

Integration Guide

Integrating SonicWALL UTM

Publication Date:

March 20, 2022

Abstract

This guide provides instructions to configure SonicWALL UTM (Unified Threat Management) to send the syslog events to EventTracker.

Audience

The SonicWALL UTM users, who wish to forward the syslog events to the EventTracker Manager.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.X and later, and SonicOS 5.8 and later for SonicWALL NSA and TZ Series.

Table of Contents

Table of Contents	3
1. Overview	5
2. Prerequisites	5
3. Integrating SonicWALL UTM with EventTracker	5
3.1 Configuring the Syslog Settings	5
3.2 Configuring the Syslog Server	8
4. Syslog Send Receive Verification	9
4.1 Verifying the Ping from SonicWALL UTM to EventTracker	9
4.2 Verifying the Syslog messages forwarding on SonicWALL UTM	10
4.3 Verifying the Syslog messages in EventTracker	12
5. EventTracker Knowledge Pack (KP)	13
5.1 Categories	13
5.2 Alerts	18
5.3 Reports	19
6. Importing SonicWALL UTM Knowledge pack into EventTracker	22
6.1 Templates	22
6.2 Importing Categories	24
6.3 Importing Alerts	25
6.4 Importing Tokens	26
6.5 Importing Flex Reports	27
7. Verifying the SonicWALL UTM Knowledge Pack in EventTracker	29
7.1 Template	29
7.2 Verifying the SonicWALL UTM Categories	29
7.3 Verifying the SonicWALL UTM Alerts	30
7.4 Verifying the SonicWALL UTM Tokens	31
7.5 Verifying the SonicWALL UTM Flex Reports	32
8. Creating Dashboards in EventTracker	32
8.1 Scheduling Reports	32
8.2 Creating Dashlets	34
9. Sample Reports	38
10. Sample Dashboards	39

About Netsurion	40
Contact Us	40

1. Overview

SonicWALL's approach to the Unified Threat Management (UTM) is the best security approach for Small- to Medium-sized Businesses (SMBs) bringing a new level of efficiency to the security field. EventTracker gathers and examines acquired logs to identify malicious traffic, fatal threats, configuration changes, VPN activity, and user behavior.

2. Prerequisites

- EventTracker Agent 9.x and later should be installed.
- SonicOS 5.8 and later should be installed.
- Port 514 must be allowed on SonicWALL UTM.
- An exception should be added to the Windows Firewall on the EventTracker Manager system for Syslog port 514.

3. Integrating SonicWALL UTM with EventTracker

To forward the logs from SonicWALL UTM to EventTracker follow the below steps:

3.1 Configuring the Syslog Settings

1. Login to **SonicWALL UTM** using the Web browser.
2. Click the **Log** option at the bottom left of the **SonicWALL UTM** screen.

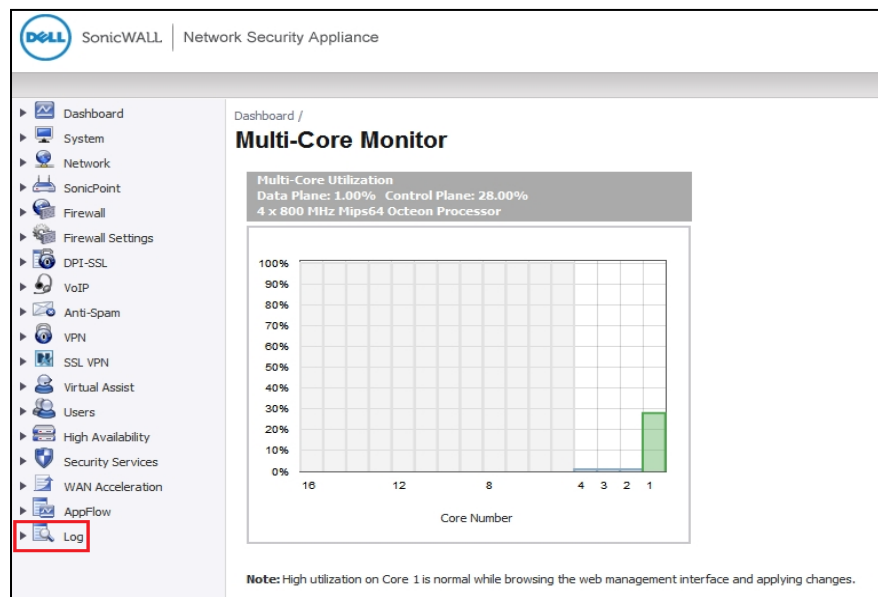


Figure 1

3. Select the **Syslog** option.

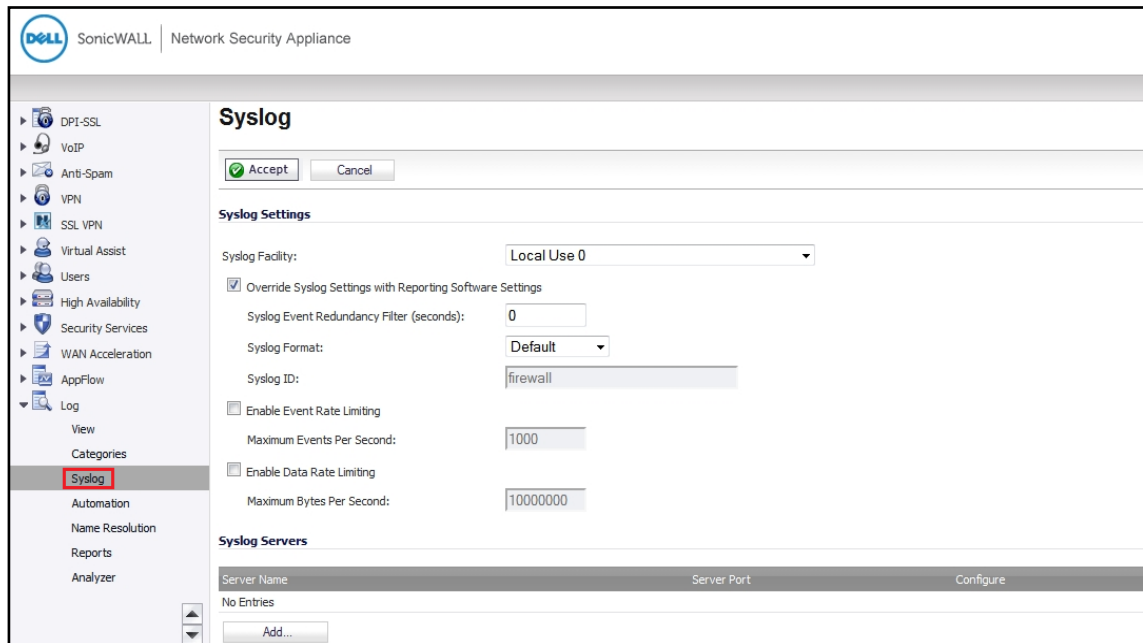


Figure 2

4. Under the **Syslog Setting** configure the following.

- **Syslog Facility**- Select the Syslog Facility you want or keep it as default.
- **Override Syslog Settings with Reporting Software Settings** - Uncheck this box to override the Syslog settings.

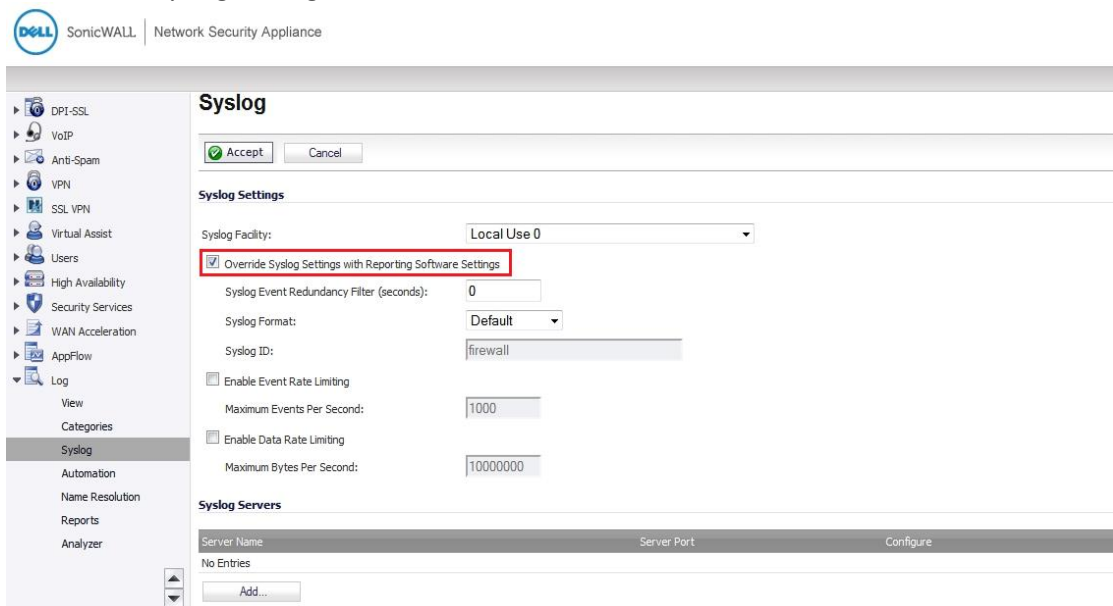


Figure 3

5. From the **Syslog Format** menu list, select the **Enhanced Syslog format**.

- Click the Configure icon . The **Enhanced Syslog Settings** configuration window appears.

Enhanced Syslog Settings

General

Host (sn) Event ID (m) Category (cat) Group Category (gcat)

Message (msg)

Interface

Src Interface Src Mac Addr (srcMac) Dst Interface Dst Mac Addr (dstMac)

Protocol

Src IP (src) Src NAT IP (natSrc) Src Port Src NAT Port

Dst IP (dst) Dst NAT IP (natDst) Dst Port Dst NAT Port

Protocol (proto) ICMP type (type) ICMP code (icmpCode)

Connection

Bytes Rcvd (rcvd) Bytes Sent (sent) Pkts Rcvd (rpkt) Pkts Sent (spkt)

User (usr) Conn Duration (cdur) Session Type (sess) Session Time (dur)

Src VPN Policy (vpnpolicy) Dst VPN Policy (vpnpolicyDst) Src Zone (srcZone) Dst Zone (dstZone)

Client Policy (rule) Interface stats SonicPoint Stats

Application

HTTP OP (op) HTTP result (result) URL (dstname) Block Reason (code)

Application (app) GMS Heartbeat GMS change URL (Change)

Others

Counter (n) NPCS (npcs) Note (note) IDP

Anti Spam App Firewall

Figure 4

- Select the **Enhanced Syslog** options you want to log into. To select all options, click **Select All**. To deselect all the options, click **Clear All**.
- Click the **Save** button.
- In the **Syslog ID** box, enter the Syslog ID that you want.

A **Syslog ID** field is included in all the generated Syslog messages, prefixed by "id=". Thus, for the default value, firewall, all Syslog messages include "id=firewall." The ID can be set to a string consisting of 0 to 32 alphanumeric and underscore characters.

- (Optional)** Select **Enable Event Rate Limiting** if required. This control allows you to enable the rate limiting of the events to prevent the internal or external logging mechanism from being overwhelmed by the log events. Specify the maximum number of events in the Maximum Events per Second field; the minimum number is 0, the maximum is 1000, and the default is 1000 per second.

NOTE: Event rate and data rate limiting are applied regardless of the Log Priority of individual events.

- (Optional)** Select the **Enable Data Rate Limiting** if required. This control allows you to enable the rate limiting of the data to prevent the internal or external logging mechanism from being overwhelmed

by the log events. Specify the maximum number of bytes in the **Maximum Bytes per Second** field; the minimum is 0, the maximum is 1000000000, and the default is 10000000 bytes per second.

12. (Optional) Select **Enable NDPP Enforcement** for the Syslog Server if required.

3.2 Configuring the Syslog Server

1. Under the **Syslog Servers** heading, click the **Add** button.

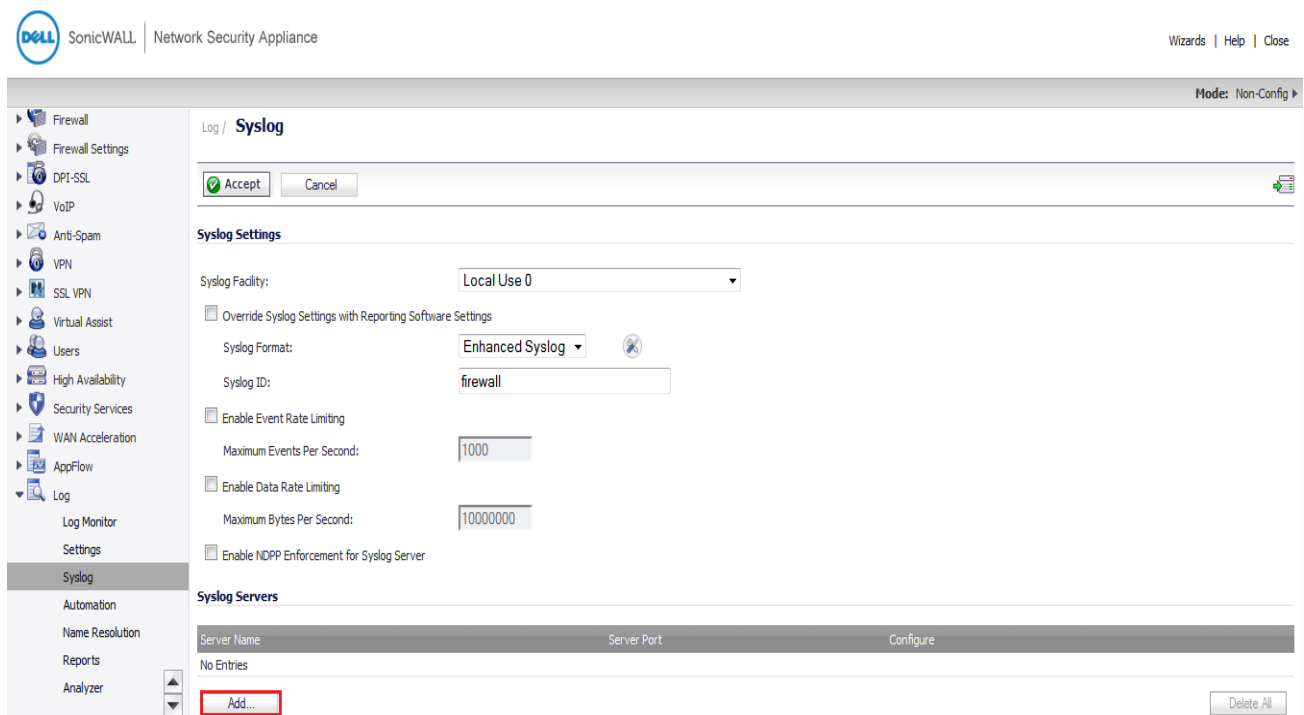


Figure 5

The Add Syslog Server window display.

