Integrate SonicWALL UTM

EventTracker Enterprise
Abstract

This guide provides instructions to configure SonicWALL UTM to send the syslog events to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 7.x and later, and SonicOS 5.8 and later for SonicWALL NSA and TZ Series.

Audience

SonicWALL UTM users, who wish to forward syslog events to EventTracker Manager.
# Table of Contents

Abstract ........................................................................................................................................................................................................... 1  
Scope ..................................................................................................................................................................................................... 1  
Audience .......................................................................................................................................................................................... 1  
Overview ...................................................................................................................................................................................... 3  
Prerequisites .................................................................................................................................................................................... 3  
Integrate SonicWALL UTM with EventTracker ......................................................................................................................... 3  
  Configure Syslog Settings .......................................................................................................................................................... 3  
  Configure Syslog Server ........................................................................................................................................................... 7  
Syslog Send Receive Verification .................................................................................................................................................. 9  
  Verify ping from SonicWALL UTM to EventTracker .............................................................................................................. 9  
  Verify Syslog messages forwarding on SonicWALL UTM ...................................................................................................... 10  
  Verify Syslog messages in EventTracker Enterprise ........................................................................................................ 13  
EventTracker Knowledge Pack (KP) ............................................................................................................................................... 13  
  Categories .................................................................................................................................................................................... 14  
  Alerts .......................................................................................................................................................................................... 22  
  Reports .......................................................................................................................................................................................... 26  
Import SonicWALL UTM Knowledge pack into EventTracker .................................................................................................. 29  
  Import Category ......................................................................................................................................................................... 31  
  Import Alerts .............................................................................................................................................................................. 33  
  Import Tokens ............................................................................................................................................................................ 34  
  Import Flex Reports ................................................................................................................................................................. 35  
Verify SonicWALL UTM knowledge pack in EventTracker ...................................................................................................... 36  
  Verify SonicWALL UTM Categories ...................................................................................................................................... 37  
  Verify SonicWALL UTM Alerts .............................................................................................................................................. 38  
  Verify SonicWALL UTM Tokens .......................................................................................................................................... 40  
  Verify SonicWALL UTM Flex Reports .................................................................................................................................. 40  
Create Dashboards in EventTracker ............................................................................................................................................ 41  
  Schedule Reports .................................................................................................................................................................... 41  
  Create Dashlets ....................................................................................................................................................................... 44  
Sample Reports ............................................................................................................................................................................... 48  
Sample Dashboards ...................................................................................................................................................................... 49
Overview

SonicWALL’s approach to UTM 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.

Prerequisites

1. EventTracker 7.x and later should be installed.
2. SonicOS 5.8 and later should be installed.
3. Port 514 must be opened on SonicWALL UTM.
4. Port 514 must not be used by other services of SonicWALL UTM.
5. An exception should be added into Windows Firewall on EventTracker machine for Syslog port 514.

Integrate SonicWALL UTM with EventTracker Enterprise

To forward logs from SonicWALL UTM to EventTracker configure as follows:

Configure Syslog Settings

1. Login to SonicWALL UTM using Web.
2. Click on Log option at bottom left of SonicWALL UTM screen.
3. Select **Syslog** option.

---

**EventTracker: Integrating SonicWALL UTM**

---

Figure 1

![Multi-Core Monitor](image)

*Note: High utilization on Core 1 is normal while browsing the web management interface and applying changes.*

Figure 2

![Syslog Settings](image)
4. Under **Syslog Setting** configure as follows.

   - **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 Syslog settings.

![Syslog Settings](image)

Figure 3

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

6. Click on the Configure icon. The **Enhanced Syslog Settings** configuration window appears.
7. Select the Enhanced Syslog options you want to log. To select all options, click **Select All**. To deselect all options, click **Clear All**.

8. Click on **Save** button.

9. In the **Syslog ID** box, enter the Syslog ID that you want.

A **Syslog ID** field is included in all 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.

10. **(Optional)** Select Enable Event Rate Limiting if you want it. This control allows you to enable rate limiting of events to prevent the internal or external logging mechanism from being overwhelmed by 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 Log Priority of individual events.

11. **(Optional)** Select the Enable Data Rate Limiting if you want it. This control allows you to enable rate limiting of data to prevent the internal or external logging mechanism from being overwhelmed by log events. Specify the maximum number of bytes in the **Maximum Bytes per Second** field; the minimum is number is 0, the maximum is 1000000000, and the default is 10000000 bytes per second.
12. **(Optional)** Select the Enable NDPP Enforcement for Syslog Server if you want it.

