EventTracker

Actionable Security Intelligence

Integrate Cisco IWAN

EventTracker v8.x and above

Publication Date: June 26, 2018

Abstract

This guide provides instructions to configure Cisco IWAN to generate logs for critical events. Once EventTracker is configured to collect and parse these logs, dashboard and reports can be configured to monitor Cisco IWAN.

Scope

The configurations detailed in this guide are consistent with EventTracker Enterprise version v8.x or above and Cisco IWAN.

Audience

Administrators who are assigned the task to monitor and manage Cisco IWAN events using EventTracker.

Table of Contents

Introduction

Cisco's IWAN is the solution that gives IT the visibility and control over the network. With Cisco Integrated Services Router (ISR) together with the ISR-AX license bundle, you can run services like Application Visibility and Control (AVC) that gives you visibility to see your network traffic from a Layer 7 point of view and see the actual application name and the protocol that it is using.

With EventTracker, you can monitor Cisco IWAN events from a single view. EventTracker can generate flex reports; trigger alerts for web access, interface status changes, user authentication failure and SSL VPN authentication.

Prerequisites

- EventTracker Agent should be installed.
- Cisco IWAN should be configured to forward logs.
- Please add exception for port 514 in Windows firewall of EventTracker Manager workstation.

Configure Cisco IWAN to forward logs to EventTracker

To configure the Cisco IWAN to forward logs to a syslog server,

1. After logging to the global settings in the CLI Credentials dialog box, from the left navigation pane, click **IWAN**.
2. After opening the **Home** page, click **Configure Hub Site & Settings**.

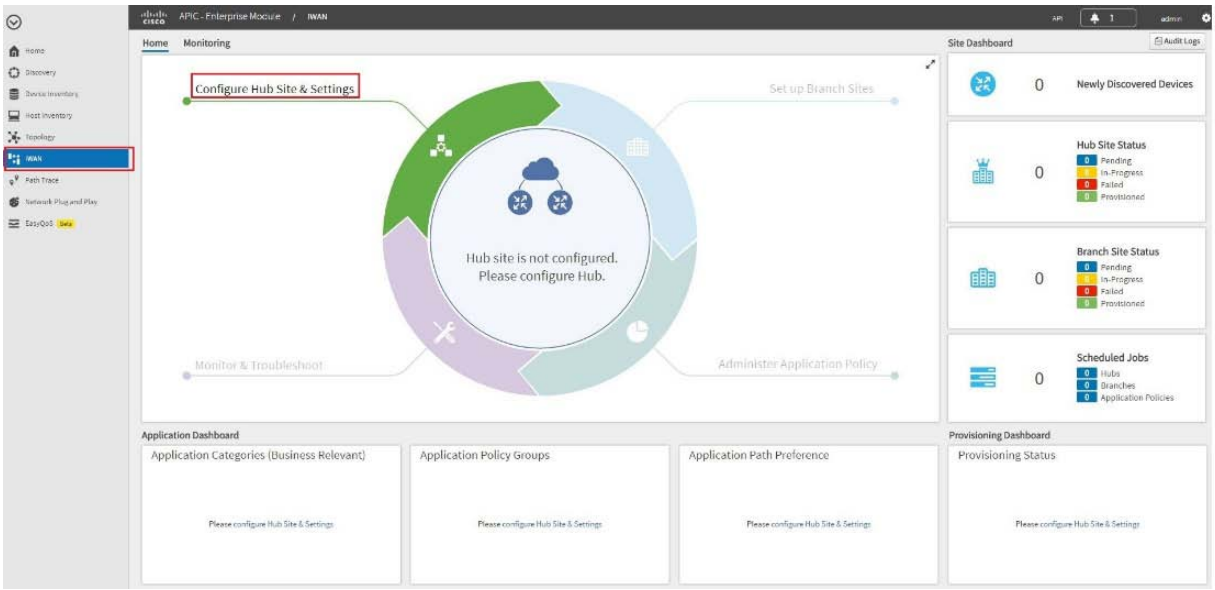

Figure 1

3. The **Settings** tab opens by default and in the **System Settings** page, click the **Show more** button to revel **Syslog server** settings.

System settings page is shown below:

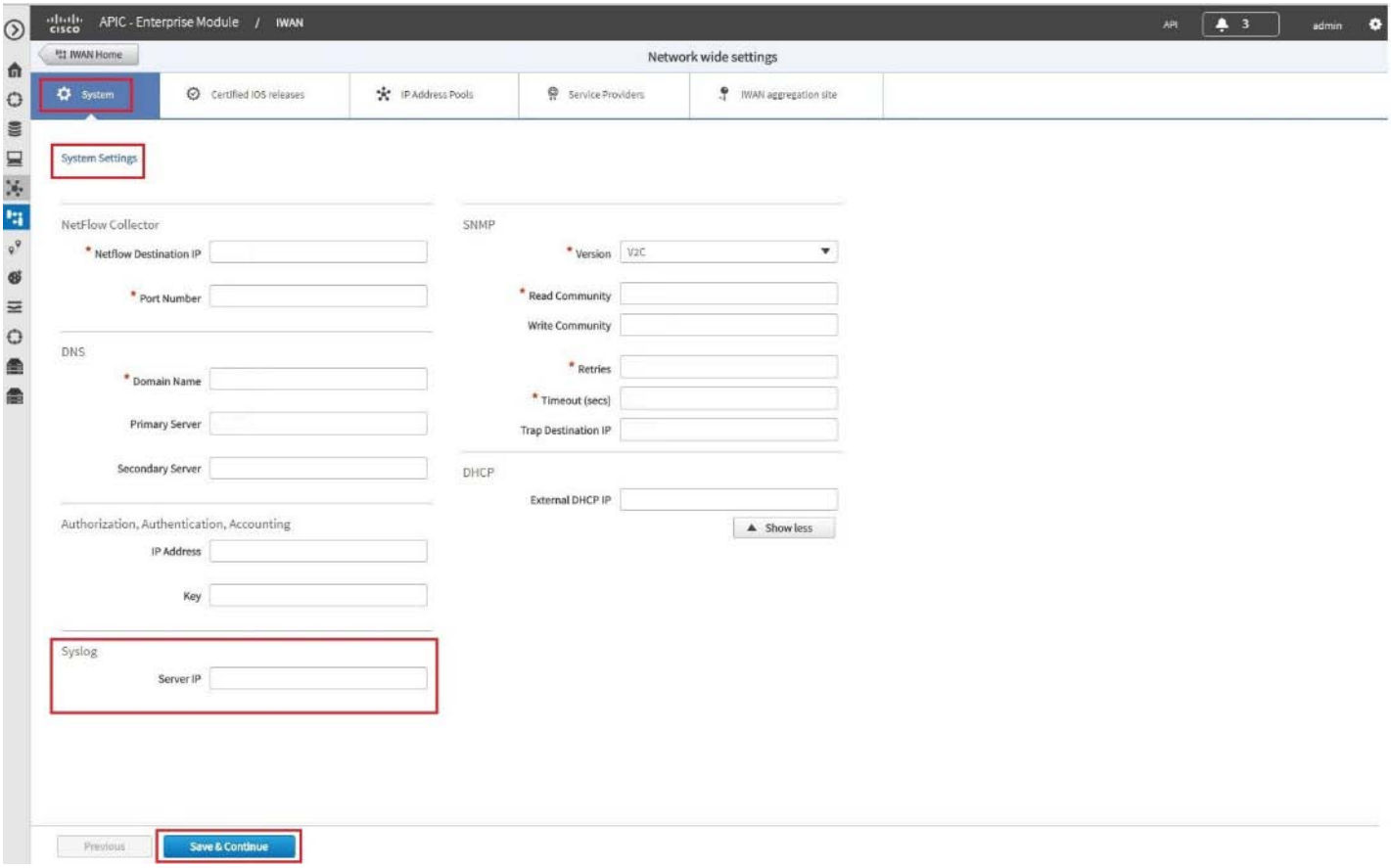

Figure 2

4. Under **Syslog** section**,** type the IP address of **EventTracker Manager IP Address** in **Server IP** box.
5. Click **Save & Continue**.

EventTracker Knowledge Pack

Once logs are received by EventTracker manager, Knowledge Packs can be configured into EventTracker.

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

Flex Reports

- **Cisco IWAN- Website Access Allowed or Denied -** This report provides information about accessed URLs allowed or blocked by Cisco IWAN.

LogTime	Computer	Source IP Address	Source Port	Destination IP Address	Destination Port	URL Name	Action
06/15/2018 10:34:13 AM	CISCO IWAN	12.54.192.6	54678	64.192.14.2	80	http://www.google.com	Access allowed
06/15/2018 10:34:13 AM	CISCO IWAN	10.54.192.6	34557	172.24.50.12	80	www.sports.com	Access allowed
06/15/2018 10:34:13 AM	CISCO IWAN	12.54.192.6	54678	64.192.14.2	80	http://www.fun8.com	Access denied
06/15/2018 10:34:13 AM	CISCO IWAN	10.54.192.6	34557	172.24.50.12	80	www.sportsspecial.com	Access denied

Figure 3

Sample logs:

Time	Description
Jun 15 10:49:11 AM	Jun 08 05:59:31 JMTN_iWAN_VPLS01 143836: 140714: *Jun 8 10:16:24.004 UTC: %URLF-4-SITE-BLOCKED: Access denied for the site ''www.sportsspecial.c...
event_log_type	+ - Application
event_type	+ - Information
event_id	+ - 3333
event_source	+ - Syslog
event_user_domain	+ - N/A
event_computer	+ - Cisco IWAN
event_user_name	+ - N/A
event_description	Jun 08 05:59:31 JMTN_iWAN_VPLS01 143836: 140714: *Jun 8 10:16:24.004 UTC: %URLF-4-SITE-BLOCKED: Access denied for the site ''www.sportsspecial.com'', client 10.54.192.6:34557 server 172.24.50.12:80

Figure 4

- **Cisco IWAN- User Login and Logout Activity -** This report provides information about successful user login and logout.

