

# Integrate Clavister Firewall

*EventTracker v7.x*

Publication Date: July 7, 2014

EventTracker  
8815 Centre Park Drive  
Columbia MD 21045  
[www.eventtracker.com](http://www.eventtracker.com)

# Abstract

The highly acclaimed Clavister cOS offers a rich palette of security service, both content-level and network-level security services. They are accompanied by a number of important infrastructural services, such as High Availability and Server Load Balancing.

This guide provides instructions to configure Clavister Firewall to send the syslog to EventTracker Enterprise. Once syslog is been configured to send to EventTracker Manager, alerts and reports can be configured into EventTracker.

## Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 7.X and later, **Clavister cOS Core** based devices with software release version 10.20.00 or higher.

## Audience

Administrators who are responsible for monitoring Clavister Security Gateways which are running the cOS Core operating system using EventTracker Manager.

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

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

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

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

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

*© 2014 Prism Microsystems Corporation. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.*

# Table of Contents

Abstract.....	1
Scope .....	1
Audience.....	1
Clavister Firewall .....	3
Prerequisites.....	3
Configure Clavister Firewall to send syslog to EventTracker .....	3
Enable Logging to a Syslog Host .....	3
Monitoring Events of Clavister Firewall.....	5
Import Clavister Firewall knowledge pack into EventTracker .....	6
Import Category.....	6
Import Alerts.....	7
Import Scheduled Reports.....	8
Import Tokens.....	8
Verify Clavister Firewall knowledge pack in EventTracker .....	9
Verify categories.....	9
Verify alerts.....	10
Verify Token Values.....	11
Verify Reports .....	12
Categories .....	14
Alerts .....	24
Reports.....	28

# Clavister Firewall

Clavister Security Gateway Appliance is an ultimate solution for enterprise security, running cOS operating systems. This makes the Clavister appliances more effective and powerful. The appliance combined with various security features such as Antivirus, Application Layer Gateways (which helps to protect different types of traffics), Intrusion Detection and Prevention and so forth.

## Prerequisites

- EventTracker v7.x should be installed.
- Clavister Firewall should be installed.

## Configure Clavister Firewall to send syslog to EventTracker

Syslog is a standardized protocol for sending log data. The format used by cOS Core is well suited to automated processing, filtering and searching. Syslog is a standard for forwarding log messages in an IP network. Syslog captures log information provided by network devices.

## Enable Logging to a Syslog Host

To enable logging of all events to a Syslog server follow the steps below:

### Command-Line Interface

Example:

Device: /> add LogReceiverSyslog Syslog\_ET IPAddress=xxx.xxx.xxx.xxx

Please follow the same steps used for the Web Interface below.

### Web Interface

1. Go to: **System > Device > Log and Event Receivers > Add > Syslog Receiver**

2. Specify a suitable name for the event receiver.

For example Syslog\_ET

3. Enter the **IP Address**.
4. Select an appropriate facility from the **Facility list**.
5. Click **OK**.

After configuring syslog successfully, the logs will appear in EventTracker as shown below.

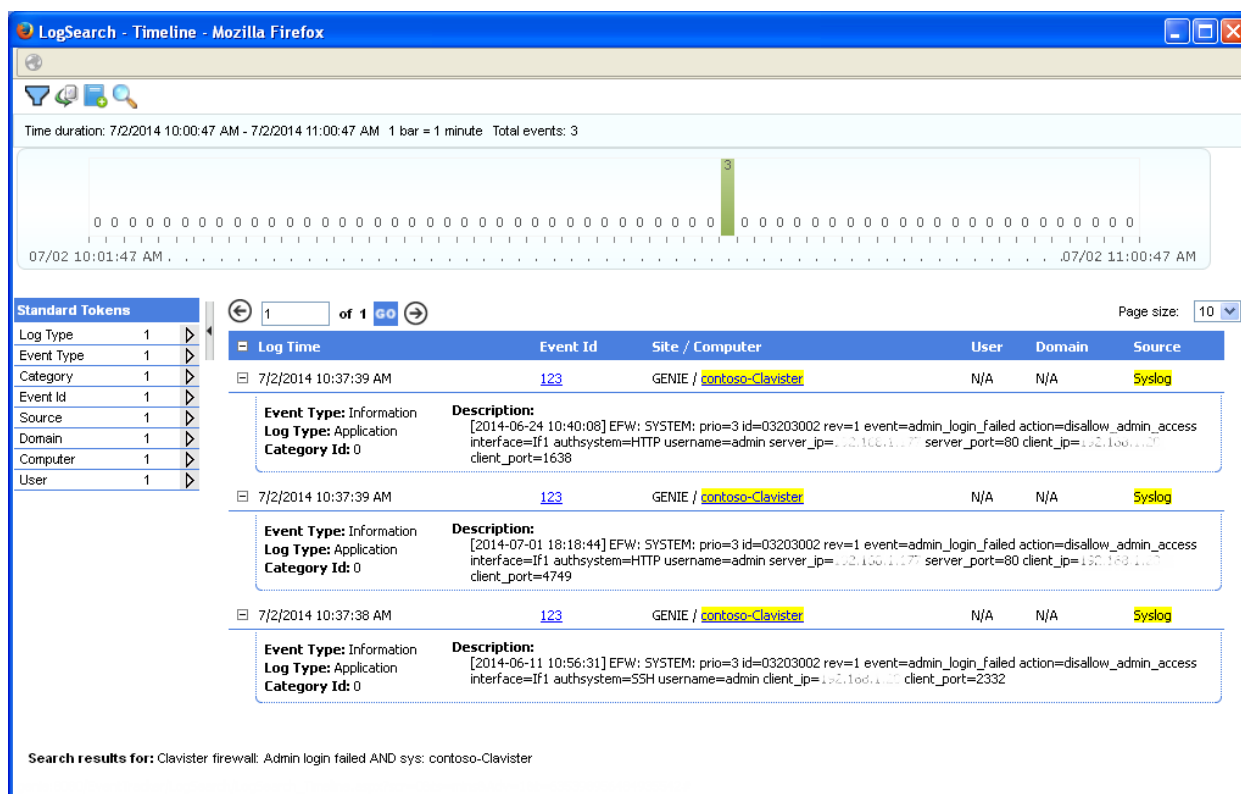


Figure 1

# Monitoring Events of Clavister Firewall

Monitoring events provides detailed information about ongoing activities in your network. Clavister Firewall events can be monitored using EventTracker Enterprise as follows:

