Netsurion™ | EventTracker

# Integrate Microsoft DHCP Server

## EventTracker v8.x and Above

Publication Date: March 29, 2019

# Abstract

The purpose of this document is to help the user(s) in monitoring the DHCP server logs by deploying Windows Agent.

# Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise v8.x** and later, and DHCP server hosted on **Windows Server 2003** and later.

# Audience

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

# Table of Contents

# Overview

The DHCP (Dynamic Host Configuration Protocol) assigns IP address to client computers automatically. DHCP auditing helps administrator to track information on successful or failed lease grants, depletion of the server's IP pool, or request for messages and their corresponding acknowledgements.

EventTracker can analyze the audit logs and generate the reports for monitoring the activity of DNS update request and DNS update success, lease renewed and denied by the DHCP server.

# Prerequisites

Prior to configuring Windows Server 2012 R2 and later and EventTracker v8.x or later, ensure that you meet the following pre-requisites:

- Administrative access to EventTracker.
- Microsoft DHCP server should to be installed and configured.
- User should have administrative rights on Microsoft DHCP Server.
- Firewall between Microsoft DHCP Server and EventTracker should be off or exception for EventTracker ports.
- EventTracker agent should be installed on Microsoft DHCP server.

# Configuration for sending logs to EventTracker

**NOTE**: To forward logs to EventTracker, DHCP auditing must be enabled and LFM need to be configured using powershell script.

1. EventTracker uses Log File Monitor (LFM) in the Windows agent to access DHCP Server audit logs. To perform LFM configuration, deploy the EventTracker agent on DHCP server.
2. Contact support team to get integrator for DHCP.
3. Refer EventTracker Agent installation guide. After installation of the ET agent run "Integrate DNS and DHCP.exe".

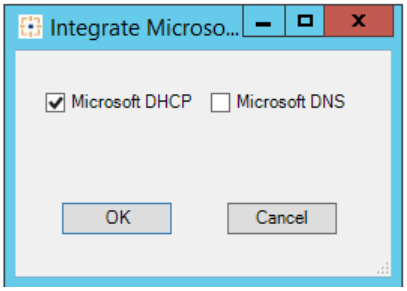



Figure 1

4. Check the option Microsoft DHCP and click ok.
5. Integrator will configure LFM for Microsoft DHCP Server and logs sent to EventTracker manager.

# EventTracker Knowledge Pack (KP)

Once logs are received in to EventTracker; Reports and Flex Dashboards can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Microsoft DHCP Server.

## Reports

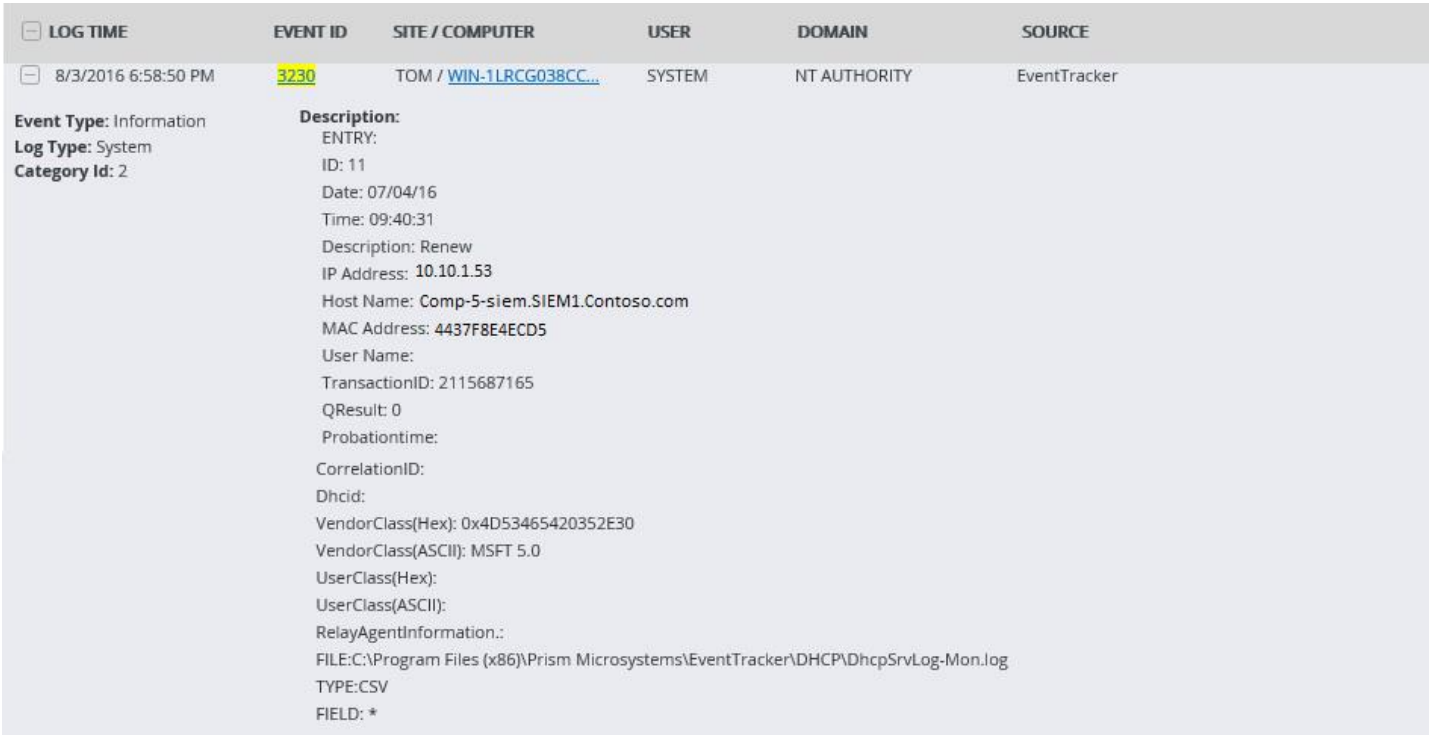
- **Microsoft DHCP Server: Lease renewed by client**

This report provides information related to lease renewed by client, when a client already has lease and needs to renew that lease with the DHCP server.