LogTime	Computer	User Name	Source IP Address	Source Port	Activity
06/15/2018 10:34:13 AM	CISCO IWAN	Support	52.23.136.220	22	LOGIN
06/15/2018 10:34:13 AM	CISCO IWAN	admin	192.168.2.183		LOGOUT
06/15/2018 10:34:18 AM	CISCO IWAN	Support	52.23.136.220	22	LOGIN
06/15/2018 10:34:18 AM	CISCO IWAN	admin	192.168.2.183		LOGOUT
06/15/2018 10:49:03 AM	CISCO IWAN	Support	52.23.136.220	22	LOGIN

Figure 5

Sample logs:

Time	Description
Jun 15 10:49:11 AM	Jun 08 05:59:31 JMTN_iWAN_VPLS01 143836: 140714: *Aug 23 10:00:16.426: %SYS-6-LOGOUT: User admin has exited tty session 388(192.168.2.183)

event_log_type	Application
event_type	Information
event_id	3333
event_source	Syslog
event_user_domain	N/A
event_computer	Cisco IWAN
event_user_name	N/A
event_description	Jun 08 05:59:31 JMTN_iWAN_VPLS01 143836: 140714: *Aug 23 10:00:16.426: %SYS-6-LOGOUT: User admin has exited tty session 388(192.168.2.183)

Figure 6

- **Cisco IWAN- User Login Failure -** This report provides information about user login failures.

LogTime	Computer	User Name	Source IP Address	Source Port	Reason
06/15/2018 10:34:13 AM	CISCO IWAN	Support	52.23.136.220	22	Login Authentication Failed
06/15/2018 10:34:18 AM	CISCO IWAN	Support	52.23.136.225	22	Login Authentication Failed

Figure 7

Sample logs:

Time	Description
Jun 15 10:49:11 AM	Jun 08 05:59:31 JMTN_iWAN_VPLS01 143836: 140714: *Jun 8 10:16:24.004 UTC: %SEC_LOGIN-4-LOGIN_FAILED: Login Failed [user: Support] [Source: 52.23....

event_log_type	Application
event_type	Information
event_id	3333
event_source	Syslog
event_user_domain	N/A
event_computer	Cisco IWAN
event_user_name	N/A
event_description	Jun 08 05:59:31 JMTN_iWAN_VPLS01 143836: 140714: *Jun 8 10:16:24.004 UTC: %SEC_LOGIN-4-LOGIN_FAILED: Login Failed [user: Support] [Source: 52.23. 136.220] [localport: 22] [Reason: Login Authentication Failed] at 06:16:24 EDT Fri Jun 8 2018

Figure 8

- **Cisco IWAN- VPN User Login and Logout Activity -** This report provides information about successful VPN user login and logout.

LogTime	Computer	User Name	Remote IP Address	Gateway	Status
06/15/2018 10:34:13 AM	CISCO IWAN	testing2	110.23.32.55	gateway_1	Authentication successful, user logged in
06/15/2018 10:34:14 AM	CISCO IWAN	product1		gateway_2	logged out
06/15/2018 10:34:18 AM	CISCO IWAN	testing	110.23.32.69	gateway_1	Authentication successful, user logged in

Figure 9

Sample logs:

Time	Description
Jun 15 10:49:12 AM	Jun 08 05:59:31 JMTN_iWAN_VPLS01 143836: 140714: *Jun 8 10:16:24.004 UTC: %SSLVPN-6-WEBVPN_TUNNEL_USER_LOGOUT: User: product1 has logged...
event_log_type	+ - Application
event_type	+ - Information
event_id	+ - 3333
event_source	+ - Syslog
event_user_domain	+ - N/A
event_computer	+ - Cisco IWAN
event_user_name	+ - N/A
event_description	Jun 08 05:59:31 JMTN_iWAN_VPLS01 143836: 140714: *Jun 8 10:16:24.004 UTC: %SSLVPN-6-WEBVPN_TUNNEL_USER_LOGOUT: User: product1 has logged out from gateway gateway_2

Figure 10

- **Cisco IWAN- VPN User Authentication Failure -** This report provides information about VPN user authentication failures.

LogTime	Computer	User Name	Remote IP Address	Gateway	Status
06/15/2018 10:34:13 AM	CISCO IWAN	testing2	110.23.32.55	gateway_1	Failed to contact authentication server
06/15/2018 10:34:13 AM	CISCO IWAN	testing3	110.23.32.56	gateway_1	Failed to authenticate user credentials
06/15/2018 10:34:18 AM	CISCO IWAN	testing	110.23.32.65	gateway_1	Failed to contact authentication server

Figure 11

Sample logs:

Time	Description
Jun 15 10:49:11 AM	Jun 08 05:59:31 JMTN_iWAN_VPLS01 143836: 140714: *Jun 8 10:16:24.004 UTC: %SSLVPN-5-LOGIN_AUTH_FAILED: vw_ctx: sslvpn vw_gw: gateway_1 remo...
event_log_type	+ - Application
event_type	+ - Information
event_id	+ - 3333
event_source	+ - Syslog
event_user_domain	+ - N/A
event_computer	+ - Cisco IWAN
event_user_name	+ - N/A
event_description	Jun 08 05:59:31 JMTN_iWAN_VPLS01 143836: 140714: *Jun 8 10:16:24.004 UTC: %SSLVPN-5-LOGIN_AUTH_FAILED: vw_ctx: sslvpn vw_gw: gateway_1 remote_ip: 110.23.32.55 user_name: testing2, Failed to contact authentication server

Figure 12

- **Cisco IWAN- SSH Authentication Failure -** This report provides information about SSH authentication failures.

LogTime	Computer	User Name	Status	TTY Mode
06/15/2018 10:34:13 AM	CISCO IWAN	ncmservice	Failed	1
06/15/2018 10:34:19 AM	CISCO IWAN	ncmsupport	Failed	1

Figure 13

Sample logs:

Time	Description
Jun 15 10:49:11 AM	Jun 08 05:59:31 JMTN_iWAN_VPLS01 143836: 140714: *Jun 8 10:16:24.004 UTC: %SSH-5-SSH_USERAUTH: User ''ncmservice'' authentication for SSH Sessi...
event_log_type	Application
event_type	Information
event_id	3333
event_source	Syslog
event_user_domain	N/A
event_computer	Cisco IWAN
event_user_name	N/A
event_description	Jun 08 05:59:31 JMTN_iWAN_VPLS01 143836: 140714: *Jun 8 10:16:24.004 UTC: %SSH-5-SSH_USERAUTH: User ''ncmservice'' authentication for SSH Sessio n from (tty = 1) using crypto cipher ''3des-cbc'' Failed

Figure 14

- **Cisco IWAN- SSH Authentication Success -** This report provides information about successful SSH authentication and session open/close.

LogTime	Computer	User Name	Source IP Address	Status	TTY Mode
06/15/2018 10:34:13 AM	CISCO IWAN	ncmsupport		Succeeded	1
06/15/2018 10:34:13 AM	CISCO IWAN	ncmservice	70.23.56.123	closed	3
06/15/2018 10:34:13 AM	CISCO IWAN	ncmservice1	11.23.56.33	closed	0

Figure 15

Sample logs:

Time	Description
Jun 15 10:49:11 AM	Jun 08 05:59:31 JMTN_iWAN_VPLS01 143836: 140714: *Jun 8 10:16:24.004 UTC: %SSH-5-SSH_CLOSE: SSH Session from 70.23.56.123 (tty = 3) for user ''nc...
event_log_type	Application
event_type	Information
event_id	3333
event_source	Syslog
event_user_domain	N/A
event_computer	Cisco IWAN
event_user_name	N/A
event_description	Jun 08 05:59:31 JMTN_iWAN_VPLS01 143836: 140714: *Jun 8 10:16:24.004 UTC: %SSH-5-SSH_CLOSE: SSH Session from 70.23.56.123 (tty = 3) for user ''ncm service'' using crypto cipher ''aes256-cbc'' closed

Figure 16

- **Cisco IWAN- Interface Status -** This report provides information about interface status changes.

LogTime	Computer	Interface Name	Interface Status
06/15/2018 10:34:13 AM	CISCO IWAN	Tunnel100	DOWN
06/15/2018 10:34:19 AM	CISCO IWAN	Tunnel105	UP

Figure 17

Sample logs:

Time	Description
− Jun 15 10:49:11 AM	Jun 08 05:59:31 JMTN_iWAN_VPLS01 143836: 140714: *Jun 8 10:16:24.004 UTC: %SAMI-5-SAMI_SUBINTERFACE_STATE_UP: Interface [Tunnel100] state cha...
event_log_type	+- Application
event_type	+- Information
event_id	+- 3333
event_source	+- Syslog
event_user_domain	+- N/A
event_computer	+- Cisco IWAN
event_user_name	+- N/A
event_description	Jun 08 05:59:31 JMTN_iWAN_VPLS01 143836: 140714: *Jun 8 10:16:24.004 UTC: %SAMI-5-SAMI_SUBINTERFACE_STATE_UP: Interface [Tunnel100] state changed to UP, based on svclc configuration on the supervisor.

Figure 18

- **Cisco IWAN- User Authentication Success -** This report provides information about successful user authentication.

LogTime	Computer	Source MAC Address	Source Interface
06/15/2018 10:34:14 AM	CISCO IWAN	000c.2986.1153	Fa2/0/7
06/15/2018 10:34:14 AM	CISCO IWAN	901a.4568.bb74	Fa0/1/1
06/15/2018 10:34:14 AM	CISCO IWAN	020c.2986.1253	Fa2/0/5
06/15/2018 10:34:19 AM	CISCO IWAN	550c.2986.1153	Fa2/0/1

Figure 19

Sample logs:

Time	Description
Jun 15 10:49:12 AM	Jun 08 05:59:31 JMTN_iWAN_VPLS01 143836: 140714: *Jun 8 10:16:24.004 UTC: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (001a.4dd8.b...

event_log_type	+- Application
event_type	+- Information
event_id	+- 3333
event_source	+- Syslog
event_user_domain	+- N/A
event_computer	+- Cisco IWAN
event_user_name	+- N/A
event_description	Jun 08 05:59:31 JMTN_iWAN_VPLS01 143836: 140714: *Jun 8 10:16:24.004 UTC: %AUTHMGR-5-SUCCESS: Authorization succeeded for client (001a.4dd8.bb74) on Interface Fa0/17 AuditSessionID 2245

Figure 20

- **Cisco IWAN- User Authentication Failure -** This report provides information about user authentication failures.

