

Integrate Cisco Wireless LAN Controller

EventTracker v8.x and above

Abstract

This guide provides instructions to configure Cisco WLC Controller to send the syslog to EventTracker Enterprise. Once syslog is configured to send to EventTracker Manager, alerts and reports can be configured into EventTracker.

Scope

The configurations detailed in this guide are consistent with **EventTracker Enterprise** version 8.x and later, **Cisco Wireless Controller 5500 Series, IOS version 8.0.140** and later.

Audience

Administrators who are responsible for monitoring **Cisco Wireless Controller** which are running the IOS Core operating system 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

Abstract	1
Scope	1
Audience	1
Cisco Wireless Controller	3
Prerequisites	3
Configure Cisco WLC to send syslog to EventTracker	3
Configure System and Message Logging	3
Enabling of Debug logs using CLI	5
EventTracker Knowledge Pack.....	5
Categories	5
Alerts	10
Flex Reports	12
Import Cisco Wireless Lan Controller knowledge pack into EventTracker	17
Category	18
Alerts	18
Token Templates	19
Flex Reports	20
Verify Cisco Wireless LAN Controller knowledge pack in EventTracker	22
Categories	22
Alerts	22
Token Template	23
Flex Reports	24
Create Flex Dashboards in EventTracker	25
Schedule Reports	25
Create Dashlets.....	28
Sample Flex Dashboards	31

Cisco Wireless Controller

Cisco Wireless Controllers provide the visibility, scalability, and reliability your business needs for building highly secure, wireless networks. Cisco Wireless Controllers reduces overall operational expenses by simplifying network deployment, operations, and management. Extending the same Cisco Borderless Networks policy and security from the wired network core to the wireless edge, Cisco Wireless Controllers deliver the industry's most scalable and highest-performing controller solution. These controllers provide unique network security and optimization for IPv6-enabled mobile clients, and next-generation hotspot functionality from branch offices, to small enterprises, to main campuses and service providers.

Prerequisites

- EventTracker v8.x should be installed.
- Cisco Wireless Controller 5500 Series version 8.0.140 and above should be installed and configured.
- Windows Version 7 or later should be installed.
- An exception should be added into windows firewall on EventTracker machine for syslog port 514.

Configure Cisco WLC to send syslog to EventTracker

System logging allows controllers to log their system events to up to three remote syslog servers. The controller sends a copy of each syslog message as it is logged to each syslog server configured on the controller. Being able to send the syslog messages to multiple servers ensures that the messages are not lost due to the temporary unavailability of one syslog server.

Configure System and Message Logging

1. Choose **Management>Logs>Config**. The Syslog Configuration page appears.

Figure 1: Syslog Configuration Page

2. In the **Syslog Server IP Address** (IPv4/IPv6) textbox, enter the IPv4/IPv6 address of the server to which you wish to send the syslog messages and click **Add**. You can add up to three syslog servers to the controller. The list of syslog servers that have already been added to the controller appears below this text box.

NOTE: If you want to remove a syslog server from the controller, click **Remove** to the right of the desired server.

3. To set the severity level for filtering syslog messages to the syslog servers, choose one of the following options from the Syslog Level drop-downlist:
 - Emergencies = Severity level 0
 - Alerts = Severity level 1(default value)
 - Critical = Severity level 2
 - Errors = Severity level 3
 - Warnings = Severity level 4
 - Notifications = Severity level 5
 - Informational = Severity level 6
 - Debugging = Severity level 7

If you set a syslog level, only those messages whose severity is equal to or less than that level are sent to the syslog servers. For example, if you set the syslog level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are sent to the syslog servers.

4. Click **Apply**.
5. To set the severity level for logging messages to the controller buffer and console, choose one of the following options from both the Buffered Log Level and Console Log Level drop-down lists:
 - Emergencies = Severity level 0
 - Alerts = Severity level 1
 - Critical = Severity level 2
 - Errors = Severity level 3 (default value)
 - Warnings = Severity level 4
 - Notifications = Severity level 5
 - Informational = Severity level 6
 - Debugging = Severity level 7
 - Disable = This option is available only for Console Log level. Select this option to disable console logging.

If you set a logging level, only those messages whose severity is equal to or less than that level are logged by the controller. For example, if you set the logging level to Warnings (severity level 4), only those messages whose severity is between 0 and 4 are logged.

6. Select the **File Info** check box if you want the message logs to include information about the source file. The default value is enabled.
7. Click **Apply**.
8. Click **Save Configuration**.

Enabling of Debug logs using CLI

For debug logs to be generated, the below given commands needs to be run via CLI (Command Line Interface)

1. Launch the Command line Interface and run the below commands.
 - debug lwapp/capwap iapp-data-echo
 - debug dot11 rogue rule enable
 - debug dot11 rogue enable
 - debug capwap ids sig
 - debug lwapp client mgmt.
 - debug client <client mac>
 - debug aaa ldap enable
 - debug capwap event
 - debug disable-all command

NOTE: Enabling of debugging will result in receiving high log volume.

EventTracker Knowledge Pack

Once logs are received into EventTracker, Categories reports can be configured into EventTracker.

The following Knowledge Packs are available in EventTracker Enterprise to support Windows.

Categories

- **Cisco Wlc: ACL configuration failed** - This category based report provides information related to Access-Control List configuration failure.
- **Cisco Wlc: Attack detected** - This category based report provides information related to attack detections.

- **Cisco Wlc: Authentication failure** - This category based report provides information related to authentication failure.
- **Cisco Wlc: BASE subsystem messages** - This category based report provides information related to BASE subsystem.
- **Cisco Wlc: BOOTP failure** - This category based report provides information related to BOOTP failure.
- **Cisco Wlc: Certificate added** - This category based report provides information about certification added.
- **Cisco Wlc: Certificate adding failed** - This category based report provides information about the failures while adding certificates.
- **Cisco Wlc: Certificate expired** - This category based report provides information about expired certificates.
- **Cisco Wlc: Certificate unknown** - This category based report provides information about unknown certificates.
- **Cisco Wlc: Command line interfaces alert messages** - This category based report provides information related to command line interfaces alert messages.
- **Cisco Wlc: Configuration changes** - This category based report provides information about configuration changes.
- **Cisco Wlc: Database API error** - This category based report provides information related to database API error.
- **Cisco Wlc: Database initialization failed** - This category based report provides information related to database initialization failure.
- **Cisco Wlc: Database lock failed** - This category based report provides information about failed database lock.
- **Cisco Wlc: Database record adding failed** - This category based report provides information about database record addition failure.
- **Cisco Wlc: Database unlock failed** - This category based report provides information about database record unlock failure.
- **Cisco Wlc: Debug messages** - This category based report provides information related to debug messages.

- **Cisco Wlc: Designated transit list error** - This category based report provides information related to designated transit list errors.
- **Cisco Wlc: DHCP binding port failed** - This category based report provides information related to DHCP binding port failure.
- **Cisco Wlc: DHCP configuration error** - This category based report provides information related to DHCP configuration errors.
- **Cisco Wlc: DHCP exceeds packet limit** - This category based report provides information related to exceeded DHCP packet limits.
- **Cisco Wlc: DHCP invalid magic cookie** - This category based report provides information related to DHCP invalid magic cookie.
- **Cisco Wlc: DHCP lease fail** - This category based report provides information related to DHCP lease failures.
- **Cisco Wlc: DHCP lease invalid** - This category based report provides information related to invalid DHCP leases.
- **Cisco Wlc: DHCP message truncated** - This category based report provides information related DHCP message truncated.
- **Cisco Wlc: DHCP packet dropped** - This category based report provides information about dropped DHCP packets.
- **Cisco Wlc: DHCP packet sending fail** - This category based report provides information about the DHCP packet sending failures.
- **Cisco Wlc: DHCP renew error** - This category based report provides information related to DHCP renew errors.
- **Cisco Wlc: DHCP socket error** - This category based report provides information related to DHCP socket errors.
- **Cisco Wlc: DHCP update failed** - This category based report provides information about failed DHCP updates.
- **Cisco Wlc: DOT3AD messages** - This category based report provides information related to DOT3AD messages.

- **Cisco Wlc: Ethernet Multisegment Topology error** - This category based report provides information related to multisegment Topology error.
- **Cisco Wlc: ETHOIP error messages** - This category based report provides information related to ETHOIP error messages.
- **Cisco Wlc: Extensible authentication protocol error** - This category based report provides information related to extensible authentication protocol error.
- **Cisco Wlc: FDB subsystem error** - This category based report provides information related to FDB subsystem error.
- **Cisco Wlc: Federal information processing error** - This category based report provides information related to federal information processing error.
- **Cisco Wlc: HIFN subsystem error** - This category based report provides information related to subsystem errors.
- **Cisco Wlc: Initialization failed** - This category based report provides information related to initialization failure to start like failed to open socket to read MAC.
- **Cisco Wlc: Inter-Access Point Protocol** - This category based report provides information related to inter-access point protocol.
- **Cisco Wlc: Internal system error** - This category based report provides information related to internal system errors.
- **Cisco Wlc: License error** - This category based report provides information related to license errors.
- **Cisco Wlc: Lightweight Access Point Protocol error** - This category based report provides information related to Lightweight Access Point Protocol errors.
- **Cisco Wlc: Location protocol error** - This category based report provides information related to location protocol errors.
- **Cisco Wlc: Mirror Module error** - This category based report provides information related to mirror module error.
- **Cisco Wlc: Mobility Management Connection error** - This category based report provides information related to mobility management connection errors.
- **Cisco Wlc: Networks-in-motion error** - This category based report provides information related to network-in-motion errors.

- **Cisco Wlc: Operating system API error** - This category based report provides information related to operating system API errors.
- **Cisco Wlc: Packet debugging messages** - This category based report provides information related to packet debugging system messages.
- **Cisco Wlc: Point-to-Point tunneling protocol error** - This category based report provides information related to point-to-point tunneling protocol errors.
- **Cisco Wlc: Power failed** - This category based report provides information related to power failure of appliance.
- **Cisco Wlc: Radio frequency identification error** - This category based report provides information related to radio frequency identification errors.
- **Cisco Wlc: Radio resource management error** - This category based report provides information related to radio resource management errors.
- **Cisco Wlc: Resource error** - This category based report provides information related to resource error, such as not able to allocate memory.
- **Cisco Wlc: Router blade control protocol error** - This category based report provides information related to router blade control protocol errors.
- **Cisco Wlc: Simple network management protocol error** - This category based report provides information related to SNMP errors, such as failed to initialize, and failed to send traps and so on.
- **Cisco Wlc: Simple network time protocol error** - This category based report provides information related to Network time protocol errors.
- **Cisco Wlc: Subscriber identity module error** - This category based report provides information related to subscriber identity module errors.
- **Cisco Wlc: Sysnet subsystem messages** - This category based report provides information related to sysnet subsystem messages.
- **Cisco Wlc: System error messages** - This category based report provides information related to system errors.
- **Cisco Wlc: System update error** - This category based report provides information related to system update errors.
- **Cisco Wlc: TFTP error** - This category based report provides information related to TFTP errors.