| Event Date | Event Time | Computer | Client Host Name | Client IP Address | Client MAC Address |
|---|---|---|---|---|---|
| 7/1/2016 | 09:50:22 | Server1-DLA | Comp-4-SALE.Support.Contoso.com | 10.10.1.112 | B087ED71C54E |
| 7/1/2016 | 08:42:13 | Server1-DLA | Comp-42-siem.SIEM1.Contoso.com | 10.10.1.163 | 4437D5F4ECD5 |
| 7/1/2016 | 08:42:24 | Server1-DLA | Comp-5-siem.SIEM1.Contoso.com | 10.10.1.53 | 4437D5F509F4 |
| 7/1/2016 | 08:43:10 | Server1-DLA | Comp-1-siem.SIEM1.Contoso.com | 10.10.1.156 | D8CE8F691994 |
| 7/1/2016 | 08:45:19 | Server1-DLA | Comp-3-siem.SIEM1.Contoso.com | 10.10.1.93 | D8DEFA0C8B99 |
| 7/1/2016 | 09:09:46 | Server1-DLA | Comp-4-gui.Contoso.com | 10.10.1.55 | D8CEFA0CFE85 |
| 7/1/2016 | 09:09:55 | Server1-DLA | obelix.Contoso.com | 10.10.1.124 | D8CF5A030852 |
| 7/1/2016 | 09:12:50 | Server1-DLA | Comp-5-siem.SIEM1.Contoso.com | 10.10.1.59 | 4437F7F509F4 |
| 7/1/2016 | 09:25:34 | Server1-DLA | Sherkhan.Contoso.com | 10.10.1.57 | 8C98F5F4284F |

Figure 2

**Logs Considered**



| LOG TIME | EVENT ID | SITE / COMPUTER | USER | DOMAIN | SOURCE |
|---|---|---|---|---|---|
| 8/3/2016 6:58:50 PM | 3230 | TOM / WIN-1LRCG038CC... | SYSTEM | NT AUTHORITY | EventTracker |

**Event Type:** Information
**Log Type:** System
**Category Id:** 2

**Description:**
ENTRY:
ID: 11
Date: 07/04/16
Time: 09:40:31
Description: Renew
IP Address: 10.10.1.53
Host Name: Comp-5-siem.SIEM1.Contoso.com
MAC Address: 4437F8E4ECD5
User Name:
TransactionID: 2115687165
QResult: 0
Probationtime:
CorrelationID:
Dhcid:
VendorClass(Hex): 0x4D53465420352E30
VendorClass(ASCII): MSFT 5.0
UserClass(Hex):
UserClass(ASCII):
RelayAgentInformation.:
FILE:C:\Program Files (x86)\Prism Microsystems\EventTracker\DHCP\DhcpSrvLog-Mon.log
TYPE:CSV
FIELD: *

Figure 3

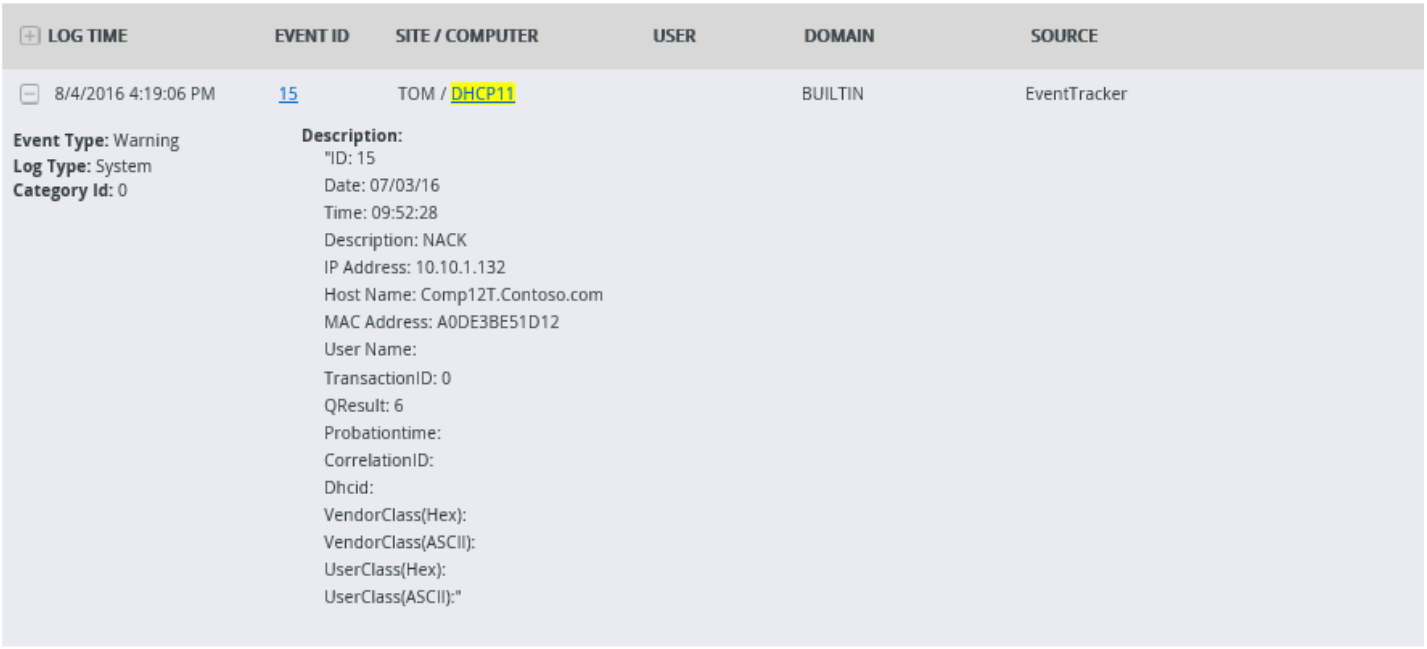
- **Microsoft DHCP Server: Lease denied**

This report provides the information related to lease denied, where client lease requests might be denied by the DHCP server for invalid (out of pool) or duplicate IP addresses to avoid IP addresses conflicts.

| Event Date | Event Time | Computer | Client MAC Address | Client IP Address | Client Host Name |
|---|---|---|---|---|---|
| 7/3/2016 | 09:52:28 | Server1-DLA | A0DE7CE51D12 | 10.10.1.157 | Comp55.Contoso.com |
| 7/3/2016 | 10:23:48 | Server1-DLA | A0DECE551F01 | 10.10.1.189 | CompTest.Contoso.com |