**Configure Syslog Server**

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

![Figure 5](image-url)

**The Add Syslog Server window is displayed.**

![Figure 6](image-url)

2. Type the EventTracker Enterprise machine name or IP address in the **Name or IP Address** field. Type the port number in the **Port Number** field. Syslog default port is 514.
3. Click on **OK** button.

Syslog server **EventTracker Enterprise** machine IP address would be added under **Syslog Servers** section.

4. Click on **Accept** button to **save** the settings.
Syslog Send Receive Verification

Verify **ping** from SonicWALL UTM to EventTracker

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

2. Click on **System->Diagnostics**.

3. Select **Ping** from the **Diagnostic Tool** menu

4. Enter the IP address or host name of the EventTracker Enterprise machine and click **Go**.

5. In the **Interface** pulldown menu, select which interface you want to test the ping from. Selecting **ANY** allows the appliance to choose among all interfaces—including those not listed in the pulldown menu.

6. If the test is successful, the SonicWALL UTM returns a message saying the IP address is alive and the time to return in milliseconds (ms).
Verify Syslog messages forwarding on SonicWALL UTM

1. Login to the SonicWALL Network Security using Web Browser.

2. Navigate to System-> Packet Monitor page in the GUI and click configure.

3. In the Monitor Filter tab, specify below information.
   - Ether Type(s): IP
   - IP Type(s): UDP
   - Destination Port(s): 514
   - Enable the check box "Enable Bidirectional Address and Port Matching"
In the **Advanced Monitor Filter** tab, **enable** the check boxes

- Monitor Firewall Generated Packets. (This will bypass interface filter).
- Monitor Intermediate Packets.
6. Click **OK** to save the packet capture setup.

7. Click on **"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.
Verify Syslog messages in EventTracker Enterprise

1. Login to EventTracker Machine

2. Perform Log Search for SonicWALL UTM device.

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

EventTracker Knowledge Pack (KP)

Once 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 SonicWALL UTM monitoring:
Categories

- **SonicWALL UTM: Application block**
  This category gives information related to applications which are being blocked on SonicWALL UTM.

- **SonicWALL UTM: Application control detection**
  This category gives information related to application control, which are being detected on SonicWALL UTM.

- **SonicWALL UTM: Application control prevention**
  This category gives information related to application control, which are being prevented on SonicWALL UTM.

- **SonicWALL UTM: Application detection**
  This category gives information related to applications, which are being detected on SonicWALL UTM.

- **SonicWALL UTM: Administrator logged out**
  This category gives information related to administrator logged out on SonicWALL UTM.

- **SonicWALL UTM: Administrator login failed**
  This category gives information related to administrator whose login failed on SonicWALL UTM.

- **SonicWALL UTM: User authentication failed**
  This category gives information related to user whose authentication failed on SonicWALL UTM.

- **SonicWALL UTM: User authentication success**
  This category gives information related to user whose authentication is a success on SonicWALL UTM.

- **SonicWALL UTM: User logged out**
  This category gives information related to user who tries to log out on SonicWALL UTM.
• **SonicWALL UTM: User login failed**
This category gives information related to user whose login fails on SonicWALL UTM.

• **SonicWALL UTM: Website access allowed**
This category gives information related to website access which is allowed on SonicWALL UTM.

• **SonicWALL UTM: Website access denied**
This category gives information related to website access which is denied on SonicWALL UTM.

• **SonicWALL UTM: DHCP lease dropped**
This category gives information related to DHCP lease dropped on SonicWALL UTM.

• **SonicWALL UTM: DHCP lease expired**
This category gives information related to DHCP lease expired on SonicWALL UTM.

• **SonicWALL UTM: DHCP lease received**
This category gives information related to DHCP lease received on SonicWALL UTM.

• **SonicWALL UTM: DHCP request received**
This category gives information related to DHCP request received on SonicWALL UTM.

• **SonicWALL UTM: DHCP Server IP conflict detected**
This category gives information related to DHCP server IP conflict which was detected on SonicWALL UTM.

• **SonicWALL UTM: DHCP Server received DHCP decline from client**
This category gives information related to DHCP server received on DHCP client, declined on SonicWALL UTM.

• **SonicWALL UTM: Connection closed**
This category gives information related to connection closed on SonicWALL UTM.

• **SonicWALL UTM: Connection dropped**
This category gives information related to connection dropped on SonicWALL UTM.

• **SonicWALL UTM: Connection established**
This category gives information related to connection established on SonicWALL UTM.
• **SonicWALL UTM: Connection opened**
  This category gives information related to connection open on SonicWALL UTM.

• **SonicWALL UTM: Connection timed out**
  This category gives information related to connection time out on SonicWALL UTM.