- **Cisco Wlc: Tool subsystem messages** - This category based report provides information related to tool subsystem.
- **Cisco Wlc: Trap manager messages** - This category based report provides information related to error in writing config file and failed registration for DTL event port trap exit and entry.
- **Cisco Wlc: User login failed** - This category based report provides information about user login failures.
- **Cisco Wlc: USM Db messages** - This category based report provides information related to invalid argument passing to USM Db.
- **Cisco Wlc: VLAN error** - This category based report provides information related to Virtual LAN errors occurring due to different causes.

Alerts

- **Cisco Wlc ACL configuration failed** - This alert is generated when Access-list configuration fails.
- **Cisco Wlc: Attack detected** - This alert is generated when attack is detected.
- **Cisco Wlc: Authentication failure** - This alert is generated when authentication failure occurs.
- **Cisco Wlc: Database API error** - This alert is generated when database API error occurs.
- **Cisco Wlc: Database initialization failed** - This alert is generated when user database fails to initialize.
- **Cisco Wlc: Database lock failed** - This alert is generated when database fails to lock.
- **Cisco Wlc: Database record adding failed** - This alert is generated when fails to add record to database.
- **Cisco Wlc: Database unlock failed** - This alert is generated when fails to unlock database.
- **Cisco Wlc: Designated transit list error** - This alert is generated when designated transit list error occurs.
- **Cisco Wlc: Ethernet Multi segment Topology error** - This alert is generated when the EMT configuration could not be saved correctly, and fails to create EMT task and Ethernet multi segment topology task fails to initialize correctly.
- **Cisco Wlc: Extensible Authentication Protocol error** - This alert is generated when unable to enqueue message to process, EAP global process Queue is not enabled and cannot init/create timer.

- **Cisco Wlc: FDB subsystem error** - This alert is generated when failed to create and exit fdb task and error retrieving files.
- **Cisco Wlc: Initialization failed** - This alert is generated when initialization fails to start.
- **Cisco Wlc: Internal system error** - This alert is generated when internal system error occurs.
- **Cisco Wlc: Location Protocol error** - This alert is generated when a location protocol error occurs such as controller LBS-SSC AuthList fails to validate certificate.
- **Cisco Wlc: Operating system API error** - This alert is generated when operating system API error occurs.
- **Cisco Wlc: Point-to-Point Tunneling Protocol error** - This alert is generated when PPTP related error occurs.
- **Cisco Wlc: Power failed** - This alert is generated when the specified power supply fails.
- **Cisco Wlc: Router Blade Control Protocol error** - This alert is generated when Router Blade Control Protocol error such as failed to create RBCP osapi queue occurs.
- **Cisco Wlc: system error messages** - This alert is generated when system related error occurs.
- **Cisco Wlc: System update error** - This alert is generated when system update related error occurs.
- **Cisco Wlc: TFTP error** - This alert is generated when error occurs while receiving and sending files.
- **Cisco Wlc: User login failed** - This alert is generated when user fails to login.
- **Cisco Wlc: ACL configuration failed** - This alert is generated when any Access list configuration fails.
- **Cisco Wlc: AP login success** – This alert is generated when any Access Point successfully logs in.
- **Cisco Wlc: AP registration failures**- This alert is generated when any Access Point registration fails.
- **Cisco Wlc: Attack detection**- This alert is generated when any Attack is detected in the Wireless Controller.
- **Cisco Wlc: AP login failures**- This alert is generated when any Access Point login fails.
- **Cisco Wlc: Port status changed**- This alert is generated when any Port status is changed.
- **Cisco Wlc: System failures**- This alert is generated when any System failure occurs.

Flex Reports

- **Cisco Wlc-ACL configuration failed-** This report provides details about any Access List configuration failures that occur in Cisco Wlc.

LogTime	Computer	Severity	Status	ACL name	Message
04/24/2017 02:08:22 PM	CISCOWLC-SYSLOG	3	ENTRY_DONOT_EXIST	Ã¶Ã¶.	acl.c:376 Unable to find an ACL by name Ã¶Ã¶.
04/24/2017 03:01:45 PM	CISCOWLC-SYSLOG	7	GET_NAME_BY_ID_FAILED	jd hfp@.	Couldnt get ACL name by ID jd hfp@.
04/24/2017 03:01:45 PM	CISCOWLC-SYSLOG	3	SET_PORT_RANGE_FAILED		MSG_TRACEBACK

- **Cisco Wlc-AP login failure-** This report provides details on Access Point logon failure attempts.

LogTime	Computer	Status	Severity	AP name	Message
04/25/2017 06:30:35 PM	CISCOWLC-SYSLOG	CONSOLE_LOGIN_ERR1	3	Mnc013-MK3-AP9	Console login failure on AP Mnc013
04/25/2017 06:30:35 PM	CISCOWLC-SYSLOG	CONSOLE_LOGIN_ERR1	3	Skynet34-MK3-AP9	Console login failure on AP Skynet34
04/25/2017 06:30:35 PM	CISCOWLC-SYSLOG	CONSOLE_LOGIN_ERR1	3	Botnet111-MK3-AP9	Console login failure on AP Botnet111

- **Cisco Wlc-AP login success-** This report provides details on all successful Access Point logon that is done.

LogTime	Computer	Status	Severity	AP name	Message
04/25/2017 06:28:32 PM	CISCOWLC-SYSLOG	CONSOLE_LOGIN	6	Mnc013-MK3-AP9	Console login success on AP Mnc013
04/25/2017 06:28:32 PM	CISCOWLC-SYSLOG	CONSOLE_LOGIN	6	Skynet34-MK3-AP9	Console login success on AP Skynet34
04/25/2017 06:28:32 PM	CISCOWLC-SYSLOG	CONSOLE_LOGIN	6	Botnet111-MK3-AP9	Console login success on AP Botnet111

- **Cisco Wlc-AP registration failures-** This report provides details about all the Access Point registration failures that is done.

LogTime	Computer	Status	Severity	AP Mac	Message
04/26/2017 03:32:18 PM	CISCOWLC-SYSLOG	MAX_AID2	3	00:60:1d:01:23:45	Reached max limit on the association ID for AP eth0 ap 00:60:1d:01:23:45.
04/26/2017 03:32:18 PM	CISCOWLC-SYSLOG	JOIN_MAX_AP_ERR	3	6c:8d:c1:ec:67:81	Received a join request from AP 6c:8d:c1:ec:67:81 - reached limit for maximum APs 703.1.1/945.31, dropping the packet
04/26/2017 03:32:18 PM	CISCOWLC-SYSLOG	AP_JDBG_ADD_FAILED	4	e8:b1:fc:f6:f4:73	Unable to create AP Join information entry for AP: e8:b1:fc:f6:f4:73, skynet11.
04/26/2017 03:32:18 PM	CISCOWLC-SYSLOG	AAA_ERR2	3	f0:db:e2:ce:fb:8f	Invalid AAA state for AP f0:db:e2:ce:fb:8f
04/26/2017 03:32:18 PM	CISCOWLC-SYSLOG	ECHO_ERR	3	e8:2a:ea:79:d7:31	Did not receive heartbeat reply; AP: e8:2a:ea:79:d7:31

- **Cisco Wlc-Attack detection-** This report provides details about any Attack that is attempted to compromise the Wlc.

LogTime	Computer	Status	Severity	AP name	AP Mac	Client name	Client Mac	Source IP Address	Target IP address	Message
04/27/2017 05:41:31 PM	CISCOWLC-SYSLOG	ARP_POISON_DETECTED	1				00:01:02:0e:54:c4	192.168.1.152	192.168.0.206	STA [00:01:02:0e:54:c4, 0.0.0.0] ARP (op 1) received with invalid SPA
04/26/2017 02:44:57 PM	CISCOWLC-SYSLOG	EAPOL_MSG_ATTACK	3				84:a1:34:cb:e9:8c			Possible authentication attack - client authentication
04/26/2017 02:44:58 PM	CISCOWLC-SYSLOG	BIG_NAV_ATTACK	1	Firedragon909						Big Nav attack detected on AP Firedragon909 - MK3-AP9, slot 2
04/26/2017 02:44:58 PM	CISCOWLC-SYSLOG	ATTACK_DETECTED	3			Firedragon909				Detecting an attack from Firedragon909 - MK3-AP9.
04/26/2017 02:44:58 PM	CISCOWLC-SYSLOG	ATTACK_DETECTED	3			Firedragon909				Detecting an attack from Firedragon909 - MK3-AP9. Disconnecting

- **Cisco Wlc-DHCP activities-** This report provides details on all the DHCP activities that is done on the Wlc.

LogTime	Computer	DHCP activity	Client Mac address
04/26/2017 04:17:22 PM	CISCOWLC-SYSLOG	DHCP DISCOVER	9c:fc:01:8a:18:5b
04/26/2017 04:17:22 PM	CISCOWLC-SYSLOG	DHCP REQUEST	9c:fc:01:8a:18:5b
04/26/2017 04:17:22 PM	CISCOWLC-SYSLOG	DHCP ACK	00:40:96:b4:8c:e1
04/26/2017 04:17:22 PM	CISCOWLC-SYSLOG	DHCP OFFER	00:1b:77:2b:cf:75
04/26/2017 04:17:22 PM	CISCOWLC-SYSLOG	BOOTREQUEST	9c:fc:01:8a:18:5b
04/26/2017 04:17:22 PM	CISCOWLC-SYSLOG	BOOTREPLY	00:40:96:b4:8c:e1

- **Cisco Wlc-Port status changed-** This report provides details on the Port status associated with the Wlc.