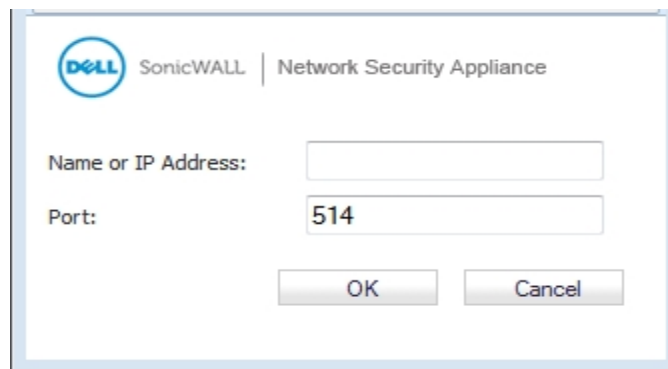


Figure 6

2. Type the **EventTracker Agent** machine name or IP address in the **Name or IP Address** field. Type the port number in the **Port Number** field. The Syslog default port is 514.

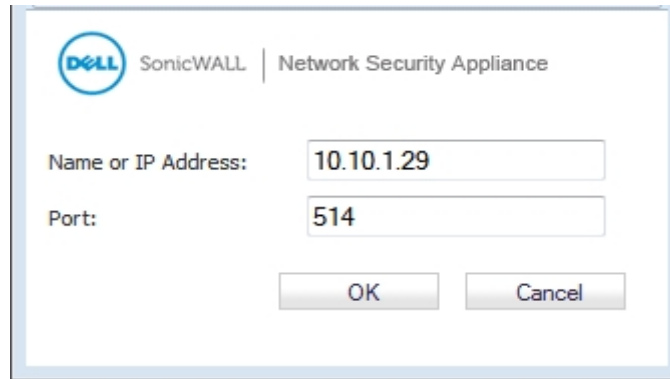


Figure 7

3. Click **OK**.

The Syslog server **EventTracker Agent** machine IP address would be added under the **Syslog Servers** section.

4. Click the **Accept** button to **Save** the settings.

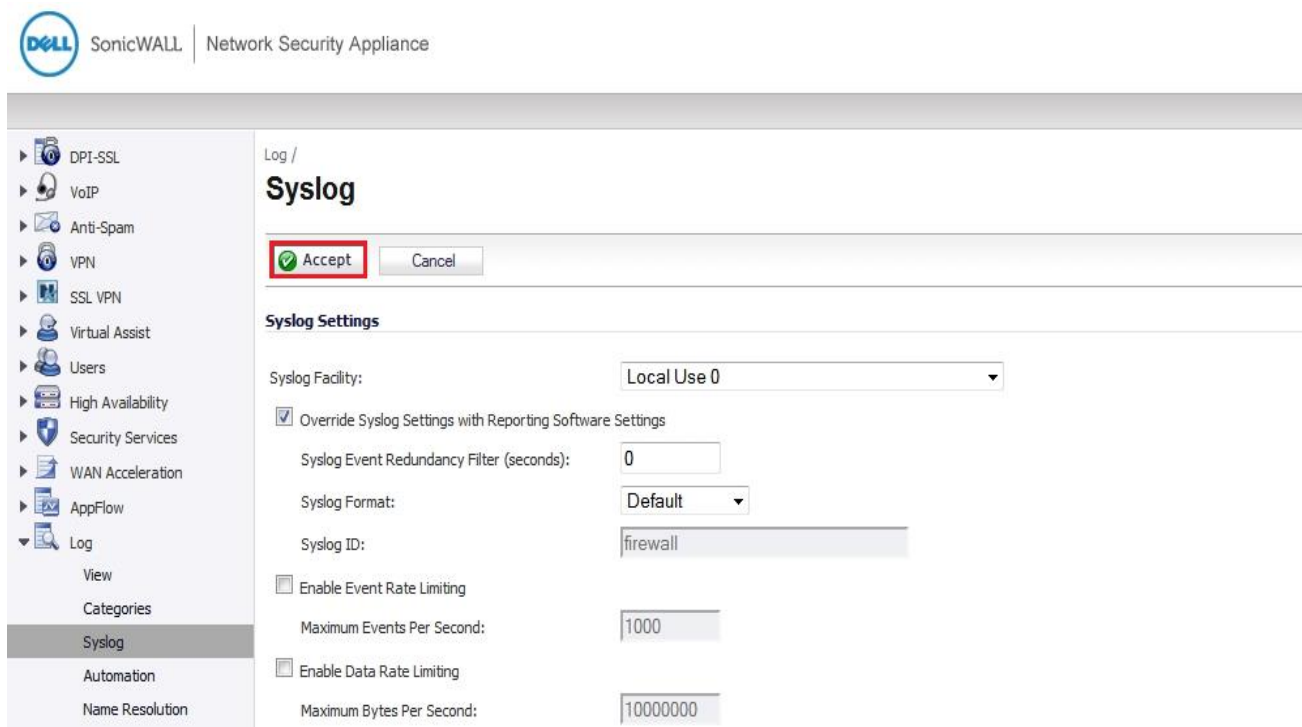


Figure 8

4. Syslog Send Receive Verification

4.1 Verifying the Ping from SonicWALL UTM to EventTracker

1. Login to SonicWALL UTM using the **Web** browser.

2. Click **System->Diagnostics**.
3. Select **Ping** from the **Diagnostic Tool** menu.

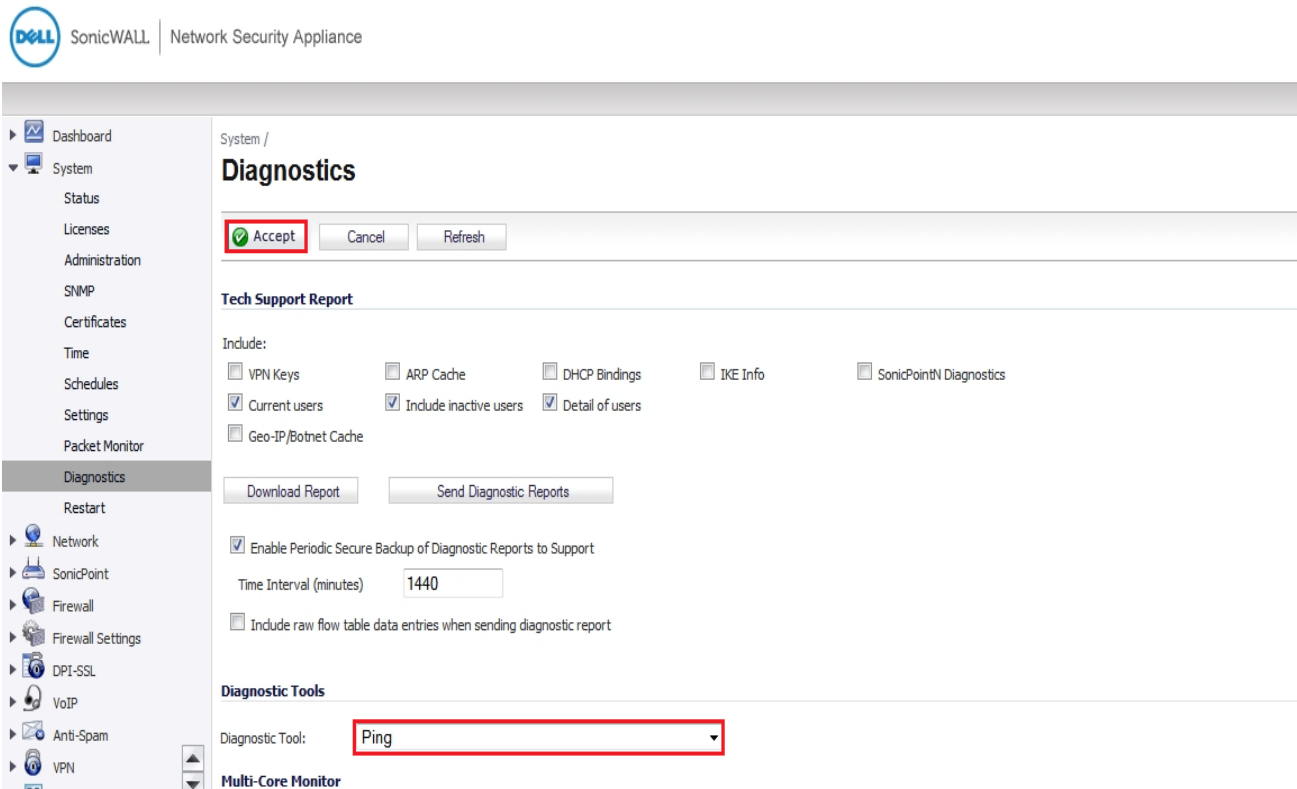


Figure 9

4. Enter the IP address or hostname of the EventTracker Manager system and click **Go**.
5. In the **Interface** pulldown menu, select the interface you want to test the ping from. Selecting the option **ANY** allows the appliance to choose among all the interfaces—including those that are not listed in the pulldown menu.
6. If the test is successful, SonicWALL UTM returns a message saying that the IP address is alive, and the time taken to return in milliseconds (ms).

4.2 Verifying the Syslog messages forwarding on SonicWALL UTM

1. Login to the SonicWALL Network Security using the Web browser.
2. Navigate to the **System-> Packet Monitor** page in the GUI and click **Configure**.

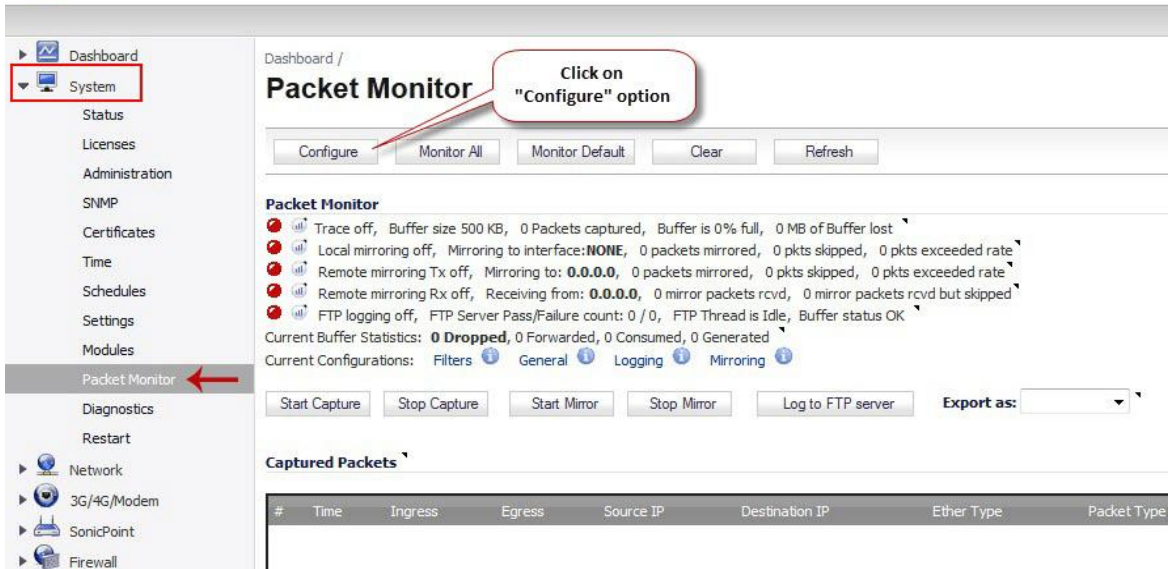


Figure 10

3. In the **Monitor Filter** tab, specify the following information.

- **Ether Type(s): IP Address**
- **IP Type(s): UDP**
- **Destination Port(s): 514**
- **Enable the check box Enable Bidirectional Address and Port Matching.**



Figure 11

4. In the **Advanced Monitor Filter** tab, **enable** the check boxes.

- **Monitor the Firewall Generated Packets. (This will bypass interface filter).**
- **Monitor the Intermediate Packets.**

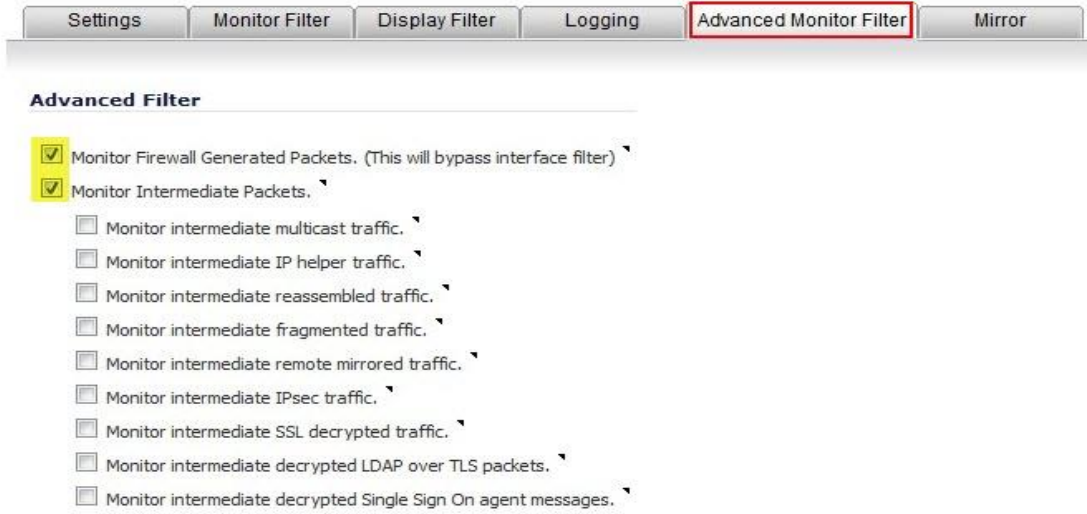


Figure 12

5. Click **OK** to save the packet capture setup.
6. Click **Start Capture** in the Packet Monitor page to see the **UDP 514** packets getting **generated** from SonicWALL destined for syslog server IP address as shown below.