LogTime	Computer	Source MAC Address	Source Interface
06/15/2018 10:34:13 AM	CISCO IWAN	000c.2986.1123	Fa2/0/7
06/15/2018 10:34:13 AM	CISCO IWAN	520c.2986.1153	Fa2/0/7
06/15/2018 10:34:13 AM	CISCO IWAN	881a.4dd8.bb74	Fa0/17
06/15/2018 10:34:19 AM	CISCO IWAN	000c.2556.1153	Fa2/0/7

Figure 21

Sample logs:

Time	Description
Jun 15 10:49:12 AM	Jun 08 05:59:31 JMTN_iWAN_VPLS01 143836: 140714: *Jun 8 10:16:24.004 UTC: %AUTHMGR-5-FAIL: Authorization failed for client (001a.4dd8.bb74) on In...

event_log_type	+- Application
event_type	+- Information
event_id	+- 3333
event_source	+- Syslog
event_user_domain	+- N/A
event_computer	+- Cisco IWAN
event_user_name	+- N/A
event_description	Jun 08 05:59:31 JMTN_iWAN_VPLS01 143836: 140714: *Jun 8 10:16:24.004 UTC: %AUTHMGR-5-FAIL: Authorization failed for client (001a.4dd8.bb74) on Interface Fa0/17 AuditSessionID 2245

Figure 22

Alerts

- **Cisco IWAN: Chassis Alarm -** This alert will be generated when a chassis alarm is triggered.

- **Cisco IWAN: Hardware Device Failed -** This alert will be generated when a hardware failure occurs.
- **Cisco IWAN: Internal Software Error -** This alert will be generated when a software error occurs.
- **Cisco IWAN: SSH Authentication Failed -** This alert will be generated when an authentication failure happens through SSH.
- **Cisco IWAN: User Authentication Failed -** This alert will be generated when a user authentication fails.
- **Cisco IWAN: VPN User Authentication Failed-** This alert will be generated when a VPN user authentication fails.

Categories and Saved Searches

- **Cisco IWAN Website access allowed or denied -** This category provides information related to websites allowed or blocked.
- **Cisco IWAN Interface status -** This category provides information related to interface status changes.
- **Cisco IWAN Login and Logout activity -** This category provides information related to user login and logout.
- **Cisco IWAN Login failure-** This category provides information related to user login failure.
- **Cisco IWAN SSH Connection details -** This category provides information related to allowed or denied SSH connections.
- **Cisco IWAN SSL VPN authentication -** This category provides information related to SSL VPN authentication.
- **Cisco IWAN User authentication failure -** This category provides information related to user authentication failures.
- **Cisco IWAN User authentication success -** This category provides information related to user authentication success.

Knowledge Objects

- **Cisco IWAN Website access allowed or denied -** This knowledge object helps to analyze logs related to website allowed or blocked.
- **Cisco IWAN Interface status -** This knowledge object helps to analyze logs related to interface status change.
- **Cisco IWAN Login and Logout activity -** This knowledge object helps to analyze logs related to user login and logout activity.
- **Cisco IWAN Login failure-** This knowledge object helps to analyze logs related to user login failure.
- **Cisco IWAN SSH Connection details -** This knowledge object helps to analyze logs related to allowed or denied SSH connections.

- **Cisco IWAN SSL VPN authentication -** This knowledge object helps to analyze logs related to SSL VPN authentication.
- **Cisco IWAN User authentication failure -** This knowledge object helps to analyze logs related to user authentication failures.
- **Cisco IWAN User authentication success -** This knowledge object helps to analyze logs related to user authentication success.

Import Cisco IWAN knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token Templates
- Knowledge Objects
- Flex Reports
- Dashboards

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

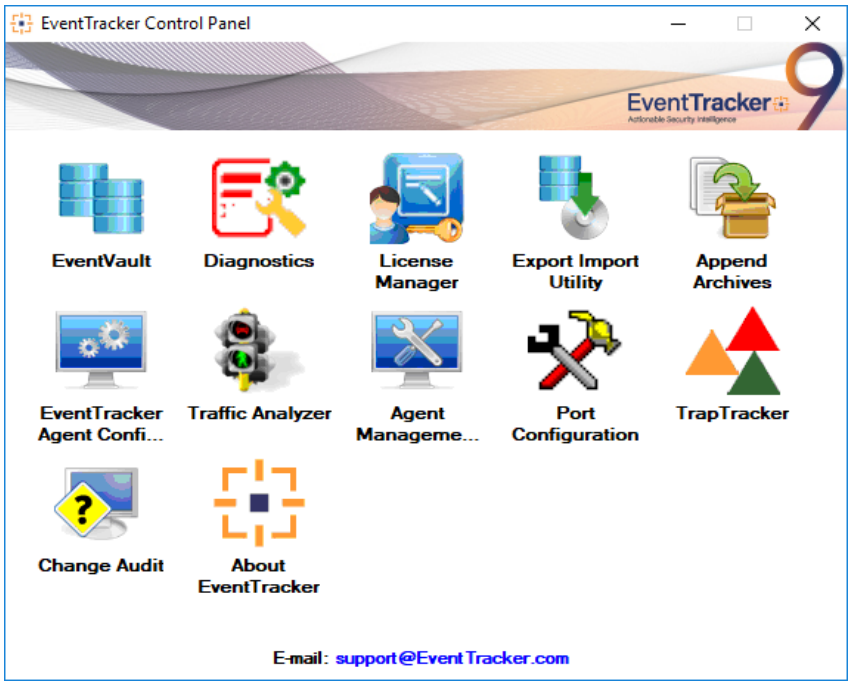

Figure 23

3. Click the **Import** tab**.**

Category

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

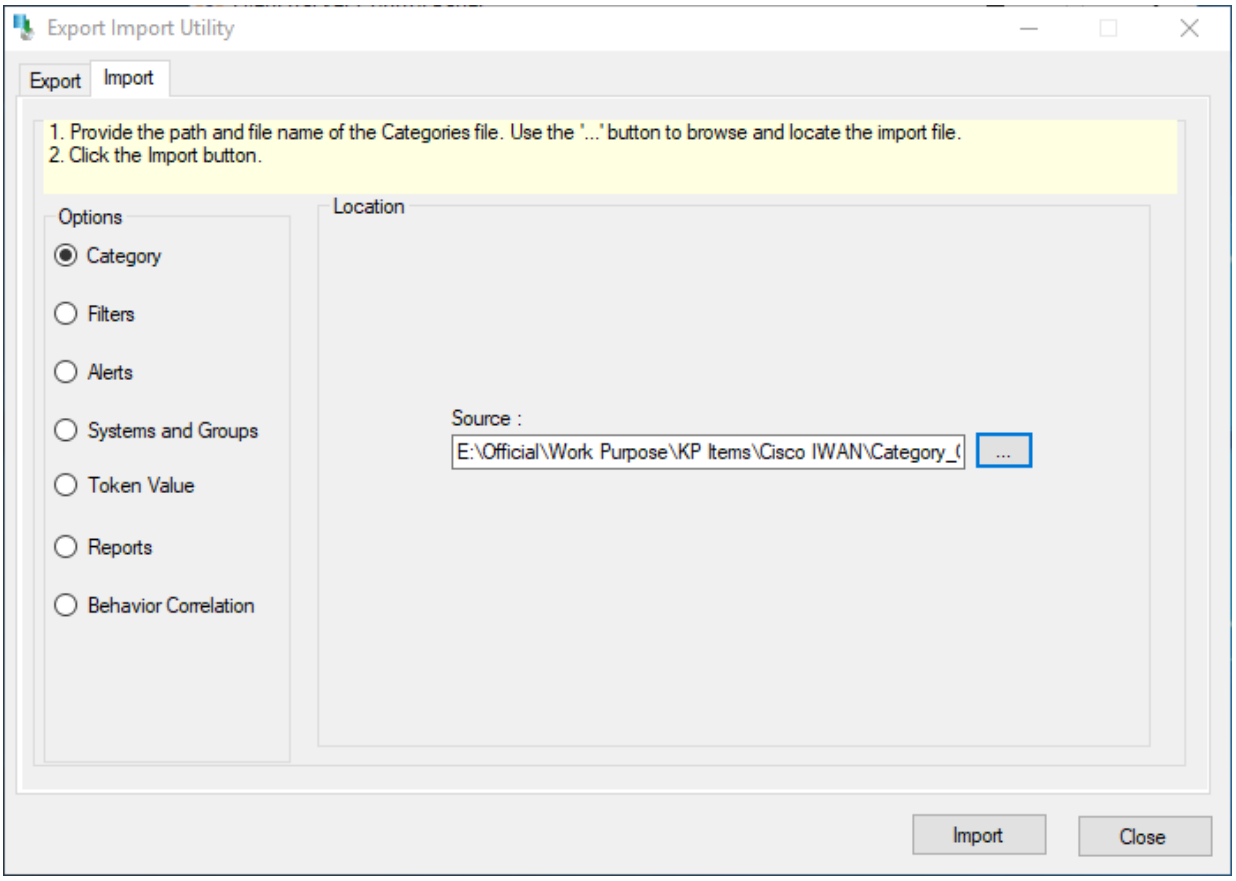

Figure 24

2. Locate **Category_Cisco IWAN.iscat** file, and then click the **Open** button.
3. To import categories, click the **Import** button. EventTracker displays success message.