LogTime	Computer	Status	Severity	Port number	Message
04/27/2017 01:35:20 PM	CISCOWLC-SYSLOG	CREATING_PORT	7	# 80,# 443	GID: Creating Port # 80,# 443.
04/27/2017 01:35:20 PM	CISCOWLC-SYSLOG	RMV_PORT	7	# 67,# 68,# 80,# 443	GID: Removing Port # 67,# 68,# 80,# 443 from the ring.
04/27/2017 01:35:20 PM	CISCOWLC-SYSLOG	CREATED_PORT	7	# 67,# 68,# 80	GID: created Port # 67,# 68,# 80 .
04/27/2017 01:35:20 PM	CISCOWLC-SYSLOG	LAG_PORT_CHANGE_FAIL	3	# 121	Failed to change the Link Aggregation port status. Port # 121
04/27/2017 01:35:20 PM	CISCOWLC-SYSLOG	PORT_ENABLED	7	# 161	Port is Enabled. Port # 161.
04/27/2017 01:35:20 PM	CISCOWLC-SYSLOG	ADMIN_MODE_ENABLE	0	# 68	Port # 68 Admin Mode is Enable.
04/27/2017 01:35:20 PM	CISCOWLC-SYSLOG	DESTROY_PORT	7	# 443,# 123	GID: Destroying Port # 443,# 123.

- **Cisco Wlc-Rogue AP activities-** This report provides details about all the Rogue Access Point that is detected in the network.

LogTime	Computer	Status	Severity	Client AP Mac address	Rogue AP Mac address	Message
04/25/2017 01:43:52 PM	CISCOWLC-SYSLOG	CHANGE_ROGUE_STATE_FAILED	1		c4:f0:81:0f:70:38	Can not change state on rogue c4:f0:81:0f:70:38
04/25/2017 01:43:52 PM	CISCOWLC-SYSLOG	AUTHMOBILE_SEND_FAILED	1	c4:f0:81:0f:70:38	f4:42:8f:c2:f9:4d	Could not send the LWAPP Authenticate Mobile command to rogue AP f4:42:8f:c2:f9:4d for mobile c4:f0:81:0f:70:38. bot221.
04/25/2017 01:43:53 PM	CISCOWLC-SYSLOG	CHANGE_ROGUE_STATE_FAILED	1		c4:f0:81:0f:70:38	Can not change state on rogue c4:f0:81:0f:70:38

- **Cisco Wlc-Successful AP registration-** This report provides details about all the successful Access Point registration or association with Wlc.

LogTime	Computer	AP Mac address	Slot	Message
04/25/2017 04:36:36 PM	CISCOWLC-SYSLOG	00:0b:85:5b:fb:d0	0	LAP registers with the WLC
04/25/2017 04:36:36 PM	CISCOWLC-SYSLOG	34:02:86:42:84:7a	5	LAP registers with the WLC
04/25/2017 04:36:36 PM	CISCOWLC-SYSLOG	38:ca:da:37:18:43	3	LAP registers with the WLC

- **Cisco Wlc-System failures-** This report provides details about all the System failures, hardware failures and memory allocation failures in the Wlc.

LogTime	Computer	Status	Severity	Messages
04/26/2017 12:08:37 PM	CISCOWLC-SYSLOG	PS_DETECT	6	Power supply is down.
04/26/2017 12:08:37 PM	CISCOWLC-SYSLOG	PS_FAIL	3	Redundant power supply failure.
04/26/2017 12:08:44 PM	CISCOWLC-SYSLOG	FAN_FAIL	3	Fans had a rotation error reported.
04/27/2017 03:45:26 PM	CISCOWLC-SYSLOG	SYSMEMFULL		Out of System buffers.
04/27/2017 03:45:26 PM	CISCOWLC-SYSLOG	MEM_THRESHOLD_REACHED	0	Memory threshold reached. Not allocating memory.
04/27/2017 03:45:26 PM	CISCOWLC-SYSLOG	MEM_ALLOC_FAILED	0	Out of memory. Unable to allocate 75423.626 bytes!.
04/27/2017 03:45:26 PM	CISCOWLC-SYSLOG	ALLOC_POOL_FAILED	0	Out of memory! Unable to allocate a chunk for pool 126569.3 bytes!.

- **Cisco Wlc-User account management-** This report provides details about all the User account management that is done in Wlc.

LogTime	Computer	Severity	Status	Message
04/24/2017 05:12:37 PM	CISCOWLC-SYSLOG	3	UNAME_TOO_LONG	Username too long. Username length:23.
04/24/2017 05:12:37 PM	CISCOWLC-SYSLOG	3	USER_NAME_INVALID	Invalid username provided hking\$#
04/24/2017 05:12:38 PM	CISCOWLC-SYSLOG	4	GUESTUSER_DEL_FAILED	Unable to delete the user '%s'. %s.
04/24/2017 05:12:39 PM	CISCOWLC-SYSLOG	6	GUEST_ACCOUNT_EXPIRE	Guest user account
04/24/2017 05:12:39 PM	CISCOWLC-SYSLOG	6	RECREATE_ADMIN_USR	Recreated the admin user.
04/24/2017 05:12:39 PM	CISCOWLC-SYSLOG	6	GUEST_ACCOUNT_DELETE	Guest user account
04/24/2017 05:12:39 PM	CISCOWLC-SYSLOG	6	GUEST_ACCOUNT_CREATE	Guest user account
04/24/2017 07:01:37 PM	CISCOWLC-SYSLOG	6	DELETE_CLIENT_ACCOUNT_DELETED	Delete client e4:a4:71:a2:ed:42 because user account akaip001 has been deleted.
04/24/2017 07:01:37 PM	CISCOWLC-SYSLOG	6	GUEST_ACCOUNT_CREATE	Guest user account

Import Cisco Wireless Lan Controller knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token templates
- Flex Reports

NOTE: Export knowledge pack items in the following sequence:

- Categories
- Alerts
- Token templates
- Flex Reports

1. Launch **EventTracker Control Panel**.
2. Double click **Export Import Utility**.

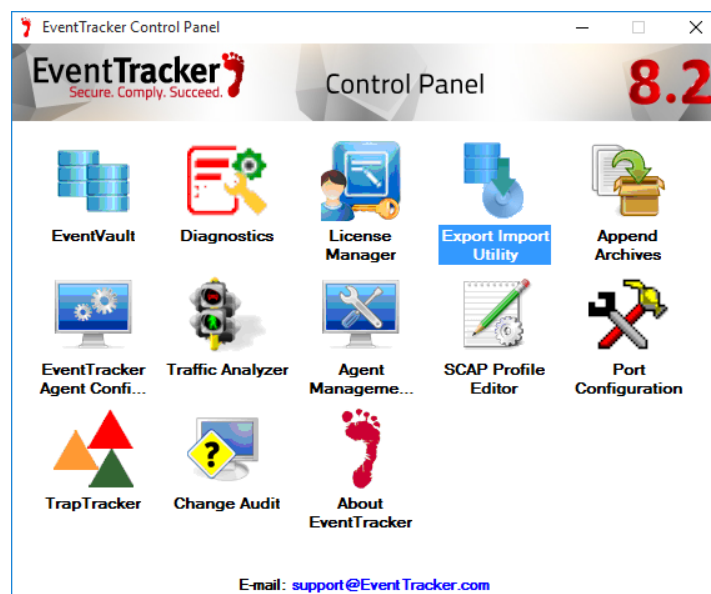



Figure 2

3. Click the **Import** tab.

Category

1. Click **Category** option, and then click the browse  button.
2. Locate the **All Cisco Wlc group of categories.iscat** file, and then click **Open** button.

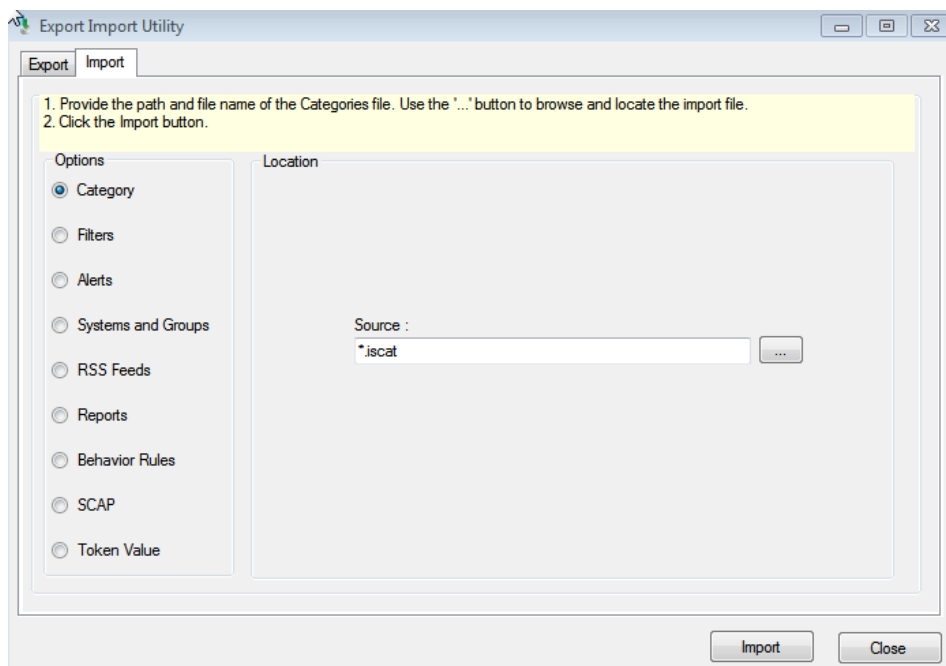


Figure 3

3. To import categories, click the **Import** button.

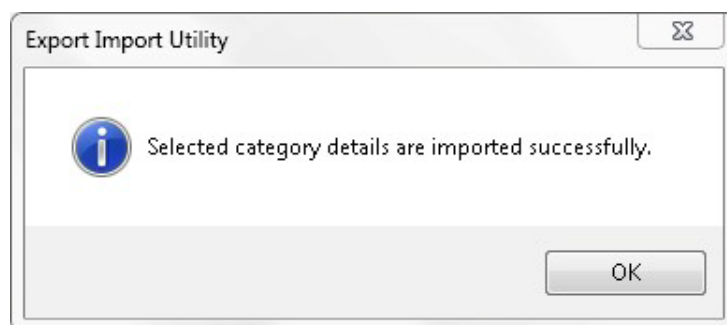



Figure 4

Alerts

1. Click **Alerts** option, and then click the browse  button.
2. Locate the **All Cisco Wlc alerts.isalt** file, and then click the **Open** button.