Figure 4

**Logs Considered**



| LOG TIME | EVENT ID | SITE / COMPUTER | USER | DOMAIN | SOURCE |
|---|---|---|---|---|---|
| 8/4/2016 4:19:06 PM | 15 | TOM / DHCP11 | | BUILTIN | EventTracker |

**Event Type:** Warning
**Log Type:** System
**Category Id:** 0

**Description:**
"ID: 15
Date: 07/03/16
Time: 09:52:28
Description: NACK
IP Address: 10.10.1.132
Host Name: Comp12T.Contoso.com
MAC Address: A0DE3BE51D12
User Name:
TransactionID: 0
QResult: 6
Probationtime:
CorrelationID:
Dhcid:
VendorClass(Hex):
VendorClass(ASCII):
UserClass(Hex):
UserClass(ASCII):"

Figure 5

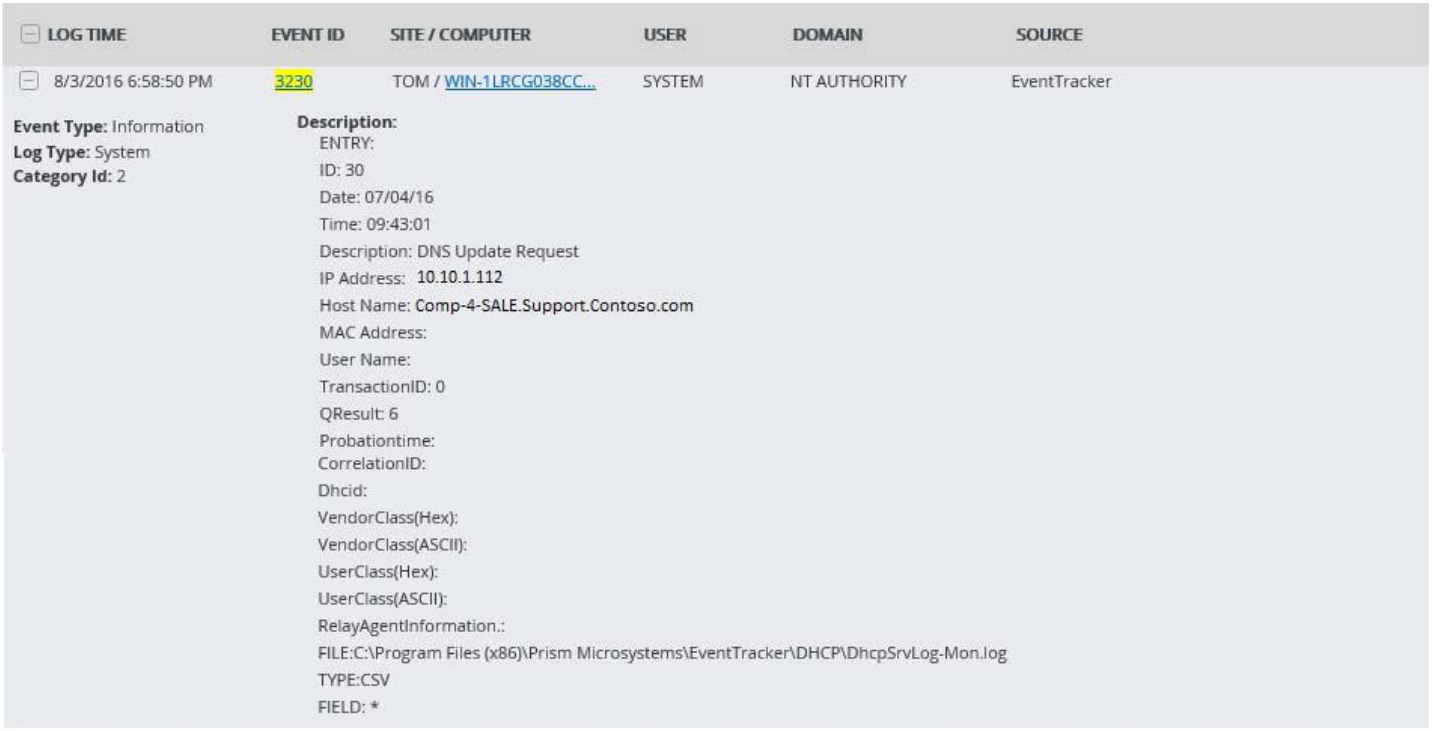
- **Microsoft DHCP Server: DNS update request**

This report provides the information related to DNS update request, where DHCP assigns IP address to DNS client machine and sends request to DNS, to dynamically update client hostname i.e. host (A) and PTR resource records.

| Event Date | Event Time | Computer | Client Host Name | Client IP Address |
|---|---|---|---|---|
| 7/1/2016 | 09:50:22 | Server1-DLA | Comp-4-SALE.Support.Contoso.com | 10.10.1.112 |
| 7/1/2016 | 08:42:13 | Server1-DLA | Comp-42-siem.SIEM1.Contoso.com | 10.10.1.163 |
| 7/1/2016 | 08:42:24 | Server1-DLA | Comp-5-siem.SIEM1.Contoso.com | 10.10.1.53 |
| 7/1/2016 | 08:43:10 | Server1-DLA | Comp-1-siem.SIEM1.Contoso.com | 10.10.1.156 |
| 7/1/2016 | 08:45:19 | Server1-DLA | Comp-3-siem.SIEM1.Contoso.com | 10.10.1.93 |
| 7/1/2016 | 09:09:46 | Server1-DLA | Comp-4-gui.Contoso.com | 10.10.1.55 |
| 7/1/2016 | 09:09:55 | Server1-DLA | obelix.Contoso.com | 10.10.1.124 |
| 7/1/2016 | 09:12:50 | Server1-DLA | Comp-5-siem.SIEM1.Contoso.com | 10.10.1.59 |
| 7/1/2016 | 09:25:34 | Server1-DLA | Sherkhan.Contoso.com | 10.10.1.57 |

Figure 6

**Logs Considered**



| LOG TIME | EVENT ID | SITE / COMPUTER | USER | DOMAIN | SOURCE |
|---|---|---|---|---|---|
| 8/3/2016 6:58:50 PM | 3230 | TOM / WIN-1LRCG038CC... | SYSTEM | NT AUTHORITY | EventTracker |