- **Antivirus events**
- **Application Control events**
- **IP Routing Events**
- **Virtual Private Networks events**
- **Intrusion Detection and Prevention events**
- **Application layer gateways events**
- **Rule set events**
- **User Authentication Events**
- **High Availability Events**
- **Hardware monitoring events**
- **System Events**

# Import Clavister Firewall knowledge pack into EventTracker

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

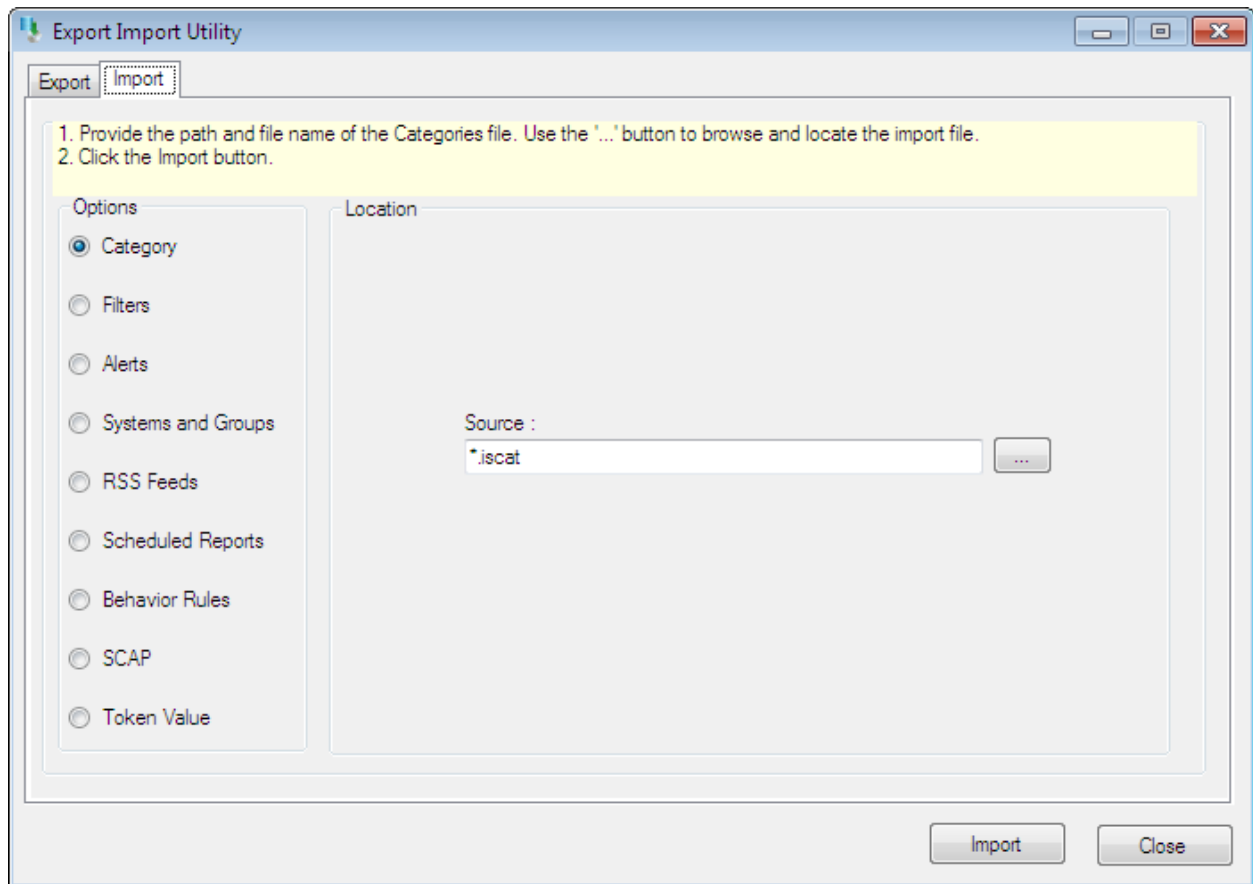


Figure 2

Import **Category/Alert/Reports/Token Values** as given below.

## Import Category

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

2. Locate **All Clavister Firewall group categories.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button.

EventTracker displays success message.

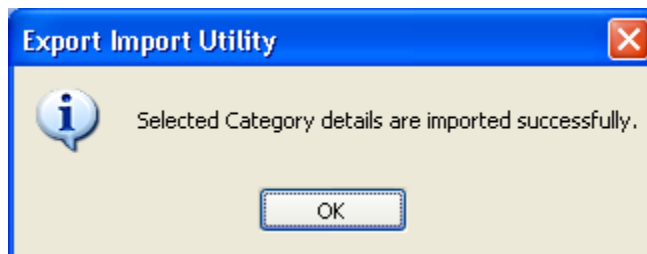



Figure 3

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

## Import Alerts

1. Click **Alert** option, and then click the **browse**  button.
2. Locate **All Clavister Firewall group alerts.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

EventTracker displays success message.