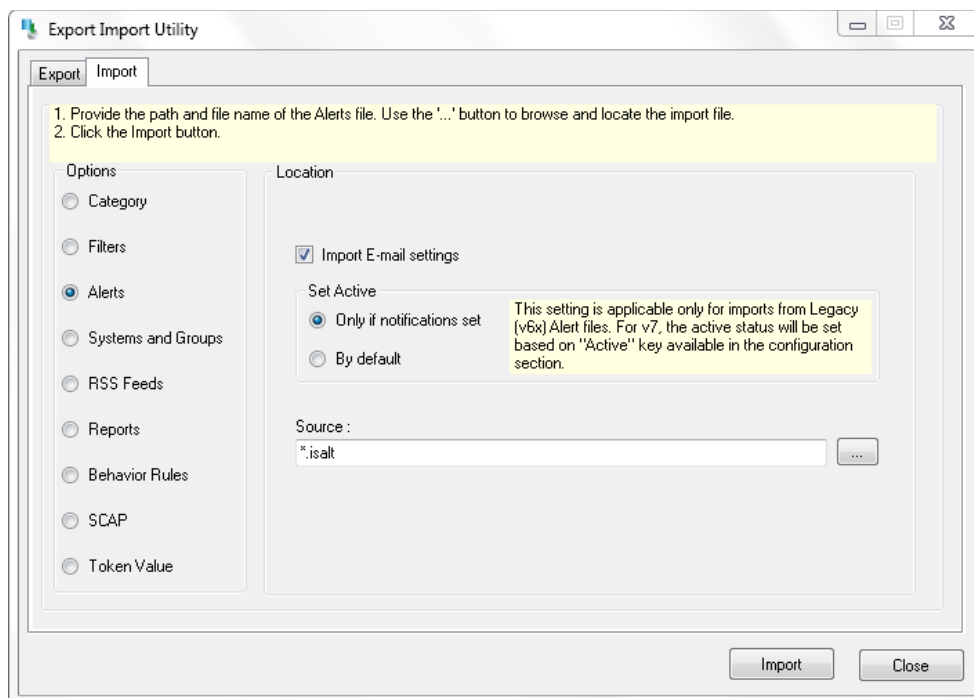


Figure 5

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

EventTracker displays success message.

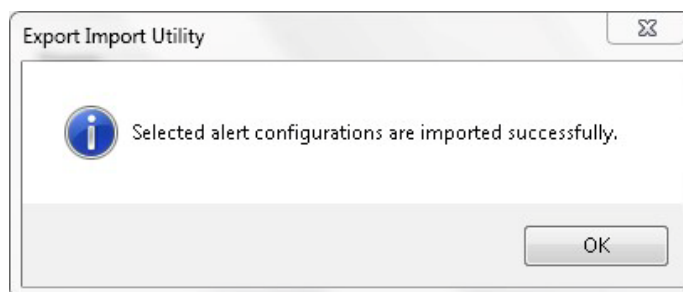


Figure 6

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

Token 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.

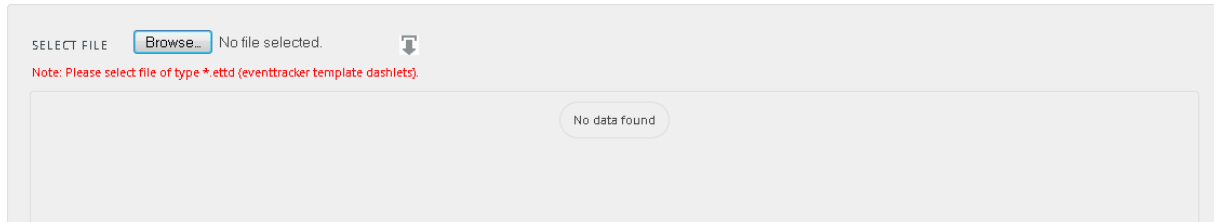


Figure 7

4. Locate **All Cisco Wlc Tokens.ettd** file, and then click the **Open** button.

SELECTED FILE IS: Cisco wlc token templates.ettd

<input type="checkbox"/>	TEMPLATE NAME	SEPARATOR	TEMPLATE DESCRIPTION	ADDED DATE	ADDED BY	GROUP NAME
<input type="checkbox"/>	Cisco Wlc-ACL configuration failed	\n	Apr 18 08:57:38 hki-wlan-con-01 HKI-WLAN-CON-01: *SNIMPTask: Apr 18 08:57:39:087: %HREAP-7-ACL_ENTRY_DONOT_EXIST: acl.c376 Unable to find an AC L by name "Axor@"	4/24/2017 3:43:59 PM	ETAdmin	Cisco Wlc
<input checked="" type="checkbox"/>	Cisco Wlc-AP login failure	\n	Apr 18 09:02:24 ams-wlan-con-01 AMS-WLAN-CON-01: *spamApTask2: Apr 18 09:02:24:573: %LWAPP-3-CONSOLE_LOGIN_ERR1: Console login failure on AP Mnc013	4/25/2017 6:41:25 PM	ETAdmin	Cisco Wlc
<input type="checkbox"/>	Cisco Wlc-AP login success	\n	Apr 18 09:02:24 ams-wlan-con-01 AMS-WLAN-CON-01: *spamApTask2: Apr 18 09:02:24:573: %LWAPP-6-CONSOLE_LOGIN: Console login success on AP Mnc013	4/25/2017 6:35:49 PM	ETAdmin	Cisco Wlc
<input checked="" type="checkbox"/>	Cisco Wlc-AP registration failures	\n	Apr 18 08:57:38 hki-wlan-con-01 HKI-WLAN-CON-01: *spamApTask4: Apr 18 08:57:39:087: %LWAPP-3-AAA_ERR2: Invalid AAA state for AP f0d8e2ce:fb:8f	4/26/2017 3:44:39 PM	ETAdmin	Cisco Wlc
<input type="checkbox"/>	Cisco Wlc-Attack detection	\n	Apr 18 08:57:38 hki-wlan-con-01 HKI-WLAN-CON-01: *spamApTask4: Apr 18 08:57:39:087: %LWAPP-3-DUP_AP_IP: Duplicate IP address detected for AP Mnc013-MK3-AP9, IP address of AP 10.12.124.36, this is a duplicate of IP on another machine 4c57:ca:b3:88:f0	4/26/2017 2:51:49 PM	ETAdmin	Cisco Wlc

Figure 8

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

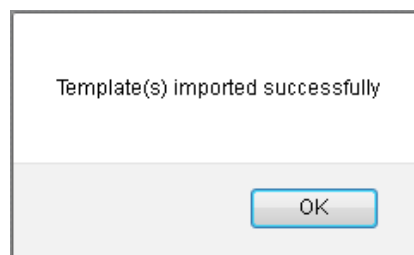



Figure 9

6. Click on **OK** button.

Flex Reports

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

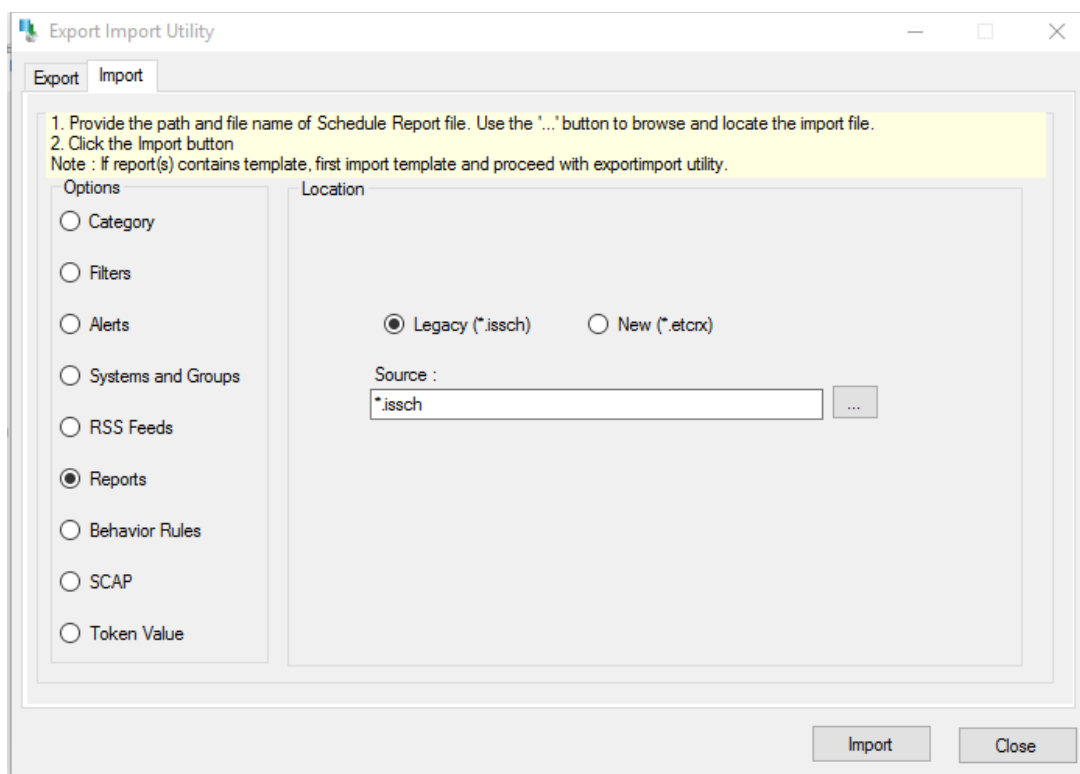


Figure 10

3. Click the **Import** button to import the **scheduled** reports. EventTracker displays success message.

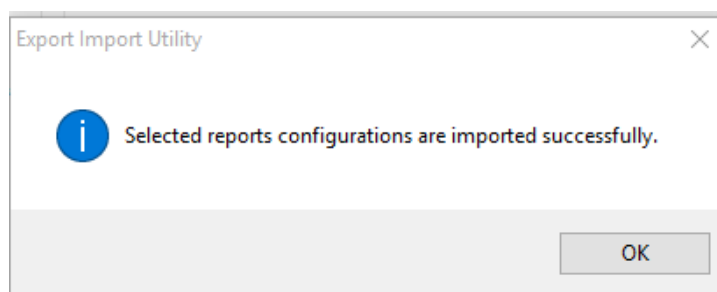


Figure 11

Verify Cisco Wireless LAN Controller knowledge pack in EventTracker

Categories

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Categories**.

In the **Category Tree**, expand **Cisco WLAN Controller** group folder to see the imported categories

The screenshot shows the 'CATEGORY MANAGEMENT' interface. On the left, the 'Category Tree' is expanded to show 'Cisco WLAN Controller' and its sub-items: Cisco WLAN Authentication, Cisco WLAN Database activities, Cisco WLAN DHCP, Cisco WLAN IDS, Cisco WLAN system messages, Cisco WLAN: ACL configuration fail, Cisco WLAN: BASE subsystem mess, Cisco WLAN: BOOTP failure, Cisco WLAN: Certificate services, Cisco WLAN: Command line interfa, and Cisco WLAN: Configuration change. On the right, a table lists the 'Last 10 modified categories'.