**Event Type:** Information
**Log Type:** System
**Category Id:** 2

**Description:**
ENTRY:
ID: 30
Date: 07/04/16
Time: 09:43:01
Description: DNS Update Request
IP Address: 10.10.1.112
Host Name: Comp-4-SALE.Support.Contoso.com
MAC Address:
User Name:
TransactionID: 0
QResult: 6
Probationtime:
CorrelationID:
Dhcid:
VendorClass(Hex):
VendorClass(ASCII):
UserClass(Hex):
UserClass(ASCII):
RelayAgentInformation.:
FILE:C:\Program Files (x86)\Prism Microsystems\EventTracker\DHCP\DhcpSrvLog-Mon.log
TYPE:CSV
FIELD: *

Figure 7

- **Microsoft DHCP Server: DNS update successful**

This report provides the information about DNS update success, when DHCP sends request to DNS to update the resource records and these records are registered successfully by the DNS.

| Event Date | Event Time | Computer | Client Host Name | Client IP Address |
|---|---|---|---|---|
| 7/1/2016 | 09:50:22 | Server1-DLA | Comp-4-SALE.Support.Contoso.com | 10.10.1.112 |
| 7/1/2016 | 08:42:13 | Server1-DLA | Comp-42-siem.SIEM1.Contoso.com | 10.10.1.163 |
| 7/1/2016 | 08:42:24 | Server1-DLA | Comp-5-siem.SIEM1.Contoso.com | 10.10.1.53 |
| 7/1/2016 | 08:43:10 | Server1-DLA | Comp-1-siem.SIEM1.Contoso.com | 10.10.1.156 |
| 7/1/2016 | 08:45:20 | Server1-DLA | Comp-3-siem.SIEM1.Contoso.com | 10.10.1.93 |
| 7/1/2016 | 09:09:46 | Server1-DLA | Comp-4-gui.Contoso.com | 10.10.1.55 |
| 7/1/2016 | 09:09:55 | Server1-DLA | obelix.Contoso.com | 10.10.1.124 |
| 7/1/2016 | 09:12:50 | Server1-DLA | Comp-5-siem.SIEM1.Contoso.com | 10.10.1.59 |
| 7/1/2016 | 09:25:34 | Server1-DLA | Sherkhan.Contoso.com | 10.10.1.57 |

