Integrate Cisco Switch
Abstract

This guide provides instructions to configure Cisco Switch 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 Switch 12.x and 15.x.

Audience

Administrators, who are responsible for monitoring Cisco Switch devices using EventTracker Manager.

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

This document is for informational purposes only. EventTracker 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 EventTracker, if its content is unaltered, nothing is added to the content and credit to EventTracker is provided.

EventTracker 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 EventTracker, 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.

© 2017 EventTracker Security LLC. All rights reserved. The names of actual companies and products mentioned herein may be the trademarks of their respective owners.
# Table of Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Abstract</td>
<td>1</td>
</tr>
<tr>
<td>Scope</td>
<td>1</td>
</tr>
<tr>
<td>Audience</td>
<td>1</td>
</tr>
<tr>
<td>Overview</td>
<td>3</td>
</tr>
<tr>
<td>Pre requisites</td>
<td>3</td>
</tr>
<tr>
<td>Configure Cisco Switch to send syslog to EventTracker</td>
<td>3</td>
</tr>
<tr>
<td>EventTracker Knowledge Pack (KP)</td>
<td>4</td>
</tr>
<tr>
<td>Categories</td>
<td>4</td>
</tr>
<tr>
<td>Alerts</td>
<td>5</td>
</tr>
<tr>
<td>Reports</td>
<td>5</td>
</tr>
<tr>
<td>Import Cisco Switch Knowledge Pack into EventTracker</td>
<td>9</td>
</tr>
<tr>
<td>Categories</td>
<td>10</td>
</tr>
<tr>
<td>Alerts</td>
<td>11</td>
</tr>
<tr>
<td>Templates</td>
<td>12</td>
</tr>
<tr>
<td>Flex Reports</td>
<td>13</td>
</tr>
<tr>
<td>Verify Cisco Switch knowledge pack in EventTracker</td>
<td>15</td>
</tr>
<tr>
<td>Categories</td>
<td>15</td>
</tr>
<tr>
<td>Alerts</td>
<td>15</td>
</tr>
<tr>
<td>Template</td>
<td>17</td>
</tr>
<tr>
<td>Flex Reports</td>
<td>17</td>
</tr>
<tr>
<td>Create Dashboards in EventTracker</td>
<td>18</td>
</tr>
<tr>
<td>Schedule Reports</td>
<td>18</td>
</tr>
<tr>
<td>Create Dashlets</td>
<td>21</td>
</tr>
<tr>
<td>Sample Dashboards</td>
<td>25</td>
</tr>
</tbody>
</table>
Overview

Switches are used to connect multiple devices together on the same network. In a properly designed network, LAN switches are responsible for directing and controlling the data flow at the access layer to networked resources.

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

NOTE: Applicable to the following series of switch 2600,2800,1900,2900,3900,4500,6500 with IOS 12.x and 15.x

Pre requisites

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

Configure Cisco Switch to send syslog to EventTracker

To enable and configure Cisco Switch 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`
   - Informational: 6
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.
Integrate Cisco switch

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 Switch monitoring.