• **SonicWALL UTM: Firewall access rule added**
  This category gives information related to rules added to firewall access on SonicWALL UTM.

• **SonicWALL UTM: Firewall access rule deleted**
  This category gives information related to rules deleted to firewall access on SonicWALL UTM.

• **SonicWALL UTM: Firewall access rule modified**
  This category gives information related to 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 FTP connection dropped on SonicWALL UTM.

• **SonicWALL UTM: FTP logon failure**
  This category gives information related to FTP logon failure on SonicWALL UTM.

• **SonicWALL UTM: FTP successful logons**
  This category gives information related to FTP which is successfully logged on, on the SonicWALL UTM.

• **SonicWALL UTM: Packet dropped**
  This category gives information related to packet dropped on SonicWALL UTM.

• **SonicWALL UTM: Back orifice attack dropped**
  This category gives information related to back orifice attack dropped on SonicWALL UTM.

• **SonicWALL UTM: DNS rebind attack detected**
  This category gives information related to attack detected on DNS rebind on SonicWALL UTM.
EventTracker: Integrating SonicWALL UTM

- **SonicWALL UTM: DOS protection on WAN**
  
  This category gives information related to WAN protected by DOS on SonicWALL UTM.

- **SonicWALL UTM: FIN-Flooding machine blacklisted**
  
  This category gives information related to FIN-flooding machine blacklisted on SonicWALL UTM.

- **SonicWALL UTM: Forbidden email attachment disabled**
  
  This category gives information related to forbidden email attachment disabled on SonicWALL UTM.

- **SonicWALL UTM: FTP port bounce attack dropped**
  
  This category gives information related to FTP port bounce attack dropped on SonicWALL UTM.

- **SonicWALL UTM: ICMP flood attack detected**
  
  This category gives information related to ICMP flood attack detected on SonicWALL UTM.

- **SonicWALL UTM: Ini killer attack dropped**
  
  This category give information related to ini killer attack dropped on SonicWALL UTM.

- **SonicWALL UTM: Initiator from country blocked**
  
  This category give information related to initiator from country blocked on SonicWALL UTM.

- **SonicWALL UTM: Intrusion detection**
  
  This category gives information related to intrusion detection on SonicWALL UTM.

- **SonicWALL UTM: IPS alert**
  
  This category gives information related to IPS alert on SonicWALL UTM.

- **SonicWALL UTM: Land attack dropped**
  
  This category gives information related to land attack dropped on SonicWALL UTM.

- **SonicWALL UTM: MAC IP anti spoof check enforced for hosts**
  
  This category gives information related to MAC IP anti spoof check enforced for hosts on SonicWALL UTM.
- **SonicWALL UTM: Machine removed from FINflood blacklist**
  This category gives information related to FINflood blacklist, removed by machine on SonicWALL UTM.

- **SonicWALL UTM: Machine removed from RSTflood blacklist**
  This category gives information related to RSTflood blacklist, removed by machine on SonicWALL UTM.

- **SonicWALL UTM: Machine removed from SYNflood blacklist**
  This category gives information related to SYNflood blacklist, removed by machine on SonicWALL UTM.

- **SonicWALL UTM: Malformed DNS packet detected**
  This category gives information related to malformer DNS packet detected on SonicWALL UTM.

- **SonicWALL UTM: Malformed or unhandled IP packet dropped**
  This category gives information related to malformed or unhandled IP packet dropped on SonicWALL UTM.

- **SonicWALL UTM: NetBus attack dropped**
  This category gives information related to netbus attack dropped on SonicWALL UTM.

- **SonicWALL UTM: Ping of death dropped**
  This category gives information related to ping of death dropped on SonicWALL UTM.

- **SonicWALL UTM: Port scan detected**
  This category gives information related port scan detected on SonicWALL UTM.

- **SonicWALL UTM: Responder from country blocked**
  This category gives information related to responder from country blocked on SonicWALL UTM.

- **SonicWALL UTM: Suspected botnet initiator blocked**
  This category gives information related to suspected botnet initiator blocked on SonicWALL UTM.

- **SonicWALL UTM: SYN flood detected on WAN**
  This category gives information related to SYN flood detected on WAN on SonicWALL UTM.
• **SonicWALL UTM: TCP SYN packet dropped**
  This category gives information related to TCP SYN packet dropped on SonicWALL UTM.

• **SonicWALL UTM: UDP Flood attack detected**
  This category gives information related to UDP flood attack detected on SonicWALL UTM.

• **SonicWALL UTM: WLAN IDS**
  This category gives information related to WLAN IDS on SonicWALL UTM.

• **SonicWALL UTM: Backup firewall transitioned to active**
  This category gives information related to backup firewall transitioned to active on SonicWALL UTM.

