Integrate Cisco VPN Concentrator

EventTracker v7.x

EventTracker
8815 Centre Park Drive
Columbia MD 21045
www.eventtracker.com

Publication Date: July 24, 2014

Abstract

This guide provides instructions to configure Cisco VPN 3000 Series Concentrators to send the syslog to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 7.X and later, **Cisco VPN 3000 Series Concentrators** and later.

Audience

Administrators who are responsible for monitoring Cisco VPN Concentrators 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.

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.

Table of Contents

Cisco VPN Concentrators

Cisco VPN Concentrators provide your business with unprecedented cost savings through flexible, reliable, and high-performance remote-access solutions. The Cisco VPN offers solutions for the most diverse remote-access deployments by offering both IP Security (IPsec) and Secure Sockets Layer (SSL) VPN connectivity on a single platform.

Prerequisites

- EventTracker v7.x should be installed.
- Cisco VPN 3000 Series concentrator and later should be installed.

Configure Cisco VPN concentrator to send syslog to EventTracker

This section describes how to configure Cisco VPN concentrators to forward syslogs to EventTracker Manager.

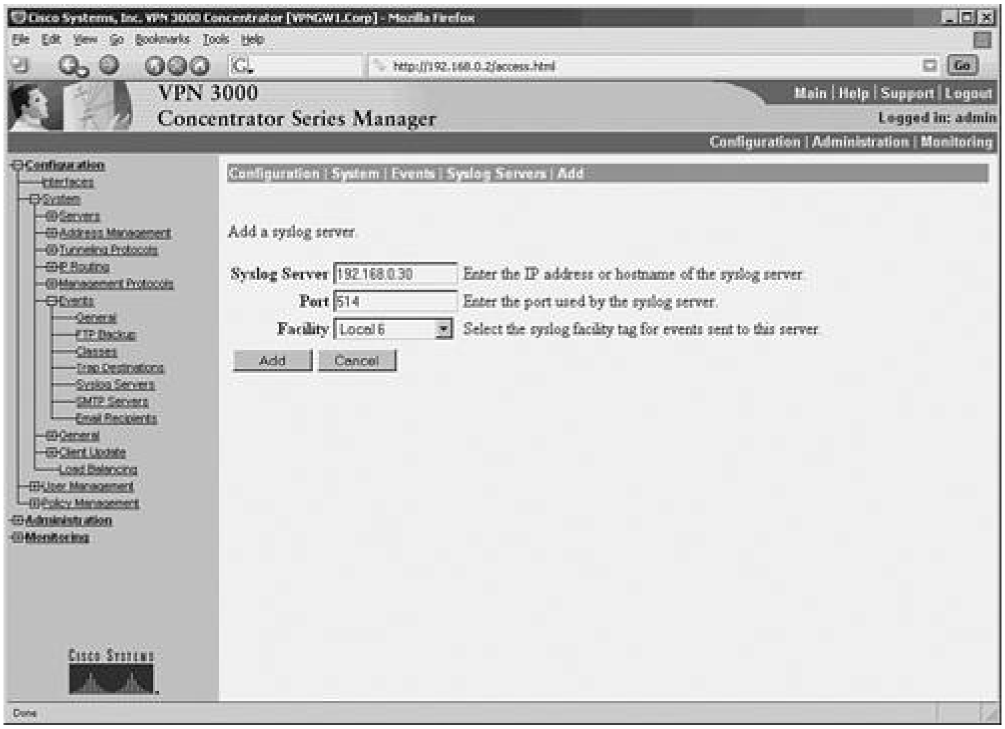
Enable Logging to a Syslog Host

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

1. Login to VPN concentrator using a web browser.
2. Navigate to the syslog server page by selecting **Configuration > System > Events > Syslog Servers.**

   NOTE: To save the configuration changes, click the **Save Needed** icon.
3. On the **Syslog Servers** page, click the **Add** button.
4. On the **Add** page enter the following information:

- **Syslog Server** - IP address of the syslog server has to be entered i.e. EventTracker Manager
- **Port** - Port used by syslog server has to be entered. By default port no is 514.
- **Facility** - Syslog Facility has to be selected from the Facility drop-down menu



Configuration | System | Events | Syslog Servers | Add

Add a syslog server.