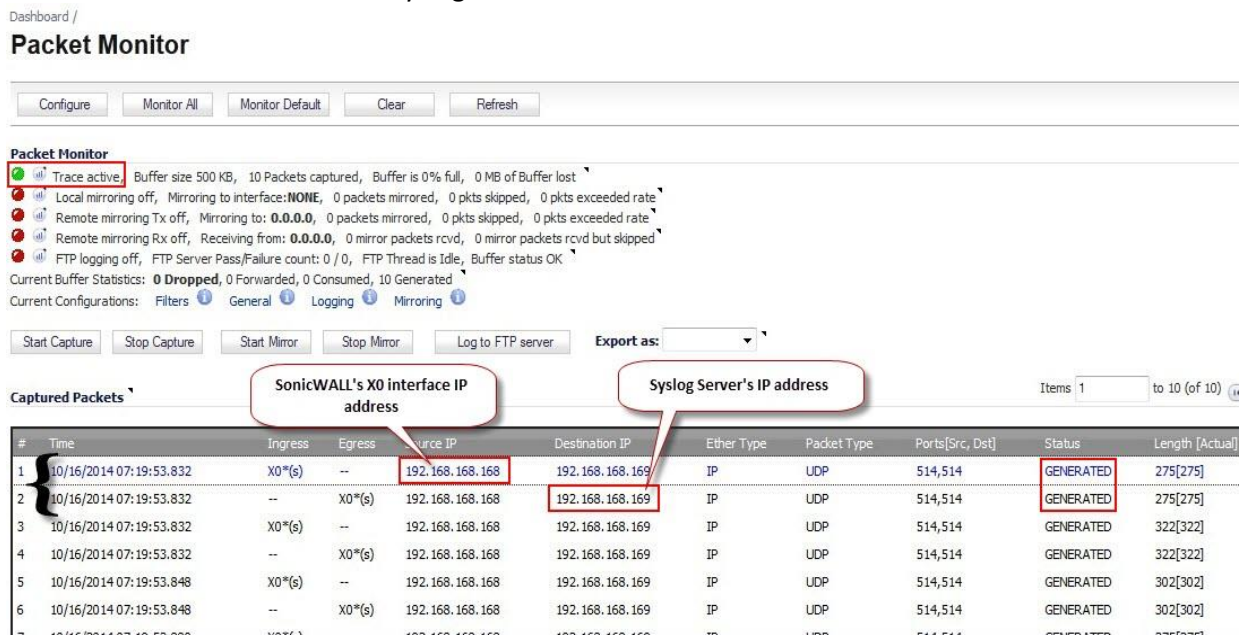


Figure 13

4.3 Verifying the Syslog messages in EventTracker

1. Login to the EventTracker Web Application.
2. Perform the Log Search for SonicWALL UTM device.

3. Log Search would display the syslog messages which EventTracker is receiving from SonicWALL UTM.

5. EventTracker Knowledge Pack (KP)

After the logs are received in EventTracker; categories, alerts, reports, and dashboards can be configured to provide valuable insight.

The following Knowledge Packs are available in EventTracker v7 and later to support the SonicWALL UTM monitoring.

5.1 Categories

- **SonicWALL UTM: Application block** - This category gives information related to the applications blocked on SonicWALL UTM.
- **SonicWALL UTM: Application control detection** - This category gives information related to the application control, detected on SonicWALL UTM.
- **SonicWALL UTM: Application control prevention** - This category gives information related to the application control, prevented on SonicWALL UTM.
- **SonicWALL UTM: Application detection** - This category gives information related to the applications, detected on SonicWALL UTM.
- **SonicWALL UTM: Administrator logged out** - This category gives information related to the administrator logged out on SonicWALL UTM.
- **SonicWALL UTM: Administrator login failed** - This category gives information related to the administrator login fail on SonicWALL UTM.
- **SonicWALL UTM: User authentication failed** - This category gives information related to the user authentication fail on SonicWALL UTM.
- **SonicWALL UTM: User authentication success** - This category gives information related to the user whose authentication is a success on SonicWALL UTM.
- **SonicWALL UTM: User logged out** - This category gives information related to the user who tries to log out on SonicWALL UTM.
- **SonicWALL UTM: User login failed** - This category gives information related to the user whose login fails on SonicWALL UTM.
- **SonicWALL UTM: Website access allowed** - This category gives information related to the website access which is allowed on SonicWALL UTM.
- **SonicWALL UTM: Website access denied** - This category gives information related to the website access which is denied on SonicWALL UTM.
- **SonicWALL UTM: DHCP lease dropped** - This category gives information related to the DHCP lease dropped on SonicWALL UTM.
- **SonicWALL UTM: DHCP lease expired** - This category gives information related to the DHCP lease expired on SonicWALL UTM.

- **SonicWALL UTM: DHCP lease received** - This category gives information related to the DHCP lease received on SonicWALL UTM.
- **SonicWALL UTM: DHCP request received** - This category gives information related to the DHCP request received on SonicWALL UTM.
- **SonicWALL UTM: DHCP Server IP address conflict detected** - This category gives information related to the DHCP server IP address conflict which was detected on SonicWALL UTM.
- **SonicWALL UTM: DHCP Server received DHCP decline from client** - This category gives information related to the DHCP server received on the DHCP client, declined on SonicWALL UTM.
- **SonicWALL UTM: Connection closed** - This category gives information related to the connection closed on SonicWALL UTM.
- **SonicWALL UTM: Connection dropped** - This category gives information related to the connection dropped on SonicWALL UTM.
- **SonicWALL UTM: Connection established** - This category gives information related to the connection established on SonicWALL UTM.
- **SonicWALL UTM: Connection opened** - This category gives information related to the connection open on SonicWALL UTM.
- **SonicWALL UTM: Connection timed out** - This category gives information related to the connection time out on SonicWALL UTM.
- **SonicWALL UTM: Firewall access rule added** - This category gives information related to the rules added to the firewall access on SonicWALL UTM.
- **SonicWALL UTM: Firewall access rule deleted** - This category gives information related to the rules deleted to firewall access on SonicWALL UTM.
- **SonicWALL UTM: Firewall access rule modified** - This category gives information related to the rules modified to firewall access on SonicWALL UTM.
- **SonicWALL UTM: Firewall access rule restored to default** - This category gives information related to rules restored by default on firewall access on SonicWALL UTM.
- **SonicWALL UTM: FTP connection dropped** - This category gives information related to the FTP connection dropped on SonicWALL UTM.
- **SonicWALL UTM: FTP logon failure** - This category gives information related to the FTP logon failure on SonicWALL UTM.
- **SonicWALL UTM: FTP successful logons** - This category gives information related to the FTP, which is successfully logged on, on the SonicWALL UTM.
- **SonicWALL UTM: Packet dropped** - This category gives information related to the packet dropped on SonicWALL UTM.
- **SonicWALL UTM: Back orifice attack dropped** - This category gives information related to the back orifice attack dropped on SonicWALL UTM.
- **SonicWALL UTM: DNS rebind attack detected** - This category gives information related to the attack detected on the DNS rebind on SonicWALL UTM.
- **SonicWALL UTM: DOS protection on WAN** - This category gives information related to the WAN protected by DOS on SonicWALL UTM.

- **SonicWALL UTM: FIN-Flooding machine blacklisted** - This category gives information related to the FIN-flooding machine blacklisted on SonicWALL UTM.
- **SonicWALL UTM: Forbidden email attachment disabled** - This category gives information related to the forbidden email attachment disabled on SonicWALL UTM.
- **SonicWALL UTM: FTP port bounce attack dropped** - This category gives information related to the FTP port bounce attack dropped on SonicWALL UTM.
- **SonicWALL UTM: ICMP flood attack detected** - This category gives information related to the ICMP flood attack detected on SonicWALL UTM.
- **SonicWALL UTM: Ini killer attack dropped** - This category gives information related to ini killer attack dropped on SonicWALL UTM.
- **SonicWALL UTM: Initiator from country blocked** - This category gives information related to the initiator from the country blocked on SonicWALL UTM.
- **SonicWALL UTM: Intrusion detection** - This category gives information related to the intrusion detection on SonicWALL UTM.
- **SonicWALL UTM: IPS alert** - This category gives information related to the IPS alert on SonicWALL UTM.
- **SonicWALL UTM: Land attack dropped** - This category gives information related to the land attack dropped on SonicWALL UTM.
- **SonicWALL UTM: MAC IP anti spoof check enforced for hosts** - This category gives information related to the MAC IP anti spoof check enforced for hosts on SonicWALL UTM.
- **SonicWALL UTM: Machine removed from FINflood blacklist** - This category gives information related to the FINflood blacklist, removed by the machine on SonicWALL UTM.
- **SonicWALL UTM: Machine removed from RSTflood blacklist** - This category gives information related to the RSTflood blacklist, removed by the machine on SonicWALL UTM.
- **SonicWALL UTM: Machine removed from SYNflood blacklist** - This category gives information related to the SYNflood blacklist, removed by the machine on SonicWALL UTM.
- **SonicWALL UTM: Malformed DNS packet detected** - This category gives information related to the malformer DNS packet detected on SonicWALL UTM.
- **SonicWALL UTM: Malformed or unhandled IP packet dropped** - This category gives information related to the malformed or the unhandled IP packet dropped on SonicWALL UTM.
- **SonicWALL UTM: NetBus attack dropped** - This category gives information related to the netbus attack dropped on SonicWALL UTM.
- **SonicWALL UTM: Ping of death dropped** - This category gives information related to the ping of death dropped on SonicWALL UTM.
- **SonicWALL UTM: Port scan detected** - This category gives information related the port scan detected on SonicWALL UTM.
- **SonicWALL UTM: Responder from country blocked** - This category gives information related to the responder from the country blocked on SonicWALL UTM.
- **SonicWALL UTM: Suspected botnet initiator blocked** - This category gives information related to the suspected botnet initiator blocked on SonicWALL UTM.
- **SonicWALL UTM: SYN flood detected on WAN** - This category gives information related to the SYN flood detected on the WAN on SonicWALL UTM.

- **SonicWALL UTM: TCP SYN packet dropped** - This category gives information related to the TCP SYN packet dropped on SonicWALL UTM.
- **SonicWALL UTM: UDP Flood attack detected** - This category gives information related to the UDP flood attack detected on SonicWALL UTM.
- **SonicWALL UTM: WLAN IDS** - This category gives information related to the WLAN IDS on SonicWALL UTM.
- **SonicWALL UTM: Backup firewall transitioned to active** - This category gives information related to the backup firewall transitioned to active on SonicWALL UTM.
- **SonicWALL UTM: Backup firewall transitioned to idle** - This category gives information related to the backup firewall transitioned to idle on SonicWALL UTM.
- **SonicWALL UTM: Interface link down** - This category gives information related to the interface link down on SonicWALL UTM.
- **SonicWALL UTM: Interface link up** - This category gives information related to the interface link up on SonicWALL UTM.
- **SonicWALL UTM: Multicast policy list added** - This category gives information related to the multicast policy added to the list on SonicWALL UTM.
- **SonicWALL UTM: Multicast policy list deleted** - This category gives information related to the multicast policy deleted from the list on SonicWALL UTM.
- **SonicWALL UTM: Network monitoring** - This category gives information related to the network monitoring on SonicWALL UTM.
- **SonicWALL UTM: Network security appliance activated** - This category gives information related to the network security appliance activated on SonicWALL UTM.
- **SonicWALL UTM: PC card device not detected** - This category gives information related to the PC card device not detected on SonicWALL UTM.
- **SonicWALL UTM: PC card inserted** - This category gives information related to the PC card inserted on SonicWALL UTM.
- **SonicWALL UTM: PC card removed** - This category gives information related to the PC card removed on SonicWALL UTM.
- **SonicWALL UTM: Primary firewall transitioned to active** - This category gives information related to the Primary firewall transitioned to active on SonicWALL UTM.
- **SonicWALL UTM: Primary firewall transitioned to idle** - This category gives information related to the primary firewall transitioned to idle on SonicWALL UTM.
- **SonicWALL UTM: System fan failure** - This category gives information related to the system fan failure on SonicWALL UTM.
- **SonicWALL UTM: System shutdown by administrator** - This category gives information related to the shutting down of the system by the administrator on SonicWALL UTM.
- **SonicWALL UTM: WAN failover** - This category gives information related to the WAN failover on SonicWALL UTM.
- **SonicWALL UTM: WAN failure** - This category gives information related to the WAN failure on SonicWALL UTM.

- **SonicWALL UTM: Antispam service disabled** - This category gives information related to the antispam service disabled on SonicWALL UTM.
- **SonicWALL UTM: Antispam service enabled** - This category gives information related to the antispam service enabled on SonicWALL UTM.
- **SonicWALL UTM: DSL device down** - This category gives information related to the DSL device down on SonicWALL UTM.
- **SonicWALL UTM: DSL device up** - This category gives information related to the DSL device up on SonicWALL UTM.
- **SonicWALL UTM: DSL WAN connected** - This category gives information related to the DSL WAN connected on SonicWALL UTM.
- **SonicWALL UTM: DSL WAN initialized** - This category gives information related to the DSL WAN initialized on SonicWALL UTM.
- **SonicWALL UTM: Dynamic DNS configuration error** - This category gives information related to the dynamic DNS configuration error on SonicWALL UTM.
- **SonicWALL UTM: SSO agent down** - This category gives information related to the SSO agent which is down on SonicWALL UTM.
- **SonicWALL UTM: Terminal Services agent down** - This category gives information related to the terminal services agent which is down on SonicWALL UTM.
- **SonicWALL UTM: Spam detected** - This category gives information related to the spam detected on SonicWALL UTM.
- **SonicWALL UTM: Maximum events per second threshold exceeded** - This category gives information related the maximum events per second threshold exceeded on SonicWALL UTM.
- **SonicWALL UTM: Maximum syslog data per second threshold exceeded** - This category gives information related to the maximum syslog data per second threshold exceeded on SonicWALL UTM.
- **SonicWALL UTM: No firewall rule associated with VPN policy** - This category gives information related to no firewall rule associated with the VPN policy on SonicWALL UTM.
- **SonicWALL UTM: Real time blacklist error** - This category gives information related to the real time blacklist error on SonicWALL UTM
- **SonicWALL UTM: Unhandled multicast IPv6 packet dropped** - This category gives information related to the packet dropped for unhandled multicast IPv6 on SonicWALL UTM.
- **SonicWALL VPN: Client activity** - This category gives information related to the VPN client activities on SonicWALL UTM.
- **SonicWALL VPN: IKE activity** - This category gives information related to the VPN IKE activities on SonicWALL UTM.
- **SonicWALL VPN: IPsec activity** - This category gives information related to the VPN IPsec activities on SonicWALL UTM.
- **SonicWALL VPN: IPsec tunnel status changed** - This category gives information related to the VPN IPsec tunneling status changed on SonicWALL UTM.
- **SonicWALL VPN: PKI error** - This category gives information related to the PKI error on SonicWALL UTM.

