Abstract

This guide provides instructions to configure Cisco IOS to send the syslog events to EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 7.x and later, and Cisco IOS 12.4 and later.

Audience

Administrators, who are responsible for monitoring Cisco’s IOS devices using EventTracker Manager.
# Table of Contents

Abstract ........................................................................................................................................ 1  
Overview .................................................................................................................................... 3  
Prerequisites ............................................................................................................................... 3  
Configure Cisco IOS to send syslog to EventTracker ................................................................. 3  
EventTracker Knowledge Pack (KP) ............................................................................................ 4  
Categories .................................................................................................................................. 4  
Alerts .......................................................................................................................................... 5  
Reports ...................................................................................................................................... 5  
Import Cisco IOS Knowledge Pack into EventTracker ............................................................... 6  
Import Categories ....................................................................................................................... 7  
Import Alerts ............................................................................................................................. 8  
Import Parsing Rules ................................................................................................................. 9  
Import Flex Reports ................................................................................................................... 10  
Verify Cisco IOS knowledge pack in EventTracker ................................................................. 11  
Verify Categories ...................................................................................................................... 11  
Verify Alerts ............................................................................................................................ 11  
Verify Parsing Rules ............................................................................................................... 13  
Verify Flex Reports ................................................................................................................ 13  
Create Dashboards in EventTracker ......................................................................................... 14  
Schedule Reports ....................................................................................................................... 14  
Create Dashlets ....................................................................................................................... 18  
Sample Dashboards .................................................................................................................. 21  
Sample Reports ......................................................................................................................... 22
Overview

Cisco IOS (Internetwork Operating System) is firmware for Cisco Routers and Switches (earlier switches ran CatOS). IOS is a package of Routing, Switching, Internetworking and Telecommunication functions integrated into a multitasking operating system.

EventTracker compiles and inspects critical events to provide an administrator insight on user behavior, traffic anomalies, link flaps etc.

Prerequisites

- EventTracker v7.x or later should be installed.
- Cisco IOS devices with software release version IOS 12.4 or higher.

Configure Cisco IOS to send syslog to EventTracker

To enable and configure Cisco Routers for Syslog,

1. Enter global configuration mode and type the command
   
   `Router# configure terminal`

2. To specify syslog server, type the command
   
   `Router(config)#logging host`

   It specifies the EventTracker Manager by IP address or host name.

3. To specify Severity level, type the command
   
   `Router(config)# logging trap level`

   The possible values for severity level are as follows:
   
   - Emergency: 0
   - Alert: 1
   - Critical: 2
   - Error: 3
   - Warning: 4
   - Notice: 5
   - Informational: 6
   - Debug: 7

4. To specify facility level, type the command
   
   `Router(config)# logging facility facility-level`

   The default is local7. Possible values are local0, local1, local2, local3, local4, local5, local6, and local7.
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 to support Cisco IOS monitoring.

Categories

- **Cisco IOS: Access control list** - This category provides information related to access control list.
- **Cisco IOS: Access information element** - This category provides information related to access information element.
- **Cisco IOS: Accounting services** - This category provides information related to accounting services.
- **Cisco IOS: Adapter messages** - This category provides information related to adapter messages.
- **Cisco IOS: Adjacency subsystem** - This category provides information related to adjacency subsystem.
- **Cisco IOS: Administration** - This category provides information related to administration.
- **Cisco IOS: Advance integration module** - This category provides information related to advance integration module.
- **Cisco IOS: Advanced interface module** - This category provides information related to advanced interface module.
- **Cisco IOS: Airline protocol support** - This category provides information related to airline protocol support.
- **Cisco IOS: Alarm interface controller mgmt** - This category provides information related to alarm interface controller management.
- **Cisco IOS: Align messages** - This category provides information related to align messages.
- **Cisco IOS: Archive configuration** - This category provides information related to archive configuration.
- **Cisco IOS: Asynchronous security protocol** - This category provides information related to asynchronous security protocol.
- **Cisco IOS: ATM interface processor** - This category provides information related to ATM interface processor.
- **Cisco IOS: ATM line card** - This category provides information related to ATM line card.
- **Cisco IOS: Attachment circuit** - This category provides information related to attachment circuit.
- **Cisco IOS: Authentication failure** - This category provides information related to authentication failure.
- **Cisco IOS: Authentication proxy** - This category provides information related to authentication proxy.
- **Cisco IOS: Automatic protection switching** - This category provides information related to automatic protection switching.
Integrate Cisco IOS