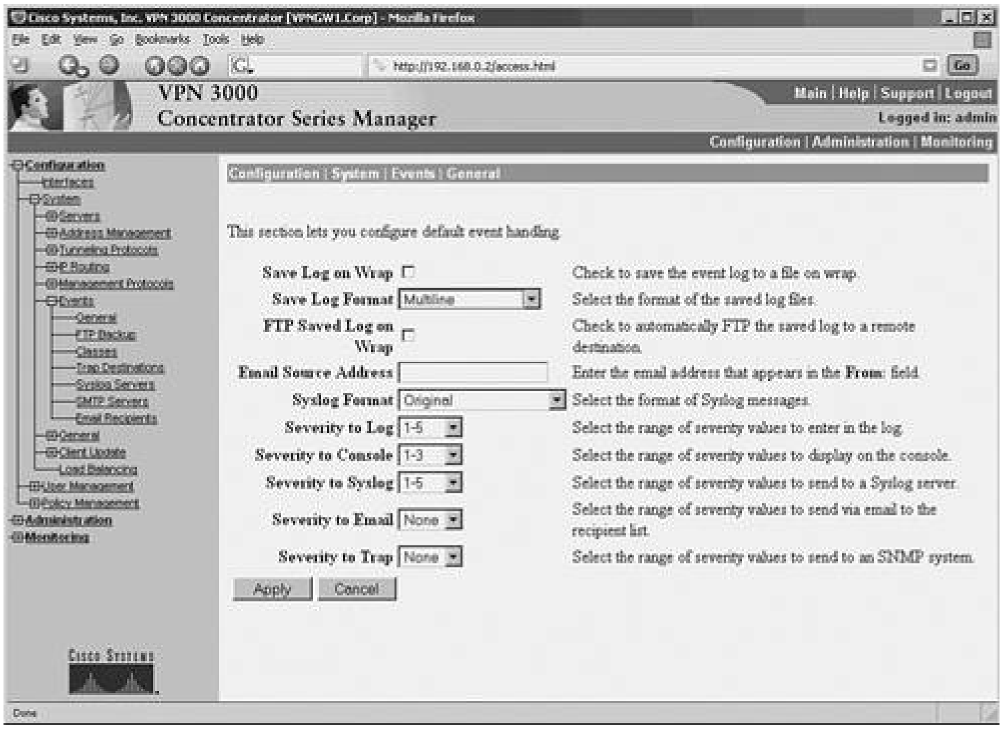
Syslog Server 192.168.0.30 Enter the IP address or hostname of the syslog server.

Port 514 Enter the port used by the syslog server.

Facility Local 6 Select the syslog facility tag for events sent to this server.

Figure 1: Cisco VPN 3000 Configuration 'Add" Screen

5. Save these settings and return to the **Syslog Servers** page by clicking the **Add** button.
6. To select the kind of messages that are to be sent to the syslog server, navigate to the **General** page by selecting **Configuration > System > Events > General**.
7. On the **General** page, select an option from the **Severity** to **Syslog** drop-down menu.
8. Set the **Syslog Format** option to **Original** or **Cisco IOS Compatible**, from the drop-down menu and click **Apply**.



Configuration | System | Events | General

This section lets you configure default event handling.