5.2 Alerts

- **SonicWALL UTM: Administrator login failed** - This alert is generated when the administrator login has failed.
- **SonicWALL: Antispam service disabled** - This alert is generated when the antispam service disable.
- **SonicWALL: Antispam service expired** - This alert is generated when the antispam service expires.
- **SonicWALL: Application control detection** - This alert is generated when the application control was detected.
- **SonicWALL: Application control prevention** - This alert is generated when the application control was prevented.
- **SonicWALL: Application filter blocked** - This alert is generated when the application filter has been blocked.
- **SonicWALL: Authentication failed** - This alert is generated when the authentication was failed.
- **SonicWALL: Back orifice attack dropped** - This alert is generated when the back orifice attack was dropped.
- **SonicWALL: Backup firewall transitioned to active** - This alert is generated when the backup of firewall was transited to active mode.
- **SonicWALL: Bad CRL format** - This alert is generated when the bad CRL was formatted.
- **SonicWALL: Certificate import failed** - This alert is generated when the certificate import was failed.
- **SonicWALL: Connectivity error** - This alert is generated when the connectivity generated an error.
- **SonicWALL: CRL validation failure** - This alert is generated when the CRL validation is failed.
- **SonicWALL: DHCP lease expired** - This alert is generated when the DHCP lease has been expired.
- **SonicWALL: DHCP Server IP conflict detected** - This alert is generated when the DHCP server IP address conflict has been detected.
- **SonicWALL: DHCP Server sanity check failed** - This alert is generated when the DHCP server sanity check has been failed.
- **SonicWALL: DNS rebind attack detected** - This alert is generated when the DNS rebind attack has been detected.
- **SonicWALL: DSL device down** - This alert is generated when the DSL device is down.
- **SonicWALL: DSL WAN connected** - This alert is generated when the DSL WAN is connected.
- **SonicWALL: DSL WAN initialized** - This alert is generated when the DSL WAN initialized.
- **SonicWALL: Failed to get CRL** - This alert is generated when it fails to get the CRL.
- **SonicWALL: Failed to process CRL** - This alert is generated when it fails to process the CRL.
- **SonicWALL: Firewall access rule added** - This alert is generated when the Firewall access rule is added.
- **SonicWALL: Firewall access rule deleted** - This alert is generated when the Firewall access rule is deleted.
- **SonicWALL: Firewall access rule modified** - This alert is generated when the Firewall access rule is modified.
- **SonicWALL: FTP connection dropped** - This alert is generated when the FTP connection is dropped.
- **SonicWALL: FTP logon failure** - This alert is generated when the FTP logon failure occurs.
- **SonicWALL: Interface link down** - This alert is generated when the Interface link is down.
- **SonicWALL: Intrusion detection** - This alert is generated when the Intrusion detection occurs.
- **SonicWALL: IPS alert** - This alert is generated when the IPS alert occurs.
- **SonicWALL: Issuer match failed** - This alert is generated when the issuer match fails.
- **SonicWALL: L2TP error** - This alert is generated when the L2TP error occurs.

- **SonicWALL: Multicast policy list deleted** - This alert is generated when the Multicast policy list deleted.
- **SonicWALL: NetBus attack dropped** - This alert is generated when the NetBus attack is dropped.
- **SonicWALL: NetSpy attack dropped** - This alert is generated when the NetSpy attack is dropped.
- **SonicWALL: Outbound access blocked** - This alert is generated when the outbound access is blocked.
- **SonicWALL: Ping of death dropped** - This alert is generated when the Ping of death is dropped.
- **SonicWALL: PPP Dial-Up dialing failed** - This alert is generated when the PPP Dial-Up dialing is failed.
- **SonicWALL: SIM detection failure** - This alert is generated when the SIM detection failure occurs.
- **SonicWALL: Spam detected** - This alert is generated when the Spam is detected.
- **SonicWALL: SSO agent down** - This alert is generated when the SSO agent is down.
- **SonicWALL: System fan failure** - This alert is generated when the System fan failure occurs.
- **SonicWALL: User login failed** - This alert is generated when the User login fails.
- **SonicWALL: Website access denied** - This alert is generated when the Website access is denied.
- **SonicWALL Firewall: VPN User authentication failed** - This alert is generated when the user authentication is failed.

5.3 Reports

- **SonicWALL Firewall-Network access report:** This report provides information related to the network access which includes the Source IP Address, Source Port, Destination IP Address, Destination Port, WAN Address and Message Column.
- **SonicWALL UTM-WLAN IDS report:** This report provides information related to the WLAN IDS which includes the Source IP address and Message Column.
- **SonicWALL UTM-FTP logon details:** This report provides information related to the FTP logon details which include the Username, Source IP address and Message Column.
- **SonicWALL UTM-Website access allowed:** This report provides information related to website access allowed which includes the Username, Source IP address, URL Category and URL Name.
- **SonicWALL Firewall-access rule change:** This report provides information related to the firewall access rule change which includes the Username, Source IP address and Message Column.
- **SonicWALL UTM-User activity:** This report provides information related to the user activity which includes the Username, Source IP address and Messages Column.
- **SonicWALL UTM-Anti-Spyware detected:** This report provides information related to the anti-spyware detected which includes Event generated time and the Source IP address Column.
- **SonicWALL UTM-DSL activity:** This report provides information related to the DSL activity which includes the Username, Source IP address and Messages Column.
- **SonicWALL UTM-Attacks detection:** This report provides information related to the attack detection which includes the Source IP address and Messages Column.

- **SonicWALL UTM-Application control prevention:** This report provides information related to application control prevention which includes the Source IP address and Messages Column.
- **SonicWALL UTM-Application control detection:** This report provides information related to application control detection which includes which includes the Source IP address and Messages Column.
- **SonicWALL UTM-Admin login failed:** This report provides information related to the admin login failed which includes the Username, Source IP address and Messages Column.
- **SonicWALL UTM-Authentication failed:** This report provides information related to the authentication failed which includes Username, Source IP address and Messages Column.
- **SonicWALL UTM-Authentication success:** This report provides information related to the authentication success which includes the Username, Source IP address and Messages Column.
- **SonicWALL UTM-Interface link status:** This report provides information related to the interface link status which includes the interface name and its status (UP OR DOWN).
- **SonicWALL UTM-Connection closed dropped or terminated:** This report provides information related to the connection status which includes the source and the destination IP address, ports and connection status (closed, dropped and terminated) with protocol used during the connection.
- **SonicWALL UTM-Connection opened or established:** This report provides information related to the connection opened and established which includes the source and the destination IP address, ports and interface, application used for making connection and protocol details.
- **SonicWALL UTM-Terminal services or SSO Agent:** This report provides information related to the terminal and the SSO services status which includes the service name (terminal or SSO) and its status and by whom these services are enabled and disabled.
- **SonicWALL UTM-Website access denied:** This report provides information related to the websites whose access are denied which includes the source and the destination IP address, port and interface and the URL and its category.
- **SonicWALL UTM-Intrusion detection:** This report provides information related to the intrusion detected by the SonicWALL firewall which includes the source details, victim details and the attack name.
- **SonicWALL UTM-Multicast policy list:** This report provides information related to the addition or deletion of the multicast policy list in interface or VPN SPI, which includes the interface Name and the VPN SPI value in which the multicast policy is added or deleted.
- **SonicWALL UTM-Antispam service:** This report provides information related to the antispam service which includes the status of the service and by whom it is enabled or disabled.

- **SonicWALL UTM-System Shutdown by Administrator:** This report provides information related to the system shutdown by the administrator which includes the user details i.e., by whom the firewall is shutdown.
- **SonicWALL UTM-Configuration change details:** This report provides information related to the configuration change. It shows the Username, the Source IP address and the Destination IP address and also what have been changed.
- **SonicWALL Firewall-VPN User authentication failed:** This report provides information related to the User authentication failure which includes the Source address and Port, Destination address and Port, Additional Information and Reason for failure.
- **SonicWALL Firewall-VPN User authentication success:** This report provides information related to the User authentication success which includes the Source address and Port, the Destination address and Port, Additional Information and the Reason for success.
- **SonicWALL Firewall-VPN activity:** This report provides information related to the VPN activity that contains the VPN Client, VPN IPsec, VPN IKE, and the VPN PKI which includes the Source address and Port, Destination address and Port, Additional Information and message.
- **SonicWALL Firewall-VPN IPsec tunnel status changed:** This report provides information related to the IPsec tunnel status that is changed to up or down which includes the Source Range, Destination Range, Gateway, Reason, Status and the VPN Details.
- **SonicWALL Firewall- Traffic flow:** This report provides information related to the traffic flow. It gives information regarding where the traffic connected is opened or closed.
- **SonicWALL UTM-Administrator login status:** This report provides information related to the administrator login status.
- **SonicWALL UTM-Application management:** This report provides information related to the application activities that have occurred.
- **SonicWALL UTM-Connection status:** This report provides information related to the connection status.
- **SonicWALL UTM-DHCP lease status:** This report provides information related to the DHCP lease status.
- **SonicWALL Firewall-Access rule change:** This report provides information related to the firewall access rule changes.
- **SonicWALL Firewall-IDS attacks:** This report provides information related to the IDS attacks that occur in the system.
- **SonicWALL UTM-FTP logon status:** This report provides information related to the FTP logon status.

- **SonicWALL-User admin login status:** This report provides information related to the user admin login status.
- **SonicWALL UTM-User authentication status:** This report provides information related to the user authentication status.
- **SonicWALL UTM-Website access status:** This report provides information related to the website access status.

6. Importing SonicWALL UTM Knowledge pack into EventTracker

1. Launch the **EventTracker Control Panel**.
2. Double click the **Export Import Utility**, and then click the **Import** tab.

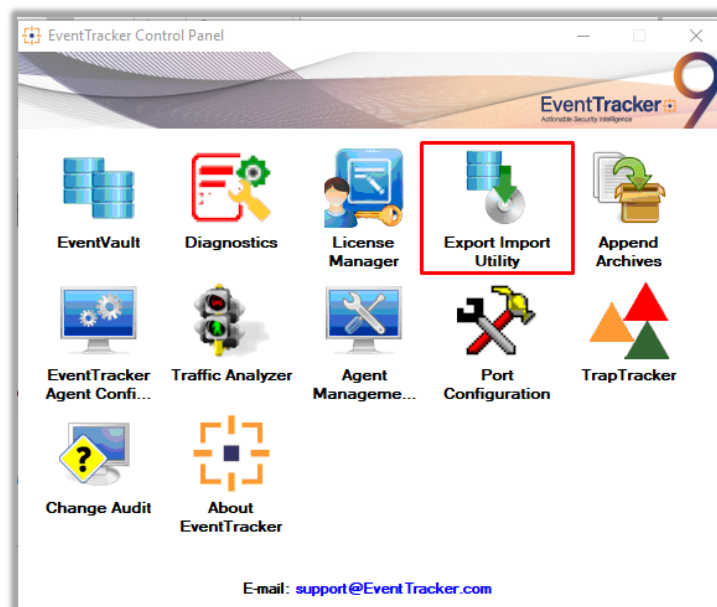


Figure 14

Import the following in the same order as mentioned below.

- **Template**
- **Category**
- **Alert**
- **Tokens**
- **Flex Reports**

6.1 Templates

1. Click the **Admin** menu, and then click the **Parsing rule**.

2. Select the **Template** tab, and then click the **Import** option.

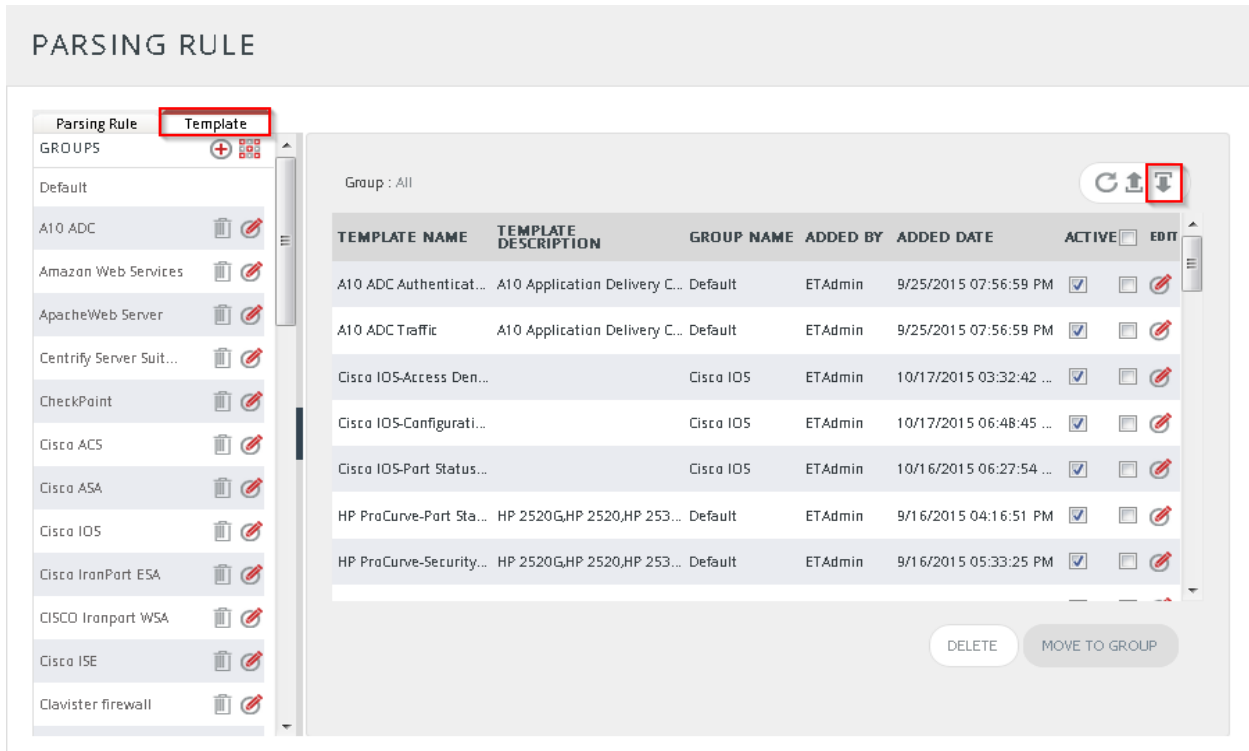


Figure 15

3. Click the **Browse** button.

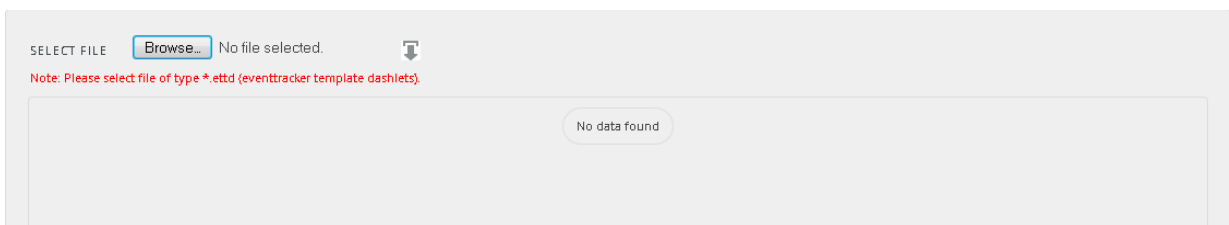


Figure 16

4. Locate the **All SonicWALL UTM group of the Template.ettd** file, and then click **Open**.

SELECTED FILE IS: All SonicWALL UTM group of Template.ettid

<input type="checkbox"/>	TEMPLATE NAME	SEPARATOR	TEMPLATE DESCRIPTION	ADDED DATE	ADDED BY	GROUP NAME
<input type="checkbox"/>	Sonicwall: Application management	\n	May 25 22:36:14 10.0.105.190 id=firewall sn=C0EAE41C2714 time="2014-05-26 02:36:14 UTC" fw=75.147.154.153 pri=1 c=0 m=649 msg="Application Filters Block Alert: facebook.com" sid=5148 appcat=PROTOCOLS appid=1277 sess=Auto n=2673709 usr="VLC ech2" src=10.0.105.86:62016:X0:VLC-TECH2 dst=72.3.209.232:80:X1:us11.systemmonitor.us	7/13/2016 3:28:24 PM	abhilanchana	Sonicwall UTM
<input type="checkbox"/>	Sonicwall: DHCP lease status	\n	May 27 18:30:12 10.0.105.190 id=firewall sn=C0EAE41C2714 time="2014-05-27 18:30:12 UTC" fw=75.147.154.153 pri=6 c=32 m=222 msg="DHCP RELEASE relayed to Central Gateway" sess=Web n=6 usr="john" src=10.0.105.202:0:X0:VLC-ADMIN dst=10.0.105.130:443:X0:	7/14/2016 5:00:09 PM	abhilanchana	Sonicwall UTM
<input type="checkbox"/>	Sonicwall: Firewall access rule change	\n	May 25 12:00:59 10.0.105.190 id=firewall sn=C0EAE41C2714 time="2014-05-25 16:00:59 UTC" fw=75.147.154.153 pri=3 c=4 m=443 msg="Access rules restored to defaults" sess=Auto n=16253 usr="ucknorth" src=10.0.105.40:53177:X0:VLC-TRUCK-N dst=184.51.207.65:80:X1: dstname=static-p-a.comcast.net arg=/api/assets/cimed-20120712/nbc.png code=4 Category="Pornography"	7/14/2016 6:12:19 PM	abhilanchana	Sonicwall UTM
<input type="checkbox"/>			May 21 12:26:08 10.0.105.190 id=firewall sn=C0EAE41C2714 time="2014-05-21 16:26:08 UTC" fw=75.147.154.153 pri=1 c=32 m=79 mse="Priority attack droop			