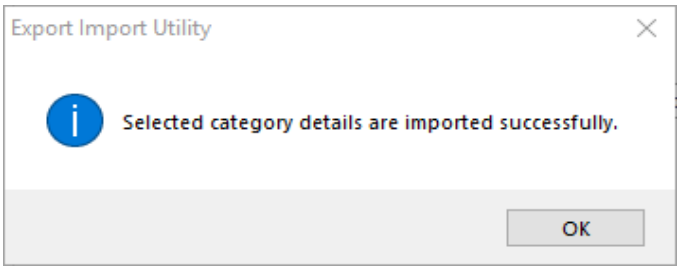

Figure 25

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

Alerts

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

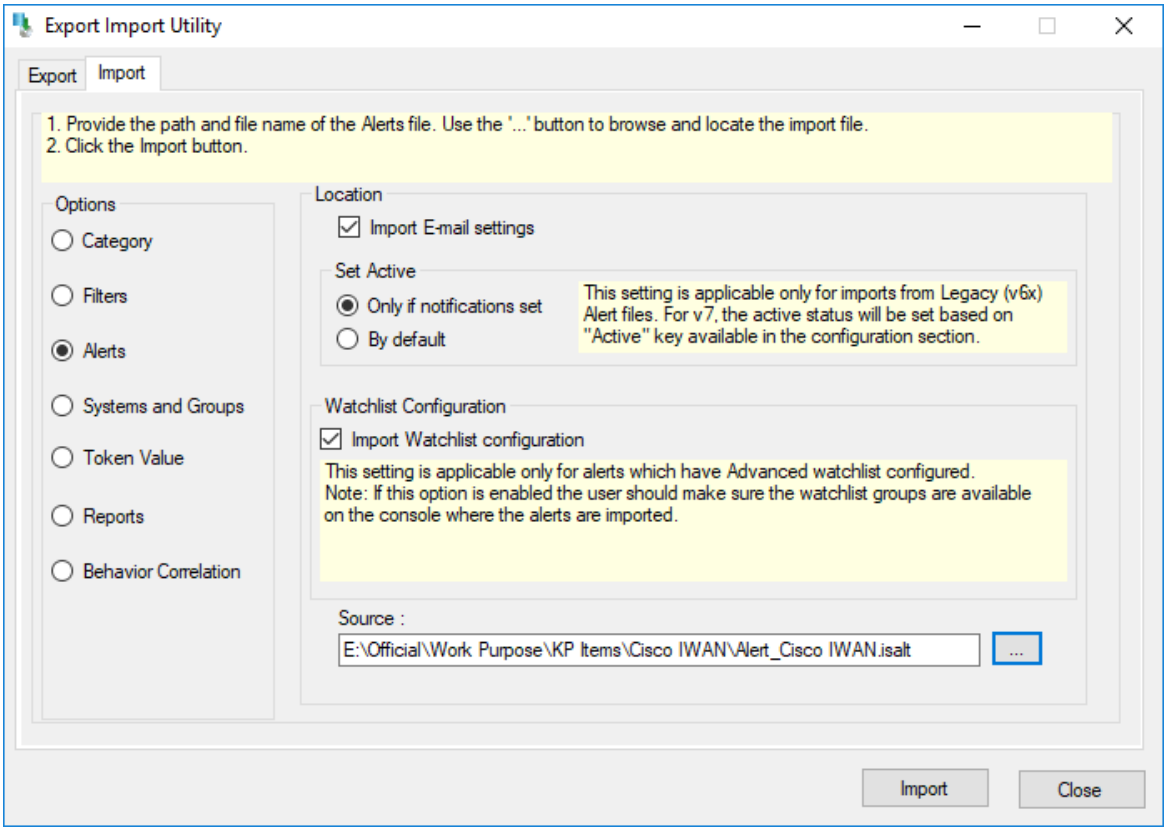

Figure 26

2. Locate **Alert_Cisco IWAN.isalt** file, and then click the **Open** button.
3. To import alerts, click the **Import** button.

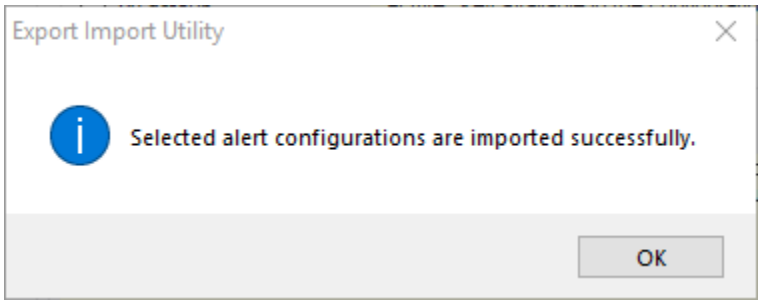

Figure 27

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

Token Templates

1. Click **Parsing rules** under **Admin** option in the EventTracker manager page.
2. Move to **Template** and click on import configuration icon on the top right corner.
3. In the popup window browse the file named **Token Template_ Cisco IWAN.ettd**.

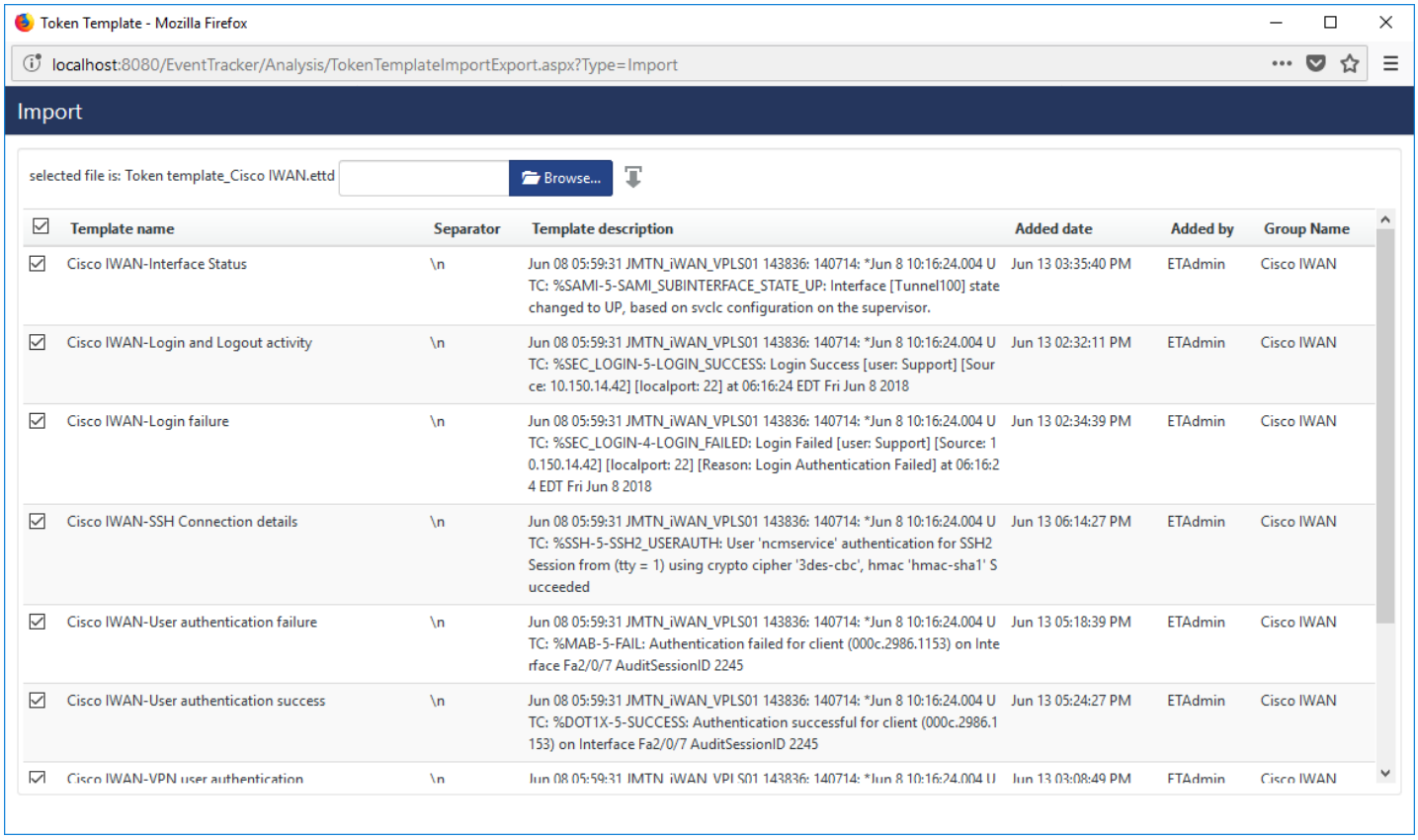

Figure 28

4. Now select all the check box and then click on Import option.

Knowledge Objects

1. Click **Knowledge objects** under **Admin** option in the EventTracker manager page.
2. Locate the **KO_Cisco IWAN.etko** file.