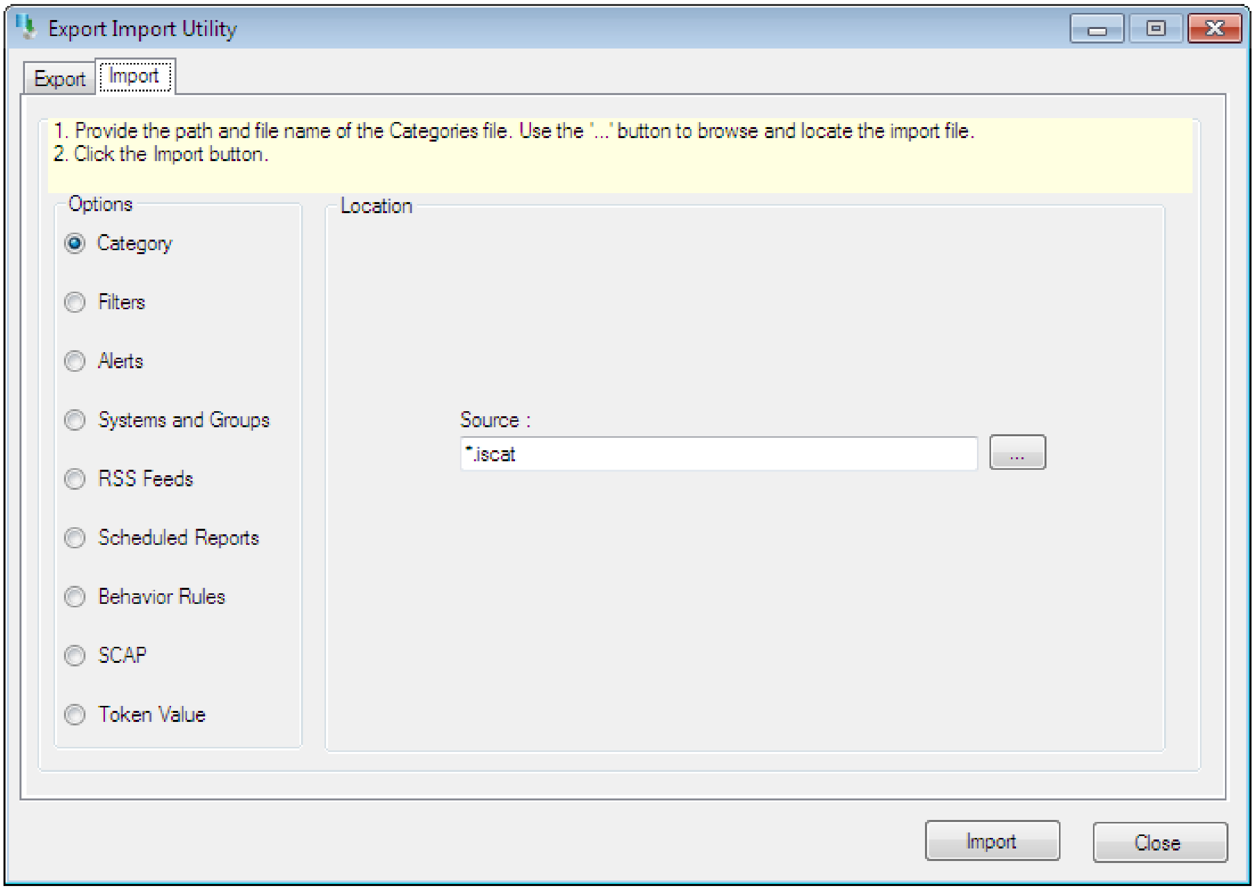
Save Log on Wrap	□	Check to save the event log to a file on wrap.
Save Log Format	Multiline	Select the format of the saved log files.
FTP Saved Log on Wrap	□	Check to automatically FTP the saved log to a remote destination.
Email Source Address		Enter the email address that appears in the **From:** field.
Syslog Format	Original	Select the format of Syslog messages.
Severity to Log	1-5	Select the range of severity values to enter in the log.
Severity to Console	1-3	Select the range of severity values to display on the console.
Severity to Syslog	1-5	Select the range of severity values to send to a Syslog server.
Severity to Email	None	Select the range of severity values to send via email to the recipient list.
Severity to Trap	None	Select the range of severity values to send to an SNMP system.

Apply Cancel

Figure 2: Cisco VPN 3000 Configuration ‘General” Screen

Import Cisco VPN concentrator knowledge pack into EventTracker

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



1. Provide the path and file name of the Categories file. Use the '...' button to browse and locate the import file.
2. Click the Import button.

Options

● Category
○ Filters
○ Alerts
○ Systems and Groups
○ RSS Feeds
○ Scheduled Reports
○ Behavior Rules
○ SCAP
○ Token Value

Source : *.iscat

Figure 3

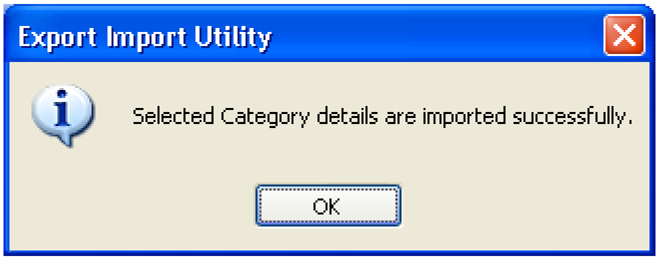
Import **Category/Alert** as given below.

Import Category

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

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

   EventTracker displays success message.



Selected Category details are imported successfully.

