Integrating Ruckus Wireless ZoneDirector

EventTracker Enterprise
Abstract

This guide provides instructions to configure Ruckus Wireless ZoneDirector to send the syslog events to EventTracker Enterprise.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version 7.x and later, and Ruckus Wireless ZD3000 9.5(MR) Software Release and later.

Audience

Ruckus Wireless ZoneDirector users, who wish to forward syslog messages to EventTracker Enterprise.
Table of Contents

Abstract .................................................................................................................................................. 1
Scope .................................................................................................................................................... 1
Audience ............................................................................................................................................. 1
Introduction ......................................................................................................................................... 3
Pre-requisite ......................................................................................................................................... 3
Enabling Log Settings .......................................................................................................................... 3
  The Log Settings options ..................................................................................................................... 4
  Debug Log Settings ............................................................................................................................ 5
EventTracker Knowledge Pack (KP) ..................................................................................................... 6
  Categories .......................................................................................................................................... 6
  Alerts ................................................................................................................................................ 11
  Flex Reports ..................................................................................................................................... 13
Import Ruckus Wireless ZD knowledge pack into EventTracker ......................................................... 19
  Category ........................................................................................................................................... 19
  Alerts ................................................................................................................................................ 21
  Templates ........................................................................................................................................ 22
  Flex Reports ..................................................................................................................................... 23
Verify Ruckus Wireless ZD knowledge pack in EventTracker ............................................................ 25
  Ruckus Wireless ZD Categories ........................................................................................................ 25
  Ruckus Wireless ZD Alerts ................................................................................................................ 25
  Ruckus Wireless ZD Template .......................................................................................................... 27
  Ruckus Wireless ZD Flex Reports .................................................................................................... 27
Create Flex Dashboards in EventTracker ............................................................................................ 28
  Schedule Reports ............................................................................................................................... 28
  Create Dashlets ................................................................................................................................. 30
Sample Flex Dashboards .................................................................................................................... 34
Introduction

Ruckus ZoneDirector is a Wireless Local Area Network (WLAN) controller. It is ideal for any enterprise that requires a high-performance wireless LAN that can be easily deployed and managed. It integrates seamlessly with existing switches, firewalls, authentication servers, and other network equipments, and can be placed within any Layer 2/3 network. All RuckusZoneFlex APs (wired or meshed) then automatically discover ZoneDirector, self-configure, and become instantly manageable.

The EventTracker Enterprise supports ZoneDirector. It provides an additional level of support by enabling you to generate reports and run searches on data to improve your ability to manage your ZoneDirector activity.

Pre-requisite

- EventTracker Enterprise should be installed.
- Ruckus ZoneDirector Controller 3000 should be deployed.
- Administrative access is required to make changes on the ZoneDirector Controller system.
- Syslog port 514 must be opened for ZoneDirector300.
- An exception should be added into windows firewall on EventTracker machine for syslog port 514.

Enabling Log Settings

Configure ZoneDirector to send event messages to a syslog server:

1. Log into ZoneDirector Web interface.
2. Go to Configure > System on the ZoneDirector Web interface.
3. Scroll down to Log Settings.
4. Make your selections from the syslog server options:
• **Event Log Level**: Select one of the three logging levels: *Show More*, *Warning and Critical Events* or *Critical Events Only*.

  Recommended – **Warning and Critical Events**

• **Remote Syslog**: To enable syslog logging, select the *Enable reporting to remote syslog server at* check box, and then type the IP address of EventTracker Enterprise in the box provided.

5. Click **Apply** to save your settings. The changes go into effect immediately.

**The Log Settings options**

![Figure 1 Configuring Remote Syslog Advanced Settings](image)

**Configuring Remote Syslog Advanced Settings**

Advanced syslog settings allow you to override the default **facility name** and **priority level** of messages sent to the syslog server. In this way, users can separate different kinds of syslog according to the facility name on the syslog server side.