Figure 8

**Logs Considered**

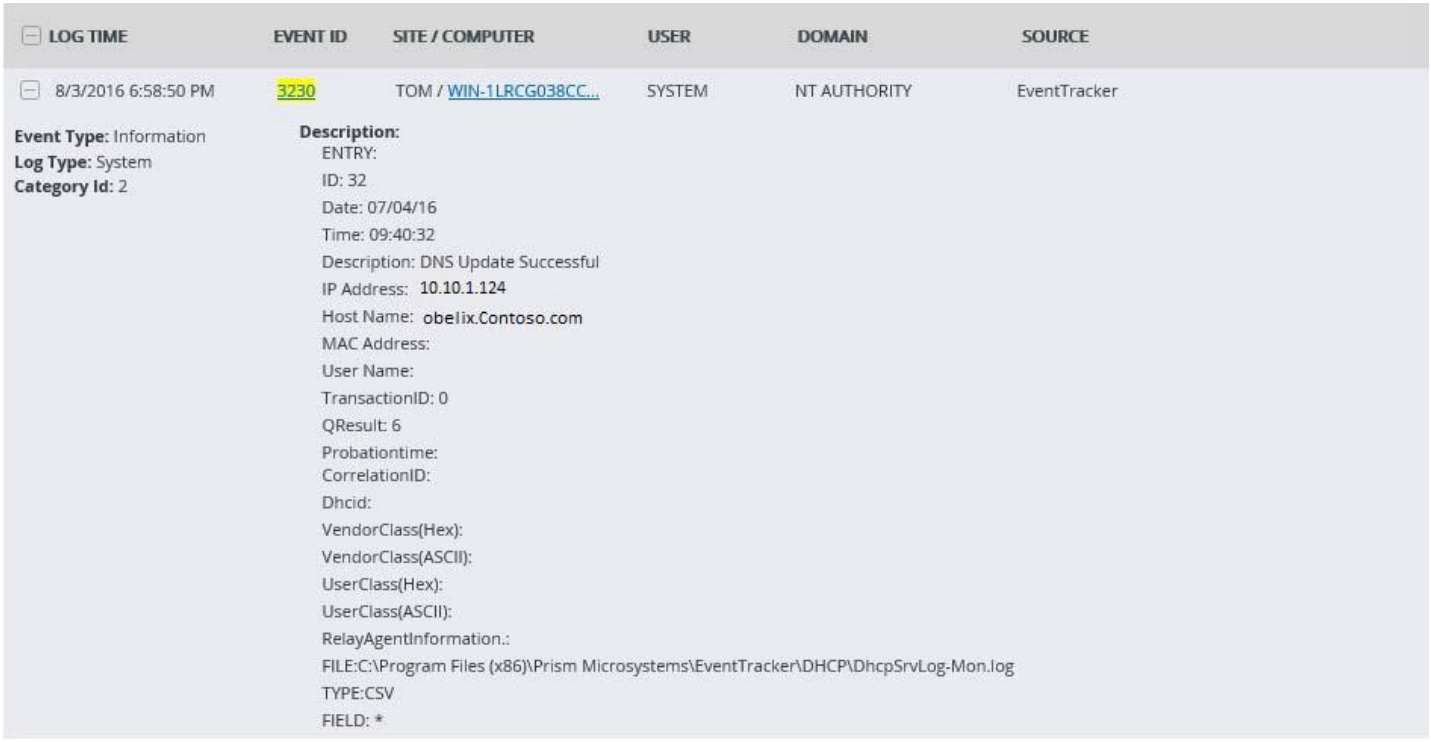



Figure 9

# Import Microsoft DHCP Server Knowledge Pack into EventTracker

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

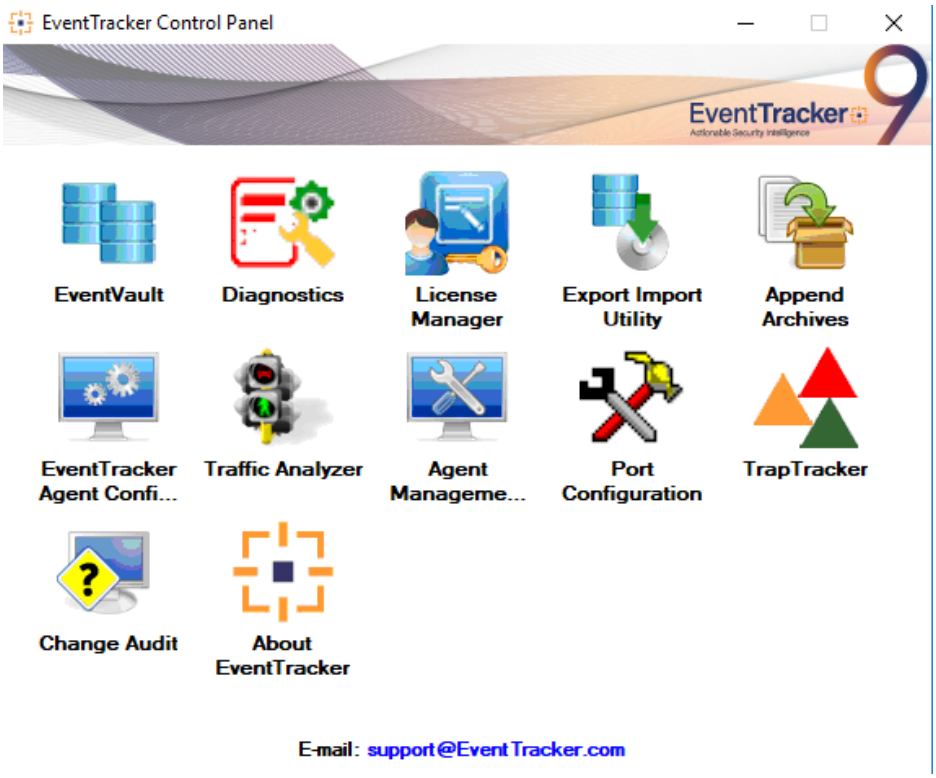



Figure 10

3. Click the **Import** tab.

**NOTE: Import knowledge pack as specified in the sequence.**

- **Parsing Rules**
- **Reports**

## Parsing Rules

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

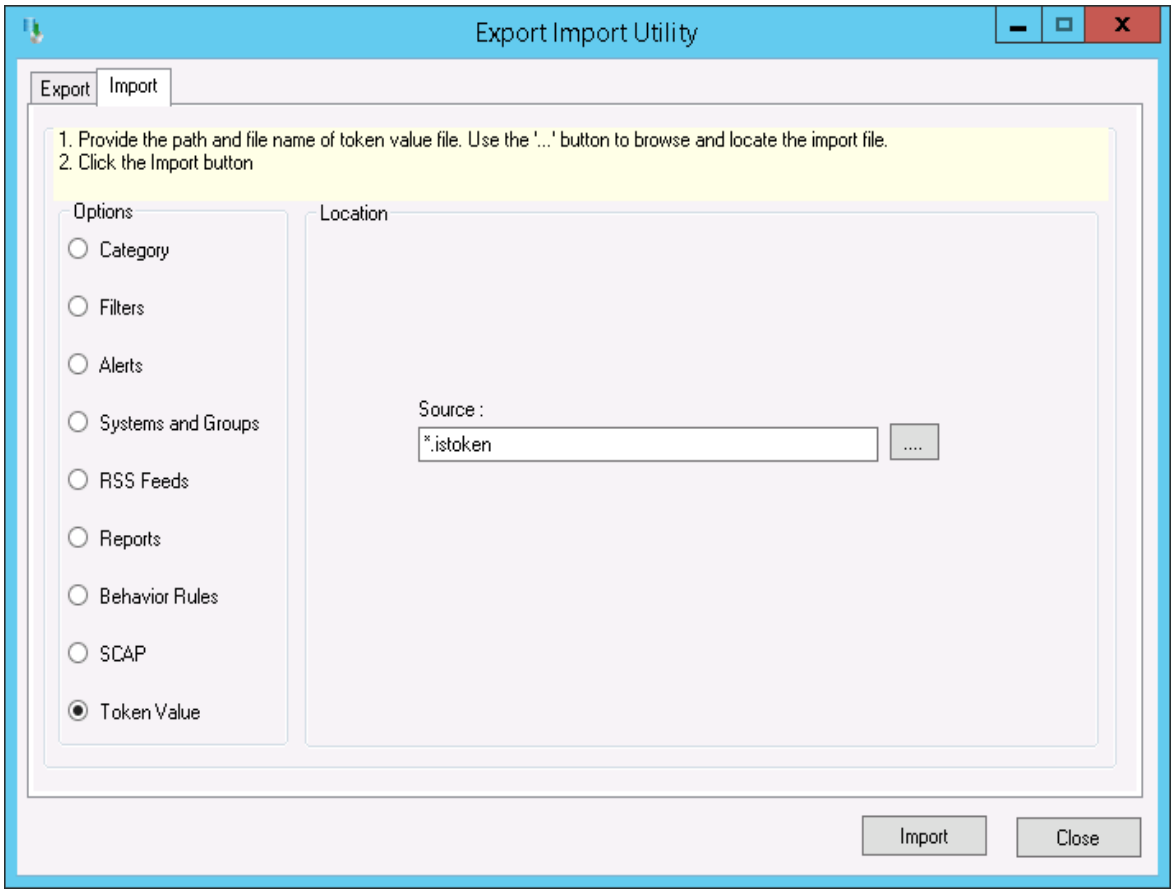



Figure 11

2. Locate the **All Microsoft DHCP Server parsing rules.istoken** file, and then click the **Open** button.
3. To import tokens, click the **Import** button.

EventTracker displays success message.

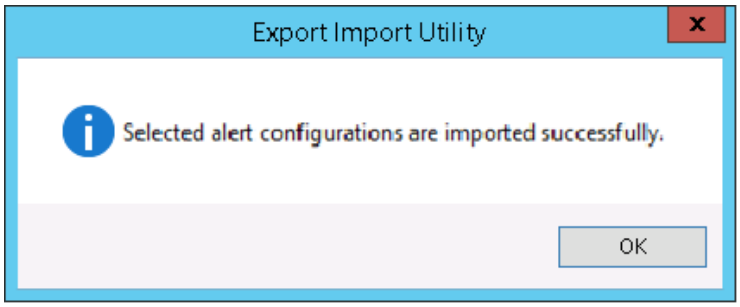



Figure 12

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

## Reports

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

2. Locate **All Microsoft DHCP Server group of reports.issch** file, and then click the **Open** button.
3. Click the **Import** button to import the reports.