Categories

- **Cisco Switch: Access control list** - This category provides information related to access control list.
- **Cisco Switch: Access information element** - This category provides information related to access information element.
- **Cisco Switch: Accounting services** - This category provides information related to accounting services.
- **Cisco Switch: Adapter messages** - This category provides information related to adapter messages.
- **Cisco Switch: Adjacency subsystem** - This category provides information related to adjacency subsystem.
- **Cisco Switch: Administration** - This category provides information related to administration.
- **Cisco Switch: Advance integration module** - This category provides information related to advance integration module.
- **Cisco Switch: Advanced interface module** - This category provides information related to advanced interface module.
- **Cisco Switch: Airline protocol support** - This category provides information related to airline protocol support.
- **Cisco Switch: Alarm interface controller mgmt** - This category provides information related to alarm interface controller management.
- **Cisco Switch: Align messages** - This category provides information related to align messages.
- **Cisco Switch: Archive configuration** - This category provides information related to archive configuration.
- **Cisco Switch: Asynchronous security protocol** - This category provides information related to asynchronous security protocol.
- **Cisco Switch: ATM interface processor** - This category provides information related to ATM interface processor.
- **Cisco Switch: ATM line card** - This category provides information related to ATM line card.
- **Cisco Switch: Attachment circuit** - This category provides information related to attachment circuit.
- **Cisco Switch: Authentication failure** - This category provides information related to authentication failure.
- **Cisco Switch: Authentication proxy** - This category provides information related to authentication proxy.
- **Cisco Switch: Automatic protection switching** - This category provides information related to automatic protection switching.
- **Cisco Switch: Cache messages** - This category provides information related to cache messages.
- **Cisco Switch: Chassis alarm** - This category provides information related to chassis alarm.
• **Cisco Switch: Ethernet devices** - This category provides information related to Ethernet devices.
• **Cisco Switch: Hardware device error** - This category provides information related to hardware device error.
• **Cisco Switch: HTTP subsystem** - This category provides information related to HTTP subsystem.
• **Cisco Switch: Intrusion detection** - This category provides information related to intrusion detection.
• **Cisco Switch: Networks** - This category provides information related to networks.

### Alerts

• **Cisco Switch: Interface down or detached** - This alert is generated when interface down or detached event occurs.
• **Cisco Switch: Internal software error** - This alert is generated when internal software error occurs.
• **Cisco Switch: Line protocol down** - This alert is generated when line protocol is down.
• **Cisco Switch: Runaway processes** - This alert is generated when runaway processes occur.

### Reports

• **Cisco Switch -Configuration changed**
  This report provides information related to configuration changes which include Device Address, User Name, and Command Issued fields.

```
%FR_VCB-5-UPDOWN: FR VC-Bundle NYKLAXLINK changed state to InActive
```

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Message</th>
<th>Facility Code</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/08/2016 05:05:27 PM</td>
<td>CISCO-IOS9</td>
<td>Controller server: changed state to Active due to unknown</td>
<td>CONTROLLER-5-DOWNDETAIL</td>
</tr>
<tr>
<td>12/08/2016 05:05:27 PM</td>
<td>CISCO-IOS9</td>
<td>Dot1x unable to start.</td>
<td>DOT1X-4-PROC_START_ERR</td>
</tr>
</tbody>
</table>

• **Cisco Switch -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.

```
Nov 7 12:20:08.139 EST: %SW_DAI-4-ACL_DENY: 1 Invalid ARPs (Res) on Gi1/3, vlan 1502.([001d.e513.8ef1/10.1.1.65/001d.e513.8ef1/10.1.1.65/12:20:07 EST Fri Nov 7 2008])
```
• **Cisco Switch - 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.

  **00:00:20: %LINEPROTO-5-UPDOWN: Line protocol on Interface Ethernet0/0, changed state to up**

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Facility Code</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/03/2017 12:07:06 PM</td>
<td>CISCO-JOS1</td>
<td>PM-4-ERR_DISABLE</td>
<td>psecure-violation error detected on Fa4/4, putting Fa4/4 in err-disable state</td>
</tr>
<tr>
<td>01/03/2017 12:07:08 PM</td>
<td>CISCO-JOS1</td>
<td>PM-4-ERR_DISABLE</td>
<td>psecure-violation error detected on Fa4/4, putting Fa4/4 in err-disable state</td>
</tr>
</tbody>
</table>

• **Cisco Switch - User logon success**
  This report provides information related to user logon success which includes User Name, Source Address and Source Port fields.

  **Oct 16 09:32:37.657: %SEC_LOGIN-5-LOGIN_SUCCESS: Login Success [user: neteng] [Source: 0.0.0.0] [localport: 0] at 09:32:37 UTC Fri Oct 16 2009**

<table>
<thead>
<tr>
<th>LogTime</th>
<th>User Name</th>
<th>Source IP Address</th>
<th>Local Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>12/01/2016 05:14:43 PM</td>
<td>David</td>
<td>10.10.2.32</td>
<td>22</td>
</tr>
</tbody>
</table>

• **Cisco Switch - User logon failure**
  This report provides information related to user logon failure which includes User Name, Source Address, Source Port and Reason fields.