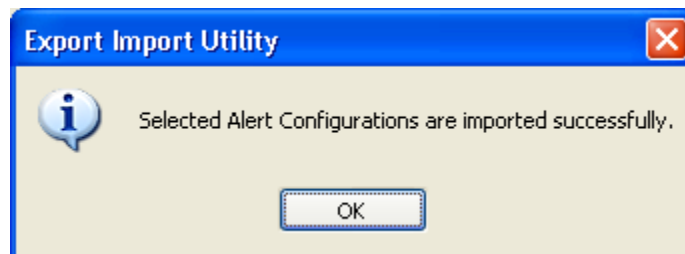



Figure 4

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



## Import Scheduled Reports

1. Click **Scheduled Reports** option, and then click the **browse**  button.
2. Locate **All Clavister Firewall group reports.issch** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

EventTracker displays success message.

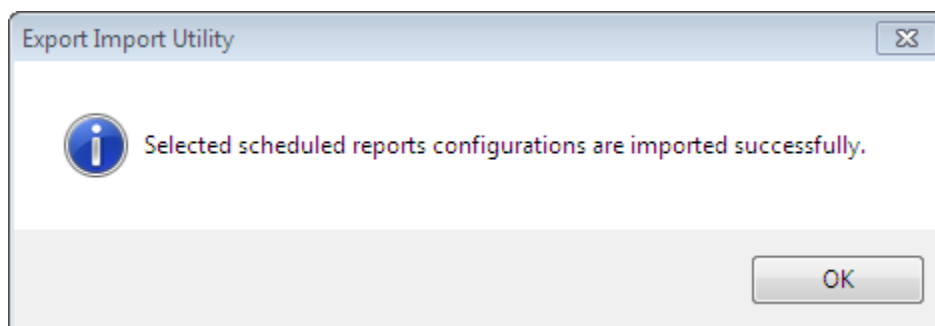



Figure 5

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 Clavister Firewall group token rules.istoken** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

EventTracker displays success message.

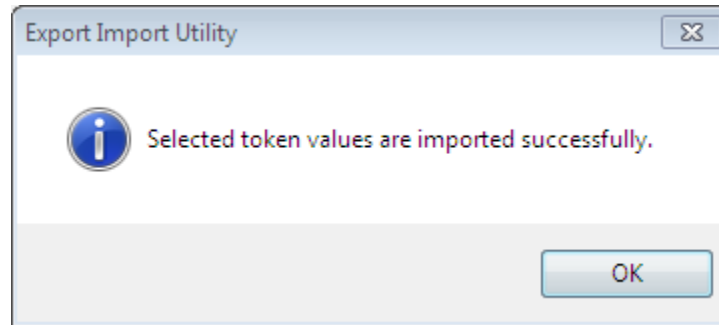


Figure 6

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

## Verify Clavister Firewall knowledge pack in EventTracker

### Verify categories

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Categories**.
3. To view the imported categories, in the **Category Tree**, expand **Clavister firewall** group folder.

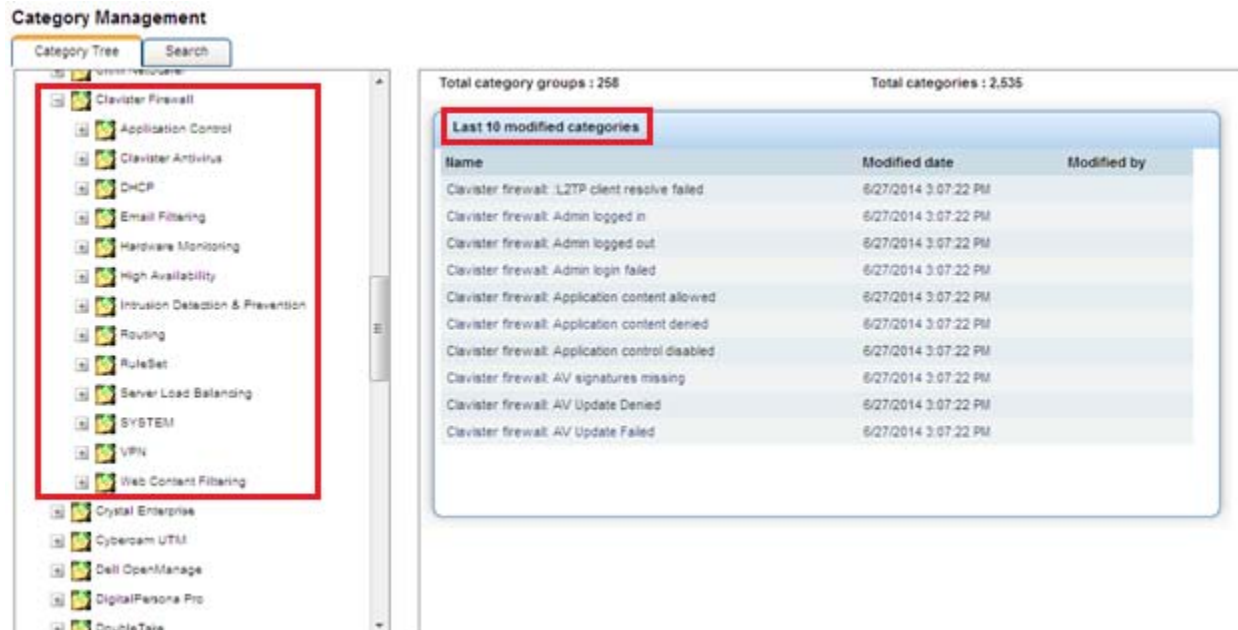


Figure 7

## Verify alerts

1. Logon to **EventTracker Enterprise**.
2. Click the **Admin** menu, and then click **Alerts**.
3. In the **Search** box, type '**Clavister firewall**', and then click the **Go** button.