EventTracker displays success message.


Figure 13

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

# Verify Knowledge Pack in EventTracker

## Parsing Rules

1. In the **EventTracker Enterprise** web interface, click the **Admin** menu, and then click **Parsing Rules**.
2. Select **Microsoft DHCP Server.**

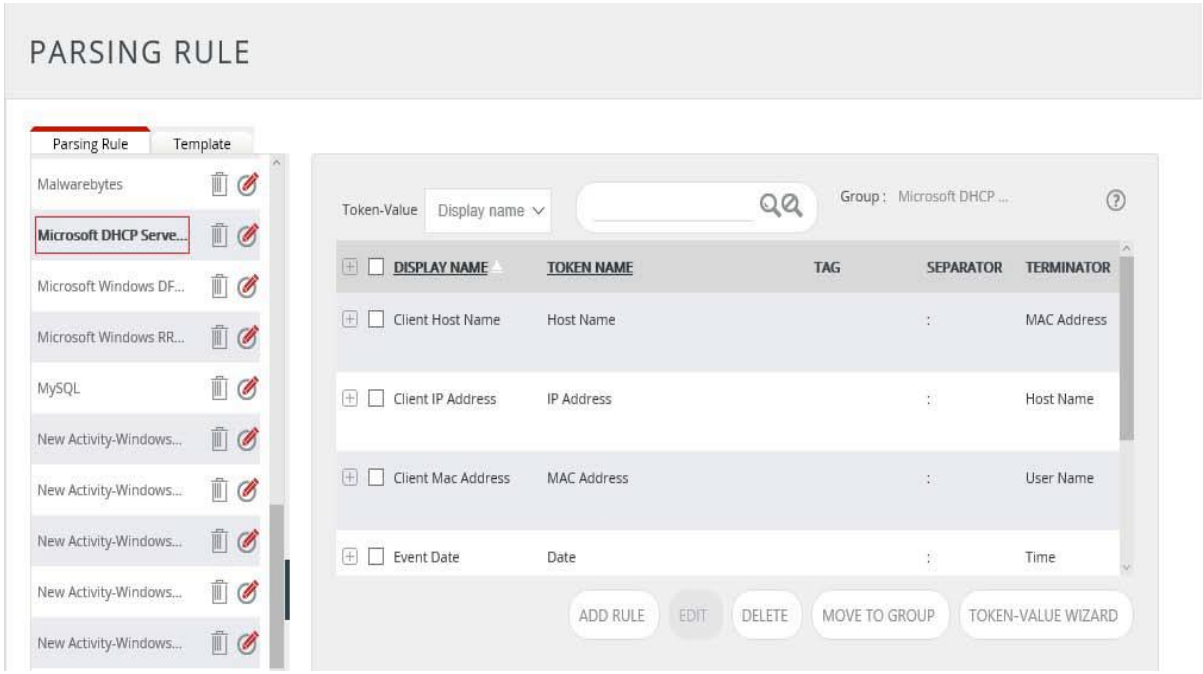



Figure 14

## Reports

1. Logon to **EventTracker Enterprise**.
2. Click the **Reports** menu, and then **Configuration**.
3. Select **Defined** in report type.
4. In **Report Groups Tree** to view imported Scheduled Reports, scroll down and click **Microsoft DHCP Server** group folder.

Reports are displayed in the Reports configuration pane.

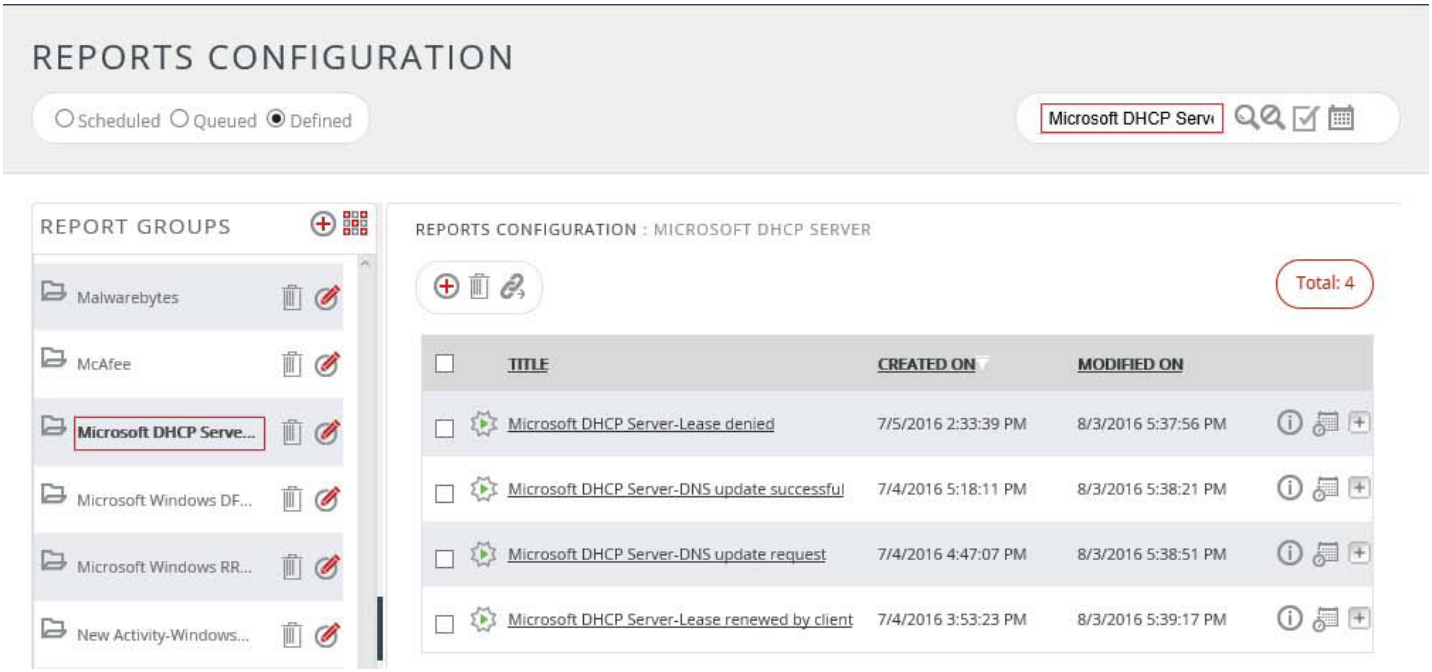



Figure 15

# Create Schedule Reports 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 login.
2. Navigate to **Reports>Configuration**.