- Cisco IOS: Cache messages - This category provides information related to cache messages.
- Cisco IOS: Chassis alarm - This category provides information related to chassis alarm.
- Cisco IOS: Ethernet devices - This category provides information related to Ethernet devices.
- Cisco IOS: Hardware device error - This category provides information related to hardware device error.
- Cisco IOS: HTTP subsystem - This category provides information related to HTTP subsystem.
- Cisco IOS: Intrusion detection - This category provides information related to intrusion detection.
- Cisco IOS: Networks - This category provides information related to networks

Alerts

- Cisco IOS: Border Gateway Protocol (BGP) neighbors up or down - This alert is generated when Border Gateway Protocol (BGP) neighbors up or down event occurs.
- Cisco IOS: Hot Standby Router Protocol (HSRP) state - This alert is generated when Hot Standby Router Protocol (HSRP) state change occurs.
- Cisco IOS: Interface down or detached - This alert is generated when interface down or detached event occurs.
- Cisco IOS: Internal software error - This alert is generated when internal software error occurs.
- Cisco IOS: IP-EIGRP neighbor is up or down - This alert is generated when IP-EIGRP neighbor is up or down.
- Cisco IOS: Line protocol down - This alert is generated when line protocol is down.
- Cisco IOS: Runaway processes - This alert is generated when runaway processes occur.

Reports

- Cisco IOS-Configuration changed
  This report provides information related to configuration changes which include Device Address, User Name, and Command Issued fields.
- Cisco IOS-Access denied
  This report provides information related to connection denial events occurring on router or switch which includes Source address, Source Port, Destination Address, Destination port and Packets Transferred fields.
- Cisco IOS-Port status change
  This report provides information related to port status changed from UP to DOWN or vice-versa which includes Device Address, Interface Name and Port Status fields.
- Cisco IOS-User logon success
  This report provides information related to user logon success which includes User Name, Source Address and Source Port fields.
- Cisco IOS-User logon failure

EventTracker
Actionable Security Intelligence
This report provides information related to user logon failure which includes User Name, Source Address, Source Port and Reason fields.

**Import Cisco IOS Knowledge Pack into EventTracker**

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

![EventTracker Control Panel](image)

**Figure 1**

Import **Categories, Alerts, and Reports** as given below.
Import Categories

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

![Figure 2](image)

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

![Figure 3](image)

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

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

![Figure 4](image)

2. Locate **All Cisco IOS group of Alerts.isalt** file, and then click the **Open** button.

3. To import alerts, click the **Import** button. EventTracker displays success message.

![Figure 5](image)

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

**NOTE**: You can select alert notification such as Beep, Email, and Message etc. Select the respective checkbox in the Alert management page, and then click the **Activate Now** button.
Import Parsing Rules

1. Click Token Value option, and then click the browse button.
2. Locate All Cisco IOS group of Tokens.istoken file, and then click the Open button.

![Figure 6](image)

3. To import token value, click the Import button. EventTracker displays success message.

![Figure 7](image)

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

1. Click **Reports** option, and then click the ‘**browse**’ button.
2. Locate **All Cisco IOS group reports.issch** file, and then click the **Open** button.

![Import Utility](image)

**Figure 8**

3. To import scheduled reports, click the **Import** button. EventTracker displays success message.

![Success Message](image)

**Figure 9**

4. Click **OK**, and then click the **Close** button.
Verify Cisco IOS knowledge pack in EventTracker

Verify Categories

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

Verify Alerts

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Alerts.
3. In Search field, type ‘Cisco IOS’, and then click the Go button.
   Alert Management page will display all the imported Cisco IOS alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

![Successfully saved configuration.](image)

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

**NOTE:** Please specify appropriate **systems** in **Alert configuration** for better performance.
Verify Parsing Rules

1. Logon to EventTracker Enterprise.
2. Click the Admin menu, and then click Parsing Rules.
3. In Token Value Group Tree to view imported token values, scroll down and click Cisco IOS group folder. Token values are displayed in the token value pane.