  **Feb 9 2015 18:34:38.236 MSK: %SEC_LOGIN-4-LOGIN_FAILED: Login failed [user: rrr] [Source: 10.0.10.169] [localport: 23] [Reason: Login Authentication Failed] at 18:34:38 MSK Mon Feb 9 2015**

<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>12/01/2016 05:14:43 PM</td>
<td>David</td>
<td>10.10.2.32</td>
<td>22</td>
<td>Invalid login</td>
</tr>
</tbody>
</table>
- **Cisco Switch -Authentication failure**
  This report provides information related to authentication failure that is whenever the user tries to login into one of the Cisco Switch.

  Sep 15 13:09:47.308: %GLBP-4-BADAUTH: Bad authentication received from 149.212.19.162, group

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Facility Code</th>
<th>Client</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/03/2017 04:09:22 PM</td>
<td>CISCO-IOS8</td>
<td>GLEBP-4-UNAVAILABLE</td>
<td>192.23.43.23</td>
<td>Bad authentication received from 192.23.43.23, group 2</td>
</tr>
<tr>
<td>01/03/2017 04:09:22 PM</td>
<td>CISCO-IOS8</td>
<td>CRYPTO-6-UNAVAILABLE</td>
<td></td>
<td>Authentication method 192.23.12.2 failed with host accel</td>
</tr>
</tbody>
</table>

- **Cisco Switch -Administrative account activity**
  This report provides information related to account activities that is done by the administrator.

  %AAA-5-USER_LOCKED: User michel locked out on authentication failure

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>User Name</th>
<th>Reason</th>
<th>Admin Name</th>
</tr>
</thead>
<tbody>
<tr>
<td>11/25/2016 07:12:17 PM</td>
<td>CISCO</td>
<td>Smith</td>
<td>locked out on authentication failure</td>
<td></td>
</tr>
<tr>
<td>11/25/2016 07:12:17 PM</td>
<td>CISCO</td>
<td>Smith</td>
<td>failed attempts reset</td>
<td>Charles</td>
</tr>
<tr>
<td>11/25/2016 07:12:18 PM</td>
<td>CISCO</td>
<td>Smith</td>
<td>unlocked</td>
<td>Charles</td>
</tr>
</tbody>
</table>

- **Cisco Switch -VTP management**
  This report provides information related to activities that occur and are related to VTP.

  %VTP-2-MODE_OFF_PVLAN_EXIST Format: VTP Mode changed to off as Private VLAN configuration exists

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Facility Code</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/03/2017 04:40:38 PM</td>
<td>CISCO-IOS2</td>
<td>VTP-4-BAD_STARTUP_VLAN_CONFIG_FILE Format</td>
<td>Failed to configure VLAN from startup-config. Fallback to use VLAN configuration file from non-volatile</td>
</tr>
<tr>
<td>01/03/2017 04:40:38 PM</td>
<td>CISCO-IOS2</td>
<td>SW_VLAN-3-VTP_PROTOCOL_ERROR</td>
<td>VTP protocol internal error: Version 1 device detected on Fa0/23</td>
</tr>
</tbody>
</table>
- **Cisco Switch-VLAN management**
  This report provides information related to activities that occur which are related to VLAN.

  %VLAN_MGR-6-VLAN_OPER_STATUS_CHG: VLAN 135367, status changed to Active

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Facility Code</th>
<th>VLAN Name</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/03/2017 04:24:29 PM</td>
<td>CISCO-IOS</td>
<td>CDP-4-NATIVE_VLAN_MISMATCH</td>
<td>Native VLAN mismatch discovered on GigabitEthernet0/1 (1), VTP with Cisco500 FastEthernet0/3(99), VTP</td>
<td></td>
</tr>
<tr>
<td>01/03/2017 04:24:20 PM</td>
<td>CISCO-IOS</td>
<td>VLAN_MGR-6-VLAN_OPER_STATUS_CHG</td>
<td>135367</td>
<td>VLAN 135367, status changed to Active</td>
</tr>
<tr>
<td>01/03/2017 04:24:29 PM</td>
<td>CISCO-IOS</td>
<td>VLAN_MGR-6-VLAN_CREATED Format</td>
<td>accel</td>
<td>VLAN accel</td>
</tr>
</tbody>
</table>

- **Cisco Switch-Port security**
  This report provides information related to port security violation.