• **SonicWALL UTM: Backup firewall transitioned to idle**
  This category gives information related to backup firewall transitioned to active on SonicWALL UTM.

• **SonicWALL UTM: Interface link down**
  This category gives information related to interface link down on SonicWALL UTM.

• **SonicWALL UTM: Interface link up**
  This category gives information related to interface link up on SonicWALL UTM.

• **SonicWALL UTM: Multicast policy list added**
  This category gives information related to multicast policy which has been added to the list on SonicWALL UTM.

• **SonicWALL UTM: Multicast policy list deleted**
  This category gives information related to multicast policy which has been deleted from the list on SonicWALL UTM.

• **SonicWALL UTM: Network monitoring**
  This category gives information related to network monitoring on SonicWALL UTM.

• **SonicWALL UTM: Network security appliance activated**
  This category gives information related to network security appliance activated on SonicWALL UTM.
• **SonicWALL UTM: PC card device not detected**
  This category gives information related to PC card device not detected on SonicWALL UTM.

• **SonicWALL UTM: PC card inserted**
  This category gives information related to PC card inserted on SonicWALL UTM.

• **SonicWALL UTM: PC card removed**
  This category gives information related to PC card removed on SonicWALL UTM.

• **SonicWALL UTM: Primary firewall transitioned to active**
  This category gives information related to Primary firewall transitioned to active on SonicWALL UTM.

• **SonicWALL UTM: Primary firewall transitioned to idle**
  This category gives information related to primary firewall transitioned to idle on SonicWALL UTM.

• **SonicWALL UTM: System fan failure**
  This category gives information related to failure of system fan on SonicWALL UTM.

• **SonicWALL UTM: System shutdown by administrator**
  This category gives information related to shutting down of system by administrator on SonicWALL UTM.

• **SonicWALL UTM: WAN failover**
  This category gives information related to WAN failover on SonicWALL UTM.

• **SonicWALL UTM: WAN failure**
  This category gives information related to WAN failure on SonicWALL UTM.

• **SonicWALL UTM: Antispam service disabled**
  This category gives information related to antispam service disabled on SonicWALL UTM.

• **SonicWALL UTM: Antispam service enabled**
  This category give information related to antispam service enabled on SonicWALL UTM.
EventTracker: Integrating SonicWALL UTM

- **SonicWALL UTM: DSL device down**
  This category gives information related to DSL device down on SonicWALL UTM.

- **SonicWALL UTM: DSL device up**
  This category gives information related to DSL device up on SonicWALL UTM.

- **SonicWALL UTM: DSL WAN connected**
  This category gives information related to DSL WAN connected on SonicWALL UTM.

- **SonicWALL UTM: DSL WAN initialized**
  This category gives information related to DSL WAN initialized on SonicWALL UTM.

- **SonicWALL UTM: Dynamic DNS configuration error**
  This category gives information related to dynamic DNS configuration error on SonicWALL UTM.

- **SonicWALL UTM: SSO agent down**
  This category gives information related to SSO agent which is down on SonicWALL UTM.

- **SonicWALL UTM: Terminal Services agent down**
  This category gives information related to terminal services agent which is down on SonicWALL UTM.

- **SonicWALL UTM: Spam detected**
  This category gives information related to spam detected on SonicWALL UTM.

- **SonicWALL UTM: Maximum events per second threshold exceeded**
  This category gives information related maximum events per second threshold exceeded on SonicWALL UTM.

- **SonicWALL UTM: Maximum syslog data per second threshold exceeded**
  This category gives information related to 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 VPN policy on SonicWALL UTM.
EventTracker: Integrating SonicWALL UTM

- **SonicWALL UTM: Real time black list error**
  This category gives information related to real time blacklist error on SonicWALL UTM.

- **SonicWALL UTM: Unhandled multicast IPv6 packet dropped**
  This category gives information related to packet dropped for unhandled multicast IPv6 on SonicWALL UTM.

- **SonicWALL VPN: Client activity**
  This category gives information related to VPN client activities on SonicWALL UTM.

- **SonicWALL VPN: IKE activity**
  This category gives information related to VPN IKE activities on SonicWALL UTM.

- **SonicWALL VPN: IPsec activity**
  This category gives information related to VPN IPsec activities on SonicWALL UTM.

- **SonicWALL VPN: IPsec tunnel status changed**
  This category gives information related to VPN IPsec tunneling status changed on SonicWALL UTM.

- **SonicWALL VPN: PKI error**
  This category gives information related to PKI error on SonicWALL UTM.

### Alerts

- **SonicWALL UTM: Administrator login failed**
  This alert is generated when administrator login has failed.