To configure remote syslog advanced settings, perform the following steps:

1. Go to **Configure > System**.
2. Scroll down to **Log Settings**, and expand the **Remote Syslog Advanced Settings** section.
3. In ZoneDirector Settings, set the facility name as follows:
   - Keep Original: Retain the original facility name.
   - local0 – local7: Specify facility name.
4. Set the priority level as follows:

- **All**: Include all syslog messages.
- **0(emerg), 1(alert), 2(crit), 3(err), 4(warning), 5(notice), 6(info), 7(debug)**: Lower numbers indicate higher priority. The syslog server will only receive logs whose priority levels are the same as or lower than the configured level.

Example: Syslog alert

5. Repeat Step 4 for Managed AP Settings. ZoneDirector and Access Points can use different facility and priority settings. All managed APs share the same facility and priority settings.

Debug Log Settings

To receive logs for access point, web authentication, system management debug log has to be enabled. The following are the settings:

Select the debug log components that should be sent to the syslog server from **Administration > Diagnostics page > Debug Logs section**.

Setting debug logs

![Debug Log Settings](image)
EventTracker Knowledge Pack (KP)

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

The following Knowledge Packs are applicable in EventTracker v7.x and later to support Ruckus Wireless ZoneDirector monitoring:

Categories

- **ZoneDirector: Access point join attempt failed** - This category provides information related to access point join attempt failure.
- **ZoneDirector: Additional management interface created** - This category provides information related to additional management interface IP address created.
- **ZoneDirector: Additional management interface removed** - This category provides information related to additional management interface IP address removed.
- **ZoneDirector: Additional management interface updated** - This category provides information related to additional management interface IP address updated.
- **ZoneDirector: Admin locked out** - This category provides information related to admin lock out.
- **ZoneDirector: Admin logged out** - This category provides information related to admin logged out.
- **ZoneDirector: Admin login failed** - This category provides information related to admin login failed.
- **ZoneDirector: Admin login success** - This category provides information related to admin login success.
- **ZoneDirector: Admin password changed** - This category provides information related to admin password changed.
- **ZoneDirector: AP configuration update request failed** - This category provides information related to AP configuration update request failure.
- **ZoneDirector: AP contact lost with ZD** - This category provides information related to AP contact lost with ZD.
- **ZoneDirector: AP limit exceeded** - This category provides information related to AP limit exceeded.

- **ZoneDirector: AP management VLAN setting disabled** - This category provides information related to AP management VLAN setting disabled.

- **ZoneDirector: AP management VLAN setting enabled** - This category provides information related to AP management VLAN setting enabled.

- **ZoneDirector: Bonjour service disabled** - This category provides information related to Bonjour service disabled

- **ZoneDirector: Bonjour service enabled** - This category provides information related to Bonjour service enabled.

- **ZoneDirector: Cable modem interface down** - This category provides information related to cable Modem interface down.

- **ZoneDirector: Client disconnected by admin** - This category provides information related to client disconnected by admin.

- **ZoneDirector: DHCP server disabled** - This category provides information related to DHCP server disabled.

- **ZoneDirector: DHCP server enabled** - This category provides information related to DHCP server enabled.

- **ZoneDirector: eMesh AP connected to Mesh AP** - This category provides information related to eMesh AP connected to Mesh AP.

- **ZoneDirector: eMesh AP disconnected from Mesh AP** - This category provides information related to eMesh AP disconnected from Mesh AP.

- **ZoneDirector: eMesh AP disconnected from uplink** - This category provides information related to eMesh AP disconnected from uplink.

- **ZoneDirector: File retrieve failure** - This category provides information related to file retrieve failure.

- **ZoneDirector: FlexMaster management disabled** - This category provides information related to FlexMaster management disabled.

- **ZoneDirector: FlexMaster management enabled** - This category provides information related to FlexMaster management enabled.
- **ZoneDirector: FM user login failed** - This category provides information related to FM user login failed.

- **ZoneDirector: FM user login success** - This category provides information related to FM user login success.

- **ZoneDirector: Global client isolation disabled** - This category provides information related to global client isolation disabled.

- **ZoneDirector: Global client isolation enabled** - This category provides information related to global client isolation enabled.

- **ZoneDirector: Location service disabled** - This category provides information related to location service disabled.