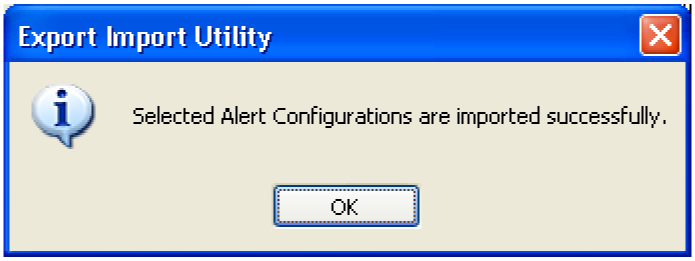
Figure 4

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

Import Alerts

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

   EventTracker displays success message.



Selected Alert Configurations are imported successfully.

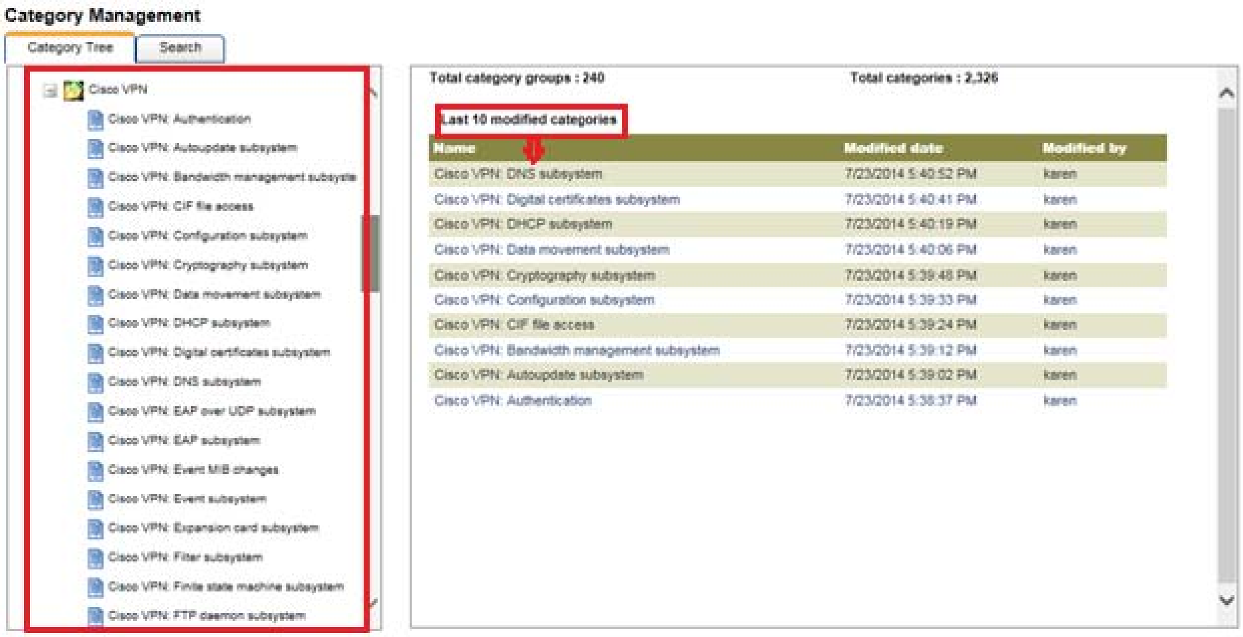
Figure 5

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

Verify Cisco VPN knowledge pack in EventTracker

Verify categories

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



Cisco VPN
Cisco VPN: Authentication
Cisco VPN: Autoupdate subsystem
Cisco VPN: Bandwidth management subsyste
Cisco VPN: CIF file access
Cisco VPN: Configuration subsystem
Cisco VPN: Cryptography subsystem
Cisco VPN: Data movement subsystem
Cisco VPN: DHCP subsystem
Cisco VPN: Digital certificates subsystem
Cisco VPN: DNS subsystem
Cisco VPN: EAP over UDP subsystem
Cisco VPN: EAP subsystem
Cisco VPN: Event MIB changes
Cisco VPN: Event subsystem
Cisco VPN: Expansion card subsystem
Cisco VPN: Filter subsystem
Cisco VPN: Finite state machine subsystem
Cisco VPN: FTP daemon subsystem