NAME	MODIFIED DATE	MODIFIED BY
Cisco WLAN: Trap manager messages	5/2/2017 12:47:34 PM	ETAdmin
Cisco WLAN: Resource error	5/2/2017 12:47:22 PM	ETAdmin
Cisco WLAN: Configuration changes	5/2/2017 12:47:10 PM	ETAdmin
Cisco WLAN: BOOTP failure	5/2/2017 12:46:55 PM	ETAdmin
Cisco WLAN: BASE subsystem messages	5/2/2017 12:46:40 PM	ETAdmin
Cisco WLAN: ACL configuration failed	5/2/2017 12:46:04 PM	ETAdmin
Cisco WLAN: Authentication failure	5/2/2017 12:45:36 PM	ETAdmin

Figure 12

Alerts

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Alerts**.
2. In the **Search** field, type **Cisco Wlc**, and then click **Go** button.
Alert Management page will display the imported Cisco Wlc alert.

ALERT MANAGEMENT

Search by

Click 'Activate Now' after making all changes Total: 7 Page Size 25

<input type="checkbox"/>	ALERT NAME ^	THREAT	ACTIVE	E-MAIL	MESSAGE	RSS	FORWARD AS SNMP	FORWARD AS SYSLOG	REMEDIAL ACTION AT CONSOLE	REMEDIAL ACTION AT AGENT	APPLIES TO
<input type="checkbox"/>	Cisco Wlc: ACL configuration failed	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco Wlc 8.0.140
<input type="checkbox"/>	Cisco Wlc: AP login success	Medium	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco WLC 8.0.140
<input type="checkbox"/>	Cisco Wlc: AP registration failures	Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco WLC 8.0.140
<input type="checkbox"/>	Cisco Wlc: Attack detection	Critical	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco WLC 8.0.140
<input type="checkbox"/>	Cisco Wlc: Login failure	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco WLC 8.0.140
<input type="checkbox"/>	Cisco Wlc: Port status changed	High	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco WLC 8.0.140
<input type="checkbox"/>	Cisco Wlc: System failures	Serious	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	Cisco WLC 8.0.140

Figure 13

- To activate the imported alerts, select the respective checkbox in the **Active** column. EventTracker displays message box.

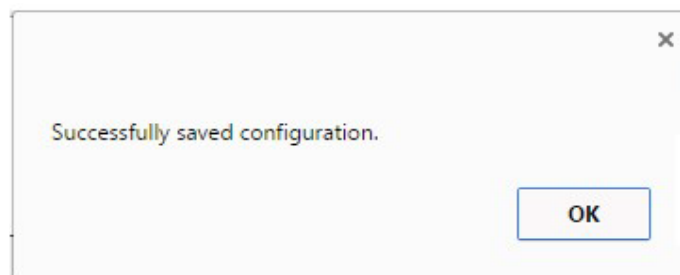


Figure 14

- 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.

Token Template

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

3. Click on **Cisco Wlc** group option.

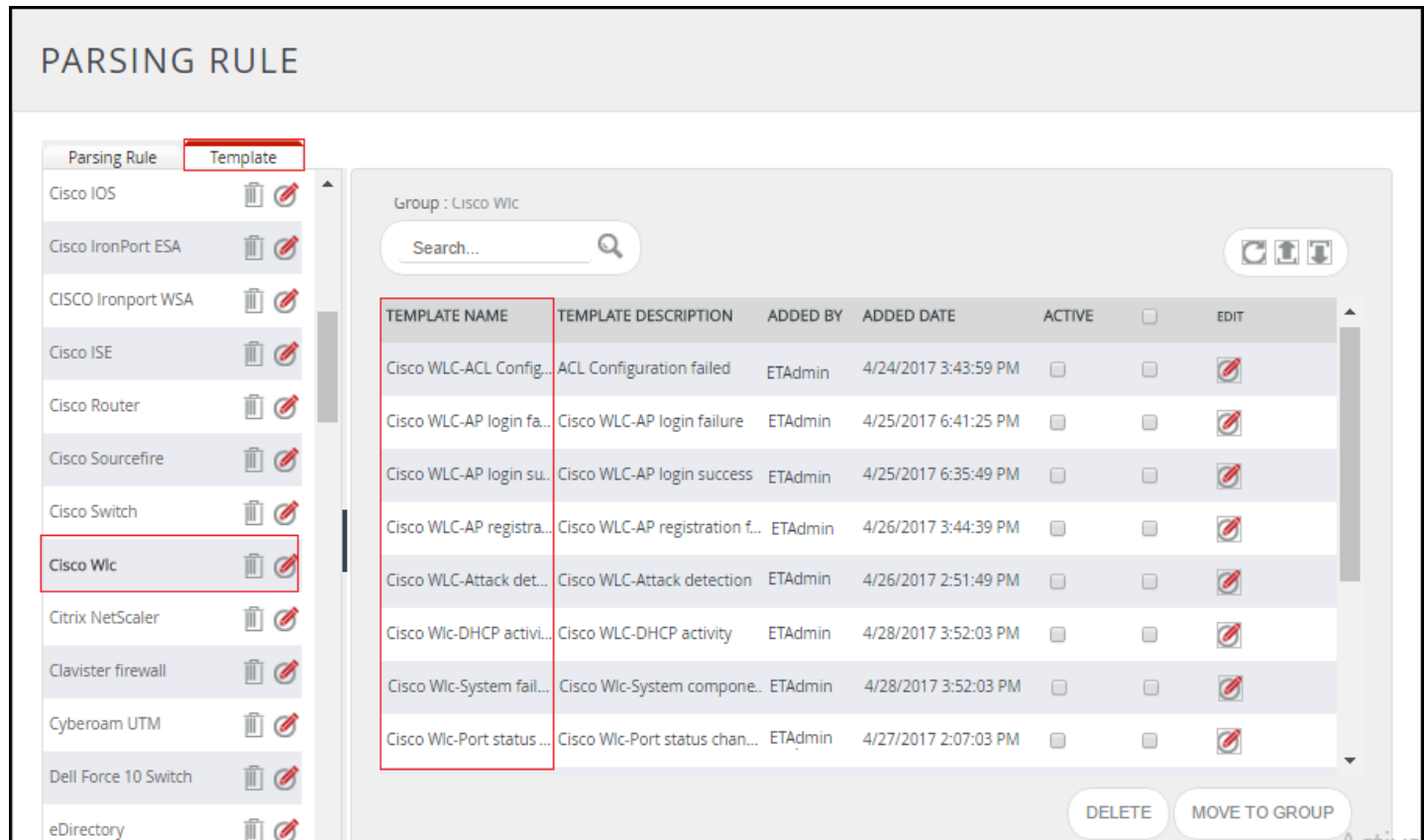


Figure 15

Flex Reports

1. In the **EventTracker Enterprise** web interface, click the **Reports** menu, and then select **Configuration**.
2. In **Reports Configuration** pane, select **Defined** option.
3. In search box enter '**Cisco Wlc**', and then click the **Search** button.

EventTracker displays Flex reports of '**Cisco Wlc**'

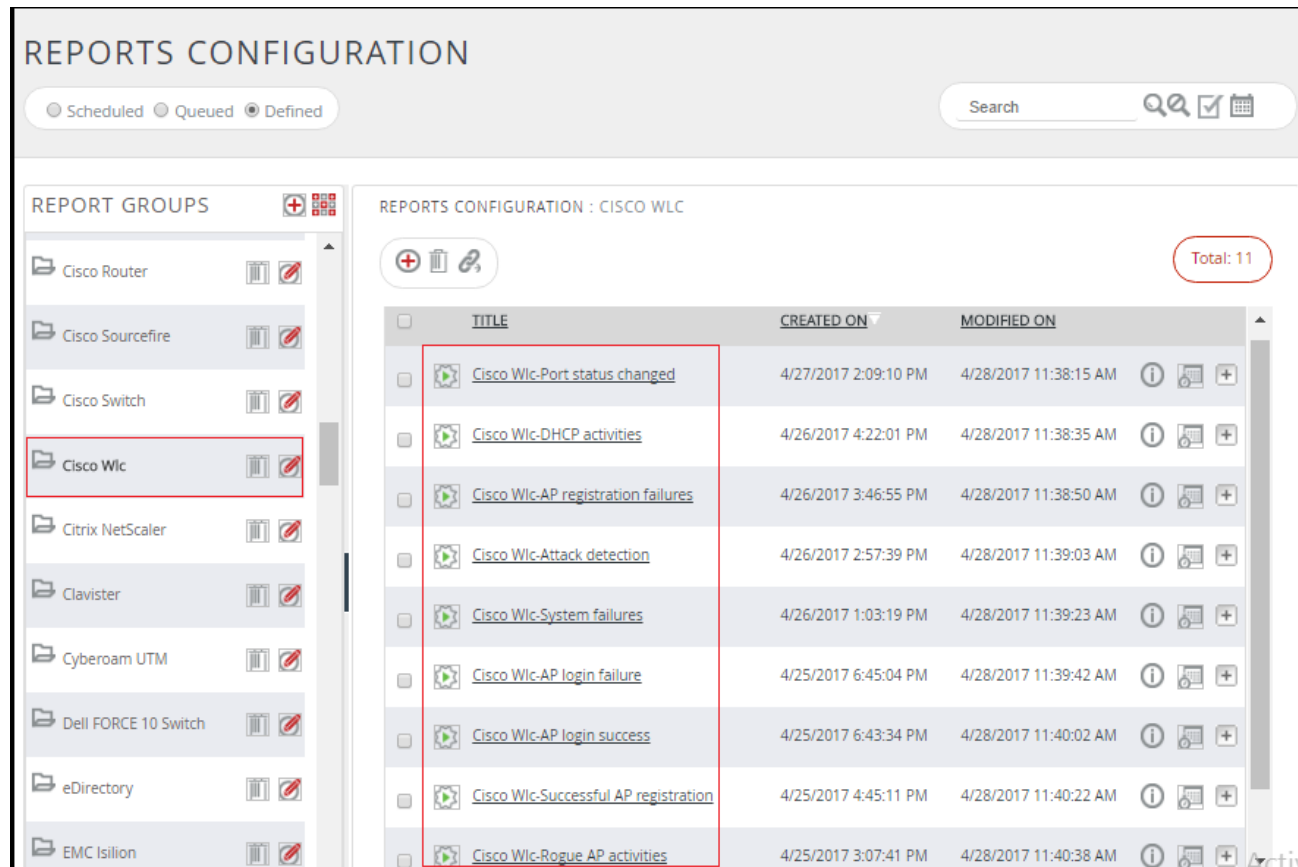


Figure 16

Create Flex Dashboards in EventTracker

NOTE: To configure the flex dashboards, schedule and generate the reports. Flex dashboard feature is available from EventTracker Enterprise v8.0.