Verify Flex Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports menu, and then Configuration.
4. In Report Groups Tree to view imported flex reports, scroll down and click Cisco IOS group folder. Imported reports are displayed in the Reports Configuration pane.
NOTE: Please specify appropriate systems in report wizard for better performance.

Create Dashboards in EventTracker

Schedule Reports

1. Open EventTracker in browser and logon.
2. Navigate to Reports>Configuration.

3. Select Cisco IOS 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 Eventvault explorer** box.
6. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.

7. Proceed to next step and click **Schedule** button.

8. Wait 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.

![Figure 19](image)

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

![Figure 20](image)

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

![Figure 21](image)
5. Fill fitting title and description and click **Save** button.
6. Click 📊 to configure a new flex dashlet. Widget configuration pane is shown.

<table>
<thead>
<tr>
<th>WIDGET TITLE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco Login Failures Today</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>DATA SOURCE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Cisco IOS-User Login Failure</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>CHART TYPE</th>
<th>DURATION</th>
<th>VALUE FIELD SETTING</th>
<th>AS OF</th>
</tr>
</thead>
<tbody>
<tr>
<td>Donut</td>
<td>12 Hours</td>
<td>COUNT</td>
<td>Recent</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>AXES LABELS [X AXIS]</th>
<th>LABEL TEXT</th>
</tr>
</thead>
<tbody>
<tr>
<td>User Name</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>VALUES [Y AXIS]</th>
<th>VALUE TEXT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select column</td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>FILTER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Select column</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>LEGEND [SERIES]</th>
<th>SELECT</th>
</tr>
</thead>
<tbody>
<tr>
<td>Reason</td>
<td>All</td>
</tr>
</tbody>
</table>

7. Locate earlier scheduled report in **Data Source** dropdown.
8. Select **Chart Type** from dropdown.
9. Select extent of data to be displayed in **Duration** dropdown.
10. Select computation type in **Value Field Setting** dropdown.
11. Select evaluation duration in **As Of** dropdown.
12. Select comparable values in **X Axis** with suitable label.
13. Select numeric values in **Y Axis** with suitable label.
14. Select comparable sequence in **Legend**.
15. Click **Test** button to evaluate.

![Figure 22](image-url)
Evaluating chart is shown.

16. If satisfied, Click **Configure** button.

17. Click ‘customize’ to locate and choose created dashlet.
18. Click to add dashlet to earlier created dashboard.
Sample Dashboards

1. **Cisco Denied Traffic Today**

![Cisco Denied Traffic Today Chart]

*Figure 25*

2. **Cisco Logon Failures Today**

![Cisco Logon Failures Today Chart]

*Figure 26*
Sample Reports

1. Cisco IOS – Access denied

<table>
<thead>
<tr>
<th>Event Time</th>
<th>Source Address</th>
<th>Source Port</th>
<th>Destination Address</th>
<th>Destination Port</th>
<th>Protocol Type</th>
<th>Packets Transferred</th>
</tr>
</thead>
<tbody>
<tr>
<td>5/19/2015 16:39</td>
<td>130.237.188.216</td>
<td>6867</td>
<td>66.201.46.53</td>
<td>49789</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td>5/19/2015 19:14</td>
<td>192.168.0.36</td>
<td>192.168.0.1</td>
<td></td>
<td></td>
<td>ICMP</td>
<td></td>
</tr>
<tr>
<td>5/19/2015 21:49</td>
<td>192.168.0.25</td>
<td>24829</td>
<td>192.168.0.36</td>
<td>50</td>
<td>tcp</td>
<td></td>
</tr>
<tr>
<td>5/20/2015 00:23</td>
<td>10.1.0.1</td>
<td>2000</td>
<td>10.1.0.189</td>
<td>21348</td>
<td>udp</td>
<td></td>
</tr>
<tr>
<td>5/20/2015 02:58</td>
<td>192.168.0.69</td>
<td>34559</td>
<td>192.168.0.10</td>
<td>50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5/20/2015 05:33</td>
<td>192.168.0.69</td>
<td>34559</td>
<td>192.168.0.10</td>
<td>50</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5/20/2015 08:08</td>
<td>192.168.0.23</td>
<td>192.168.0.98</td>
<td>128</td>
<td>icmp</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>5/20/2015 10:43</td>
<td>192.168.0.78</td>
<td>192.168.154</td>
<td>50</td>
<td></td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>5/20/2015 13:18</td>
<td>192.168.0.95</td>
<td>192.168.0.35</td>
<td>52</td>
<td>tcp</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>5/20/2015 15:52</td>
<td>192.168.0.23</td>
<td>192.168.0.98</td>
<td>128</td>
<td>igmp</td>
<td>1</td>
<td></td>
</tr>
</tbody>
</table>