Total category groups : 240

Total categories : 2,326

Last 10 modified categories

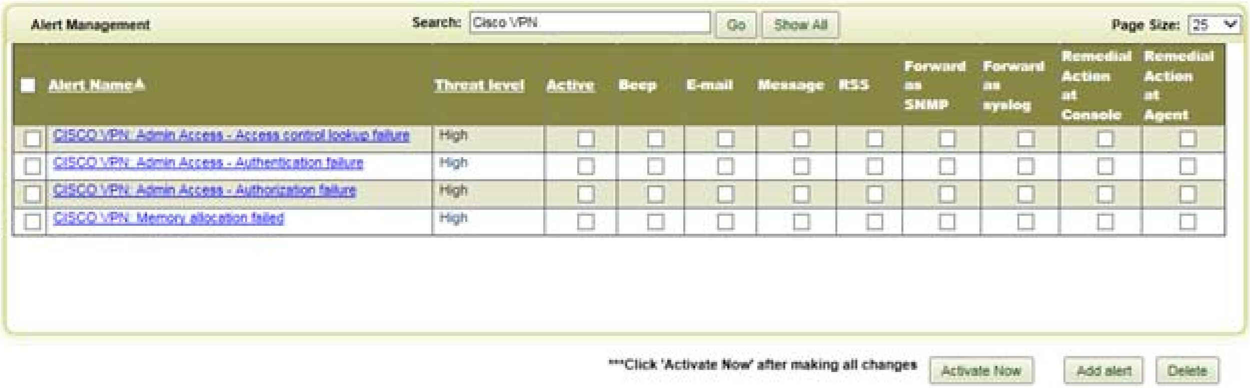
Name	Modified date	Modified by
Cisco VPN: DNS subsystem	7/23/2014 5:40:52 PM	karen
Cisco VPN: Digital certificates subsystem	7/23/2014 5:40:41 PM	karen
Cisco VPN: DHCP subsystem	7/23/2014 5:40:19 PM	karen
Cisco VPN: Data movement subsystem	7/23/2014 5:40:06 PM	karen
Cisco VPN: Cryptography subsystem	7/23/2014 5:39:48 PM	karen
Cisco VPN: Configuration subsystem	7/23/2014 5:39:33 PM	karen
Cisco VPN: CIF file access	7/23/2014 5:39:24 PM	karen
Cisco VPN: Bandwidth management subsystem	7/23/2014 5:39:12 PM	karen
Cisco VPN: Autoupdate subsystem	7/23/2014 5:39:02 PM	karen
Cisco VPN: Authentication	7/23/2014 5:38:37 PM	karen

Figure 6

Verify alerts

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

   Alert Management page will display all the imported alerts.



Alert Management   Search: Cisco VPN   Go   Show All   Page Size: 25

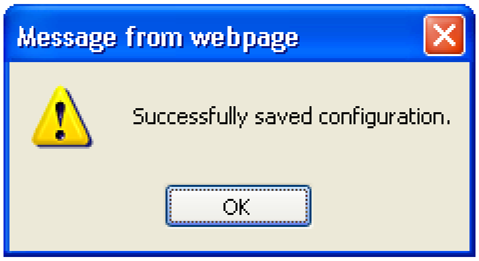
□	Alert Name▲	Threat level	Active	Beep	E-mail	Message	RSS	Forward as SNMP	Forward as syslog	Remedial Action at Console	Remedial Action at Agent
□	CISCO VPN: Admin Access - Access control lookup failure	High	□	□	□	□	□	□	□	□	□
□	CISCO VPN: Admin Access - Authentication failure	High	□	□	□	□	□	□	□	□	□
□	CISCO VPN: Admin Access - Authorization failure	High	□	□	□	□	□	□	□	□	□
□	CISCO VPN: Memory allocation failed	High	□	□	□	□	□	□	□	□	□

***Click 'Activate Now' after making all changes

Figure 7

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

   EventTracker displays message box.



Message from webpage

Successfully saved configuration.

Figure 8

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

EventTracker Knowledge Pack (KP)

Once logs are received in to EventTracker, Alerts and Reports can be configured into EventTracker

The following Knowledge Packs are available in EventTracker v7.x to support Cisco VPN concentrators monitoring.

Categories

Events which can be monitored using Event Tracker are

- **Clavister Application control disabled -** This category based report provides information related to application Control disabled.
- **Cisco VPN Authentication -** This category based report provides the information about VPN authentications.
- **Cisco VPN Autoupdate subsystem -** This category based report provides the information about auto updates subsytem.
- **Cisco VPN Bandwidth management subsystem -** This category based report provides the information related to bandwidth management subsystem.
- **Cisco VPN CIF file access -** This category based report provides the information related to CIF file access.
- **Cisco VPN Configuration subsystem -** This category based report provides the information related to system configurations subsytem.
- **Cisco VPN Cryptography subsystem -** This category based report provides the information related to cryptography subsytem.
- **Cisco VPN Data movement subsystem -** This category based report provides the information related to data movements subsytem.
- **Cisco VPN DHCP subsystem -** This category based report provides the information related to DHCP server subsystem.
- **Cisco VPN Digital certificates subsystem -** This category based report provides the information related to digital certificate subsystem.