Schedule Reports

1. Open **EventTracker** in browser and login.

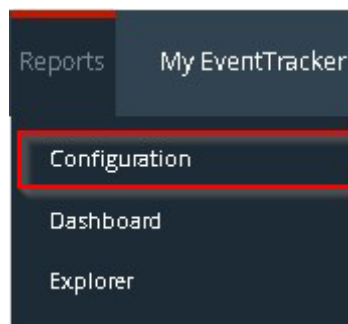


Figure 17

2. Navigate to **Reports>Configuration**.
3. Select **Cisco Wlc** in report groups. Check **Defined** dialog box.

REPORTS CONFIGURATION

Scheduled Queued **Defined**

Search

REPORT GROUPS

- Cisco Router
- Cisco Sourcefire
- Cisco Switch
- Cisco Wlc**
- Citrix NetScaler
- Clavister
- Cyberoam UTM
- Dell FORCE 10 Switch
- eDirectory
- EMC Isilon

REPORTS CONFIGURATION : CISCO WLC

Total: 11

TITLE	CREATED ON	MODIFIED ON
Cisco Wlc-Port status changed	4/27/2017 2:09:10 PM	4/28/2017 11:38:15 AM
Cisco Wlc-DHCP activities	4/26/2017 4:22:01 PM	4/28/2017 11:38:35 AM
Cisco Wlc-AP registration failures	4/26/2017 3:46:55 PM	4/28/2017 11:38:50 AM
Cisco Wlc-Attack detection	4/26/2017 2:57:39 PM	4/28/2017 11:39:03 AM
Cisco Wlc-System failures	4/26/2017 1:03:19 PM	4/28/2017 11:39:23 AM
Cisco Wlc-AP login failure	4/25/2017 6:45:04 PM	4/28/2017 11:39:42 AM
Cisco Wlc-AP login success	4/25/2017 6:43:34 PM	4/28/2017 11:40:02 AM
Cisco Wlc-Successful AP registration	4/25/2017 4:45:11 PM	4/28/2017 11:40:22 AM
Cisco Wlc-Rogue AP activities	4/25/2017 3:07:41 PM	4/28/2017 11:40:38 AM

Figure 18

4. Click on **'schedule'** to plan a report for later execution.
5. Click **Next** button to proceed.
6. In review page, check **Persist data in EventVault Explorer** option.

REPORT WIZARD

TITLE: CISCO WLC-PORT STATUS CHANGED

LOGS

Review cost details and configure the publishing options. Step 8 of 10

DISK COST ANALYSIS

Estimated time for completion: 00:00:38(HH:MM:SS)
 Number of cab(s) to be processed: 4
 Available disk space: 174 GB
 Required disk space: 50 MB

☐ Enable publishing option (Configure SMTP Server in manager configuration screen to use this option)
☒ Deliver results via E-mail
☐ Notify results via E-mail

To E-mail: [Use comma(,) to separate multiple e-mail recipients]

Update status via RSS:

Show in:

☒ Persist data in Eventvault Explorer

Figure 19

7. In next page, check column names to persist using **PERSIST** checkboxes beside them. Choose suitable **Retention period**.

REPORT WIZARD

TITLE: CISCO WLC-PORT STATUS CHANGED

DATA PERSIST DETAIL

Select columns to persist Step 9 of 10

RETENTION SETTING

Retention period: days ⓘ

☐ Persist in database only [Reports will not be published and will only be stored in the respective database]

SELECT COLUMNS TO PERSIST

COLUMN NAME	PERSIST
Computer	<input checked="" type="checkbox"/>
Status	<input checked="" type="checkbox"/>
Severity	<input checked="" type="checkbox"/>
Port number	<input checked="" type="checkbox"/>
Message	<input checked="" type="checkbox"/>
Event Description	<input checked="" type="checkbox"/>

Figure 20

8. Proceed to next step and click **Schedule** button.
9. Wait till the reports get generated.

Create Dashlets

1. Open **EventTracker Enterprise** in browser and logon.

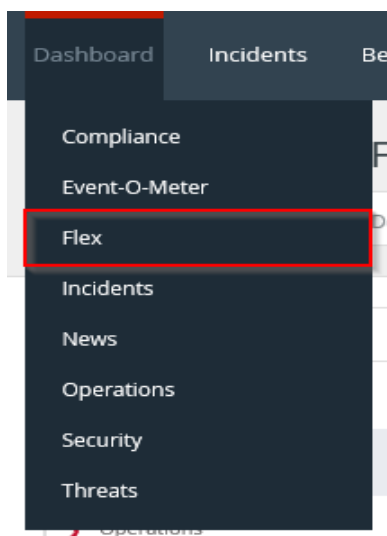


Figure 21

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

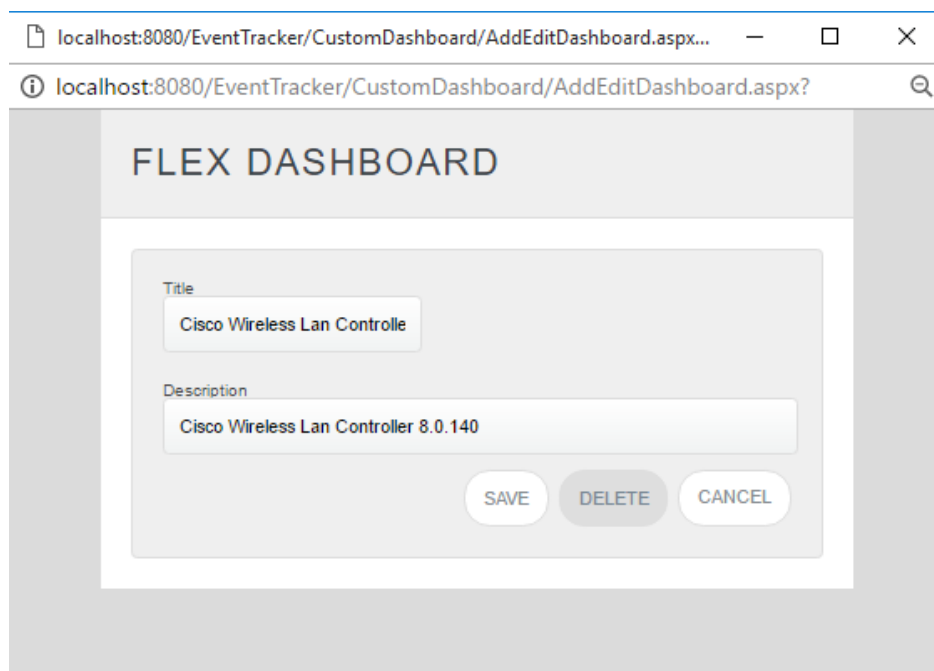

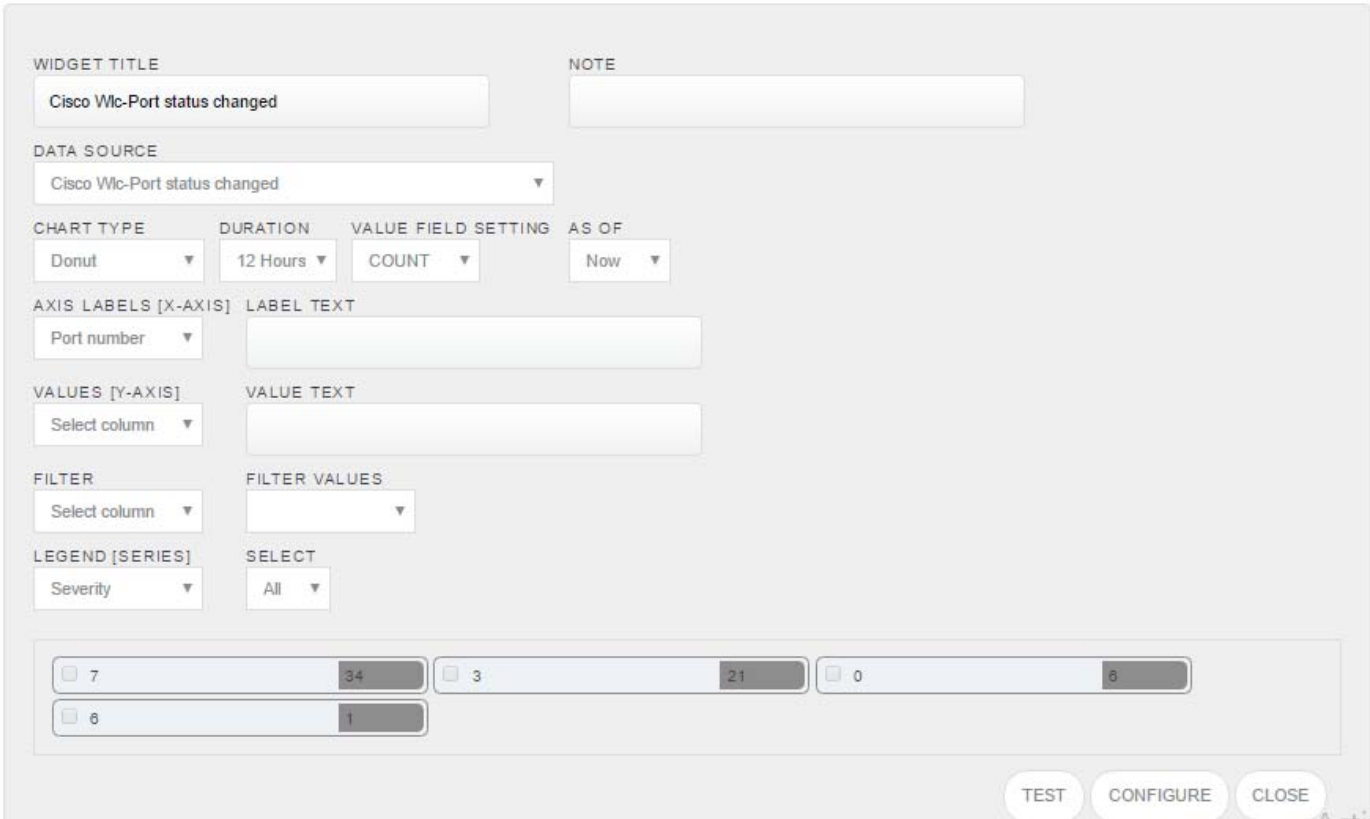


Figure 22

3. Fill suitable title and description and click **Save** button.
4. Click  to configure a new flex dashlet. Widget configuration pane is shown.