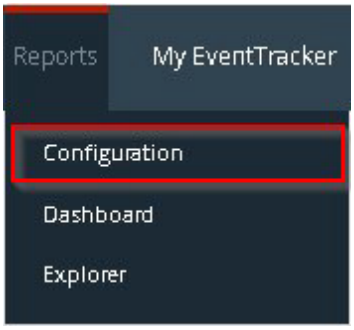



Figure 16

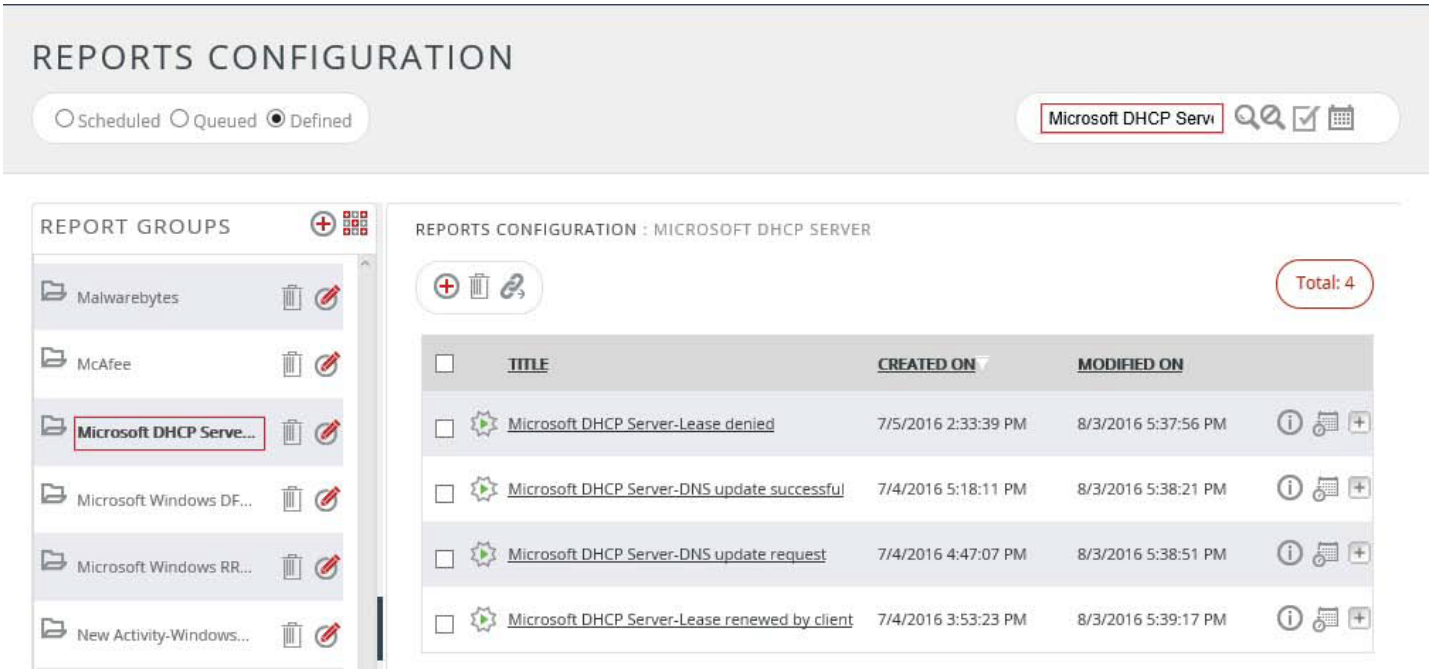



Figure 17

3. Select **Microsoft DHCP Server** in report groups. Check **Defined** option.
4. Click 'schedule' to plan a report for later execution.