- **SonicWALL: Antispam service disabled**
  This alert is generated when antispam service was disabled.

- **SonicWALL: Antispam service expired**
  This alert is generated when antispam service was expired.

- **SonicWALL: Application control detection**
  This alert is generated when application control has been detected.
• **SonicWALL: Application control prevention**
  This alert is generated when application control was prevented.

• **SonicWALL: Application filter blocked**
  This alert is generated when application filter has been blocked.

• **SonicWALL: Authentication failed**
  This alert is generated when authentication was failed.

• **SonicWALL: Back orifice attack dropped**
  This alert is generated when back orifice attack was dropped.

• **SonicWALL: Backup firewall transitioned to active**
  This alert is generated when back up of firewall was transited to active mode.

• **SonicWALL: Bad CRL format**
  This alert is generated when bad CRL was formatted.

• **SonicWALL: Certificate import failed**
  This alert is generated when certificate import was failed.

• **SonicWALL: Connectivity error**
  This alert is generated when connectivity generated an error.

• **SonicWALL: CRL validation failure**
  This alert is generated when CRL validation is failed.

• **SonicWALL: DHCP lease expired**
  This alert is generated when DHCP lease has been expired.

• **SonicWALL: DHCP Server IP conflict detected**
  This alert is generated when DHCP server IP conflict has been detected.

• **SonicWALL: DHCP Server sanity check failed**
  This alert is generated when DHCP server sanity check has been failed.

• **SonicWALL: DNS rebind attack detected**
  This alert is generated when DNS rebind attack has been detected.

• **SonicWALL: DSL device down**
  This alert is generated when DSL device is down.
- **SonicWALL: DSL WAN connected**
  This alert is generated when DSL WAN is being connected.

- **SonicWALL: DSL WAN initialized**
  This alert is generated when DSL WAN initialized.

- **SonicWALL: Failed to get CRL**
  This alert is generated when it fails to get CRL.

- **SonicWALL: Failed to process CRL**
  This alert is generated when it fails to process CRL.

- **SonicWALL: Firewall access rule added**
  This alert is generated when Firewall access rule is added.

- **SonicWALL: Firewall access rule deleted**
  This alert is generated when Firewall access rule is deleted.

- **SonicWALL: Firewall access rule modified**
  This alert is generated when Firewall access rule is modified.

- **SonicWALL: FTP connection dropped**
  This alert is generated when FTP connection is dropped.

- **SonicWALL: FTP logon failure**
  This alert is generated when FTP logon failure occurs.

- **SonicWALL: Interface link down**
  This alert is generated when Interface link is down.

- **SonicWALL: Intrusion detection**
  This alert is generated when Intrusion detection occurs.

- **SonicWALL: IPS alert**
  This alert is generated when IPS alert occurs.

- **SonicWALL: Issuer match failed**
  This alert is generated when issuer match fails.

- **SonicWALL: L2TP error**
  This alert is generated when L2TP error occurs.

- **SonicWALL: Multicast policy list deleted**
  This alert is generated when Multicast policy list deleted.
• **SonicWALL: NetBus attack dropped**  
This alert is generated when NetBus attack is dropped.

• **SonicWALL: NetSpy attack dropped**  
This alert is generated when NetSpy attack is dropped.

• **SonicWALL: Outbound access blocked**  
This alert is generated when outbound access is blocked.

• **SonicWALL: Ping of death dropped**  
This alert is generated when Ping of death is dropped.

• **SonicWALL: PPP Dial-Up dialing failed**  
This alert is generated when PPP Dial-Up dialing is failed.

• **SonicWALL: SIM detection failure**  
This alert is generated when SIM detection failure occurs.

• **SonicWALL: Spam detected**  
This alert is generated when Spam is detected.

• **SonicWALL: SSO agent down**  
This alert is generated when SSO agent is down.

• **SonicWALL: System fan failure**  
This alert is generated when System fan failure occurs.

• **SonicWALL: User login failed**  
This alert is generated when User login fails.

• **SonicWALL: Website access denied**  
This alert is generated when Website access is denied.

• **SonicWALL Firewall: VPN User authentication failed**  
This alert is generated when user authentication is failed.
EventTracker: Integrating SonicWALL UTM

Reports

- **SonicWALL Firewall-Network access report**: This report provides information related to network access which includes 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 WLAN IDS which includes Source IP and Message Column.

- **SonicWALL UTM-FTP logon details**: This report provides information related to FTP logon details which include User Name, Source IP and Message Column.

- **SonicWALL UTM-Website access allowed**: This report provides information related to website access allowed which includes User Name, Source IP, URL Category and URL Name.