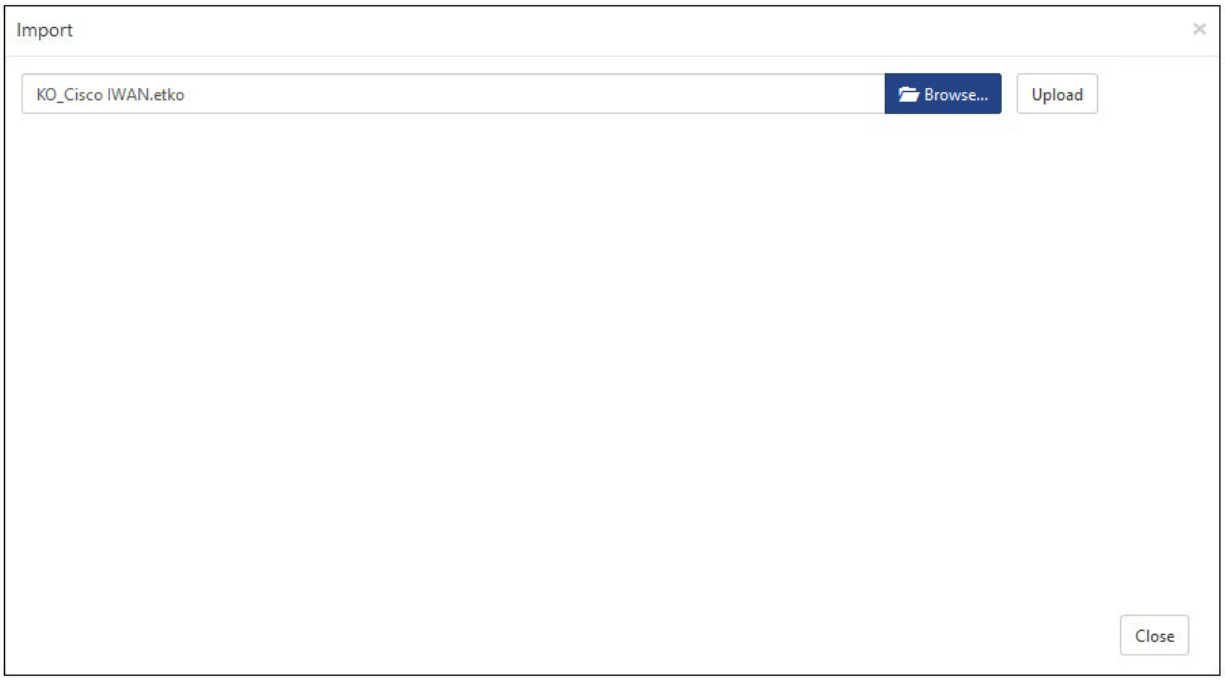

Figure 29

3. Click the '**Upload'** option.

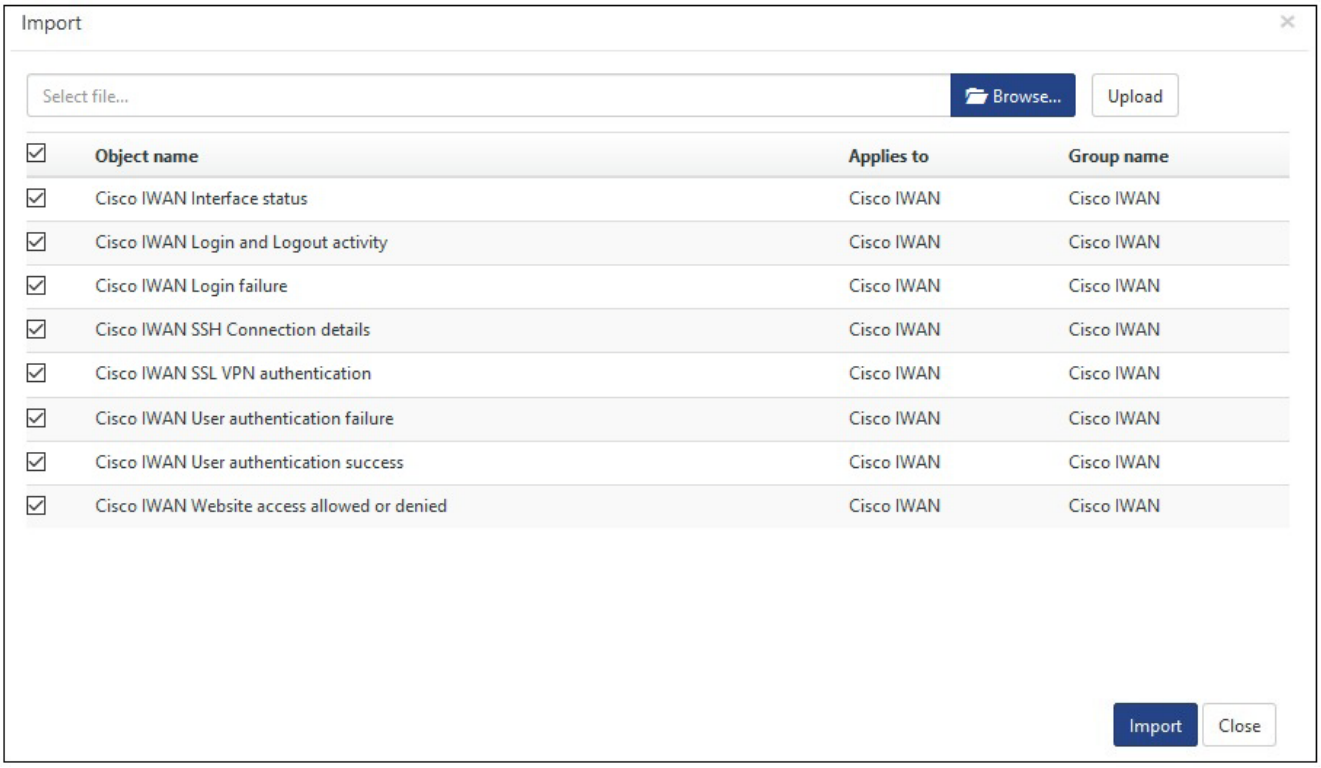

Figure 30

4. Now select all the check box and then click on '**Import**' option.

5. Knowledge objects are now imported successfully.

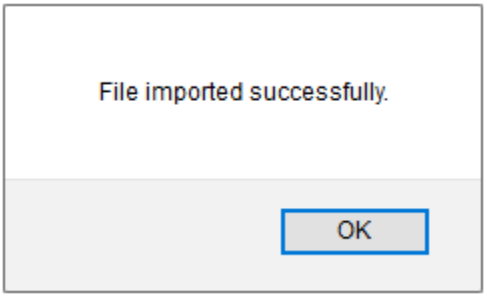

Figure 31

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

Flex Reports

On EventTracker Control Panel,

1. Click **Reports** option, and select new (*.etcrx) from the option.

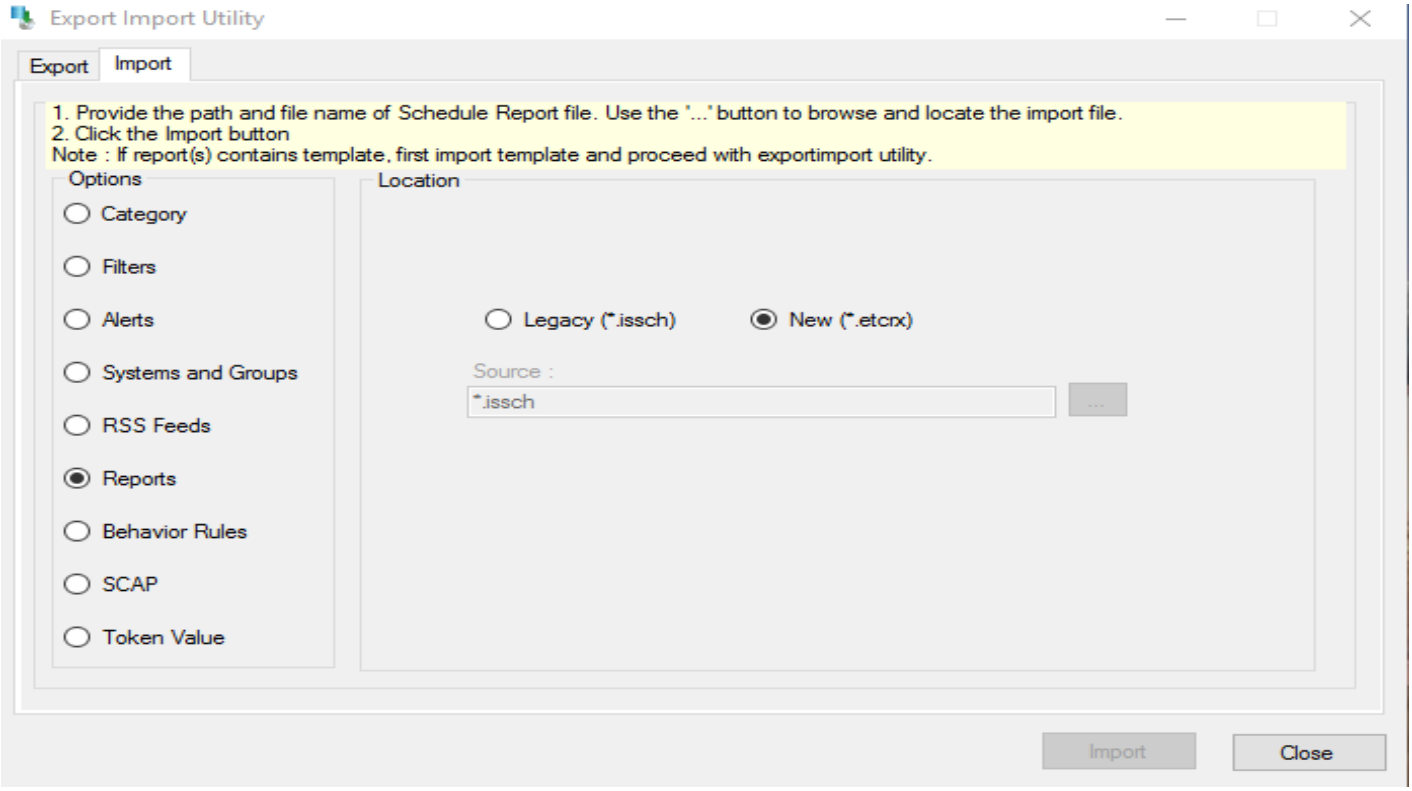

Figure 32

2. Locate the **Reports_Cisco IWAN.etcrx** file, and select all the check box.

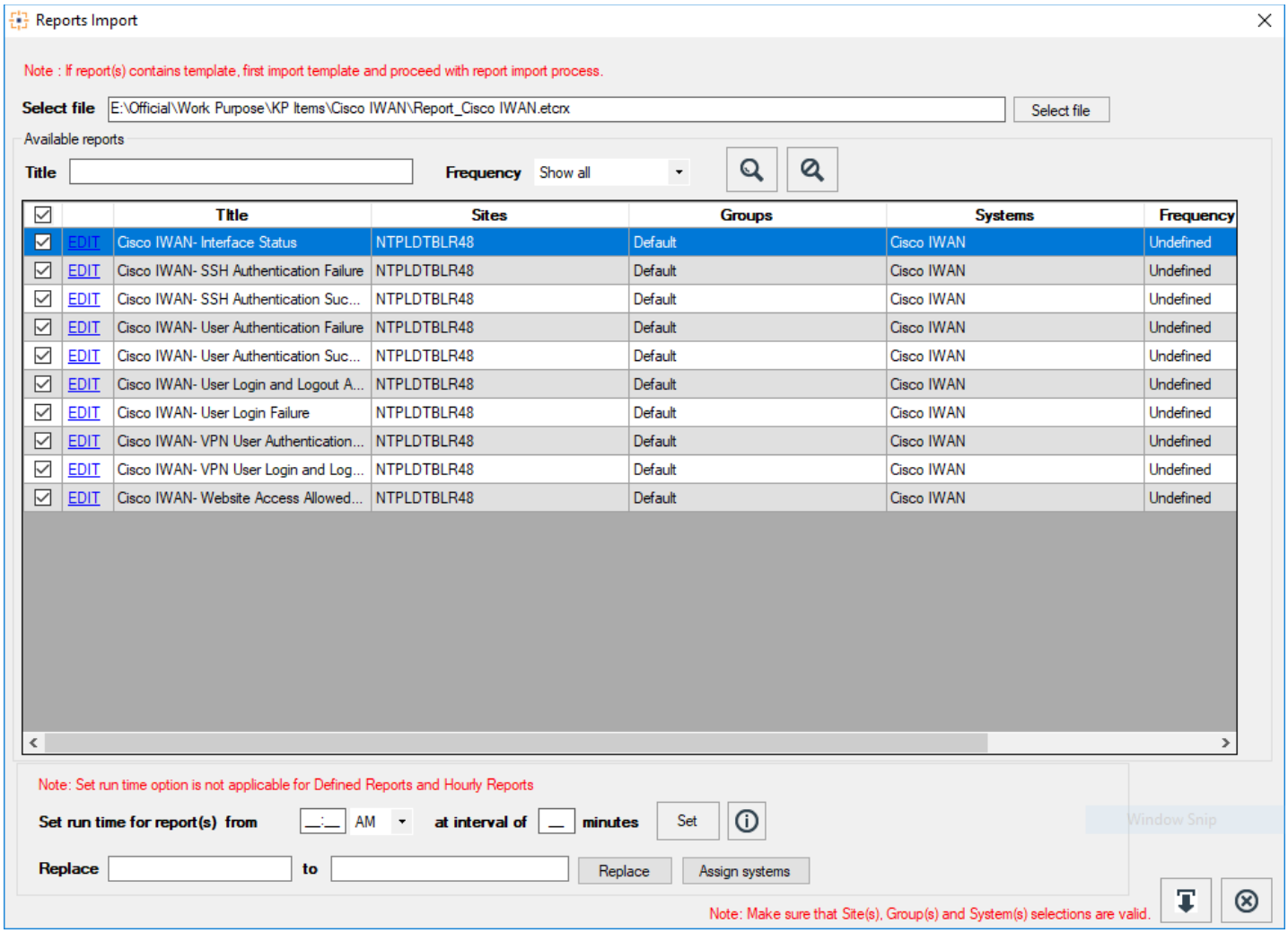

Figure 33

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

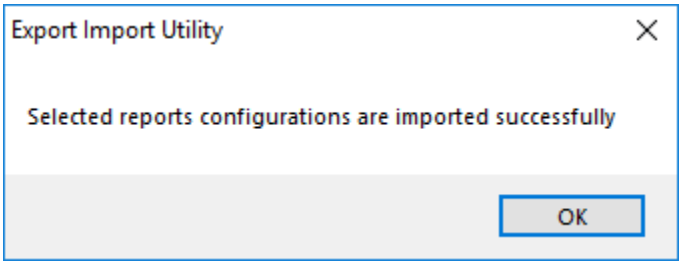

Figure 34

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

Dashboards

NOTE: If you have EventTracker Enterprise version **v9.0**, you can import dashboards.