Alert Management page will display all the imported alerts.

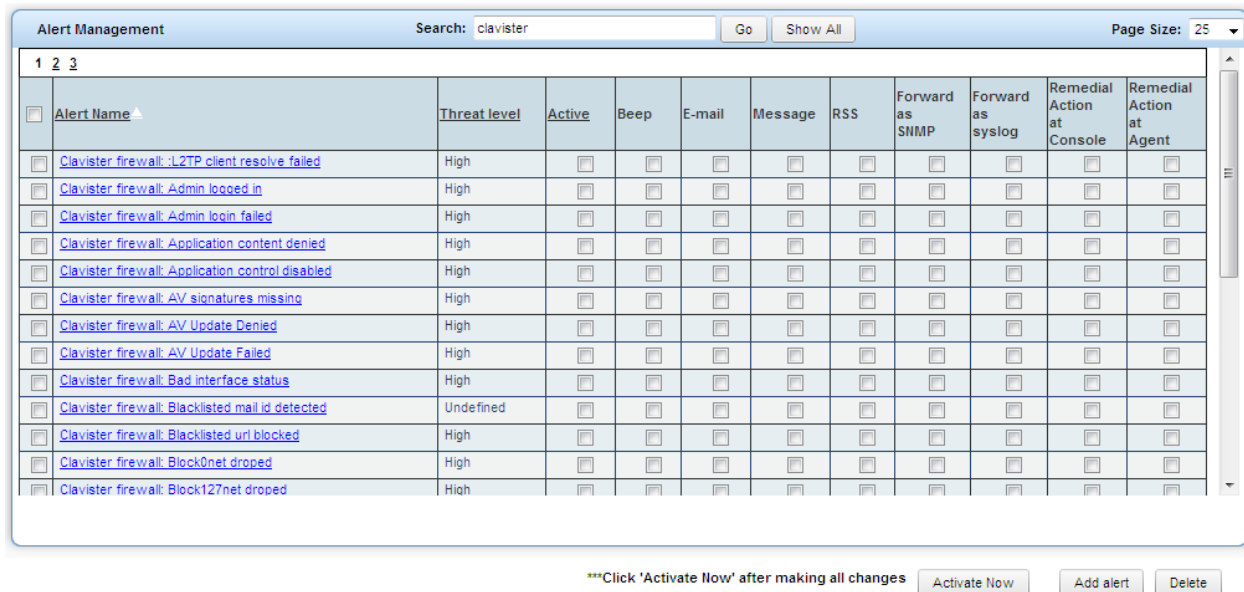


Figure 8

- To activate the imported alerts, select the respective checkbox in the **Active** column.

EventTracker displays message box.

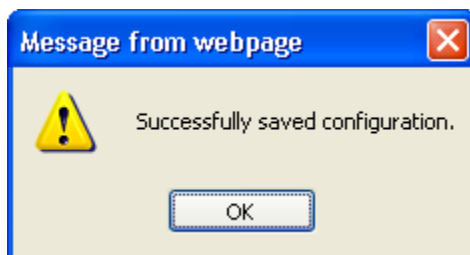


Figure 9

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

## Verify Token Values

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

Imported Clavister Firewall tokens are added in Token-Value Groups list at left side of **Parsing rule** tab of EventTracker Enterprise (as shown in below figure).



Figure 10



## Verify Reports

1. Logon to **EventTracker Enterprise**.
2. Select **Reports**, and then select **Configuration**.
3. In **Reports Configuration** pane, select **Defined** option.  
EventTracker displays **Defined** page.
4. In search box enter '**Clavister**', and then click the **Search** button.  
EventTracker displays Flex Reports of Clavister Firewall.






























## EventTracker – Integrate Clavister Firewall



Reports configuration

Scheduled  Queued  Defined

Search    

New

<input type="checkbox"/>	Title	Created on	Modified on			
<input type="checkbox"/>	<a href="#">Clavister DHCP lease acquired - Detail</a>	6/27/2014 2:43:35 PM	6/27/2014 2:45:40 PM			
<input type="checkbox"/>	<a href="#">Clavister rule set packet dropped - Detail</a>	6/27/2014 12:37:05 PM	6/27/2014 2:57:43 PM			
<input type="checkbox"/>	<a href="#">Clavister routing table activities - Detail</a>	6/27/2014 12:12:47 PM	6/27/2014 12:12:47 PM			
<input type="checkbox"/>	<a href="#">Clavister ssl vpn user login - Detail</a>	6/27/2014 11:33:28 AM	6/27/2014 11:33:28 AM			
<input type="checkbox"/>	<a href="#">Clavister IPsec maximum allowed tunnels limit reached - Detail</a>	6/27/2014 11:18:32 AM	6/27/2014 12:38:50 PM			
<input type="checkbox"/>	<a href="#">Clavister restricted site notice - Detail</a>	6/27/2014 10:50:24 AM	6/27/2014 12:39:59 PM			
<input type="checkbox"/>	<a href="#">Clavister user authentication failed - Detail</a>	6/26/2014 7:40:12 PM	6/26/2014 7:40:12 PM			
<input type="checkbox"/>	<a href="#">Clavister blacklisted email id detected - Detail</a>	6/26/2014 7:31:05 PM	6/27/2014 10:37:27 AM			
<input type="checkbox"/>	<a href="#">Clavister blacklisted url blocked - Detail</a>	6/26/2014 5:56:20 PM	6/27/2014 12:41:03 PM			
<input type="checkbox"/>	<a href="#">Clavister PPP authenticationn failed - Detail</a>	6/26/2014 2:55:01 PM	6/27/2014 4:50:36 PM			

1 of 2  

Delete

Figure 11

# Categories

EventTracker Categories can alert on all critical events such as Virus detection, Login failures etc.