Figure 17

5. Select the check box and then click the **Import** option. EventTracker displays a success message.

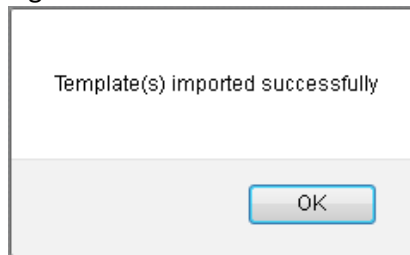


Figure 18

6. Click the **OK** button.

6.2 Importing Categories

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

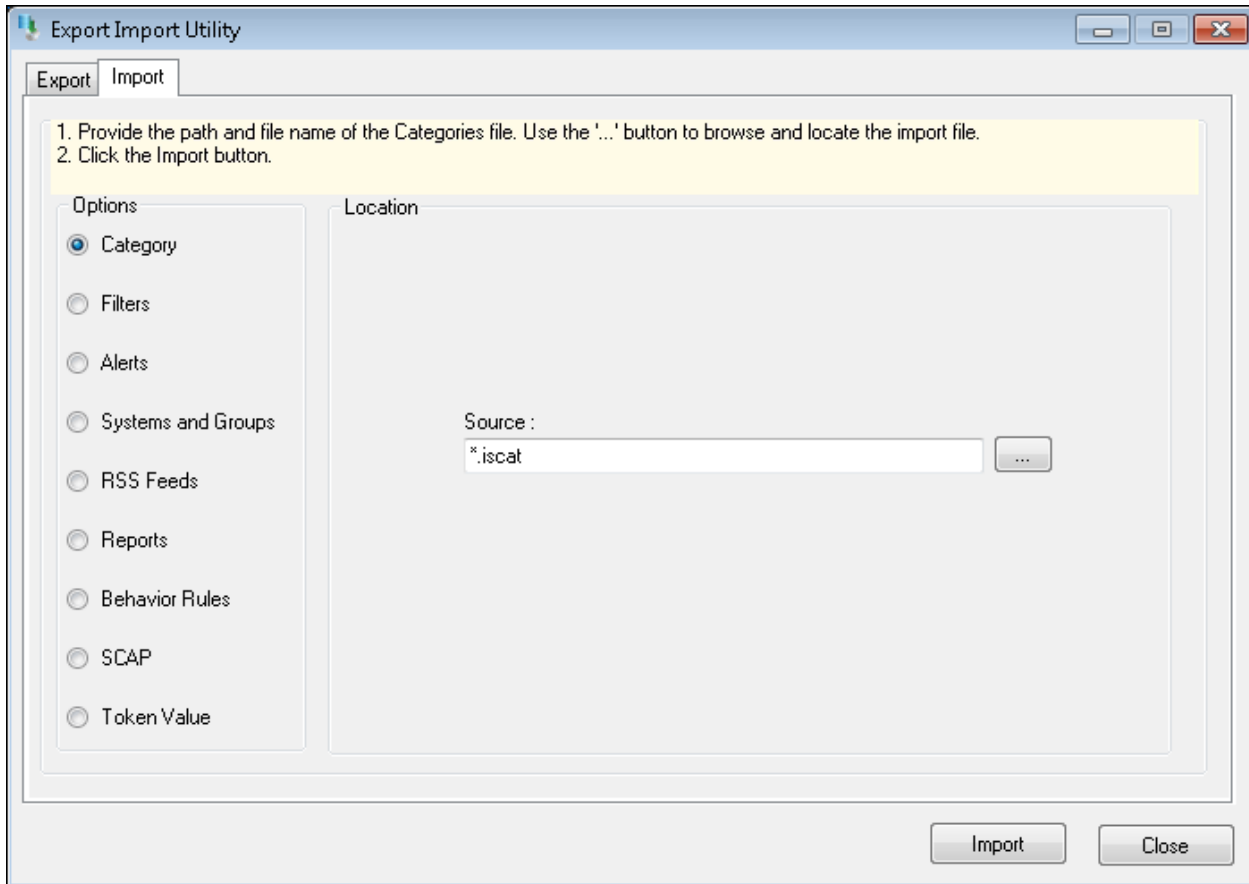


Figure 19

2. Locate the **All SonicWALL UTM group of the Categories.iscat** file, and then click **Open**.
3. To import the categories, click the **Import** button.
EventTracker displays a success message.

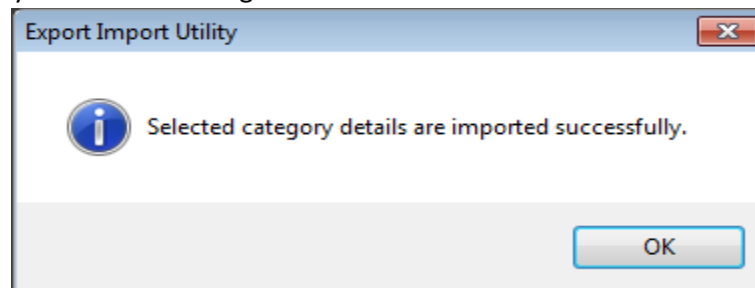



Figure 20

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

6.3 Importing Alerts

1. Click the **Alert** option, and then click the **Browse**  button.

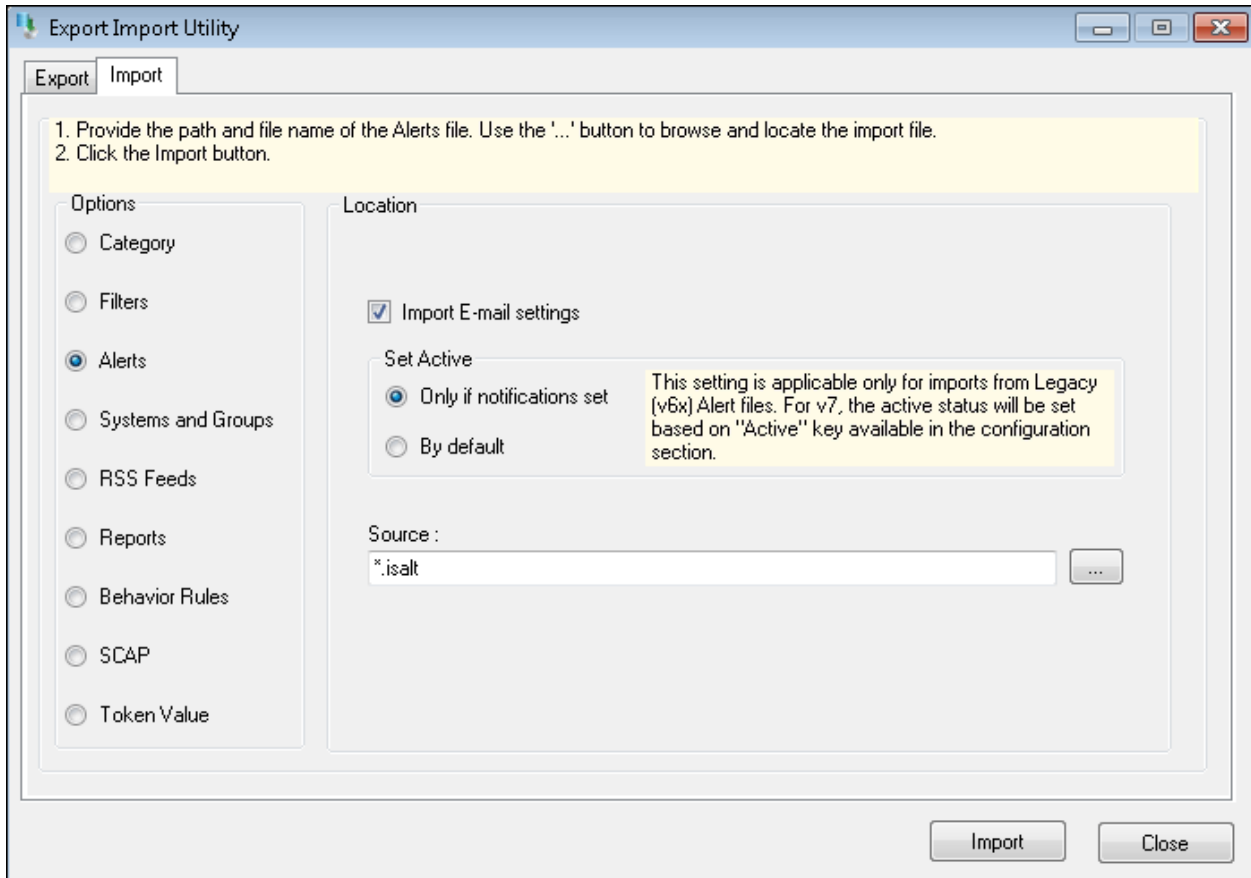


Figure 21

2. Locate the **All SonicWALL UTM group of the Alerts.isalt** file, and then click **Open**.
3. To import the alerts, click the **Import** button.
EventTracker displays a success message.

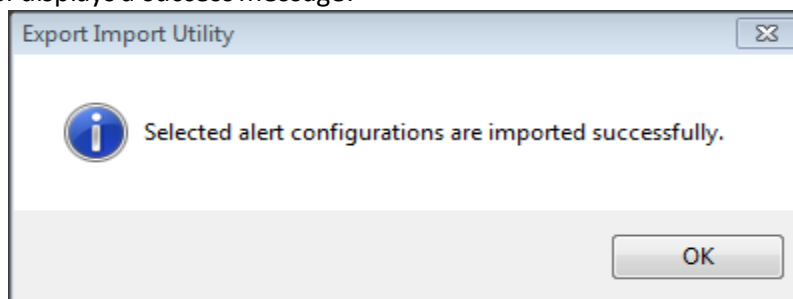



Figure 22

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

6.4 Importing Tokens

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

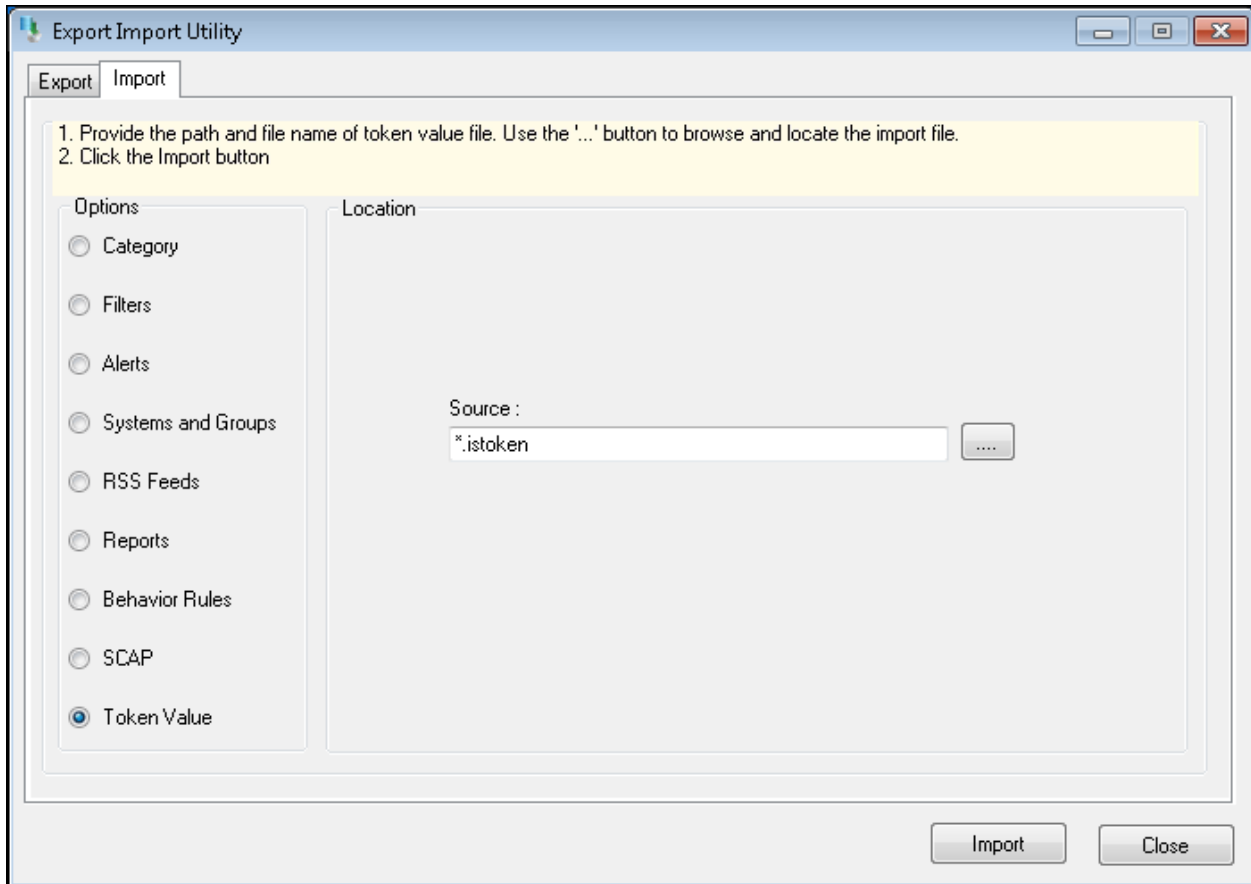


Figure 23

2. Locate the **All SonicWALL UTM group of the Tokens.istoken** file, and then click **Open**.
 3. To import the tokens, click the **Import** button.
- EventTracker displays a success message.