1. Open **EventTracker Enterprise**.

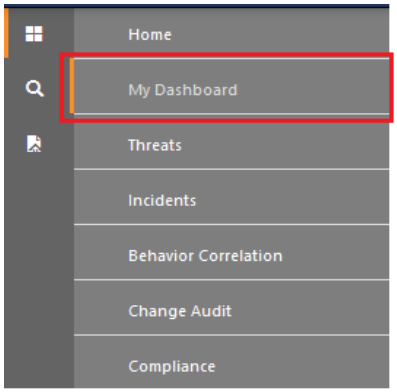

Figure 35

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

3. Click the **'Import'** button to import the dashlets.

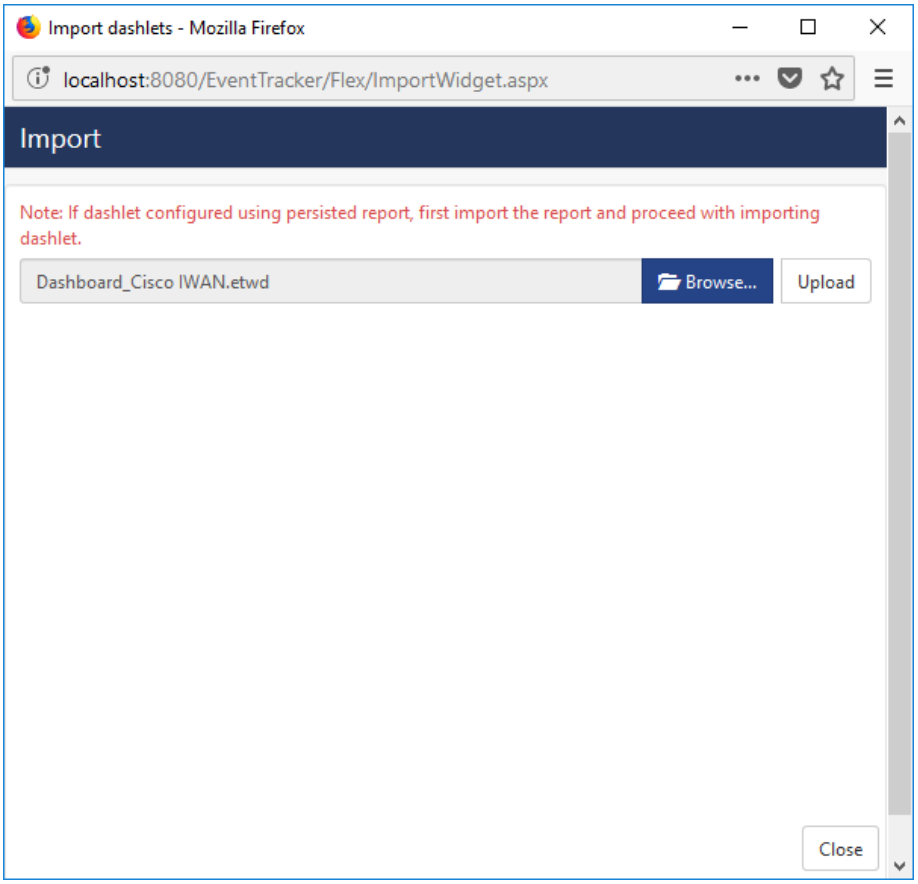

Figure 36

4. Locate the **Dashboard_Cisco IWAN.etwd** file.
5. Click the '**Upload'** option.

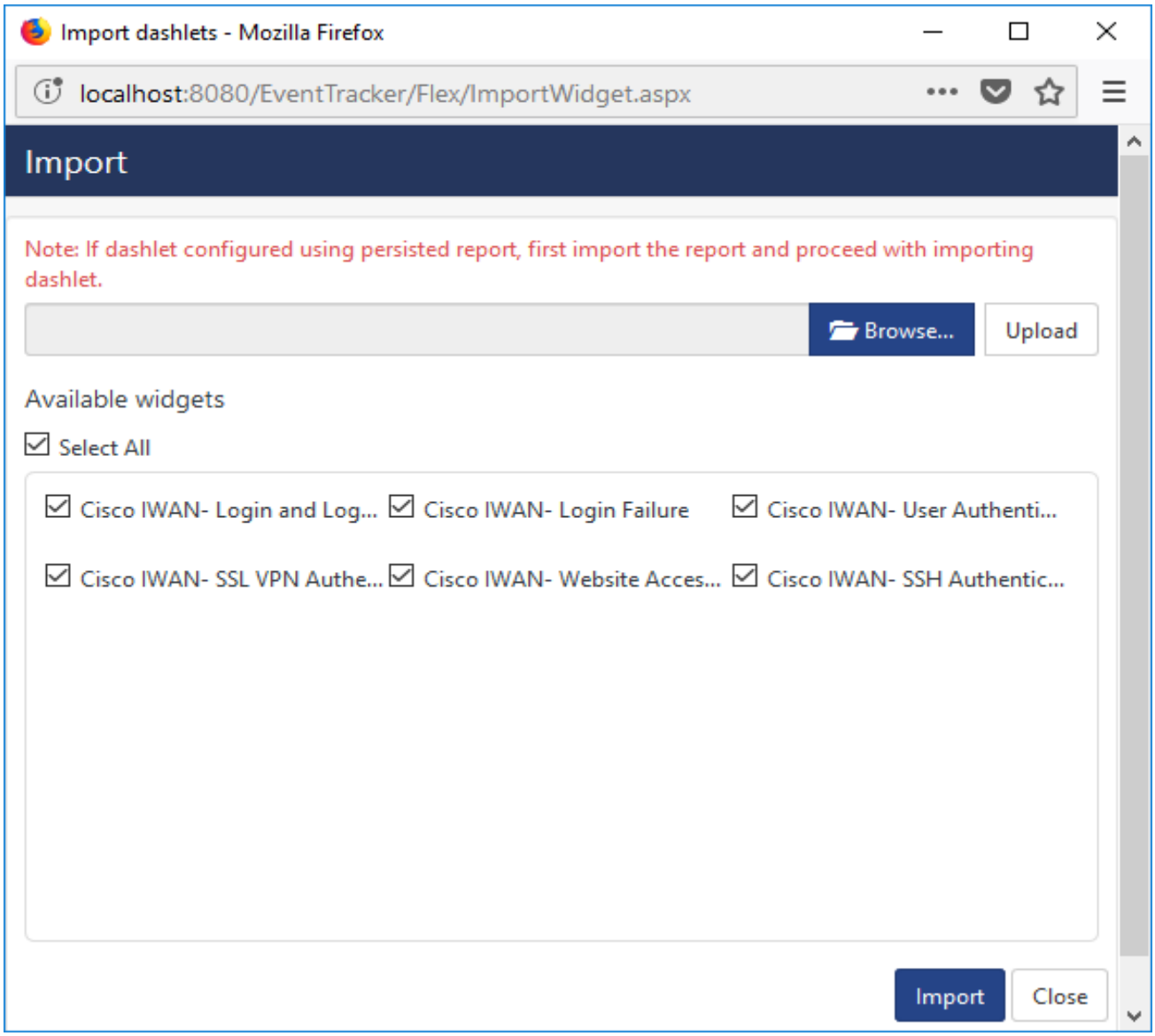

Figure 37

6. Now select all the check box and then click on '**Import**' option.
   Dashlets are now imported successfully.
7. Click the '**Add'** button to create a new dashlets.

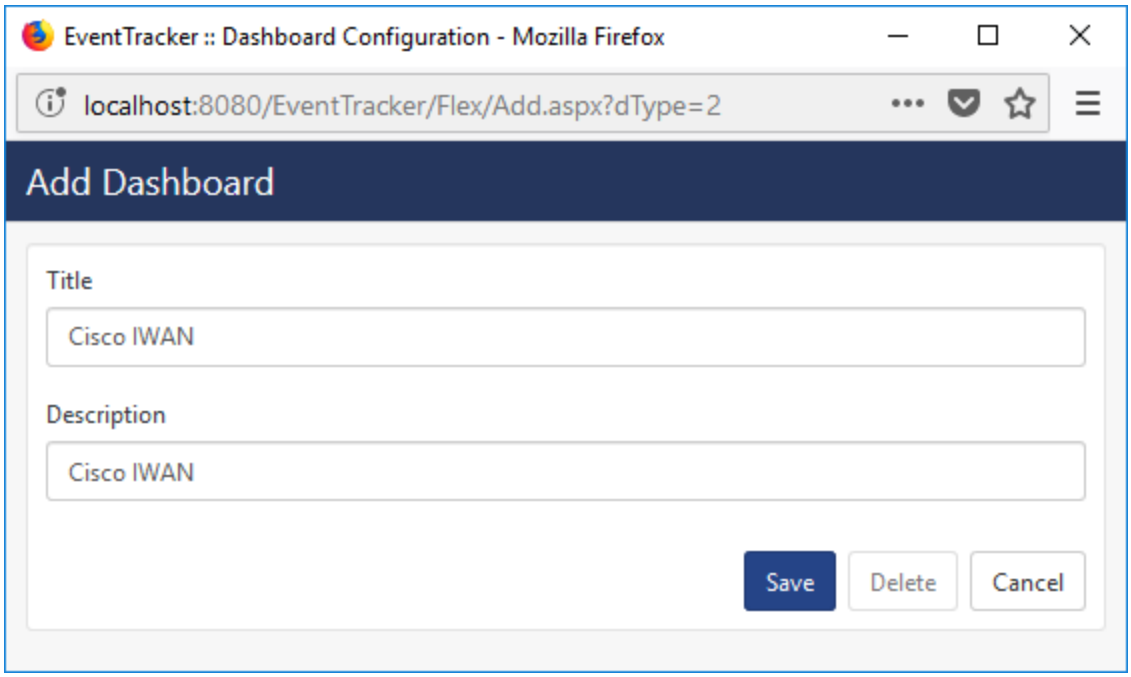

Figure 38

8. Fill suitable Title and Description and click **Save** button.
9. Click **'Customize'** to locate **Cisco IWAN** dashlets and choose all created dashlets for **Cisco IWAN**.