- ❖ **Application control:** Application control logs are able to provide the information about the data connections relating to particular applications.

Events which can be monitored using Event Tracker:

- **Clavister Application control disabled:** This category based report provides information related to application Control disabled.
  - **Clavister Application content allowed:** This category based report provides information related to application content allowed control policy.
  - **Clavister Application content denied:** This category based report provides information related to application content denied control policy.
- 
- ❖ **Antivirus:** Clavister firewall cOS Core features integrated anti-virus functionality. Traffic passing through the Clavister Security Gateway can be subjected to in-depth scanning for viruses; Clavister Antivirus logs will allows you to monitor those activities.

Events which can be monitored using Event Tracker:

- **Clavister Virus found:** This category based report provides information about viruses which are detected by Clavister firewall antivirus.
- **Clavister Decompression error:** This category based report provides information related to file decompression error.
- **Clavister Compression ratio violation:** This category based report provides information related to scanning of compressed file with a compression ratio higher than the specified value.
- **Clavister Out of memory:** This category based report provides information related to scan engine which is running out of memory.
- **Clavister Virus scan failure:** This category based report provides information related to scanning error occurred in the anti-virus scan engine.

- **Clavister AV signatures missing:** This category based report provides information related to local anti-virus signature databases missing.
  - **Clavister Virus url detected:** This category based report provides information related to virus infected URL detection.
  - **Clavister AV Update Denied:** This category based report provides information related to anti-virus database updated denied.
  - **Clavister AV Update Failed:** This category based report provides information related to anti-virus database updated failure.
- ❖ **DHCP:** Dynamic Host Configuration Protocol (DHCP) logs that let you monitor IP Address Assignments, DHCP Leases and Lease Expiration activities.

Events which can be monitored using EventTracker:

- **Clavister DHCP lease acquired:** This category based report provides information when interfaces successfully acquired a lease.
  - **Clavister DHCP lease renewed:** This category based report provides information about renewal of interface's lease.
  - **Clavister DHCP lease expired:** This category based report provides information about interface lease expiration.
  - **Clavister IP collision:** This category based report provides information when an interface receives a lease which is already used.
- ❖ **Hardware monitor:** Hardware monitor allow the administrator to get alert about Critical values of various hardware operational parameters such as the current temperature inside the security gateway.

Events which can be monitored using Event Tracker:

- **Clavister Temperature alarm:** This category based report provides information related to the temperature of unit.
- **Clavister Voltage alarm:** This category based report provides information related to the power supply of this unit.



- **Clavister Fan RPM alarm:** This category based report provides information about if the fan of the unit is behaving strange; it may be failing or blocked.
  - **Clavister GPIO alarm:** This category based report provides information related to General-purpose input/output (GPIO).
  - **Clavister Memory low:** This category based report provides information the amount of free memory is getting low.
- ❖ **High Availability:** High Availability events (HA) allow you to monitor the fault tolerant capability of Clavister Security Gateway.

Events which can be monitored using EventTracker

- **Clavister Peer firewall disappeared:** This category based report provides information of when peer firewall disappeared.
  - **Clavister Both peers are active:** This category based report provides information related to conflict occurred as both peers are active.
  - **Clavister Both peers inactive:** This category based report provides information about conflict occurred as both peers are inactive at the same time.
  - **Clavister Received HA heartbeat:** This category based report provides information about received HA heartbeat from unknown IP.
  - **Clavister HASync connection failed:** This category based report provides information related to HASync connection failure.
  - **Clavister Peer synchronization failed:** This category based report provides information related to peer synchronization failure.
- ❖ **Intrusion Detection & Prevention:** Intrusion Detection and Prevention (IDP) events allow monitoring the intrusion attempts happening in the Clavister Security Gateway.

Events which can be monitored using Event Tracker:

- **Clavister Intrusion detected:** This category based report provides information related to the intrusion attack detection.
- **Clavister IDP Virus detected:** This category based report provides information related to virus signature detection which is detected by IDP.

- **Clavister IDP evasion:** This category based report provides information related to reassemble data failure.
  - **Clavister IDP out of memory:** This category based report provides information related to out of memory.
  - **Clavister IDP DB update failure:** This category based report provides information when updating of the Intrusion Detection & Prevention database failed.
- ❖ **Routing:** Routing logs allow you to monitor routing table activities of the unit. This is the most fundamental functions of cOS Core. Any IP packet flowing through a Clavister Security Gateway will be subjected to at least one routing decision..

Events which can be monitored using Event Tracker:

- **Clavister Failed to add OSPF route:** This category based report provides information related to OSPF route add failure to the routing table.
- **Clavister OSPF Neighbor Connectivity lost:** This category based report provides information when lose connectivity with neighbor router.
- **Clavister OSPF Authentication mismatch:** This category based report provides information related to authentication mismatch with neighboring OSPF router.
- **Clavister Received OSPF data mismatch:** This category based report provides information when received OSPF mismatch data from a neighboring router.
- **Clavister Unable to export route:** This category based report provides information when unable to export route to an OSPF process.
- **Clavister Failed to add route:** This category based report provides information when failed to add a route.
- **Clavister Route added:** This category based report provides information when a route added to the routing table.
- **Clavister Route removed:** This category based report provides information a route removed from the routing.
- **Clavister PPPOE tunnel up:** This category based report provides information when the PPPoE tunnel for a specific interface has been established.
- **Clavister PPPOE tunnel closed:** This category based report provides information when the PPPoE tunnel for a specific interface has been closed.