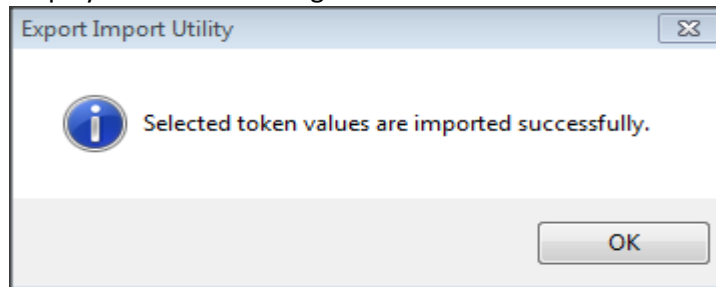



Figure 24

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

6.5 Importing Flex Reports

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

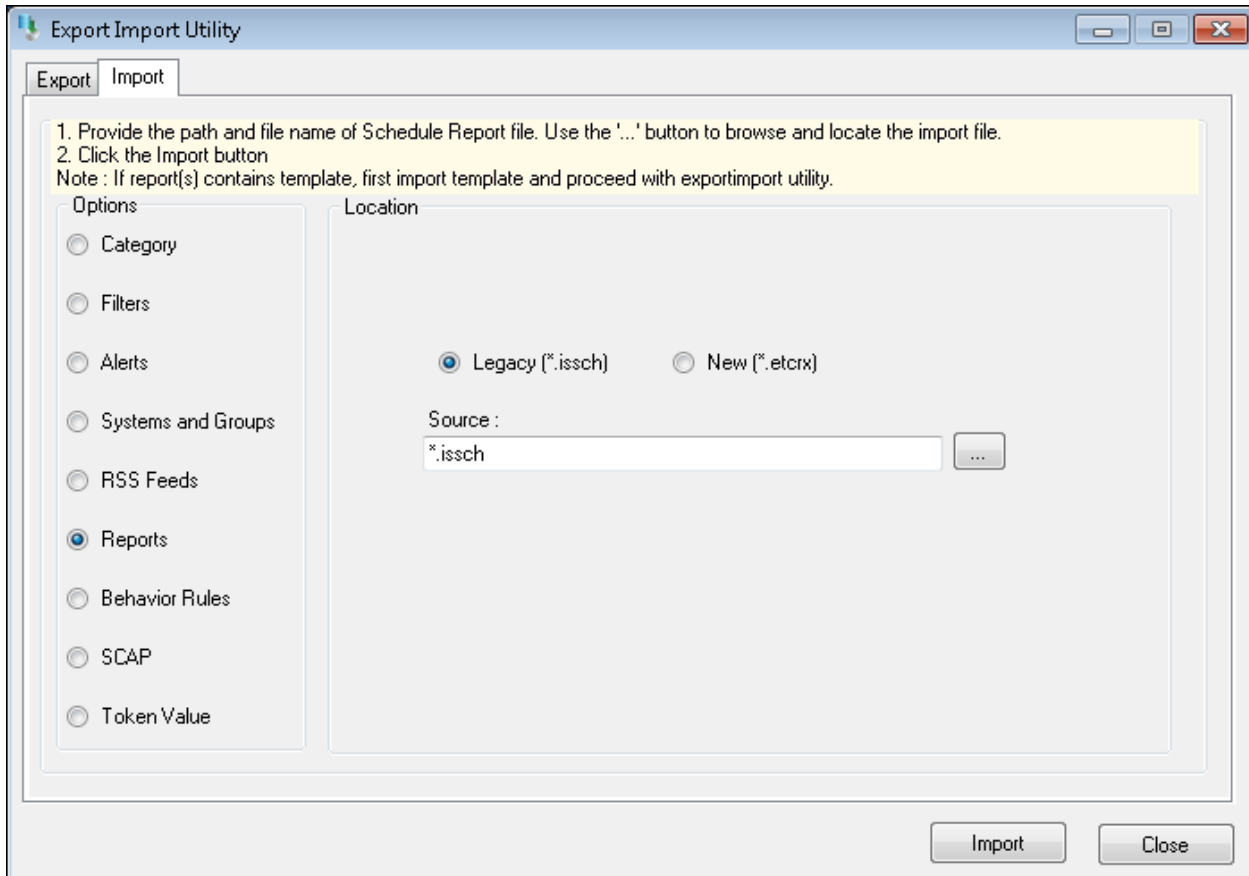


Figure 25

2. Locate the **All SonicWALL UTM group of the Flex Report.issch** file, and then click **Open**.
3. To import the scheduled reports, click the **Import** button.
 EventTracker displays a success message.

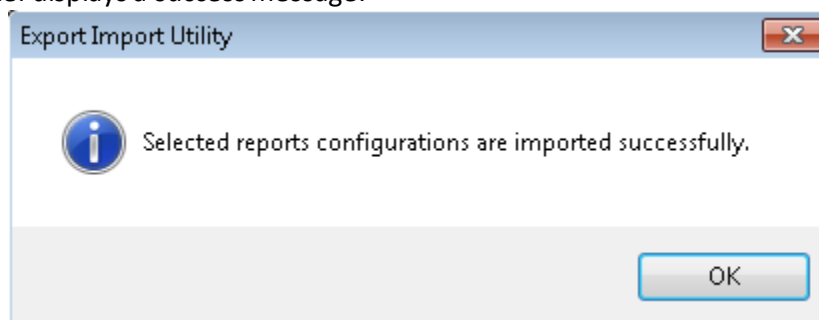


Figure 26

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

7. Verifying the SonicWALL UTM Knowledge Pack in EventTracker

7.1 Template

1. Logon to the **EventTracker** web interface.
2. Click the **Admin** menu, and then click **Parsing Rules** and click **Template**.

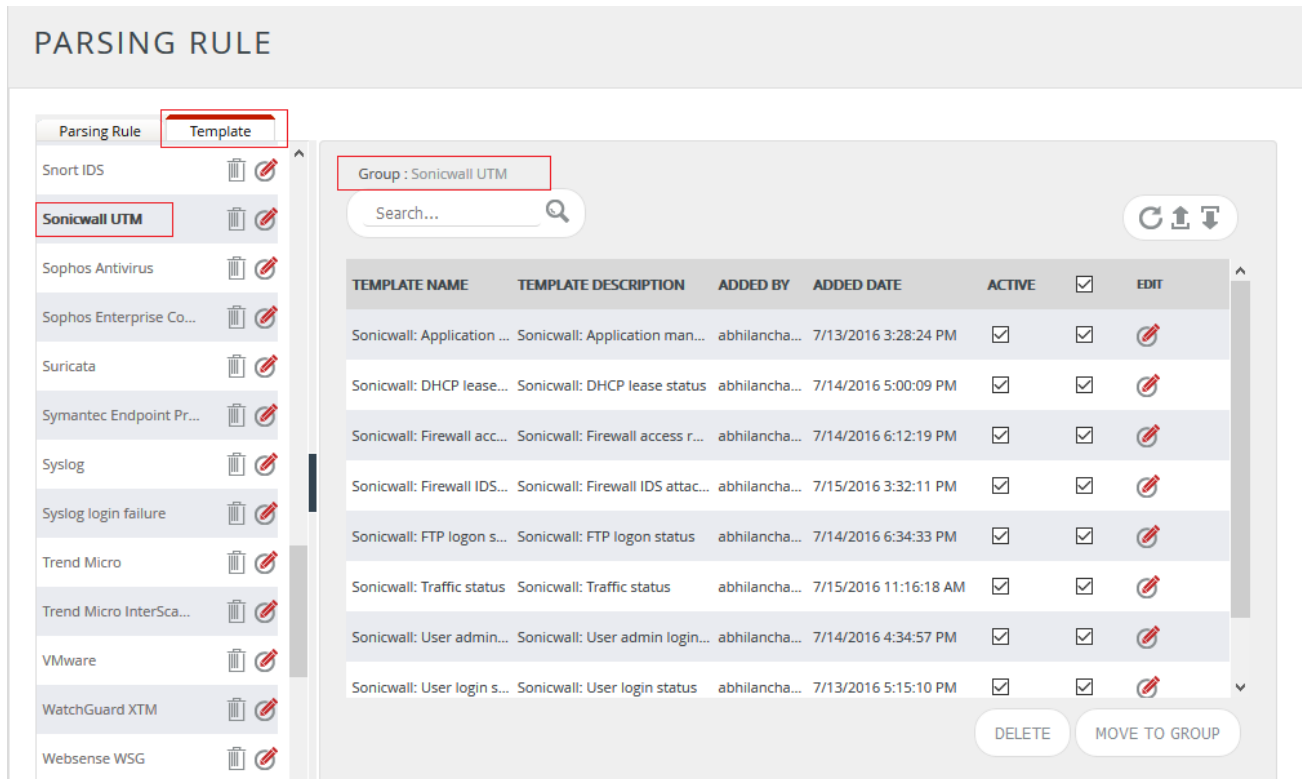


Figure 27

7.2 Verifying the SonicWALL UTM Categories

1. Logon to **EventTracker**.
2. Click the **Admin** menu, and then click **Categories**.
3. In the **Category Tree**, expand the **SonicWALL UTM** group folder to view the imported categories.

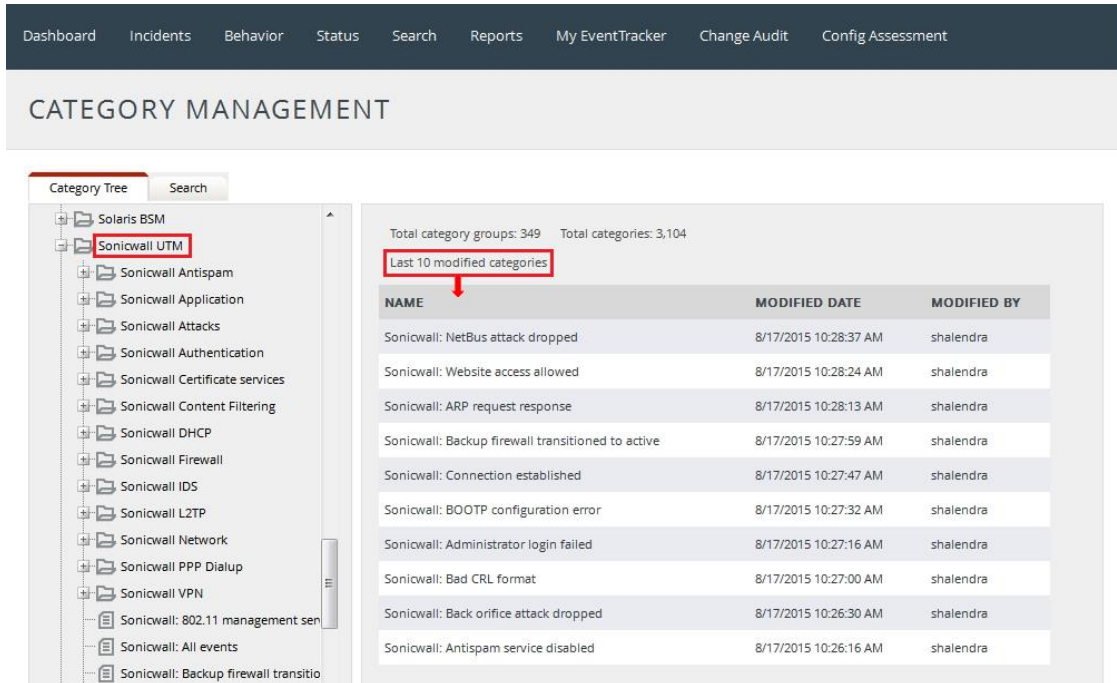


Figure 28

7.3 Verifying the SonicWALL UTM Alerts

1. Logon to **EventTracker**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In the **Search** field, type **SonicWALL**, and then click the **Go** button.
The Alert Management page will display all the imported SonicWALL UTM alerts.

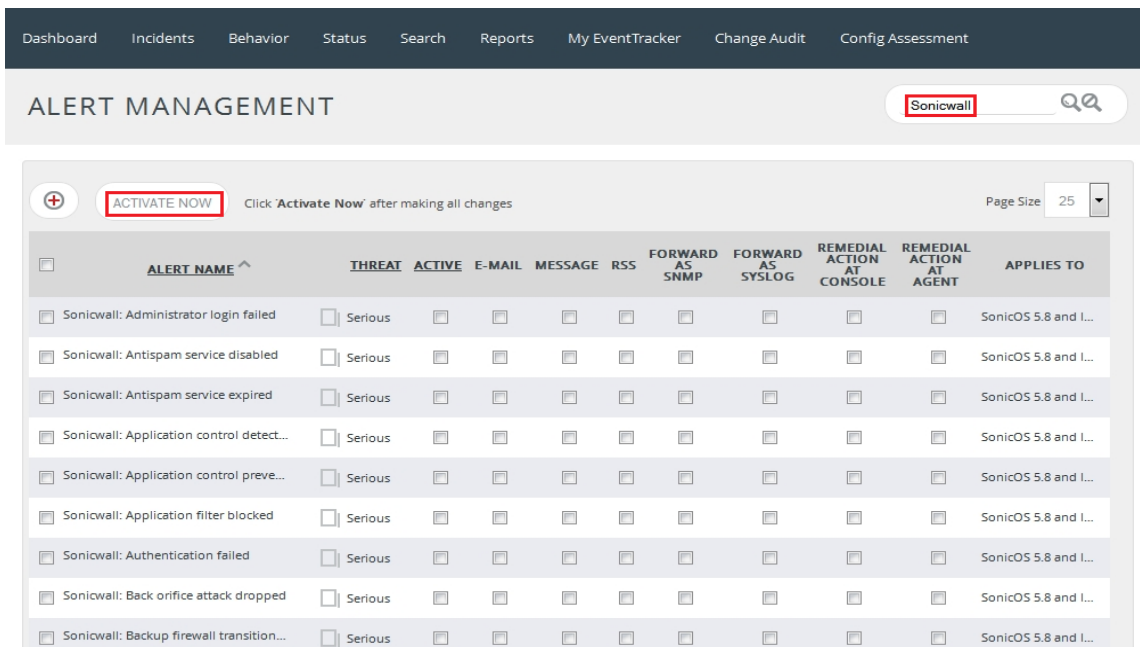


Figure 29

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

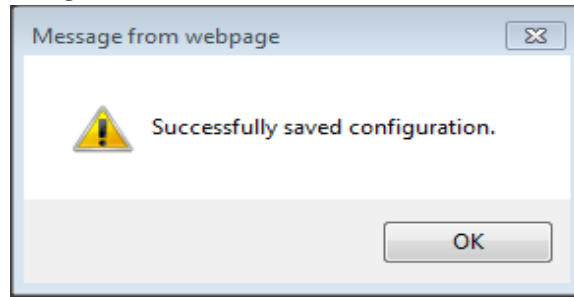


Figure 30

- Click the **OK** button, and then click the **Activate Now** button.
NOTE: You can select the 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.

7.4 Verifying the SonicWALL UTM Tokens

- Logon to **EventTracker**.
- Click the **Admin** menu, and then click the **Parsing rule**.
 The imported SonicWALL UTM tokens are added to the Token-Value Groups list.