WIDGET CONFIGURATION



WIDGET TITLE: Cisco Wlc-Port status changed

NOTE:

DATA SOURCE: Cisco Wlc-Port status changed

CHART TYPE: Donut

DURATION: 12 Hours

VALUE FIELD SETTING: COUNT

AS OF: Now

AXIS LABELS [X-AXIS]: Port number

VALUES [Y-AXIS]: Select column

FILTER: Select column

LEGEND [SERIES]: Severity

SELECT: All

Preview: 7 (34), 3 (21), 0 (6)

TEST CONFIGURE CLOSE

Figure 23

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



Figure 24

14. If satisfied, click **Configure** button.

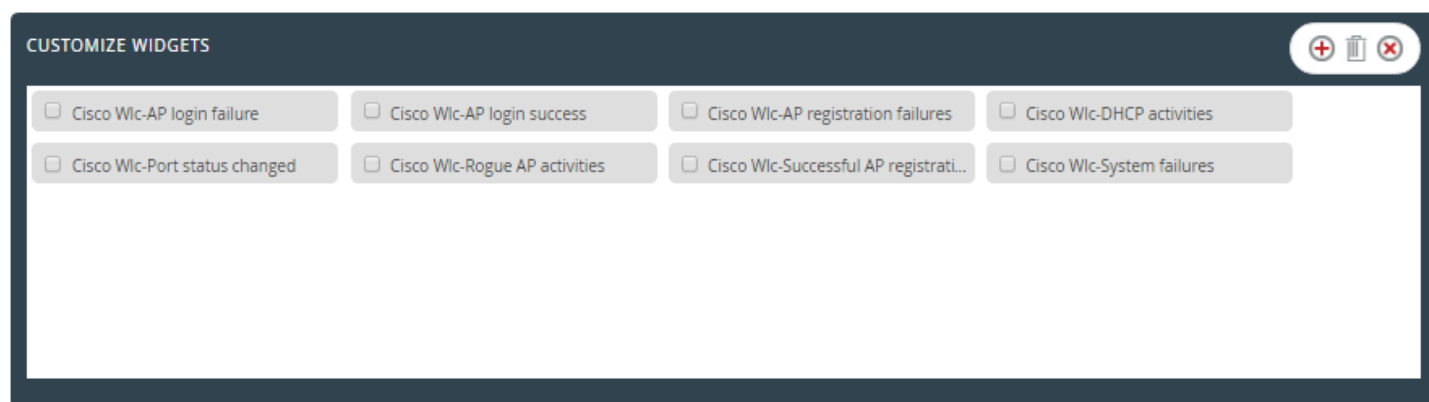



Figure 25

15. Click 'customize'  to locate and choose created dashlet.

16. Click  to add dashlet to earlier created dashboard.

Sample Flex Dashboards

- REPORT: Cisco Wlc-Ap login failure**
WIDGET TITLE: Cisco Wlc- AP login failure
CHART TYPE: Donut
AXIS LABELS [X-AXIS]: AP name
LEGEND [SERIES]: Severity

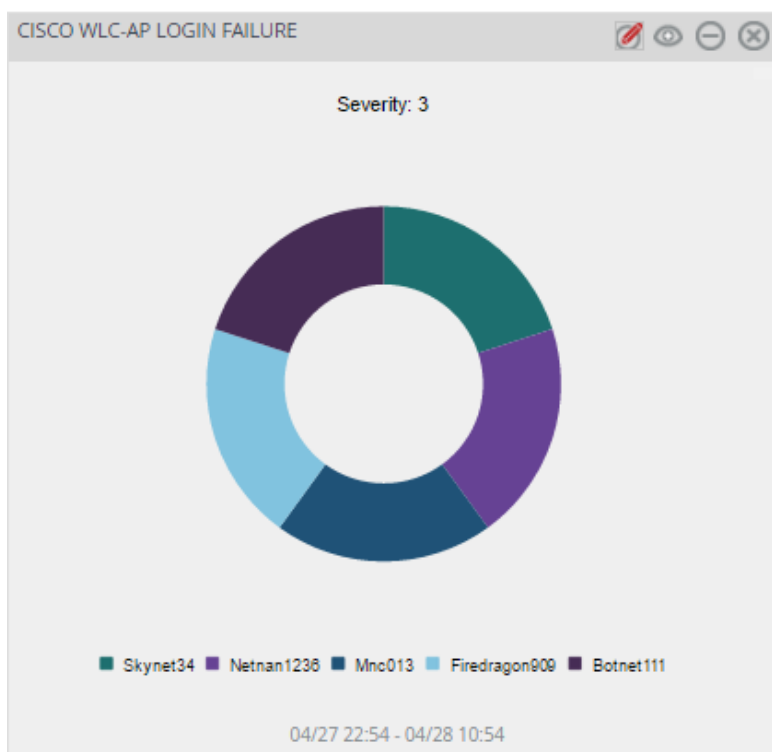


Figure 26

- **REPORT:** Cisco Wlc-AP login success
WIDGET TITLE: Cisco Wlc-AP login success
CHART TYPE: Donut
AXIS LABELS [X-AXIS]: AP name
LEGEND[SERIES]: Severity

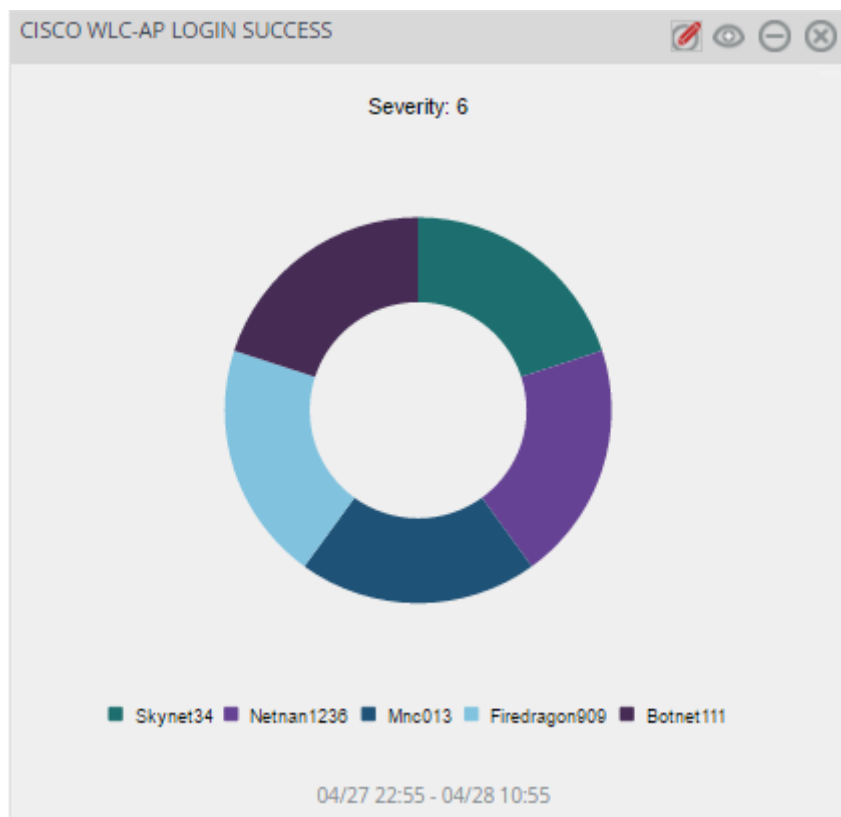


Figure 27

- **REPORT: Cisco Wlc-AP registration failures**
WIDGET TITLE: Cisco Wlc-AP registration failures
CHART TYPE: Stacked Column
AXIS LABELS [X-AXIS]: AP Mac Address
LEGEND[SERIES]: Severity

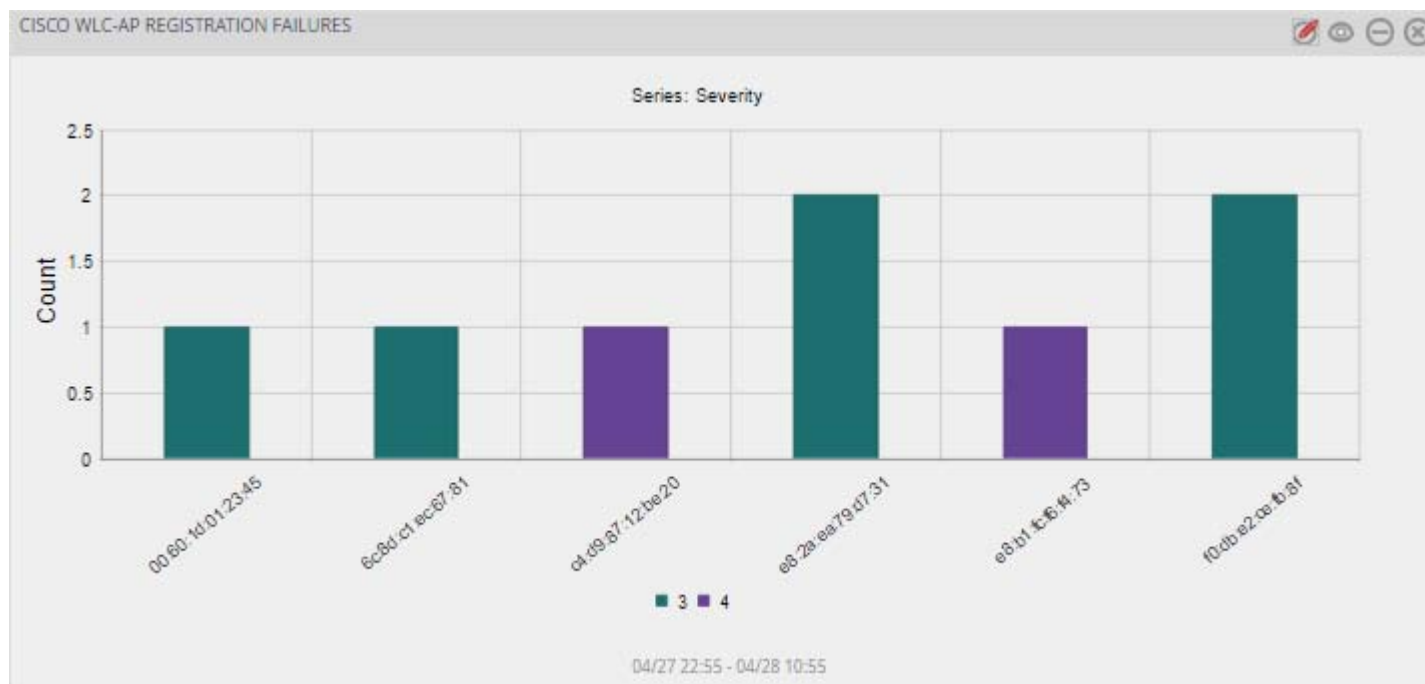


Figure 28

- **REPORT: Cisco Wlc-Rogue AP activities**
WIDGET TITLE: Cisco Wlc- Rogue AP activities
CHART TYPE: Stacked Column
AXIS LABELS [X-AXIS]: AP Mac Address
LEGEND[SERIES]: Severity