- **ZoneDirector: Location service enabled** - This category provides information related to location service enabled.

- **ZoneDirector: Mesh AP connected to eMesh AP** - This category provides information related to mesh AP connected to eMesh AP.

- **ZoneDirector: Mesh AP disconnected from eMesh AP** - This category provides information related to mesh AP disconnected from eMesh AP.

- **ZoneDirector: Mesh AP disconnected from uplink** - This category provides information related to mesh AP disconnected from uplink.

- **ZoneDirector: Mesh name changed by admin** - This category provides information related to mesh name changed by admin.

- **ZoneDirector: Mesh packet forwarding filter disabled** - This category provides information related to mesh packet forwarding filter disabled.

- **ZoneDirector: Mesh packet forwarding filter enabled** - This category provides information related to mesh packet forwarding filter enabled.

- **ZoneDirector: Mesh packet forwarding filter modified** - This category provides information related to mesh packet forwarding filter modified.

- **ZoneDirector: Mesh passphrase changed by admin** - This category provides information related to mesh passphrase changed by admin.

- **ZoneDirector: Peer ZD configuration restored** - This category provides information related to peer ZD configuration restored.
- **ZoneDirector: Peer ZD connected** - This category provides information related to peer ZD connected.

- **ZoneDirector: Peer ZD disconnected** - This category provides information related to peer ZD disconnected.

- **ZoneDirector: Peer ZD firmware version mismatched** - This category provides information related to peer ZD firmware version mismatched.

- **ZoneDirector: Peer ZD license mismatched** - This category provides information related to peer ZD license mismatched.

- **ZoneDirector: Peer ZD model mismatched** - This category provides information related to peer ZD model mismatched.

- **ZoneDirector: Peer ZD upgrade failure** - This category provides information related to peer ZD upgrade failure.

- **ZoneDirector: Peer ZD upgrade pending** - This category provides information related to peer ZD upgrade pending.

- **ZoneDirector: Remote syslog disabled** - This category provides information related to remote syslog disabled.

- **ZoneDirector: Remote syslog enabled** - This category provides information related to remote syslog enabled.

- **ZoneDirector: Rogue AP detected** - This category provides information related to rogue AP detected.

- **ZoneDirector: Rogue DHCP server detected** - This category provides information related to rogue DHCP server detected.

- **ZoneDirector: Rogue DHCP server detector process disabled** - This category provides information related to rogue DHCP server detector process disabled.

- **ZoneDirector: Rogue DHCP server detector process enabled** - This category provides information related to rogue DHCP server detector process enabled.

- **ZoneDirector: SNMP authentication failed** - This category provides information related to SNMP authentication failed.

- **ZoneDirector: System configuration restored by administrator** - This category provides information related to system configuration restored by administrator.
• **ZoneDirector: System name changed** - This category provides information related to system name changed.

• **ZoneDirector: System received failover command** - This category provides information related to system received failover command.

• **ZoneDirector: System restarted by administrator** - This category provides information related to system restarted by administrator.

• **ZoneDirector: System restore command received** - This category provides information related to system restore command received.

• **ZoneDirector: System state changed** - This category provides information related to system state changed.

• **ZoneDirector: System upgrade command received** - This category provides information related to system upgrade command received.

• **ZoneDirector: System warm restarted** - This category provides information related to system warm restarted.

• **ZoneDirector: Telnet service disabled** - This category provides information related to telnet service disabled.

• **ZoneDirector: Telnet service enabled** - This category provides information related to telnet service enabled.

• **ZoneDirector: Temp license expired** - This category provides information related to temp license expired.

• **ZoneDirector: Unrecognized command received** - This category provides information related to unrecognized command received.

• **ZoneDirector: ZD authentication to location server failed** - This category provides information related to ZD authentication to location server failed.

• **ZoneDirector: ZD auto-recovery failed** - This category provides information related to ZD auto-recovery failed.

• **ZoneDirector: ZD auto-recovery successful** - This category provides information related to ZD auto-recovery successful.