- **SonicWALL Firewall-access rule change**: This report provides information related to firewall access rule change which includes User Name, Source IP and Message Column.

- **SonicWALL UTM-User activity**: This report provides information related to user activity which includes User Name, Source IP and Messages Column.

- **SonicWALL UTM-Anti-Spyware detected**: This report provides information related to anti-spyware detected which includes Event generated time and Source IP Column.

- **SonicWALL UTM-DSL activity**: This report provides information related to DSL activity which includes User Name, Source IP and Messages Column.

- **SonicWALL UTM-Attacks detection**: This report provides information related to attack detection which includes Source IP Address and Messages Column.

- **SonicWALL UTM-Application control prevention**: This report provides information related to application control prevention which includes Source IP and Messages Column.

- **SonicWALL UTM-Application control detection**: This report provides information related to application control detection which includes which includes Source IP and Messages Column.

- **SonicWALL UTM-Admin login failed**: This report provides information related to admin login failed which includes User Name, Source IP and Messages Column.

- **SonicWALL UTM-Authentication failed**: This report provides information related to authentication failed which includes User Name, Source IP and Messages Column.
• **SonicWALL UTM-Authentication success**: This report provides information related to authentication success which includes User Name, Source IP and Messages Column.

• **SonicWALL UTM-Interface link status**: This report provides information related to interface link status which includes interface name and its status (UP OR DOWN).

• **SonicWALL UTM-Connection closed dropped or terminated**: This report provides information related to connection status which includes source and destination IP and ports and connection status (closed, dropped and terminated) with protocol used during connection.

• **SonicWALL UTM-Connection opened or established**: This report provides information related to connection opened and established which includes source and destination IP, ports and interface, application used for making connection and protocol details.

• **SonicWALL UTM-Terminal services or SSO Agent**: This report provides information related to terminal and SSO services status which includes 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 websites those access are denied which includes source and destination IP, port and interface and URL and its category.

• **SonicWALL UTM-Intrusion detection**: This report provides information related to intrusion detected by SonicWALL firewall which includes source and victim details and attack name.

• **SonicWALL UTM-Multicast policy list**: This report provides information related to addition or deletion of multicast policy list in interface or VPN SPI, which includes the interface Name and VPN SPI value in which multicast policy is added or deleted.

• **SonicWALL UTM-Antispam service**: This report provides information related to antispam service which includes status of service and by whom it is enabled or disabled.

• **SonicWALL UTM-System Shutdown by Administrator**: This report provides information related to system shutdown by administrator which includes user details i.e. by whom firewall is shutdown.

• **SonicWALL UTM-Configuration change details**: This report provides information related to configuration change. It shows the Username, Source IP and Destination IP and also what have been changed.

• **SonicWALL Firewall-VPN User authentication failed**: This report provides information related to User authentication failure which includes 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 User authentication success which includes Source address and Port, Destination address and Port, Additional Information and Reason for success.

- **SonicWALL Firewall-VPN activity**: This report provides information related to VPN activity that contains VPN Client, VPN IPsec, VPN IKE, and VPN PKI which includes 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 IPsec tunnel status that is changed to up or down which includes Source Range, Destination Range, Gateway, Reason, Status and VPN Details.

- **SonicWALL Firewall- Traffic flow**: This report provides information related to 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 administrator login status.

- **SonicWALL UTM-Application management**: This report provides information related to application activities that have occurred.

- **SonicWALL UTM-Connection status**: This report provides information related to connection status.

- **SonicWALL UTM-DHCP lease status**: This report provides information related to DHCP lease status.

- **SonicWALL Firewall-Access rule change**: This report provides information related to firewall access rule changes.

- **SonicWALL Firewall-IDS attacks**: This report provides information related to IDS attacks that occur in the system.

- **SonicWALL UTM-FTP logon status**: This report provides information related to FTP logon status.

- **SonicWALL-User admin login status**: This report provides information related to user admin login status.

- **SonicWALL UTM-User authentication status**: This report provides information related to user authentication status.

- **SonicWALL UTM-Website access status**: This report provides information related to website access status.
Import SonicWALL UTM Knowledge pack into EventTracker

1. Launch EventTracker Control Panel.

2. Double click Export Import Utility, and then click the Import tab.

   ![EventTracker Control Panel](image)

   Figure 14

   Import the following in the same order as mentioned below

   - Template
   - Category
   - Alert
   - Tokens
   - Flex Reports
Templates

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

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

3. Click on **Browse** button.

4. Locate **All SonicWALL UTM** group of **Template.ettd** file, and then click the **Open** button.
5. Now select the check box and then click on 'Import' option. EventTracker displays success message.