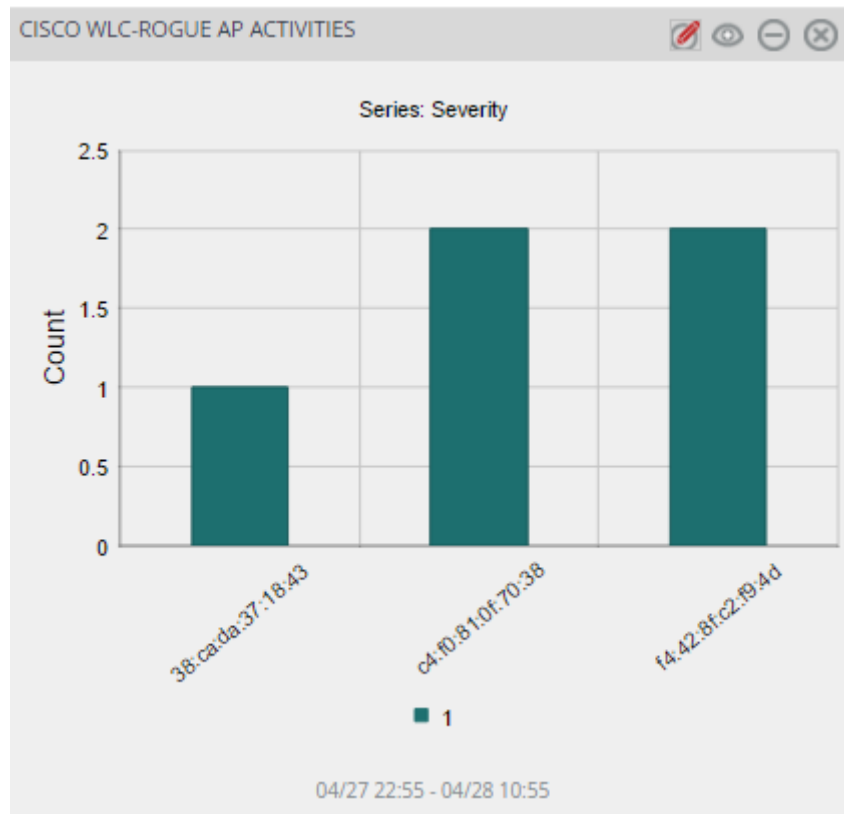


Figure 29

- **REPORT: Cisco Wlc-Successful AP registration**
WIDGET TITLE: Cisco Wlc- Successful AP registration
CHART TYPE: Stacked Column
AXIS LABELS [X-AXIS]: AP Mac address

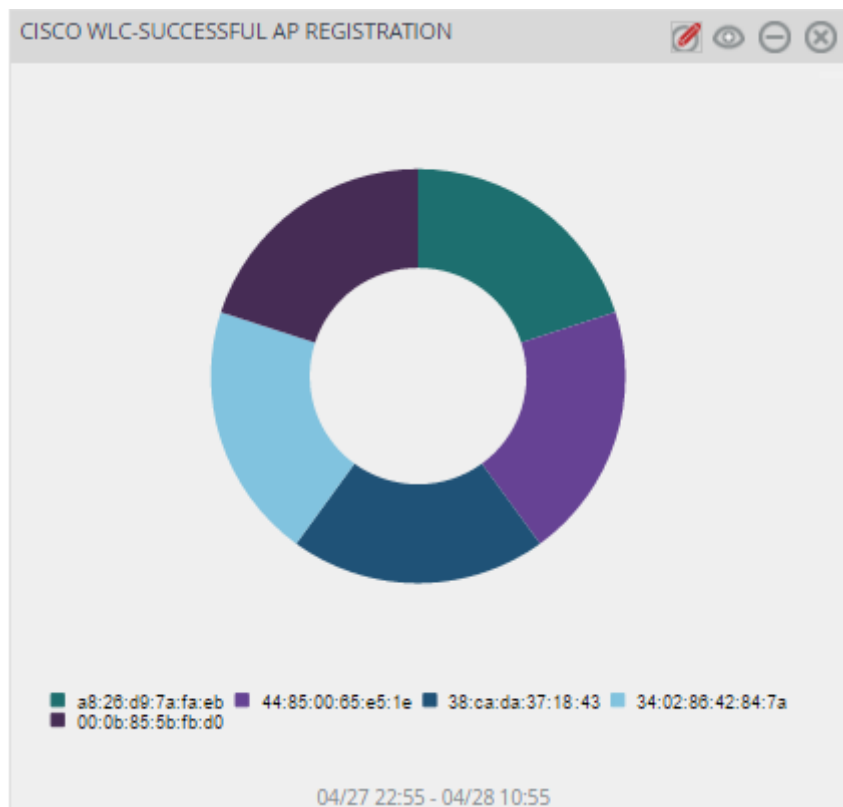


Figure 30

- **REPORT: Cisco Wlc-System failures**
WIDGET TITLE: Cisco Wlc- System failures
CHART TYPE: Donut
AXIS LABELS [X-AXIS]: Severity

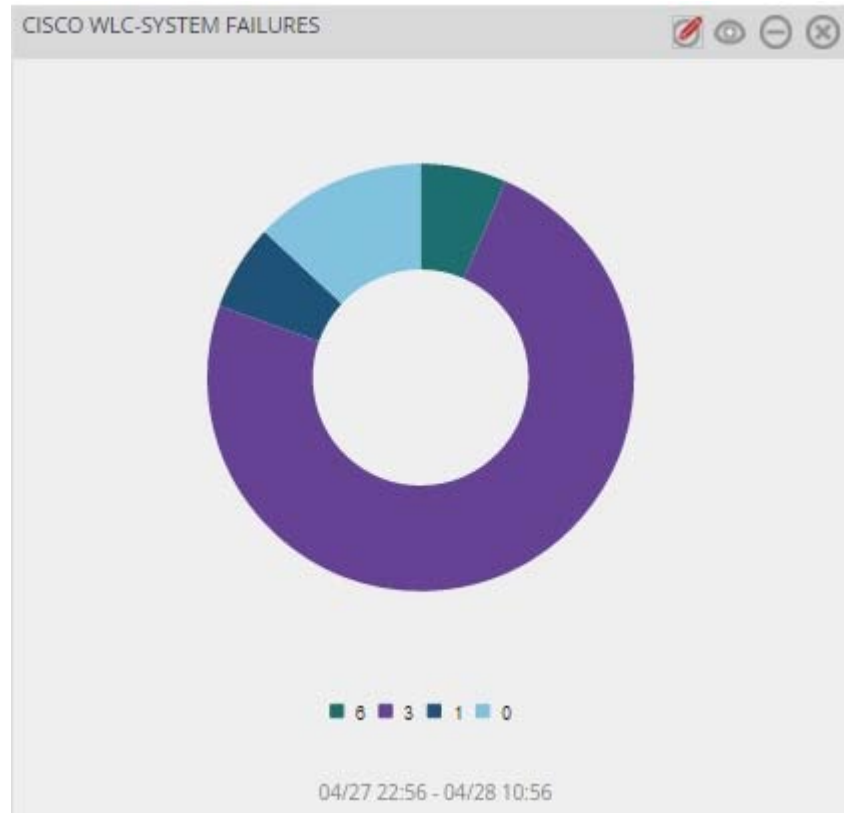


Figure 31

- **REPORT: Cisco Wlc-DHCP activities**
WIDGET TITLE: Cisco Wlc- DHCP activities
CHART TYPE: Stacked Column
AXIS LABELS [X-AXIS]: Client Mac address
LEGEND[SERIES]: DHCP activity

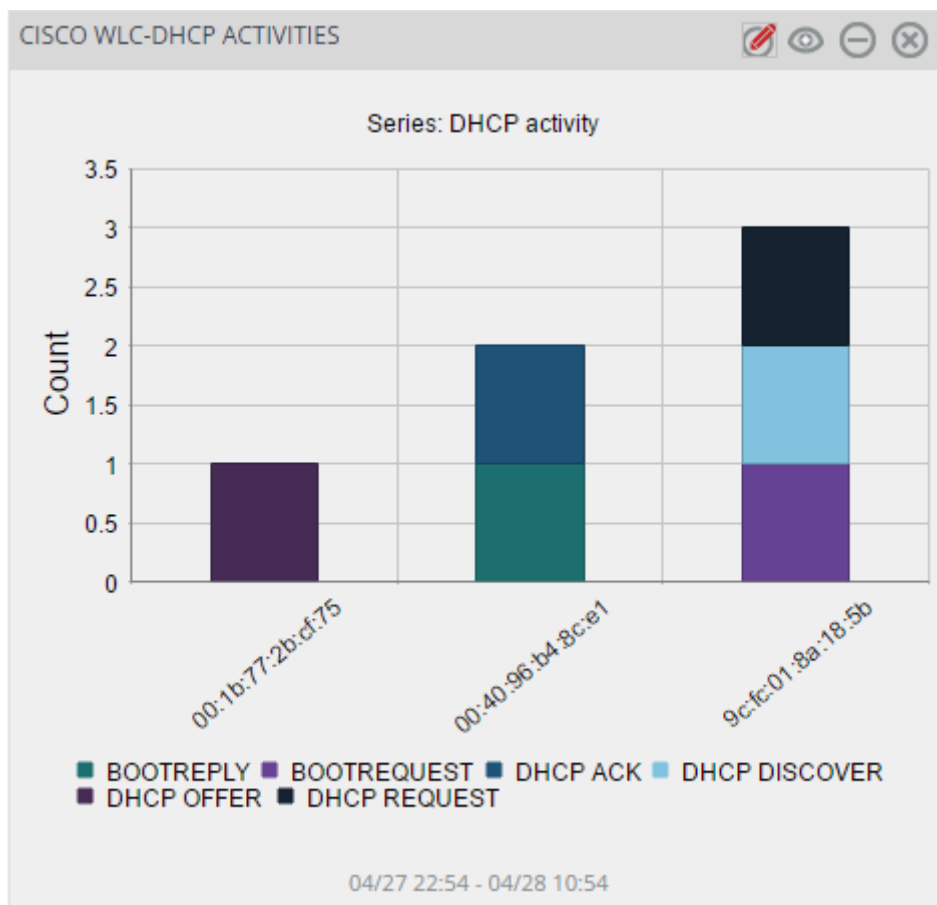


Figure 32