- ❖ **Server Load Balancing:** Server Load Balancing (SLB) events feature allows the administrator to monitor load balancing server status. SLB is a powerful tool that can improve Performance, Scalability, Reliability and Ease of administration

Events which can be monitored using EventTracker:

- **Clavister SLB server online:** This category based report provides information when SLB server is online.
  - **Clavister SLB server offline:** This category based report provides information when SLB server is offline.
- 
- ❖ **SYSTEM:** System events provide the information related to system activities, such as user authentication activities, system up and down status etc..

Events which can be monitored using EventTracker:

- **Clavister Placed in reduced functionality:** This category based report provides information when Security Gateway has been placed in reduced functionality mode.
- **Clavister Exited reduced functionality:** This category based report provides information when Security Gateway has been exited from reduced functionality mode.
- **Clavister Placed in local lockdown mode:** This category based report provides information when firewall has been placed in local lockdown mode.
- **Clavister Out of memory:** This category based report provides information when RAM memory becomes low.
- **Clavister Failed to bind port:** This category based report provides information when unit failed to allocate a dynamic port.
- **Clavister Shutdown:** This category based report provides information when the unit is shutting down.
- **Clavister Startup normal:** This category based report provides information when the Security Gateway is starting up.
- **Clavister Admin logged in:** This category based report provides information when an administrative user has logged in to the configuration system.

- **Clavister Admin logged out:** This category based report provides information when an administrative user has logged out from the configuration system.
- **Clavister Admin login failed:** This category based report provides information when an administrative user failed to log in to configuration system.
- **Clavister Bad interface status:** This category based report provides information when an Interface Monitor has discovered problems on an interface.
- **Clavister connection table is full:** This category based report provides information when connection table memory becomes full.
- **Clavister buffers flooded:** This category based report provides information when unit running out of buffers.

#### ❖ User Authentication

- **Clavister User authentication successful:** This category based report provides information when a user successfully logged in.
- **Clavister User authentication failed:** This category based report provides information when a user failed to log in.
- **Clavister LDAP Authentication failed:** This category based report provides information related to LDAP failed authentication attempts.
- **Clavister LDAP Authentication successful:** This category based report provides information related to LDAP Successful authentication attempts.
- **Clavister User logged out:** This category based report provides information when a user manually logged out.
- **Clavister RADIUS user authenticated:** This category based report provides information when a user was authenticated through RADIUS server.
- **Clavister User authentication rejected:** This category based report provides information when user authentication rejected.
- **Clavister RADIUS User logged out:** This category based report provides information a user logged out.

- ❖ **RuleSet:** Rules can be created for either inbound traffic or outbound traffic. The rule can be configured to specify the computers or users, program, service, or port and protocol. You can specify which type of network adapter the rule will be applied to: local area network (LAN), remote access, such as a virtual private network (VPN) connection, or all types. You can also configure the rule to be applied when any profile is being used.
  - **Clavister Block0net dropped:** This category based report provides information when destination address is the 0.\* net. And dropped
  - **Clavister Block127net dropped:** This category based report provides information when destination address is the 127.\* net. And dropped.
  - **Clavister Unknown vlan id:** This category based report provides information when received VLAN packet with unknown tag.
  - **Clavister Ruleset reject packet:** This category based report provides information when a packet rejected by rule-set.
  - **Clavister Ruleset drop packet:** This category based report provides information when a packet is dropped by a rule-set.
  
- ❖ **VPN:** Virtual Private Network(VPN) logs is a powerful tool where you will be able to monitor VPN related activities such as user authentication events, IPSec VPN events, SSL VPN events, activities of different types of tunneling protocols etc.,

Events which can be monitored using Event Tracker:

- **Clavister L2TP client resolve successful:** This category based report provides information when L2TP client successfully resolved the DNS name of the remote gateway.
- **Clavister L2TP client resolve failed:** This category based report provides information when L2TP client failed to resolve the DNS name of the remote gateway.
- **Clavister L2TP connection disallowed:** This category based report provides information when L2TP connection is disallowed.
- **Clavister L2TP session closed:** This category based report provides information when L2TP session closed.
- **Clavister L2TP tunnel closed:** This category based report provides information when L2TP tunnel closed.

- **Clavister L2TP Session up:** This category based report provides information when L2TP session up.
- **Clavister L2TP client tunnel up:** This category based report provides information when L2TP tunnel negotiated successfully.
- **Clavister Malformed packet received:** This category based report provides information about malformed packet received by the L2TP interface.
- **Clavister IPsec initialization failed:** This category based report provides information related to IPsec initialization failure.
- **Clavister IPsec tunnel disabled:** This category based report provides information related to tunnels which are disabled due to configuration error.
- **Clavister Remote Peer is dead:** This category based report provides information when a remote peer has been detected as dead.
- **Clavister Maximum tunnel connection reached:** This category based report provides information about aborted negotiation due to license restrictions.
- **Clavister Failed to start IPsec:** This category based report provides information when IPsec failed to start.
- **Clavister IPsec started successfully:** This category based report provides information when IPsec started successfully.
- **Clavister PPP tunnel limit exceeded:** This category based report provides information when PPP tunnel is terminated due to the license restrictions.
- **Clavister PPP authentication failed:** This category based report provides information when PPP terminated due to authentication failure.
- **Clavister PPTP connection disallowed:** This category based report provides information about disallowed PPTP connections.
- **Clavister PPTP user disconnected:** This category based report provides information about the forcibly disconnected clients.
- **Clavister PPTP session closed:** This category based report provides information about closed PPTP sessions.
- **Clavister PPTP session up:** This category based report provides information of established PPTP sessions.