- **Cisco VPN DNS subsystem -** This category based report provides the information related to DNS traffics subsytem.
- **Cisco VPN EAP over UDP subsystem -** This category based report provides the information related to EAP over UDP authentication subsytem.
- **Cisco VPN EAP subsystem -** This category based report provides the information related to EAP authentications subsytem.
- **Cisco VPN Event MIB changes -** This category based report provides the information related to event MIB changes.
- **Cisco VPN: Event subsystem -** This category based report provides the information related to event subsystem.
- **Cisco VPN: Expansion card subsystem -** This category based report provides the information related to expansion card subsystem.
- **Cisco VPN: Filter subsystem -** This category based report provides the information related Filter subsystem.
- **Cisco VPN: Finite state machine subsystem -** This category based report provides the information related to finite state machine subsystem.
- **Cisco VPN: FTP daemon subsystem -** This category based report provides the information related to FTP daemon subsystem.
- **Cisco VPN: GRE subsystem -** This category based report provides the information related to GRE subsystem.
- **Cisco VPN: Hardware monitoring -** This category based report provides the information related to hardware monitoring.
- **Cisco VPN: HTTP subsystem -** This category based report provides the information related to HTTP subsystem.
- **Cisco VPN: IP router subsystem -** This category based report provides the information related to IP router subsystem.
- **Cisco VPN: IP security subsystem -** This category based report provides the information related to IP security subsystem.
- **Cisco VPN: ISAKMP/Oakley subsystem -** This category based report provides the information related to ISAKMP/Oakley subsystem.

- **Cisco VPN: L2TP subsystem -** This category based report provides the information related to L2TP tunnel subsystem.
- **Cisco VPN: Load balancing subsystem -** This category based report provides the information related to load balancing subsystem.
- **Cisco VPN: MIB-II trap subsystem -** This category based report provides the information related to MIB-II trap subsystem.
- **Cisco VPN: NAC subsystem -** This category based report provides the information related to NAC subsystem.
- **Cisco VPN: NTP subsystem and general events -** This category based report provides the information related to NTP subsystem and general events.
- **Cisco VPN: Operating system command shell -** This category based report provides the information related to operating system command shell.
- **Cisco VPN: OSPF subsystem -** This category based report provides the information related to OSPF routing.
- **Cisco VPN: PPP subsystem -** This category based report provides the information related to PPP subsystem.
- **Cisco VPN: PPTP subsystem -** This category based report provides the information related to PPTP tunnel.
- **Cisco VPN: Resource manager subsystem -** This category based report provides the information related to resource manager subsystem.
- **Cisco VPN: SMTP event handling -** This category based report provides the information related to SMTP event handling.
- **Cisco VPN: SNMP trap subsystem -** This category based report provides the information related to SNMP trap subsystem.
- **Cisco VPN: SSH subsystem -** This category based report provides the information related to SSH subsystem.
- **Cisco VPN: SSL subsystem -** This category based report provides the information related to SSL VPN subsytem.
- **Cisco VPN: System queue -** This category based report provides the information related to VPN system queue.

- **Cisco VPN: System reboot -** This category based report provides the information related to system reboot.
- **Cisco VPN: System time -** This category based report provides the information about system time.
- **Cisco VPN: System utilities -** This category based report provides the information related to system utilities.
- **Cisco VPN: TCP subsystem -** This category based report provides the information related to TCP subsystem.
- **Cisco VPN: Telnet subsystem -** This category based report provides the information related to telnet subsystem.
- **Cisco VPN: VRRP subsystem -** This category based report provides the information related to VRRP subsystem.
- **Cisco VPN: WebVPN sessions -** This category based report provides the information related WebVPN sessions.
- **Cisco VPN: XML -** This category based report provides the information related to WebVPN XML sessions.

Alerts

- **CISCO VPN: Admin Access Authentication failure -** This alert is generated when an admin user failed to login.
- **CISCO VPN: Admin Access Authorization failure -** This alert is generated when user authorization failure occurs.
- **CISCO VPN: Memory allocation failed -** This alert is generated when memory allocation failed.
- **CISCO VPN: Admin Access Access control lookup failure -** This alert is generated when access control lookup failure occurs.