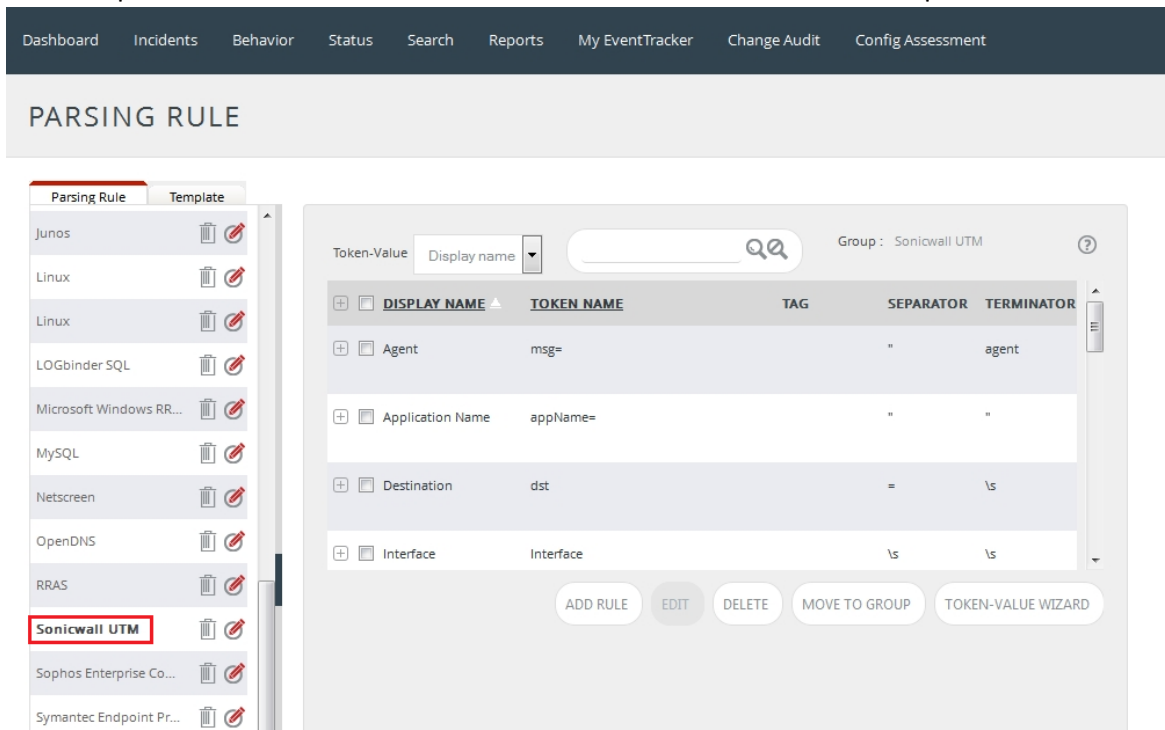


Figure 31

7.5 Verifying the SonicWALL UTM Flex Reports

1. Logon to **EventTracker**.
 2. Click the **Reports** menu, and then select **Configuration**.
 3. In **Reports Configuration**, select the **Defined** option.
 4. In the search box enter **SonicWALL**, and then click the **Search** button.
- EventTracker displays a Flex report of SonicWALLUTM.

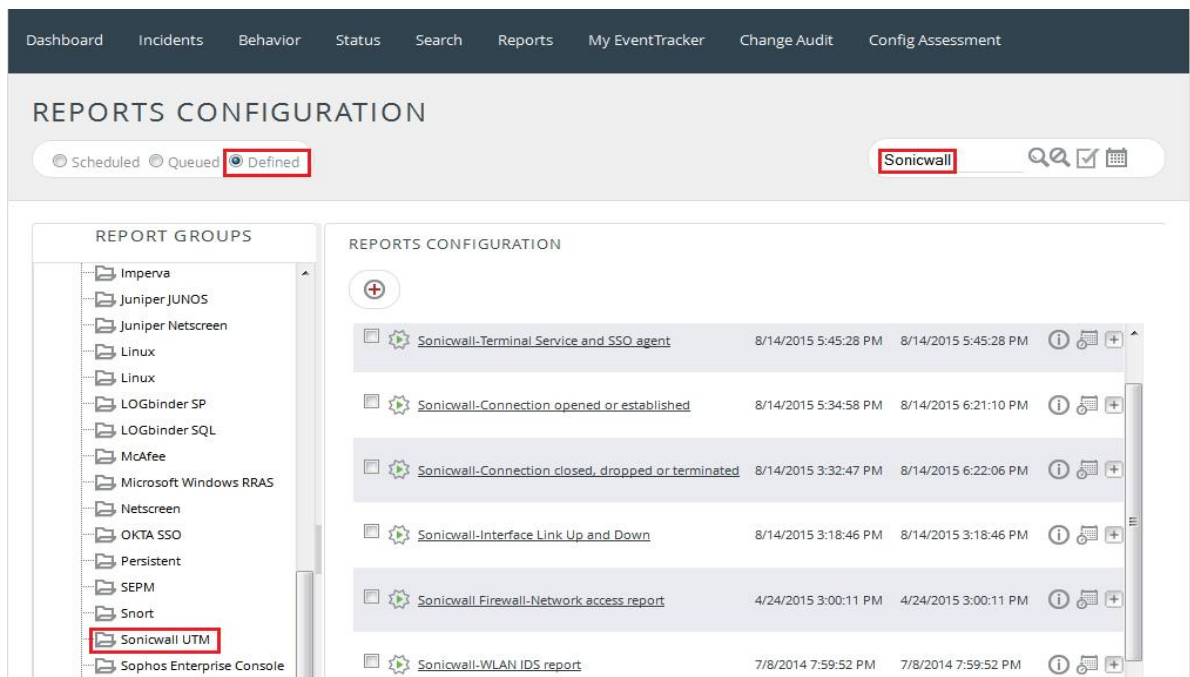


Figure 32

8. Creating Dashboards in EventTracker

8.1 Scheduling Reports

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

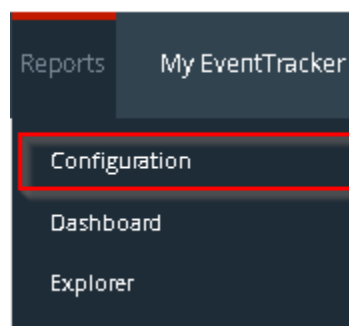


Figure 33

2. Navigate to **Reports>Configuration**.

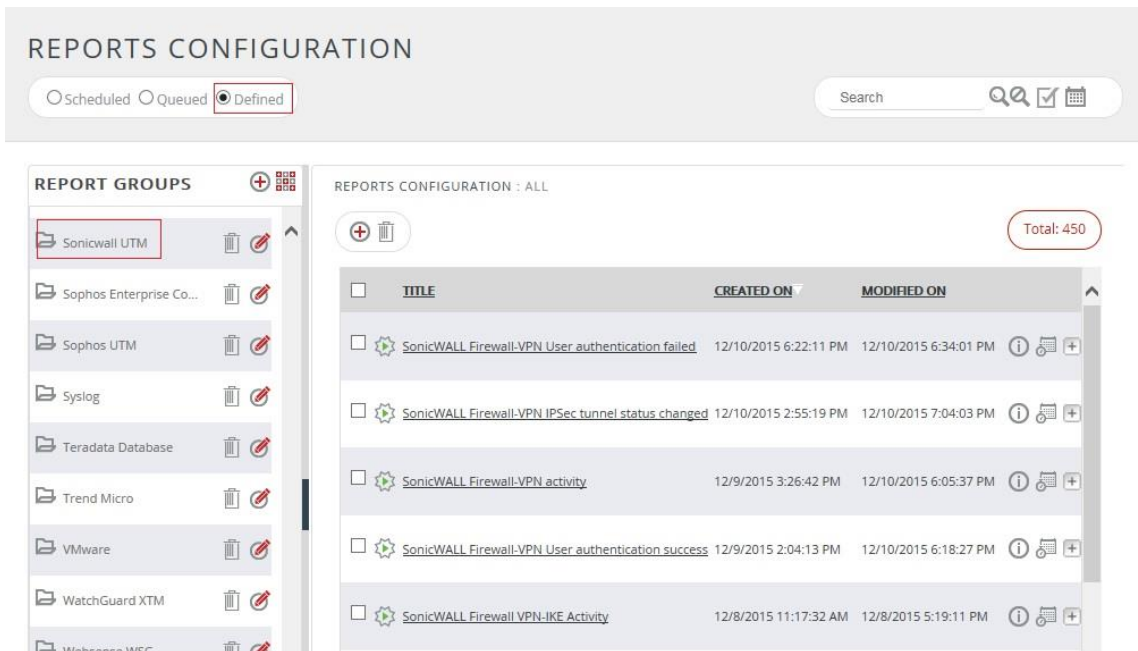



Figure 34

3. Select SonicWALL UTM in report groups. Check the **Defined** dialog box.
4. Click **Schedule**  to plan a report for later execution.
5. Choose the appropriate time for the report execution and in **Step 8** check **Persist data in the Event vault explorer** box.

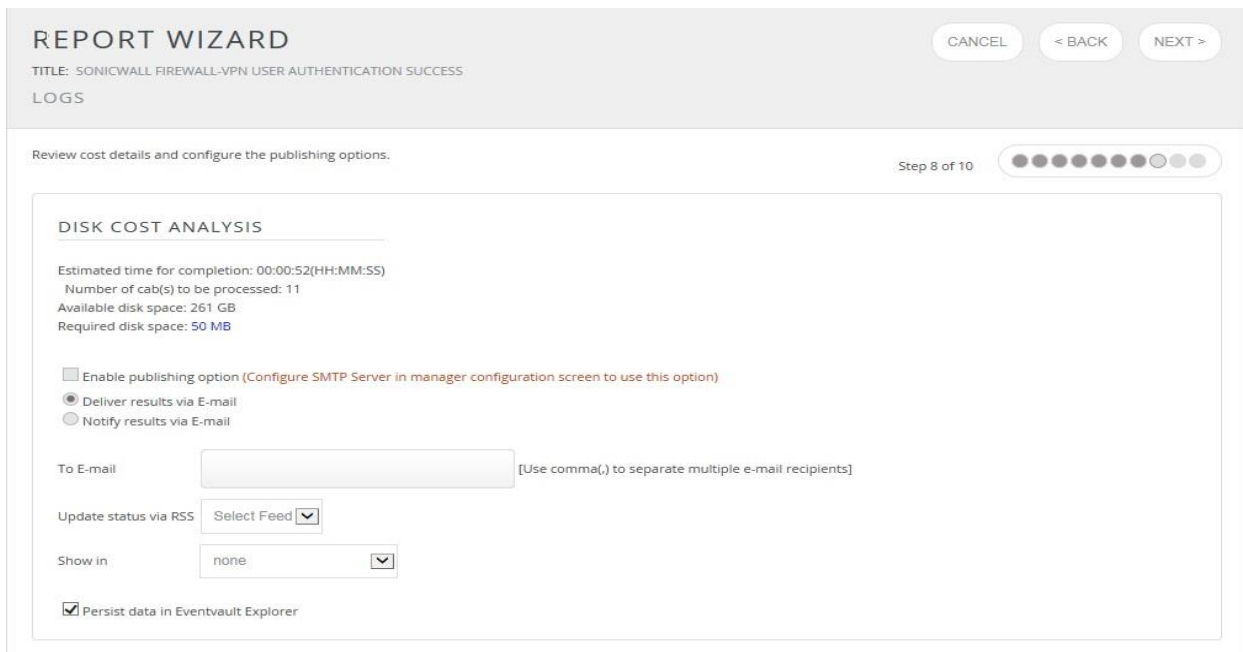


Figure 35

REPORT WIZARD

TITLE: INFOBLOX-USER LOGON DETAILS
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
Device Address	<input checked="" type="checkbox"/>
User Name	<input checked="" type="checkbox"/>
Source Address	<input checked="" type="checkbox"/>
Console Type	<input checked="" type="checkbox"/>
Logon Status	<input checked="" type="checkbox"/>

Figure 36

6. Check column names to persist using **PERSIST** checkboxes beside them. Choose a suitable **Retention period**.
7. Proceed to the next step and click the **Schedule** button.
8. Wait for the scheduled time or generate a report manually.

8.2 Creating Dashlets

1. **EventTracker 8** is required to configure the Flex dashboard.
2. Open **EventTracker** in browser and logon.

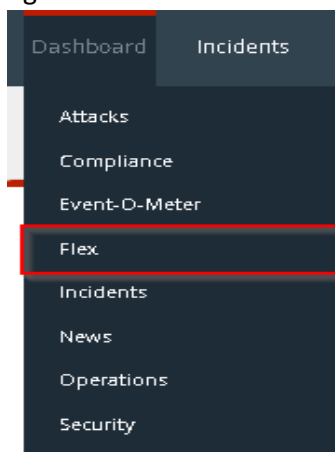


Figure 37

3. Navigate to **Dashboard>Flex**.
Flex Dashboard pane display.

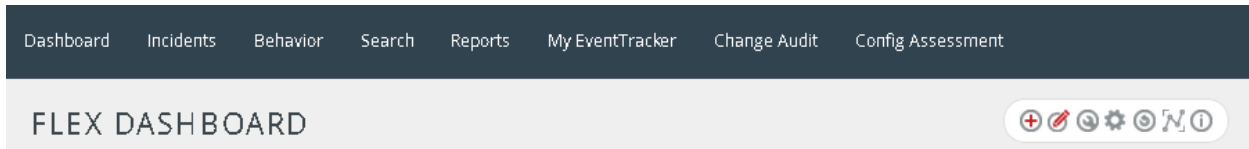



Figure 38

4. Click  to add a new dashboard.
Flex Dashboard configuration pane display.

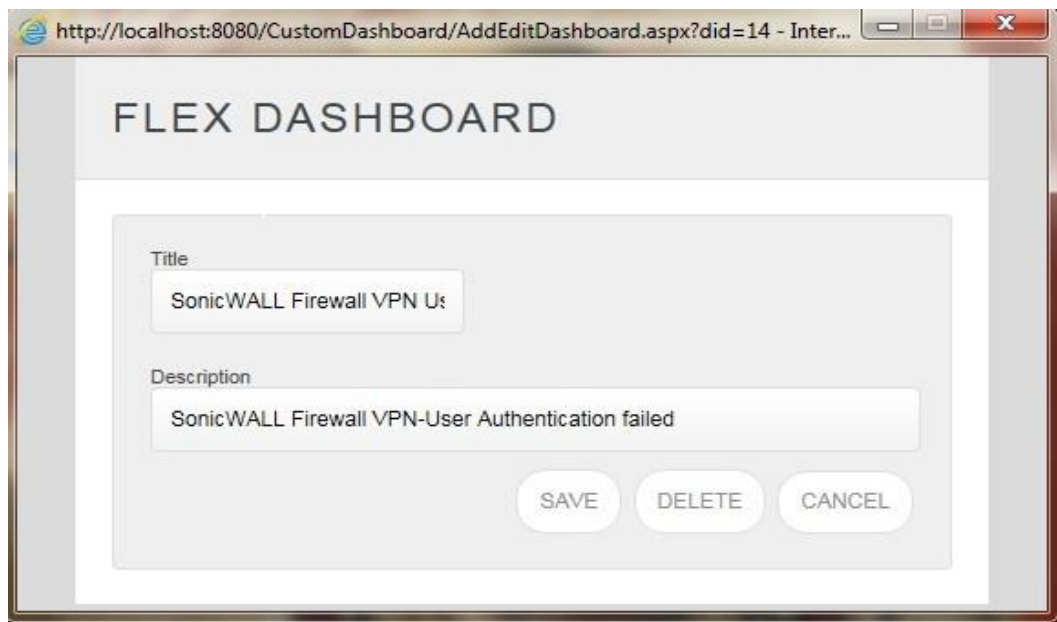



Figure 39

5. Fill in the title and description and click **save**.
6. Click settings  to configure a new Flex dashlet.
The Widget configuration pane display.