• **ZoneDirector: ZD connection to location server dropped** - This category provides information related to ZD connection to location server dropped.
• **ZoneDirector: ZD DHCP pool full** - This category provides information related to ZD DHCP pool full.

• **ZoneDirector: ZD image upgrade failed** - This category provides information related to ZD image upgrade failed.

• **ZoneDirector: ZD image upgrade success** - This category provides information related to ZD image upgrade success.

• **ZoneDirector: ZD/AP high entropy certificate install failed** - This category provides information related to ZD/AP high entropy certificate install failed.

• **ZoneDirector: ZD/AP high entropy certificate install success** - This category provides information related to ZD/AP high entropy certificate install success.

• **ZoneDirector: ZoneDirector management VLAN disabled** - This category provides information related to ZoneDirector management VLAN disabled.

• **ZoneDirector: ZoneDirector management VLAN enabled** - This category provides information related to ZoneDirector management VLAN enabled.

**Alerts**

• **ZoneDirector: Access point join attempt failed** - This alert is generated when access point join attempt failed.

• **ZoneDirector: AP configuration update request failed** - This alert is generated when AP configuration update request failed.

• **ZoneDirector: AP contact lost with ZD** - This alert is generated when AP contact lost with ZD.

• **ZoneDirector: AP limit exceeded** - This alert is generated when AP limit exceeded.

• **ZoneDirector: Cable modem interface down** - This alert is generated when cable modem interface down.

• **ZoneDirector: eMesh AP connected to Mesh AP** - This alert is generated when eMesh AP connected to Mesh AP.

• **ZoneDirector: eMesh AP disconnected from Mesh AP** - This alert is generated when eMesh AP disconnected from Mesh AP.
- **ZoneDirector: eMesh AP disconnected from uplink** - This alert is generated when eMesh AP disconnected from uplink.

- **ZoneDirector: Mesh AP connected to eMesh AP** - This alert is generated when mesh AP connected to eMesh AP.

- **ZoneDirector: Mesh AP disconnected from eMesh AP** - This alert is generated when Mesh AP disconnected from eMesh AP.

- **ZoneDirector: Mesh AP disconnected from uplink** - This alert is generated when Mesh AP disconnected from uplink.

- **ZoneDirector: Peer ZD disconnected** - This alert is generated when peer ZD disconnected.

- **ZoneDirector: Peer ZD firmware version mismatched** - This alert is generated when peer ZD firmware version.

- **ZoneDirector: Peer ZD license mismatched** - This alert is generated when peer ZD license mismatched.

- **ZoneDirector: Peer ZD model mismatched** - This alert is generated when peer ZD model mismatched.

- **ZoneDirector: Peer ZD upgrade failure** - This alert is generated when peer ZD upgrade failed.

- **ZoneDirector: Rogue AP detected** - This alert is generated when rogue AP detected.

- **ZoneDirector: System ready to sync** - This alert is generated when system is ready to sync.

- **ZoneDirector: System received failover command** - This alert is generated when system received failover command.

- **ZoneDirector: System state changed** - This alert is generated when system state changed.

- **ZoneDirector: Temp license expire** - This alert is generated when temp license expire.

- **ZoneDirector: Unrecognized command received** - This alert is generated when unrecognized command received.

- **ZoneDirector: Administrator password changed** - This alert is generated when admin password has been changed.

- **ZoneDirector: Administrator account locked out** - This alert is generated when administrator account is locked out.
• **ZoneDirector: System configuration restored** – This alert is generated when system configuration is restored.

• **ZoneDirector: System restarted** – This alert is generated when admin has restarted the system.

• **ZoneDirector: System name changed** – This alert is generated when admin has changed the system name.

