	DFS-SERVER	Sophie	Contoso	cam	192.168.11.111	50459	3
01/08/2016 07:19:55 PM	DFS-SERVER	Thomas	Contoso	harry	192.168.11.158	51459	3
01/08/2016 07:22:40 PM	DFS-SERVER	Vinci	Contoso	moe	192.168.11.51	42559	3
01/08/2016 07:25:43 PM	DFS-SERVER	Jonny	Contoso	pluto	192.168.11.128	61385	3
01/08/2016 07:30:39 PM	DFS-SERVER	Leonard	Contoso	huei	192.168.11.161	51559	3

Figure 29

2) Microsoft Windows DFS-Auditing settings changed

Micorsoft Windows DFS-Auditing settings changed							
LogTime	Computer	Account Name	Account Domain	Object Server	Object Type	Object Path	New Security Descriptor
01/04/2016 05:15:45 PM	DFS-SERVER	emctadmin	Contoso	Security	File	F:\DFSRoots\perryyc	S:PARAI
01/04/2016 05:16:42 PM	DFS-SERVER	Ammy	Contoso	Security	File	F:\DFSRoots\rayg	S:ARAI
01/04/2016 05:20:45 PM	DFS-SERVER	Mike	Contoso	Security	File	F:\DFSRoots\perryyc	S:PARAI
01/04/2016 05:26:22 PM	DFS-SERVER	Michel	Contoso	Security	File	F:\DFSRoots\rayg	S:ARAI
01/04/2016 05:32:45 PM	DFS-SERVER	Joseph	Contoso	Security	File	F:\DFSRoots\perryyc	S:PARAI
01/04/2016 05:48:42 PM	DFS-SERVER	Jack	Contoso	Security	File	F:\DFSRoots\rayg	S:ARAI
01/04/2016 05:55:22 PM	DFS-SERVER	Jerry	Contoso	Security	File	F:\DFSRoots\perryyc	S:PARAI
01/04/2016 05:58:12 PM	DFS-SERVER	Henry	Contoso	Security	File	F:\DFSRoots\rayg	S:ARAI

Figure 30

Sample Dashboards

1. Microsoft Windows DFS- User logon

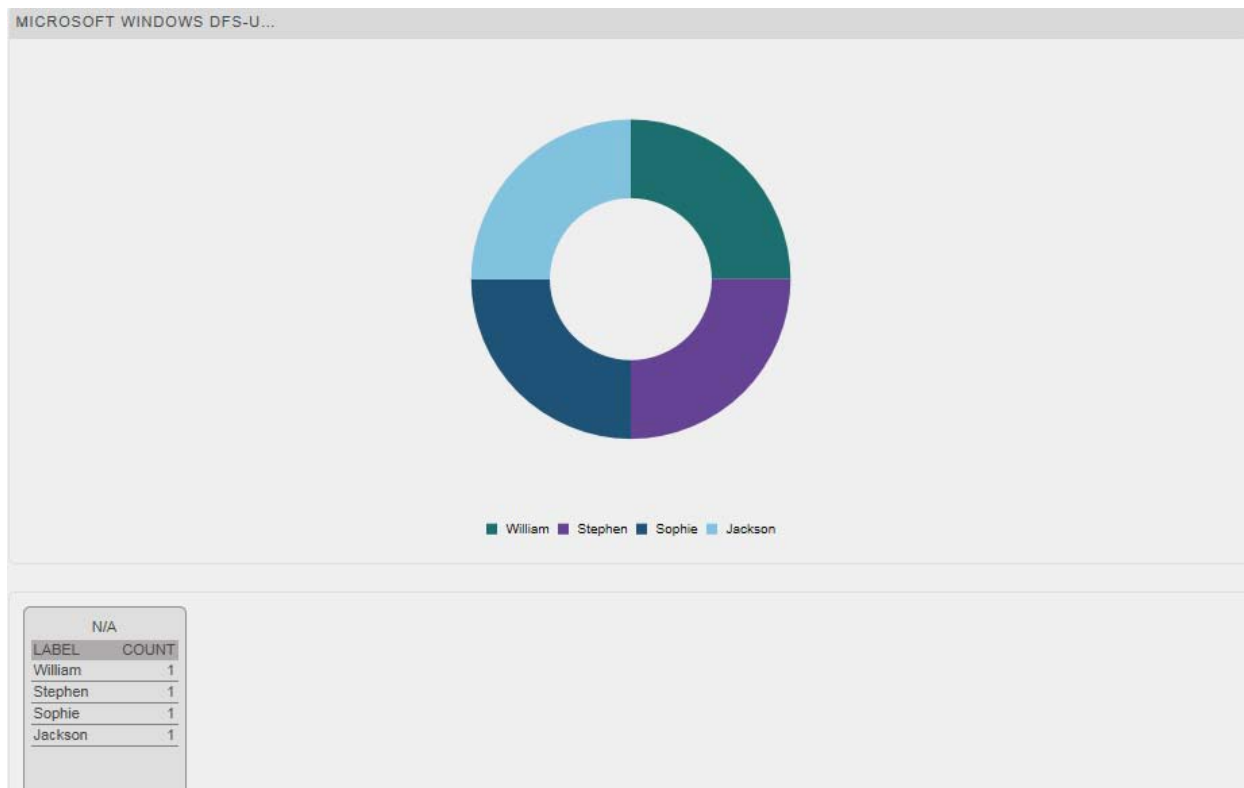


Figure 31