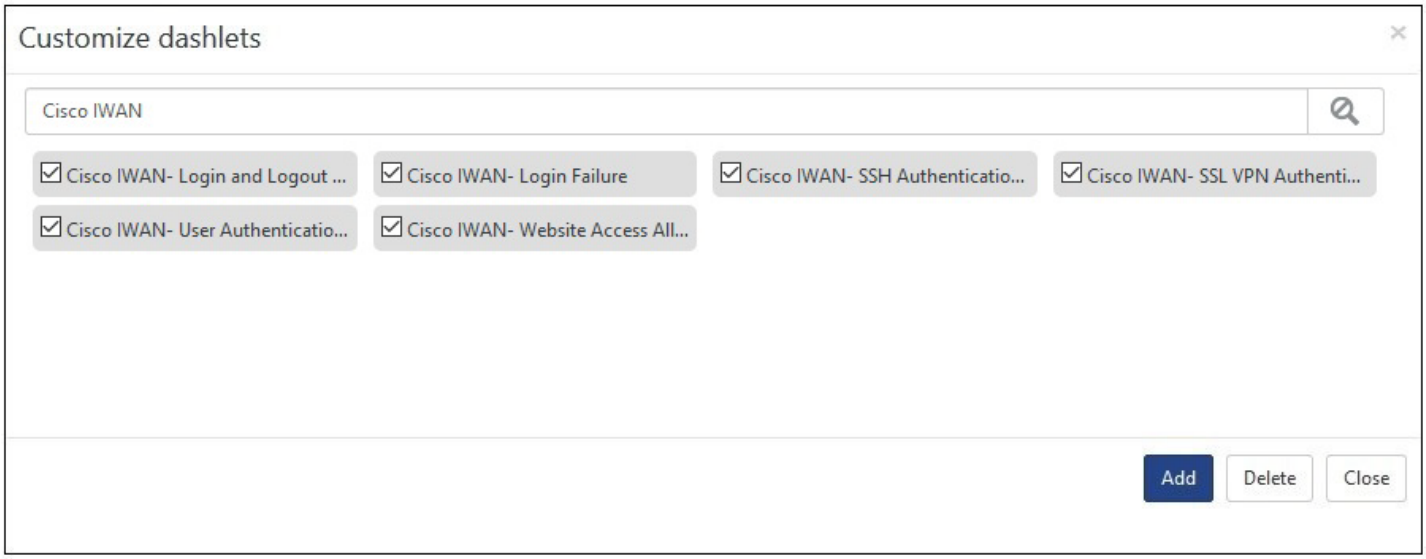

Figure 39

10. Click '**Add'** dashlet to create dashboard.

Verify Cisco IWAN knowledge pack in EventTracker

Categories

1. Logon to **EventTracker Enterprise**.
2. Click **Admin** dropdown, and then click **Categories**.
3. In **Category Tree** to view imported categories, scroll down and expand **Cisco IWAN** group folder to view the imported categories.

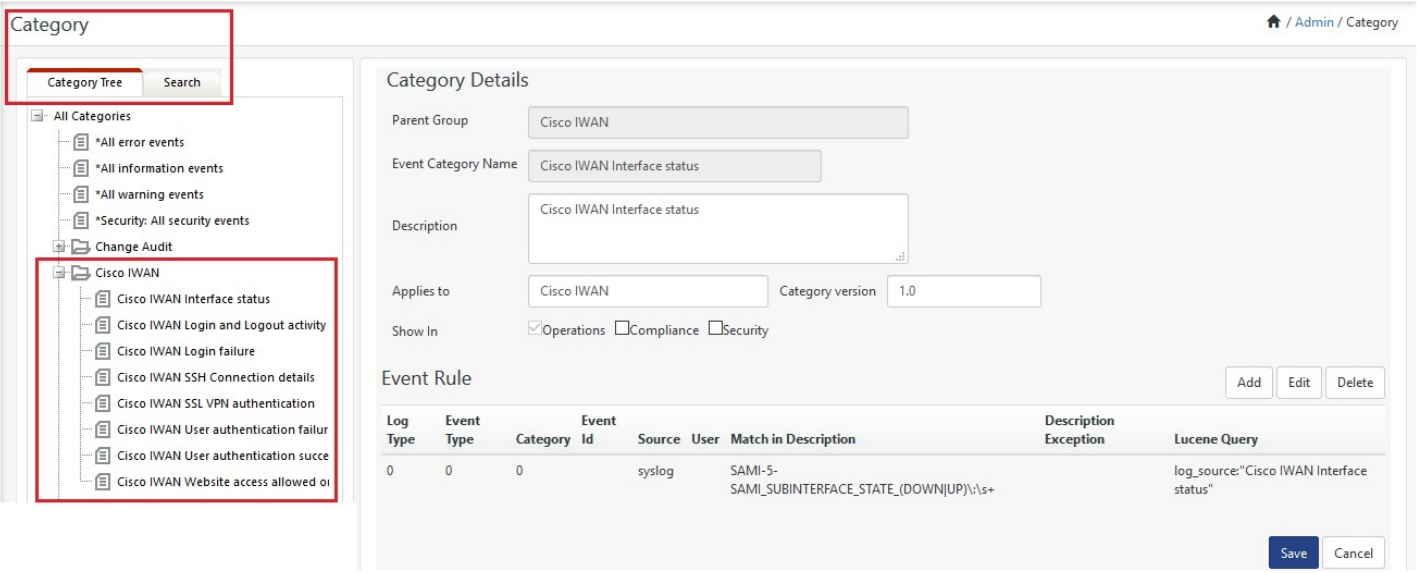

Figure 40

Alerts

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Alerts.**
2. In search box, enter **Cisco IWAN** and then click the **Search** button.
   EventTracker displays alert of **Cisco IWAN.**

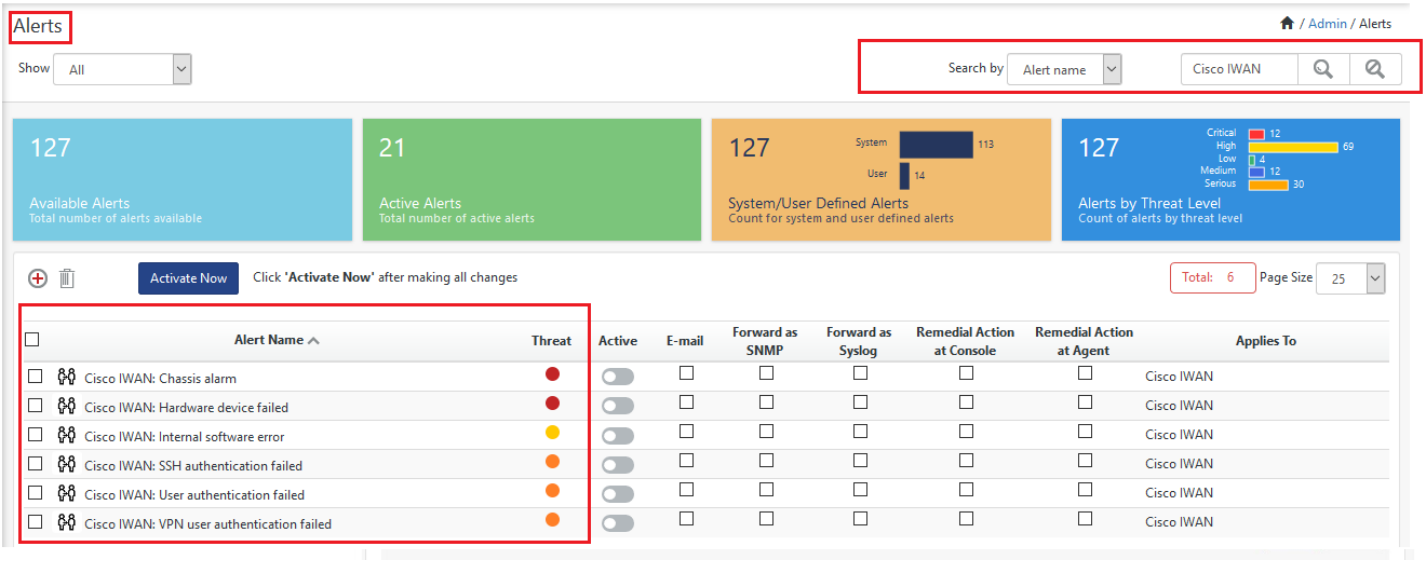

Figure 41

Token Templates

1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Parsing Rules.**
2. On **Template** tab, click on the **Cisco IWAN** group folder to view the imported Token Values.