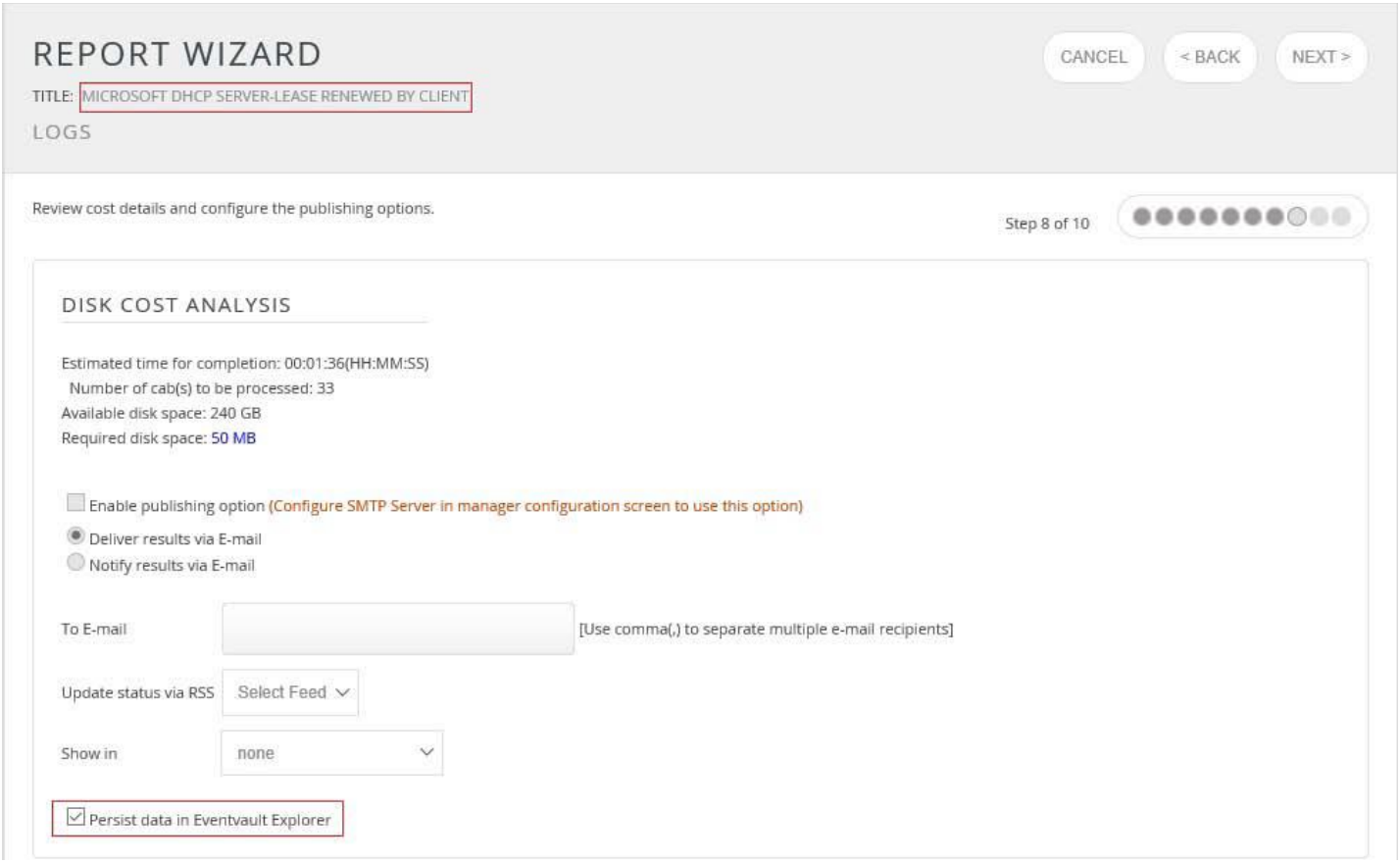

REPORT WIZARD
CANCEL
< BACK
NEXT >
TITLE: MICROSOFT DHCP SERVER-LEASE RENEWED BY CLIENT
LOGS
Review cost details and configure the publishing options.
Step 8 of 10
DISK COST ANALYSIS
Estimated time for completion: 00:01:36(HH:MM:SS)
Number of cab(s) to be processed: 33
Available disk space: 240 GB
Required disk space: 50 MB
Enable publishing option (Configure SMTP Server in manager configuration screen to use this option)
Deliver results via E-mail
Notify results via E-mail
To E-mail
[Use comma(,) to separate multiple e-mail recipients]
Update status via RSS
Select Feed
Show in
none
Persist data in Eventvault Explorer

Figure 18

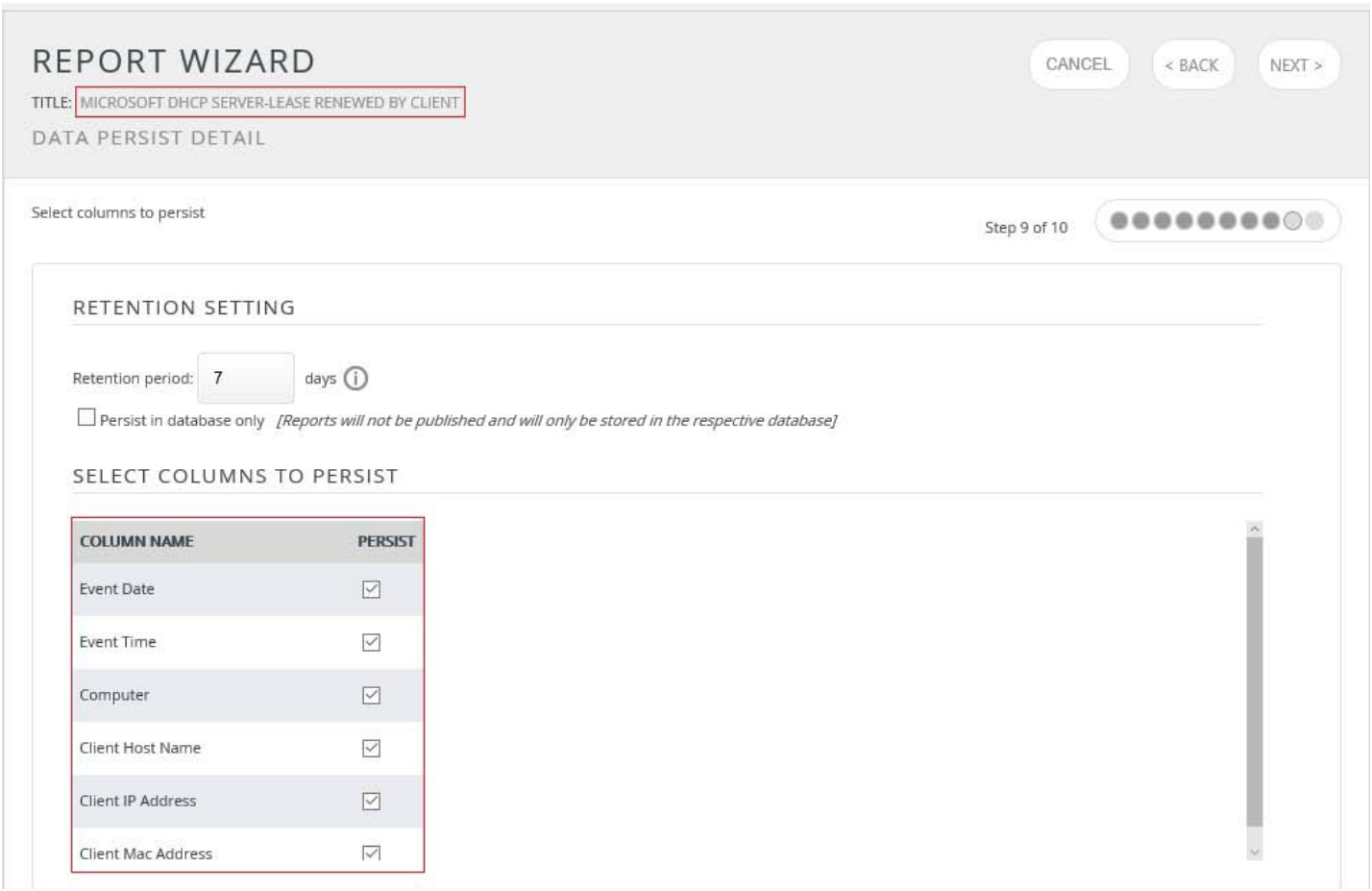



Figure 19

5. Choose appropriate time for report execution and in **Step 8** check **Persist data in Eventvault explorer** box.
6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period.**
7. Proceed to next step and click **Schedule** button.
8. Wait till the reports get generated.

# Dashboards

1. **Microsoft DHCP Server**


Figure 20