![Template(s) imported successfully](image)

6. Click on OK button.

**Import Category**

1. Click **Category** option, and then click the **browse** button.
2. Locate **All sonicwall UTM group of Categories.iscat** file, and then click the **Open** button.

3. To import categories, click the **Import** button.

   EventTracker displays success message.

   ![Figure 20](image)

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

1. Click Alert option, and then click the browse button.

2. Locate All sonicwall UTM group of Alerts.isalt file, and then click the Open button.

3. To import alerts, click the Import button.

   EventTracker displays success message.
4. Click **OK**, and then click the **Close** button.

## Import Tokens

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

2. Locate **All sonicwall UTM group of Tokens.istoken** file, and then click the **Open** button.

3. To import tokens, click the **Import** button.

   EventTracker displays success message.
4. Click **OK**, and then click the **Close** button.

### Import Flex Reports

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

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

![Image](image.png)

Figure 26

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

Verify SonicWALL UTM knowledge pack in EventTracker Template

1. Logon to EventTracker Enterprise web interface.
2. Click the Admin menu, and then click Parsing Rules and click Template.
Verify SonicWALL UTM Categories

7. Logon to EventTracker Enterprise.

8. Click the Admin menu, and then click Categories.

9. In the Category Tree, expand Sonicwall UTM group folder to view the imported categories.
Verify SonicWALL UTM Alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Alerts.
3. In the Search field, type ‘Sonicwall’, and then click the Go button.

   Alert Management page will display all the imported Sonicwall UTM alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column.

EventTracker displays message box.

![Message from webpage](image)

**Figure 30**

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

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

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

The imported SonicWALL UTM tokens are added in Token-Value Groups list.

Verify SonicWALL UTM Flex Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports menu, and then select Configuration.
3. In Reports Configuration, select Defined option.
4. In search box enter ‘Sonicwall’, and then click the Search button.

EventTracker displays Flex reports of Sonicwall UTM.
Create Dashboards in EventTracker

Schedule Reports

1. Open EventTracker in browser and logon.

2. Navigate to Reports>Configuration.
3. Select SonicWALL UTM in report groups. Check defined dialog box.

4. Click on ‘schedule’ to plan a report for later execution.

5. Choose appropriate time for report execution and in Step 8 check Persist data in Event vault explorer box.
Figure 35

Figure 36
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 for scheduled time or generate report manually.

### Create Dashlets

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

![Dashboard](image1.png)

**Figure 37**

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

![Dashboard](image2.png)

**Figure 38**

2. Click **+** to add a new dashboard.
   Flex Dashboard configuration pane is shown.
5. Fill fitting title and description and click **save** button.

6. Click ** Gear** to configure a new flex dashlet.

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

Evaluated chart is shown.
10. If satisfied, Click **Configure** button.

17. Click ‘customize’ 🔄 to locate and choose created dashlet.

18. Click 📦 to add dashlet to earlier created dashboard.
Sample Reports

- SonicWALL Firewall - Configuration Change Details

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Username</th>
<th>Source IP Address</th>
<th>Destination IP Address</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/12/2015 12:16:36 PM</td>
<td>SONIC</td>
<td>mike</td>
<td>10.20.2.100</td>
<td>10.20.2.1</td>
<td>High Availability is disabled</td>
</tr>
<tr>
<td>10/12/2015 12:16:38 PM</td>
<td>SONIC</td>
<td>john</td>
<td>10.20.2.110</td>
<td>10.20.2.1</td>
<td>High Availability is enabled</td>
</tr>
<tr>
<td>10/12/2015 12:15:40 PM</td>
<td>SONIC</td>
<td>robin</td>
<td>10.20.2.45</td>
<td>10.20.2.1</td>
<td>User created</td>
</tr>
<tr>
<td>10/12/2015 12:15:40 PM</td>
<td>SONIC</td>
<td>jenness</td>
<td>10.20.2.78</td>
<td>10.20.2.1</td>
<td>logging configured</td>
</tr>
</tbody>
</table>