2. Cisco IOS – User logon failure

<table>
<thead>
<tr>
<th>LogTime</th>
<th>User Name</th>
<th>Source IP Address</th>
<th>Local Port</th>
<th>Reason</th>
</tr>
</thead>
<tbody>
<tr>
<td>10/27/2015 04:49:11 PM</td>
<td>Kirk</td>
<td>10.0.10.169</td>
<td>22</td>
<td>BadUser</td>
</tr>
<tr>
<td>10/27/2015 09:44:17 PM</td>
<td>Kirk</td>
<td>10.0.10.169</td>
<td>22</td>
<td>BadUser</td>
</tr>
<tr>
<td>10/28/2015 02:39:23 AM</td>
<td>Scott</td>
<td>10.0.10.17</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>10/28/2015 07:34:29 AM</td>
<td>Burt</td>
<td>10.0.10.172</td>
<td>50</td>
<td>BadPassword</td>
</tr>
<tr>
<td>10/28/2015 12:29:35 PM</td>
<td>Adam</td>
<td>10.0.10.170</td>
<td>23</td>
<td>BadUser</td>
</tr>
<tr>
<td>10/28/2015 05:24:41 PM</td>
<td>John</td>
<td>10.0.10.173</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>10/28/2015 10:19:47 PM</td>
<td>Burt</td>
<td>10.0.10.172</td>
<td>50</td>
<td>BadPassword</td>
</tr>
<tr>
<td>10/28/2015 03:14:53 AM</td>
<td>Evan</td>
<td>10.0.10.17</td>
<td>25</td>
<td>BadPassword</td>
</tr>
<tr>
<td>10/29/2015 08:00:59 AM</td>
<td>Adam</td>
<td>10.0.10.170</td>
<td>23</td>
<td>BadUser</td>
</tr>
<tr>
<td>10/29/2015 01:05:05 PM</td>
<td>Kirk</td>
<td>10.0.10.169</td>
<td>22</td>
<td>BadUser</td>
</tr>
<tr>
<td>10/29/2015 09:00:11 PM</td>
<td>Scott</td>
<td>10.0.10.173</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>10/29/2015 10:55:17 PM</td>
<td>Evan</td>
<td>10.0.10.17</td>
<td>25</td>
<td>BadPassword</td>
</tr>
<tr>
<td>10/30/2015 03:50:23 AM</td>
<td>John</td>
<td>10.0.10.173</td>
<td>22</td>
<td></td>
</tr>
<tr>
<td>10/30/2015 08:45:29 AM</td>
<td>John</td>
<td>10.0.10.171</td>
<td>25</td>
<td>BadPassword</td>
</tr>
<tr>
<td>10/30/2015 01:40:35 PM</td>
<td>Burt</td>
<td>10.0.10.172</td>
<td>50</td>
<td>BadPassword</td>
</tr>
<tr>
<td>10/30/2015 06:35:41 PM</td>
<td>Adam</td>
<td>10.0.10.17</td>
<td>23</td>
<td>BadUser</td>
</tr>
<tr>
<td>10/30/2015 11:30:47 PM</td>
<td>Kirk</td>
<td>10.0.10.169</td>
<td>22</td>
<td>BadUser</td>
</tr>
<tr>
<td>10/31/2015 04:25:53 AM</td>
<td>Kirk</td>
<td>10.0.10.169</td>
<td>22</td>
<td>BadUser</td>
</tr>
</tbody>
</table>