- **Clavister PPTP client connected:** This category based report provides information of established PPTP client connections.
  - **Clavister PPTP tunnel up:** This category based report provides information of established PPTP tunnels.
  - **Clavister PPTP tunnel closed:** This category based report provides information about closed PPTP tunnels.
  - **Clavister SSLVPN session created:** This category based report provides information when SSL VPN Session created.
  - **Clavister SSLVPN session closed:** This category based report provides information when SSLVPN session closed
  - **Clavister SSLVPN maximum sessions reached:** This category based report provides information when maximum allowed SSLVPN tunnels reached.
  - **Clavister SSLVPN connection disallowed:** This category based report provides information about disallowed SSL VPN connections.
  - **Clavister SSLVPN user disconnected:** This category based report provides information when a user is forcibly disconnected.
  - **Clavister SSLVPN user logged in:** This category based report provides information when SSL VPN user has logged in to the SSL VPN user page.
- ❖ **Application Layer gateways:** Application Layer gateways log is a powerful feature which can monitor low-level packet filtering. Clavister Security Gateways provide Application Layer Gateways (ALGs) which provide filtering at the higher application OSI level.
- **Clavister ALG session opened:** This category based report provides information when Application Layer Gateways session opened
  - **Clavister DNS resolution failed:** This category based report provides information when an attempt to resolve DNS failed.
  - **Clavister Failed create new ALG session:** This category based report provides information when user failed to create new Application Layer Gateways session.
  - **Clavister Suspicious data received:** This category based report provides information about the suspicious data which has been received from the server.

- **Clavister Compressed data received:** This category based report provides information when the compressed data received.
- **Clavister Maximum download size reached:** This category based report provides information when data received from the server exceeds the maximum allowed download file size.
- **Clavister Restricted site notice:** This category based report provides information about web content access which is being restricted.
- **Clavister Blocked filetype:** This category based report provides information blocked file which are present in the block list.
- **Clavister Blacklisted url blocked:** This category based report provides information when a connection to blacklisted URL closed.
- **Clavister Content filtering disabled:** This category based report provides information when Web Content Filtering disabled.
- **Clavister WCF server authentication failed:** This category based report provides information when failed to authenticate with WCF server.
- **Clavister Blacklisted mail id detected:** This category based report provides information about SMTP ALG rejected Client requests due to blacklisted email Ids.
- **Clavister Sender email id mismatched:** This category based report provides information when sender address mismatch detected.



## Alerts

- **Clavister Application content denied:** This alert is generated when application control denied a application content.
- **Clavister Application control disabled:** This alert is generated when application control is disabled.
- **Clavister AV signatures missing:** This alert is generated when anti-virus scanning is aborted since there is local anti-virus signature database is missing.
- **Clavister AV Update Denied:** This alert is generated when antivirus update denied.
- **Clavister AV Update Failed:** This alert is generated when antivirus database failed to update.
- **Clavister Compression ratio violation:** This alert is generated when Compression ratio violation occurs for a specific file.
- **Clavister Virus found:** This alert is generated when a virus detected by antivirus.
- **Clavister Virus url detected:** This alert is generated when a virus infected URL found
- **Clavister DHCP lease acquired:** This alert is generated when an interface successfully acquired a lease.
- **Clavister IP collision:** This alert is generated when an Interface received a lease which is already used.
- **Clavister Blacklisted mail id detected:** This alert is generated when blacklisted email id detected by mail filtering.
- **Clavister Sender email id mismatched:** This alert is generated when sender email id mismatched.
- **Clavister Fan RPM alarm:** This alert is generated when fan RPM is behaving strange.
- **Clavister GPIO alarm:** This alert is generated when GPIO is outside the specified limit.
- **Clavister Memory low:** This alert is generated when Unit memory becomes low.
- **Clavister Temperature alarm:** This alert is generated when unit temperature is high.
- **Clavister Voltage alarm:** This alert is generated when voltage variation occurs.

- **Clavister Both peers are active:** This alert is generated when HA both peers become active mode.
- **Clavister Both peers inactive:** This alert is generated when HA both peers become inactive mode.
- **Clavister Peer firewall disappeared:** This alert is generated when peer unit disappeared from Cluster.
- **Clavister Peer synchronization failed:** This alert is generated when HA peer synchronization failed.
- **Clavister DB update failure:** This alert is generated when IDP database failed to update.
- **Clavister IDP evasion:** This alert is generated when IDP evasion occurs.
- **Clavister IDP out of memory:** This alert is generated when memory becomes low which is allotted for IDP.
- **Clavister Intrusion detected:** This alert is generated when intrusion detected.
- **Clavister IDP Virus detected:** This alert is generated when virus detected by IDP.
- **Clavister OSPF Neighbour Connectivity lost:** This alert is generated when lose connectivity to the OSPF neighbour
- **Clavister Route removed:** This alert is generated when a route entry removed from routing table.
- **Clavister SLB server offline:** This alert is generated when Load balancing server goes offline.
- **Clavister Admin logged in:** This alert is generated when admin user logged into the unit.
- **Clavister Admin login failed:** This alert is generated when admin user failed to login to the unit.
- **Clavister Bad interface status:** This alert is generated when NIC status goes down.
- **Clavister LDAP Authentication failed:** This alert is generated when authentication to LDAP failed.
- **Clavister Placed in local lockdown mode:** This alert is generated when the unit placed in local lockdown mode.