**Flex Reports**

• **ZoneDirector: Access point activity**

This report provides the information related to access point group name in which user machine mac address joins, leaves, disconnects from source access point and roams out from the source access point to target access point.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Device Name</th>
<th>User Address</th>
<th>Source AP</th>
<th>Status</th>
<th>Destination AP</th>
<th>Group Name</th>
<th>Wireless Standard</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/02/2016 12:08:48 PM</td>
<td>zd3000primary</td>
<td>0c:3e:9f:22:01:ff</td>
<td>KC-BSHOP-AP01@2c:e6:cc:26:a0:40</td>
<td>joins</td>
<td></td>
<td>KGuest</td>
<td></td>
</tr>
<tr>
<td>05/02/2016 12:15:46 PM</td>
<td>zd3000primary</td>
<td>70:81:eb:57:9f:1f</td>
<td>KC-PREOWN-AP01@2c:e6:cc:26:9f:e0</td>
<td>roams out</td>
<td>KC-PREOWN-AP03@2c:e6:cc:26:9a:d0</td>
<td>KGuest</td>
<td>11g</td>
</tr>
<tr>
<td>05/02/2016 12:22:30PM</td>
<td>zd3000primary</td>
<td>b4:f0:ab:39:ed:0f</td>
<td>KC-SVC-AP01@2c:e6:cc:26:90:40</td>
<td>disconnects</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>05/02/2016 12:36:25 PM</td>
<td>zd3000primary</td>
<td>0c:32:6b:cc:1c:0f</td>
<td>KC-EST2IND-AP01@2c:e6:cc:26:70:70</td>
<td>leave</td>
<td></td>
<td>KGuest</td>
<td>11g</td>
</tr>
<tr>
<td>05/02/2016 12:48:40 PM</td>
<td>zd3000primary</td>
<td>70:81:eb:57:9f:1f</td>
<td>KC-PREOWN-AP01@2c:e6:cc:26:9f:e0</td>
<td>roams out</td>
<td>KC-PREOWN-AP03@2c:e6:cc:26:9a:d0</td>
<td>KGuest</td>
<td>11g</td>
</tr>
</tbody>
</table>

Figure 3

Logs Considered:

```
Apr 20 06:48:44 zd3000primary Apr 20 06:48:47 syslog: eventd_to_syslog():User[0c:3e:9f:22:01:ff] joins WLAN[KGuest] from AP[KC-BSHOP-AP01@2ce6cc26a040]

Apr 20 06:49:11 zd3000primary Apr 20 06:49:15 syslog: eventd_to_syslog():AP[KC-PREOWN-AP01@2ce6cc269ad0] radio [11g/n] detects User[70B1:eb:57:9f:1f] in WLAN[KGuest] roams out to AP[KC-PREOWN-AP03@2ce6cc269ad0]

Apr 20 06:49:02 zd3000primary Apr 20 06:49:06 syslog: eventd_to_syslog():User[b4:f0:ab:39:ed:0f] disconnects from WLAN[KGuest] at AP[KC-SVC-AP03@2ce6cc26:9640]
```
• **ZoneDirector: Access point management**

This report provides information related to access point management that access point being released, restarted and reset to factory default and access point group was created, deleted and modified by the admin.

![Figure 4](image)

Logs Considered:

- Apr 20 06:49:11 zd3000primary Apr 20 06:49:15 syslog: eventd_to_syslog() AP[KC-PREOWN-AP03@2ce6:cc26:9a:d0] deleted by William

• **ZoneDirector: Admin locked out**

This report provides the information related to admin locked out duration and the reason for being locked.

![Figure 5](image)

Logs Considered:

- Apr 28 06:49:13 zd3000primary Apr 28 06:49:13 ruckus syslog: Peter is locked out for 1 hour (10 failed login attempts in 5 minutes)
• **ZoneDirector: Admin login failure**

This report provides the information related to admin log in failure from specific IP address.

![Log Time, Device Name, User Name, Source IP]

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Device Name</th>
<th>User Name</th>
<th>Source IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/28/2016 02:39:50 PM</td>
<td>zd3000primary</td>
<td>Peter</td>
<td>192.168.1.23</td>
</tr>
<tr>
<td>04/28/2016 04:39:50 PM</td>
<td>zd3000primary</td>
<td>Jennifer</td>
<td>192.168.1.42</td>
</tr>
</tbody>
</table>

Figure 6

Apr 20 06:49:13 zd3000primary Apr 20 06:49:13 ruckus syslog: Peter logs in failure from 192.168.1.23

• **ZoneDirector: Admin logon and logout success**

This report provides the information related to admin logged in and logged out success details from specified source IP address.