WIDGET CONFIGURATION

WIDGET TITLE: SonicWALL Firewall-VPN User authentication success

NOTE: [Empty text box]

DATA SOURCE: SonicWALL Firewall-VPN User authentication success

CHART TYPE: Donut

DURATION: 12 Hours

VALUE FIELD SETTING: COUNT

AS OF: Now

AXIS LABELS [X-AXIS]: Additional Information

LABEL TEXT: [Empty text box]

VALUES [Y-AXIS]: Select column

VALUE TEXT: [Empty text box]

FILTER: Select column

FILTER VALUES: [Empty dropdown]

LEGEND [SERIES]: Select column

SELECT: All

Figure 40

- Locate the earlier scheduled report in the **Data Source** dropdown.
- Select **Chart Type** from the dropdown.
- Select the extent of data to be displayed in the **Duration** dropdown.
- Select the computation type in the **Value Field Setting** dropdown.
- Select the evaluation duration in the **As Of** dropdown.
- Select the comparable values in the **X-Axis** with a suitable label.
- Select the numeric values in the **Y-Axis** with a suitable label.
- Select the comparable sequence in **Legend**.
- Click the **Test** button to evaluate.

Evaluated chart display.

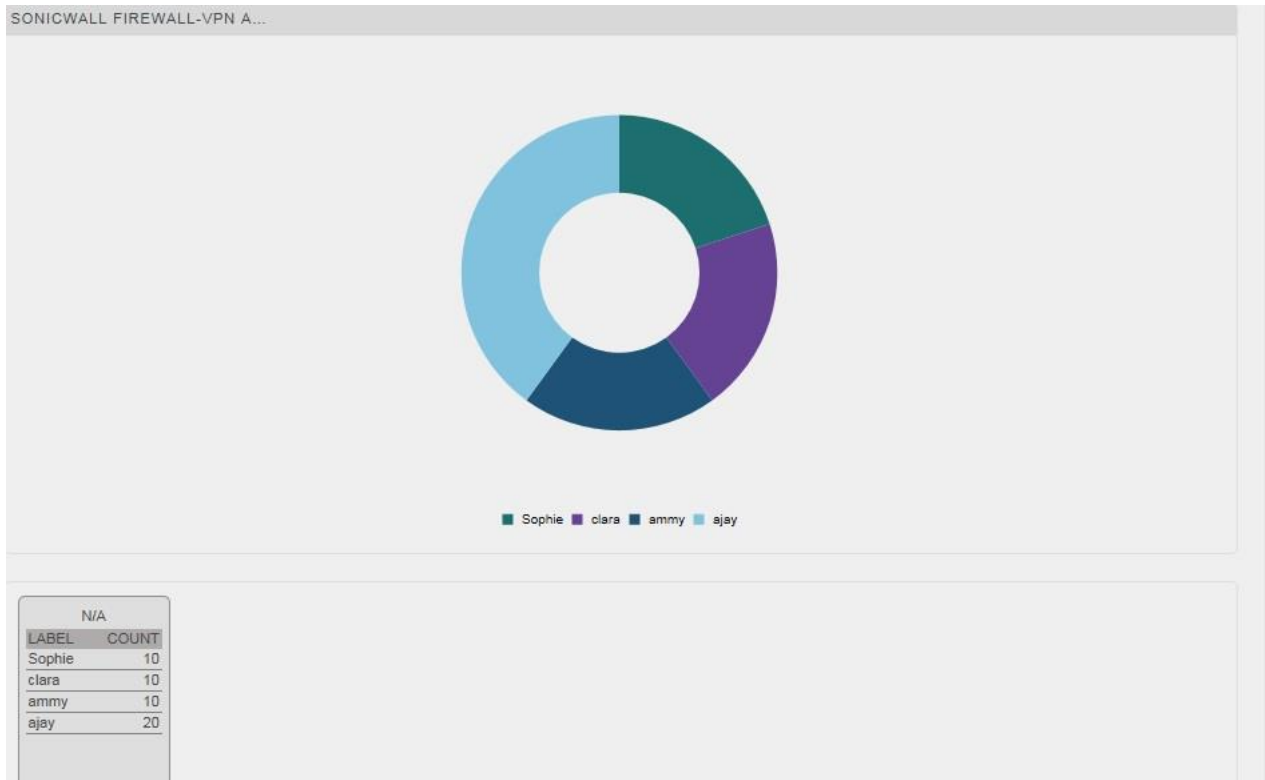




Figure 41

j. Once done, click the **Configure** button.



Figure 42

7. Click **Customize**  to locate and choose created dashlet.
8. Click  to add dashlet to earlier created dashboard.

9. Sample Reports

- **SonicWALL Firewall - Configuration Change Details**

LogTime	Computer	Username	Source IP Address	Destination IP Address	Message
10/12/2015 12:15:39 PM	SONIC	mike	10.20.2.100	10.20.2.1	High Availability is disabled
10/12/2015 12:15:39 PM	SONIC	john	10.20.2.110	10.20.2.1	High Availability is enabled
10/12/2015 12:15:40 PM	SONIC	robin	10.20.2.45	10.20.2.1	User created
10/12/2015 12:15:40 PM	SONIC	james	10.20.2.78	10.20.2.1	logging configured

Figure 43

- **SonicWALL Firewall-VPN IPsec tunnel status changed**

LogTime	Computer	Source Range	Destination Range	Gateway	Reason	Status	VPN Details
12/08/2015 03:27:44 PM	SONIC	172.28.7.113 - 172.28.7.113	172.27.255.249 - 172.27.255.249	67.99.3.149	Commit Renew IPsec (Existed dstNode)	Tunnel Up	policy 36(SYMITAR JHA VPN)
12/08/2015 03:27:44 PM	SONIC	172.28.7.113 - 172.28.7.113	172.27.255.249 - 172.27.255.249	67.99.3.149	Commit Renew IPsec (Existed dstNode)	Tunnel Up	policy 36(SYMITAR JHA VPN)
12/08/2015 03:27:44 PM	SONIC	172.28.7.113 - 172.28.7.113	172.27.255.249 - 172.27.255.249	67.99.3.149	Commit Renew IPsec (Existed dstNode)	Tunnel Up	policy 36(SYMITAR JHA VPN)
12/08/2015 03:27:44 PM	SONIC	172.28.7.113 - 172.28.7.113	172.27.255.249 - 172.27.255.249	67.99.3.149	Commit Renew IPsec (Existed dstNode)	Tunnel Up	policy 36(SYMITAR JHA VPN)
12/08/2015 03:27:44 PM	SONIC	172.28.7.113 - 172.28.7.113	172.27.255.249 - 172.27.255.249	67.99.3.149	Commit Renew IPsec (Existed dstNode)	Tunnel Up	policy 36(SYMITAR JHA VPN)
12/08/2015 03:28:02 PM	SONIC	172.22.15.73 - 172.22.15.73	199.195.218.14 - 199.195.218.14	199.195.218.20	Remove IPsec SaNode	Tunnel Down	policy 39(DataVailVPN218)
12/08/2015 03:28:02 PM	SONIC	172.22.15.73 - 172.22.15.73	199.195.218.14 - 199.195.218.14	199.195.218.20	Remove IPsec SaNode	Tunnel Down	policy 39(DataVailVPN218)
12/08/2015 03:28:02 PM	SONIC	172.22.15.73 - 172.22.15.73	199.195.218.14 - 199.195.218.14	199.195.218.20	Remove IPsec SaNode	Tunnel Down	policy 39(DataVailVPN218)
12/08/2015 03:28:02 PM	SONIC	172.22.15.73 - 172.22.15.73	199.195.218.14 - 199.195.218.14	199.195.218.20	Remove IPsec SaNode	Tunnel Down	policy 39(DataVailVPN218)
12/08/2015 03:28:02 PM	SONIC	172.22.15.73 - 172.22.15.73	199.195.218.14 - 199.195.218.14	199.195.218.20	Remove IPsec SaNode	Tunnel Down	policy 39(DataVailVPN218)

Figure 44

- **SonicWALL Firewall – Network Access Report**

LogTime	Source Address	Source Port	Destination Address	Destination Port	Wan Address	Message
04/26/2015 11:17:06 AM	1.214.119.227	55499	98.191.208.24	80	98.191.208.24	Connection Closed
04/26/2015 11:17:03 AM	1.214.119.227	55499	98.191.208.24	80	98.191.208.24	Connection Opened
04/26/2015 12:32:47 PM	1.214.119.227	56995	98.191.208.24	80	98.191.208.24	Web access request dropped
04/26/2015 12:32:47 PM	1.214.119.227	57658	98.191.208.24	80	98.191.208.24	Connection Closed
04/26/2015 12:32:47 PM	1.214.119.227	56603	98.191.208.24	80	98.191.208.24	Connection Closed
04/26/2015 12:32:47 PM	1.214.119.227	56239	98.191.208.24	80	98.191.208.24	Web access request dropped
04/26/2015 12:32:47 PM	1.214.119.227	55788	98.191.208.24	80	98.191.208.24	Connection Closed
04/26/2015 12:32:44 PM	1.214.119.227	58256	98.191.208.24	80	98.191.208.24	UDP packet dropped
04/26/2015 12:32:44 PM	1.214.119.227	57658	98.191.208.24	80	98.191.208.24	Connection Opened
04/26/2015 12:32:43 PM	1.214.119.227	56995	98.191.208.24	80	98.191.208.24	Connection Opened
04/26/2015 12:32:43 PM	1.214.119.227	56603	98.191.208.24	80	98.191.208.24	Web access request dropped
04/26/2015 12:32:42 PM	1.214.119.227	56239	98.191.208.24	80	98.191.208.24	UDP packet dropped
04/26/2015 12:32:42 PM	1.214.119.227	137	98.191.208.24	137	98.191.208.24	Connection Closed
04/26/2015 12:32:42 PM	1.214.119.227	137	98.191.208.24	137	98.191.208.24	ICMP packet dropped due to policy
04/26/2015 12:32:42 PM	1.214.119.227	55788	98.191.208.24	80	98.191.208.24	Connection Opened
04/26/2015 12:32:47 PM	1.214.119.227	58256	98.191.208.24	80	98.191.208.24	Connection Closed
04/26/2015 05:37:36 AM	1.30.20.148	137	98.191.208.24	137	98.191.208.24	Connection Closed
04/26/2015 05:37:36 AM	1.30.20.148	137	98.191.208.24	137	98.191.208.24	ICMP packet dropped due to policy
04/26/2015 05:37:35 AM	1.30.20.148	12238	98.191.208.24	22	98.191.208.24	UDP packet dropped
04/26/2015 05:37:35 AM	1.30.20.148	12238	98.191.208.24	22	98.191.208.24	Connection Opened

Figure 45

10. Sample Dashboards

- SonicWALL Firewall-VPN user authentication success

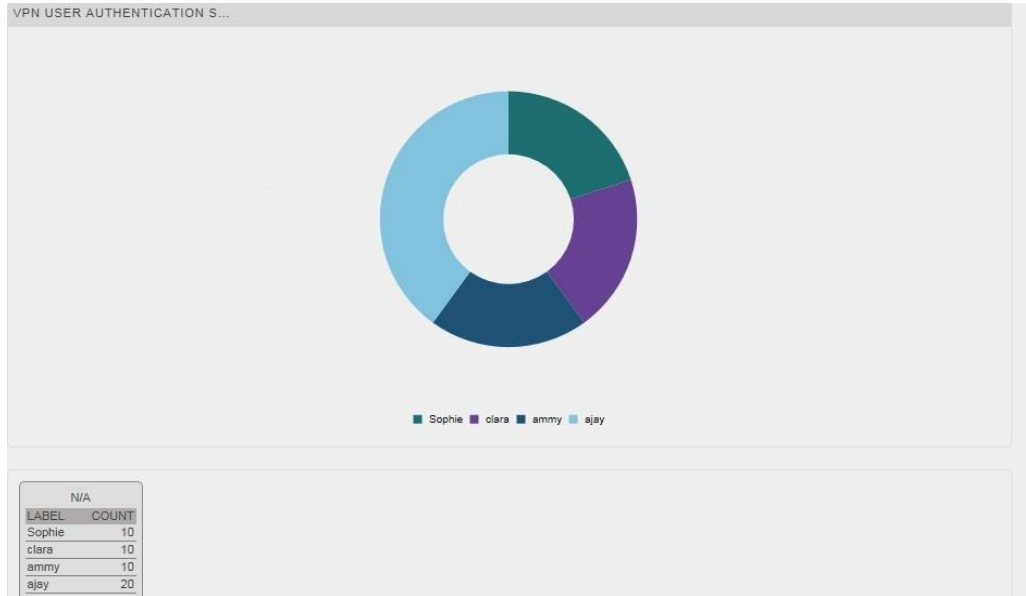


Figure 46

About Netsurion

Flexibility and security within the IT environment are two of the most important factors driving business today. Netsurion's managed cybersecurity platforms enable companies to deliver on both.

Netsurion [Managed Threat Protection](#) combines our ISO-certified security operations center (SOC) with our own award-winning cybersecurity platform to better predict, prevent, detect, and respond to threats against your business. Netsurion [Secure Edge Networking](#) delivers our purpose-built edge networking platform with flexible managed services to multi-location businesses that need optimized network security, agility, resilience, and compliance for all branch locations. Whether you need technology with a guiding hand or a complete outsourcing solution, Netsurion has the model to help drive your business forward. To learn more visit [netsurion.com](https://www.netsurion.com) or follow us on [Twitter](#) or [LinkedIn](#).

Contact Us

Corporate Headquarters

Netsurion
Trade Centre South
100 W. Cypress Creek Rd
Suite 530
Fort Lauderdale, FL 33309

Contact Numbers

EventTracker Enterprise SOC: 877-333-1433 (Option 2)
EventTracker Enterprise for MSP's SOC: 877-333-1433 (Option 3)
EventTracker Essentials SOC: 877-333-1433 (Option 4)
EventTracker Software Support: 877-333-1433 (Option 5)
<https://www.netsurion.com/eventtracker-support>