Figure 43

- SonicWALL Firewall-VPN IPsec tunnel status changed

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Computer</th>
<th>Source Range</th>
<th>Destination Range</th>
<th>Gateway</th>
<th>Reason</th>
<th>Status</th>
<th>VPN Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/08/2015 03:27:44 PM</td>
<td>SONIC</td>
<td>172.28.7.113 - 172.28.7.113</td>
<td>172.27.255.249 - 172.27.255.248</td>
<td>67.99.3.149</td>
<td>Commit Renew IPsec (Existed distnode)</td>
<td>Tunnel Up</td>
<td>policy 36/SYMTARGHA VPN</td>
</tr>
<tr>
<td>12/08/2015 03:27:44 PM</td>
<td>SONIC</td>
<td>172.28.7.113 - 172.28.7.113</td>
<td>172.27.255.249 - 172.27.255.248</td>
<td>67.99.3.149</td>
<td>Commit Renew IPsec (Existed distnode)</td>
<td>Tunnel Up</td>
<td>policy 36/SYMTARGHA VPN</td>
</tr>
<tr>
<td>12/08/2015 03:27:44 PM</td>
<td>SONIC</td>
<td>172.28.7.113 - 172.28.7.113</td>
<td>172.27.255.249 - 172.27.255.248</td>
<td>67.99.3.149</td>
<td>Commit Renew IPsec (Existed distnode)</td>
<td>Tunnel Up</td>
<td>policy 36/SYMTARGHA VPN</td>
</tr>
<tr>
<td>12/08/2015 03:27:44 PM</td>
<td>SONIC</td>
<td>172.28.7.113 - 172.28.7.113</td>
<td>172.27.255.249 - 172.27.255.248</td>
<td>67.99.3.149</td>
<td>Commit Renew IPsec (Existed distnode)</td>
<td>Tunnel Up</td>
<td>policy 36/SYMTARGHA VPN</td>
</tr>
<tr>
<td>12/08/2015 03:28:02 PM</td>
<td>SONIC</td>
<td>172.22.15.73 - 172.22.15.73</td>
<td>189.195.218.14 - 189.195.218.14</td>
<td>189.195.218.20</td>
<td>Remove IPsec distnode</td>
<td>Tunnel Down</td>
<td>policy 39/DataValVPN216</td>
</tr>
<tr>
<td>12/08/2015 03:28:02 PM</td>
<td>SONIC</td>
<td>172.22.15.73 - 172.22.15.73</td>
<td>189.195.218.14 - 189.195.218.14</td>
<td>189.195.218.20</td>
<td>Remove IPsec distnode</td>
<td>Tunnel Down</td>
<td>policy 39/DataValVPN216</td>
</tr>
<tr>
<td>12/08/2015 03:28:02 PM</td>
<td>SONIC</td>
<td>172.22.15.73 - 172.22.15.73</td>
<td>189.195.218.14 - 189.195.218.14</td>
<td>189.195.218.20</td>
<td>Remove IPsec distnode</td>
<td>Tunnel Down</td>
<td>policy 39/DataValVPN216</td>
</tr>
<tr>
<td>12/08/2015 03:28:02 PM</td>
<td>SONIC</td>
<td>172.22.15.73 - 172.22.15.73</td>
<td>189.195.218.14 - 189.195.218.14</td>
<td>189.195.218.20</td>
<td>Remove IPsec distnode</td>
<td>Tunnel Down</td>
<td>policy 39/DataValVPN216</td>
</tr>
<tr>
<td>12/08/2015 03:28:02 PM</td>
<td>SONIC</td>
<td>172.22.15.73 - 172.22.15.73</td>
<td>189.195.218.14 - 189.195.218.14</td>
<td>189.195.218.20</td>
<td>Remove IPsec distnode</td>
<td>Tunnel Down</td>
<td>policy 39/DataValVPN216</td>
</tr>
<tr>
<td>12/08/2015 03:28:02 PM</td>
<td>SONIC</td>
<td>172.22.15.73 - 172.22.15.73</td>
<td>189.195.218.14 - 189.195.218.14</td>
<td>189.195.218.20</td>
<td>Remove IPsec distnode</td>
<td>Tunnel Down</td>
<td>policy 39/DataValVPN216</td>
</tr>
</tbody>
</table>

Figure 44
• SonicWALL Firewall – Network Access Report

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Source Address</th>
<th>Source Port</th>
<th>Destination Address</th>
<th>Destination Port</th>
<th>Wan Address</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/26/2015 11:17:05 AM</td>
<td>1.214.119.227</td>
<td>55499</td>
<td>98.191.208.24</td>
<td>60</td>
<td>98.191.208.24</td>
<td>Connection Closed</td>
</tr>
<tr>
<td>04/26/2015 11:17:03 AM</td>
<td>1.214.119.227</td>
<td>55499</td>
<td>98.191.208.24</td>
<td>60</td>
<td>98.191.208.24</td>
<td>Connection Closed</td>
</tr>
<tr>
<td>04/26/2015 11:17:03 AM</td>
<td>1.214.119.227</td>
<td>55499</td>
<td>98.191.208.24</td>
<td>60</td>
<td>98.191.208.24</td>
<td>Connection Closed</td>
</tr>
</tbody>
</table>

**Figure 45**

Sample Dashboards

• SonicWALL Firewall-VPN user authentication success

**Figure 46**