![Log Time, Device Name, User Name, Source IP, Status]

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Device Name</th>
<th>User Name</th>
<th>Source IP</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/02/2016 06:22:19 PM</td>
<td>zd3000primary</td>
<td>William</td>
<td>192.168.1.23</td>
<td>logged out</td>
</tr>
<tr>
<td>05/02/2016 06:48:19 PM</td>
<td>zd3000primary</td>
<td>Jennifer</td>
<td>192.168.1.42</td>
<td>logged out</td>
</tr>
<tr>
<td>05/03/2016 10:44:58 AM</td>
<td>zd3000primary</td>
<td>William</td>
<td>192.168.1.23</td>
<td>logged in</td>
</tr>
<tr>
<td>05/03/2016 11:10:42 AM</td>
<td>zd3000primary</td>
<td>Jennifer</td>
<td>192.168.1.42</td>
<td>logged in</td>
</tr>
</tbody>
</table>

Figure 7

Logs Considered:

Apr 20 06:49:13 zd3000primary Apr 20 06:49:13 ruckus syslog: William logged out from 192.168.1.23

Apr 20 06:49:13 zd3000primary Apr 20 06:49:13 ruckus syslog: Jennifer logged out from 192.168.1.42

• **ZoneDirector: Admin password changed**

This report provides the information related to admin password changed from specified source IP address.

![Log Time, Device Name, User Name, Source IP]

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Device Name</th>
<th>User Name</th>
<th>Source IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/28/2016 10:49:29 AM</td>
<td>zd3000primary</td>
<td>William</td>
<td>192.168.1.42</td>
</tr>
<tr>
<td>04/28/2016 11:15:30 AM</td>
<td>zd3000primary</td>
<td>Jennifer</td>
<td>192.168.1.23</td>
</tr>
</tbody>
</table>

Figure 8
EventTracker: Integrating Ruckus Wireless ZoneDirector

Log Considered:

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Device Name</th>
<th>User</th>
<th>Source IP</th>
<th>Action</th>
<th>VLAN</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/03/2016 12:02:08 PM</td>
<td>zd3000primary</td>
<td>William</td>
<td>192.168.1.23</td>
<td>AP settings</td>
<td></td>
<td>enabled</td>
</tr>
<tr>
<td>05/03/2016 12:10:36 PM</td>
<td>zd3000primary</td>
<td>William</td>
<td>192.168.1.23</td>
<td>VLAN setting</td>
<td></td>
<td>disabled</td>
</tr>
<tr>
<td>05/03/2016 12:22:48 PM</td>
<td>zd3000primary</td>
<td>William</td>
<td>192.168.1.23</td>
<td></td>
<td></td>
<td>disabled</td>
</tr>
<tr>
<td>05/03/2016 12:45:35 PM</td>
<td>zd3000primary</td>
<td>William</td>
<td>192.168.1.23</td>
<td></td>
<td>20</td>
<td>enabled</td>
</tr>
</tbody>
</table>

Figure 9

Logs Considered:

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Device Name</th>
<th>User</th>
<th>Source IP</th>
<th>Action</th>
<th>VLAN</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr 28 06:49:13 zd3000primary Apr 28 06:49:13 ruckus syslog: AP management VLAN enabled with AP settings by William from 192.168.1.23</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Apr 28 06:49:13 zd3000primary Apr 28 06:49:13 ruckus syslog: ZoneDirector management VLAN enabled with 20 by William from 192.168.1.23</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **ZoneDirector: All VLAN management status**

This report provides the information related to VLAN management status enabled or disabled by the admin.