- **Clavister Placed in reduced functionality:** This alert is generated when unit place in reduced functionality mode.
- **Clavister Registration hijack detected:** This alert is generated when registration hijack detected.
- **Clavister User authentication failed:** This alert is generated when user authentication failed.
- **Clavister User authentication rejected:** This alert is generated when user authentication rejected.
- **Clavister L2TP client resolve failed:** This alert is generated when VPN client resolve failed through L2TP.
- **Clavister IPsec initialization failed:** This alert is generated when IPsec VPN failed to initialize.
- **Clavister IPsec tunnel disabled:** This alert is generated when IPsec VPN tunnel disabled.
- **Clavister IPsec tunnels limit reached:** This alert is generated when IPsec maximum tunnels limit reached.
- **Clavister IPsec Remote Peer is dead:** This alert is generated when IPsec remote peer goes down.
- **Clavister L2TP connection disallowed:** This alert is generated when The L2TP connection is disallowed according to the specified userauth rule.
- **Clavister L2TP tunnel closed:** This alert is generated when L2TP tunnel closed.
- **Clavister Malformed packet received:** This alert is generated when a malformed packet was received by the L2TP interface.
- **Clavister PPP authentication failed:** This alert is generated when PPP authentication failed.
- **Clavister PPP tunnel limit exceeded:** This alert is generated when maximum PPP tunnels limit exceeded.
- **Clavister PPTP connection disallowed:** This alert is generated when PPTP connection is disallowed according to the specified userauth rule.
- **Clavister PPTP tunnel closed:** This alert is generated when PPTP tunnel closed.
- **Clavister SSLVPN connection disallowed:** This alert is generated when SSLVPN connection is disallowed according to the specified userauth rule.

- **Clavister SSLVPN maximum sessions reached:** This alert is generated when SSLVPN maximum sessions reached.
- **Clavister SSLVPN user logged in:** This alert is generated when SSLVPN user logged in.
- **Clavister Blacklisted url blocked:** This alert is generated when Blacklisted url blocked.
- **Clavister Blocked filetype :** This alert is generated when blocked filetype detected.
- **Clavister Compressed data received:** This alert is generated when compressed data received.
- **Clavister Content filtering disabled:** This alert is generated when content filtering disabled.
- **Clavister Maximum download size reached:** This alert is generated when exceed maximum allowed download file size.
- **Clavister Maximum protocol sessions reached:** This alert is generated when maximum protocol sessions limit exceeded.
- **Clavister Restricted site notice:** This alert is generated when restricted site access noticed.
- **Clavister Suspicious data received:** This alert is generated when suspicious data received.
- **Clavister WCF server authentication failed:** This alert is generated when Web Content Filtering server authentication failed.
- **Clavister WCF server unreachable:** This alert is generated when Web Content Filtering server unreachable.
- **Clavister BlockOnet dropped:** This alert is generated when a packet's destination address is the 0.\* net.
- **Clavister Block127net dropped:** This alert is generated when a packet's destination address is the 127.\* net.
- **Clavister Ruleset reject packet:** This alert is generated when a packet rejected by rule-set.
- **Clavister Ruleset drop packet:** This alert is generated when a packet is dropped by a rule-set.
- **Clavister connection table is full:** This alert is generated when connection table memory becomes full.
- **Clavister buffers flooded:** This alert is generated when unit running out of buffers.

# Reports

EventTracker provides an exclusive reporting tool to generate requirement specific reports. Below are sample reports created by EventTracker for specific Clavister Firewall logs.

## Clavister blacklisted url blocked - Detail

### User Selection :

From Date:7/1/2014 10:49:19 AM

To Date: 7/2/2014 10:49:19 AM

Limit Time Range: None

Refine: Match In Source = syslog; Match In Event Description = event=request\_url;

Filter: None

Categories Selected: N/A

Computers Selected: GENIE, CONTOSO-CLAVISTER, CONTOSO-MS, CONTOSO-CVPM, 17.68.1.3-SYSLOG, CONTOSO-CYBEROAM, 17.68.1.3

Description: None

### Summary :

Connection destination IP	Total Event Occured	Event Id(Total Count)
63.243.241.50	8	123(8)
65.55.157.146	4	123(4)
Connection destination port	Total Event Occured	Event Id(Total Count)
80	12	123(12)
Connection Source IP	Total Event Occured	Event Id(Total Count)
12.68.10.27	12	123(12)
Connection source port	Total Event Occured	Event Id(Total Count)
63,921	8	123(8)
63,763	4	123(4)
URL	Total Event Occured	Event Id(Total Count)
www.hotmail.com/	4	123(4)
static.ak.facebook.com/connect/xd_arbiter/Dhmk J2TR0QN.js?version=41	4	123(4)
naukri.com	4	123(4)

Figure 12

## Clavister blocked file types - Detail

### User Selection :

From Date: 7/1/2014 11:05:33 AM

To Date: 7/2/2014 11:05:33 AM

Limit Time Range: None

Refine: Match In Source = syslog; Match In Event Description = event=blocked\_filetype;

Filter: None

Categories Selected: N/A

Computers Selected: GENIE, CONTOSO-CLAVISTER, CONTOSO-MS, CONTOSO-CVPN, 92.65.1.3-SYSLOG, CONTOSO-CYBEROAM, 92.65.1.3

Description: None

### Summary :

ALG Mode	Total Event Occured	Event Id(Total Count)
http	12	123(12)
File name	Total Event Occured	Event Id(Total Count)
putty.exe	4	123(4)
dump.doc	4	123(4)
86-0-Intended-use.html	4	123(4)
File type	Total Event Occured	Event Id(Total Count)
html	4	123(4)
exe	4	123(4)
doc	4	123(4)

Figure 13