  %PORT_SECURITY-2-PSECURE_VIOLATION: Security violation occurred, caused by MAC address 0023.339c.e1cf on port FastEthernet4/4

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Computer</th>
<th>Facility Code</th>
<th>Message</th>
</tr>
</thead>
<tbody>
<tr>
<td>01/03/2017 12:07:06 PM</td>
<td>CISCO-IOS1</td>
<td>PM-4-ERR_DISABLE</td>
<td>psecure-violation error detected on Fa4/4, putting Fa4/4 in err-disable state</td>
</tr>
<tr>
<td>01/03/2017 12:07:06 PM</td>
<td>CISCO-IOS1</td>
<td>PM-4-ERR_DISABLE</td>
<td>psecure-violation error detected on Fa4/4, putting Fa4/4 in err-disable state</td>
</tr>
<tr>
<td>01/03/2017 12:07:06 PM</td>
<td>CISCO-IOS1</td>
<td>PORT_SECURITY-2-PSECURE_VIOLATION</td>
<td>Security violation occurred, caused by MAC address 0023.339c.e1cf on port FastEthernet4/4.</td>
</tr>
<tr>
<td>01/03/2017 12:07:06 PM</td>
<td>CISCO-IOS1</td>
<td>PM-4-ERR_RECOVER</td>
<td>Attempting to recover from psecure-violation err-disable state on Fa4/4</td>
</tr>
</tbody>
</table>
Import Cisco Switch Knowledge Pack into EventTracker

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

Figure 1

Import in the same order as mentioned:

- Templates
- Categories
- Alerts
- Reports as given below:
Categories

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

2. Locate All Cisco Switch group of Categories.iscat file, and then click the Open button.

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

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

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

![Figure 4](image1.png)

2. Locate All Cisco Switch 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](image2.png)

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.

**Templates**

1. Click the **Admin** menu, and then click **Parsing rule**.
2. Select **Template** tab, and then click on 'Import' option.

![Figure 6](image)

3. Click on **Browse** button.

![Figure 7](image)

4. Locate **All Cisco Switch 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.

**Flex Reports**

1. Click **Reports** option, and then click the **browse** button.
2. Locate **All Cisco Switch group reports.issch** file, and then click the **Open** button.
3. To import scheduled reports, click the **Import** button.

EventTracker displays success message.

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

Categories

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

![Category Management](image)

Figure 13

Alerts

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

![Successfully saved configuration.](image)

Figure 15

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

**NOTE:** Please specify appropriate systems in Alert configuration for better performance.
Template

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

![ParsIMG_20220524_003832.png](attachment:ParsIMG_20220524_003832.png)

Figure 16

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 Switch 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 Switch** in report groups. Check **Defined** dialog box.

4. Click on ‘schedule’ ![schedule icon] 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.
3. Navigate to **Dashboard>Flex**.
   Flex Dashboard pane is shown.

4. Click 📅 to add a new dashboard.
   Flex Dashboard configuration pane is shown.
4. Fill fitting title and description and click **Save** button.

5. Click ⚙️ to configure a new flex dashlet.

Widget configuration pane is shown.

![Widget Configuration Pane](image)

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

Evaluated chart is shown.
15. If satisfied, click **Configure** button.

16. Click ‘customize’ to locate and choose created dashlet.

17. Click to add dashlet to earlier created dashboard.
Sample Dashboards

1. Cisco Logon Failures Today

![Cisco Logon Failures Today](image_url)

Figure 28