- **ZoneDirector: FM user login failed**

This report provides the information related to flex master user logon failure from specified source ip address and user detail, which are listed below:

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Device Name</th>
<th>User Name</th>
<th>Source IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/02/2016 10:31:01 AM</td>
<td>zd3000primary</td>
<td>Charles</td>
<td>192.168.1.15</td>
</tr>
<tr>
<td>05/02/2016 11:22:41 AM</td>
<td>zd3000primary</td>
<td>Andrew</td>
<td>192.168.1.17</td>
</tr>
</tbody>
</table>

Figure 10

Log Considered:

<table>
<thead>
<tr>
<th>Log Time</th>
<th>Device Name</th>
<th>User</th>
<th>Source IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>Apr 28 06:49:13 zd3000primary Apr 20 06:49:13 ruckus syslog: FM user Charles logs in failure from 192.168.1.15</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

- **ZoneDirector: FM user login success**

This report provides the information related to flex master user logon success from specified source IP address.
EventTracker: Integrating Ruckus Wireless ZoneDirector

Log Considered:

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Device Name</th>
<th>Interface IP</th>
<th>Source IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>05/02/2016 10:30:56 AM</td>
<td>zd3000primary</td>
<td>Charles</td>
<td>192.168.1.15</td>
</tr>
<tr>
<td>05/02/2016 11:48:32 AM</td>
<td>zd3000primary</td>
<td>Smith</td>
<td>192.168.1.12</td>
</tr>
</tbody>
</table>

Figure 11

- ZoneDirector: Interface management
  
  This report provides the information related to interface management for ipv4 and ipv6 addresses created, removed and updated by the admin.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Device Name</th>
<th>Interface IP</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td>04/28/2016 03:36:48 PM</td>
<td>zd3000primary</td>
<td>fe80::2e0:b6ff:fe01:3b8d</td>
<td>updated</td>
</tr>
<tr>
<td>04/28/2016 03:36:48 PM</td>
<td>zd3000primary</td>
<td>fe80::2e0:b6ff:fe01:3b7a</td>
<td>created</td>
</tr>
<tr>
<td>04/28/2016 03:36:48 PM</td>
<td>zd3000primary</td>
<td>192.168.1.120</td>
<td>updated</td>
</tr>
<tr>
<td>04/28/2016 03:36:48 PM</td>
<td>zd3000primary</td>
<td>192.168.1.100</td>
<td>created</td>
</tr>
<tr>
<td>04/28/2016 04:27:44 PM</td>
<td>zd3000primary</td>
<td>192.168.1.100</td>
<td>removed</td>
</tr>
<tr>
<td>04/28/2016 04:27:44 PM</td>
<td>zd3000primary</td>
<td>fe80::2e0:b6ff:fe01:3b7a</td>
<td>removed</td>
</tr>
</tbody>
</table>

Figure 12

- ZoneDirector: Service status
  
  This report provides the information related to services enabled or disabled by the admin from specified source IP address.
Logs Considered:

- **ZoneDirector: WLAN group management**
  
  This report provides the information related to WLAN group created, deleted, modified, enabled or disabled by admin from specified source ip address.

<table>
<thead>
<tr>
<th>LogTime</th>
<th>Device Name</th>
<th>User Name</th>
<th>Status</th>
<th>Group Name</th>
<th>Source IP</th>
</tr>
</thead>
<tbody>
<tr>
<td>2016-05-06 20:45:22 PM</td>
<td>zd3000primary</td>
<td>Charles</td>
<td>created</td>
<td>KGMarketing</td>
<td>192.168.1.46</td>
</tr>
<tr>
<td>2016-05-06 12:30:23 PM</td>
<td>zd3000primary</td>
<td>Charles</td>
<td>deleted</td>
<td>KGMarketing</td>
<td>192.168.1.46</td>
</tr>
<tr>
<td>2016-05-06 12:38:36 PM</td>
<td>zd3000primary</td>
<td>Charles</td>
<td>enabled</td>
<td>KGMarketing</td>
<td>192.168.1.46</td>
</tr>
<tr>
<td>2016-05-06 12:55:36 PM</td>
<td>zd3000primary</td>
<td>Charles</td>
<td>disabled</td>
<td>KGMarketing</td>
<td>192.168.1.46</td>
</tr>
<tr>
<td>2016-05-06 12:58:42 PM</td>
<td>zd3000primary</td>
<td>Charles</td>
<td>created</td>
<td>KGMarketing</td>
<td>192.168.1.46</td>
</tr>
</tbody>
</table>

Logs Considered:

- Apr 20 06:49:11 zd3000primary Apr 20 06:49:15 syslog:WLAN[KGMarketing] deleted by Charles from IP[192.168.1.48]
- Apr 20 06:49:11 zd3000primary Apr 20 06:49:15 syslog:WLAN[KGMarketing] created by Charles from IP[192.168.1.48]
- Apr 20 06:49:11 zd3000primary Apr 20 06:49:15 syslog:WLAN[KGMarketing] disabled by Charles
Import Ruckus Wireless ZD knowledge pack into EventTracker

**NOTE:** Import knowledge pack items in the following sequence

- Categories
- Alerts
- Templates
- Flex Reports

1. Launch **EventTracker Control Panel**.
2. Double click **Import Export Utility**.
3. Click the **Import** tab.

### Category

1. Click **Category** option, and then click the browse button.
2. Locate the **All Ruckus ZD group of categories.iscat** file, and then click **Open** button.
3. To import categories, click the **Import** button.

   EventTracker displays success message.

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

1. Click **Alert** option, and then click the browse button.
2. Locate the **All Ruckus ZD group of alerts.isalt** file, and then click the **Open** button.

To import alerts, click the **Import** button.

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

Templates

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

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

3. Click on Browse button.

Figure 20

Figure 21
4. Locate **All Ruckus ZD group of token templates.ettd** file, and then click the **Open** button.

![Figure 22](image)

5. Now select the check box and then click on **Import** option. EventTracker displays success message.

![Figure 23](image)

6. Click on **OK** button.

**Flex Reports**

1. Click **Report** option, and then click the browse **...** button.
2. Locate the **All Ruckus ZD group of flex reports.issch** file, and then click the **Open** button.
3. Click the **Import** button to import the scheduled reports, EventTracker displays success message.
Verify Ruckus Wireless ZD knowledge pack in EventTracker

Ruckus Wireless ZD Categories

1. Logon to **EventTracker Enterprise**.

2. Click the **Admin** dropdown, and then click **Categories**.

3. In the **Category Tree**, expand **Ruckus Wireless ZoneDirector** group folder to see the imported categories.

![Category Management](image)

**Figure 26**

Ruckus Wireless ZD Alerts

1. Logon to **EventTracker Enterprise**.

2. Click the **Admin** dropdown, and then click **Alerts**.

3. In the **Search** field, type **ZoneDirector**, and then click **Go** button.

   Alert Management page will display all the imported Ruckus Wireless ZoneDirector alerts.
4. To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

![Figure 27](image)

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

**Note**
You can select alert notification such as Beep, Email, and Message etc. For this, select the respective checkbox in the Alert management page, and then click the **Activate Now** button.
Ruckus Wireless ZD Template

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

---

Ruckus Wireless ZD Flex Reports

1. Logon to EventTracker Enterprise.
2. Click the Reports menu, and then select Configuration.
3. In Reports Configuration pane, select Defined option.
   EventTracker displays Defined page.
4. In search box enter ‘ZoneDirector’, and then click the Search button.
   EventTracker displays Flex reports of Ruckus ZoneDirector
Create Flex Dashboards in EventTracker

Schedule Reports

1. Open EventTracker in browser and logon.

2. Navigate to Reports>Configuration.
3. Select **Ruckus ZoneDirector** in report groups. Check **defined** dialog box.

4. Click on 'schedule' to plan a report for later execution.
5. Check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.

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

7. 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.
4. Navigate to **Dashboard>Flex**.

   Flex Dashboard pane is shown.

![Figure 34](image.png)

4. Fill suitable title and description and click **Save** button.

5. Click 📜 to configure a new flex dashlet. Widget configuration pane is shown.
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 Flex Dashboards

1. Ruckus ZoneDirector: WLAN Group management

Figure 39
2. Ruckus ZoneDirector: Service Status

![Chart showing service status for Ruckus ZoneDirector](image)

*Figure 40*

3. Ruckus ZoneDirector: Access Point Activity

![Chart showing access point activity for Ruckus ZoneDirector](image)

*Figure 41*