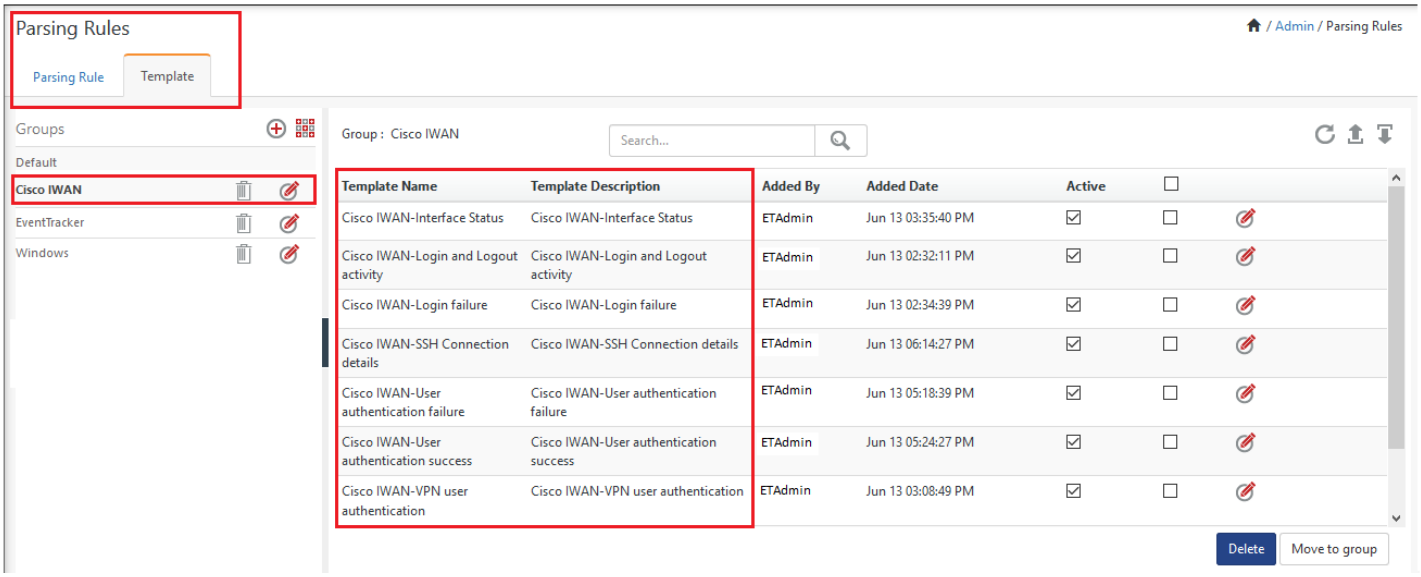

Figure 42

Knowledge Objects

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

2. In the **Knowledge Object** tree, expand **Cisco IWAN** group folder to view the imported Knowledge objects.

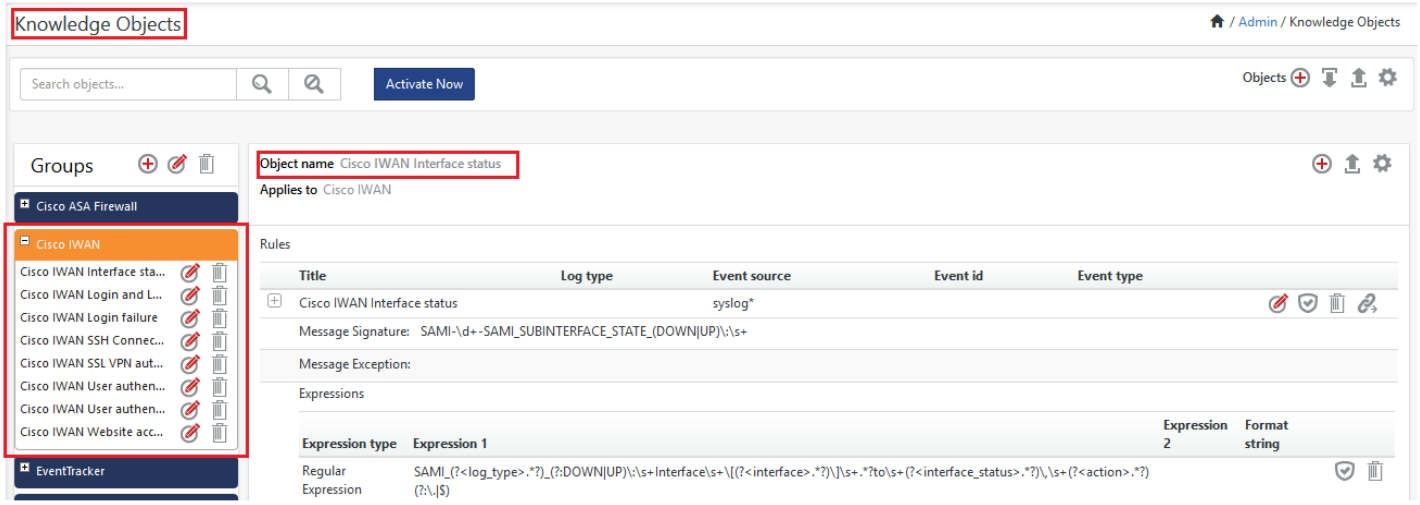

Figure 43

Flex Reports

1. In the **EventTracker Enterprise** web interface, click the **Reports** menu, and then select **Report Configuration**.

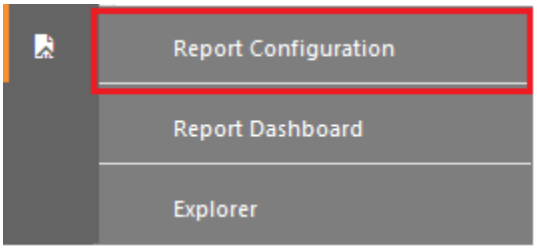

Figure 44

2. In **Reports Configuration** pane, select **Defined** option.
3. Click on the **Cisco IWAN** group folder to view the imported Cisco IWAN reports.

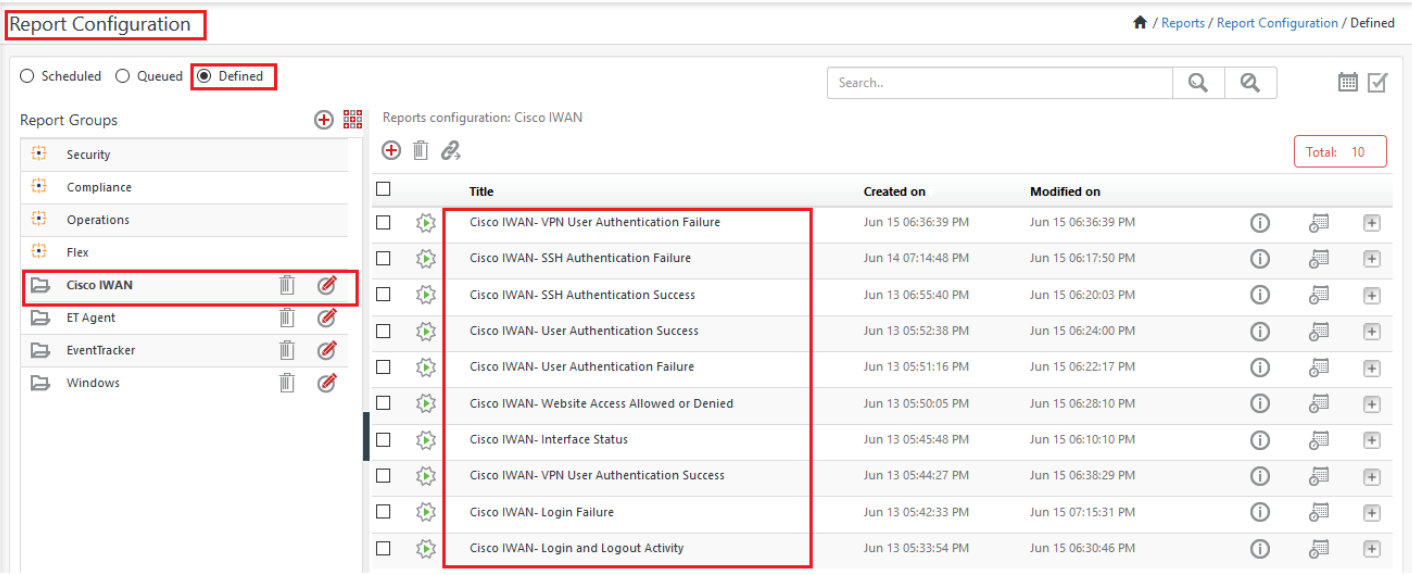

Figure 45

Dashboards

1. Open **EventTracker Enterprise** in browser and logon.
2. Navigate to **Dashboard>My Dashboard**.
   My Dashboard pane is shown.

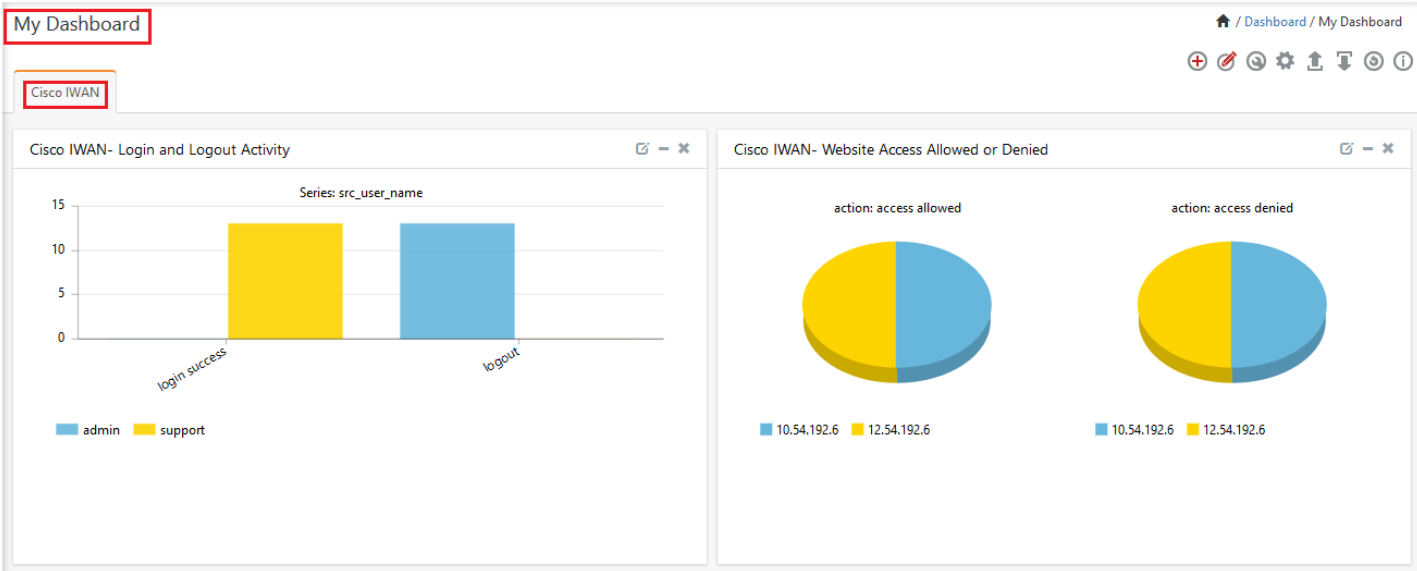

Figure 46

Sample Flex Dashboards

1. **Cisco IWAN- Login and Logout Activity**: This dashboard provides information related to login and logout activity.

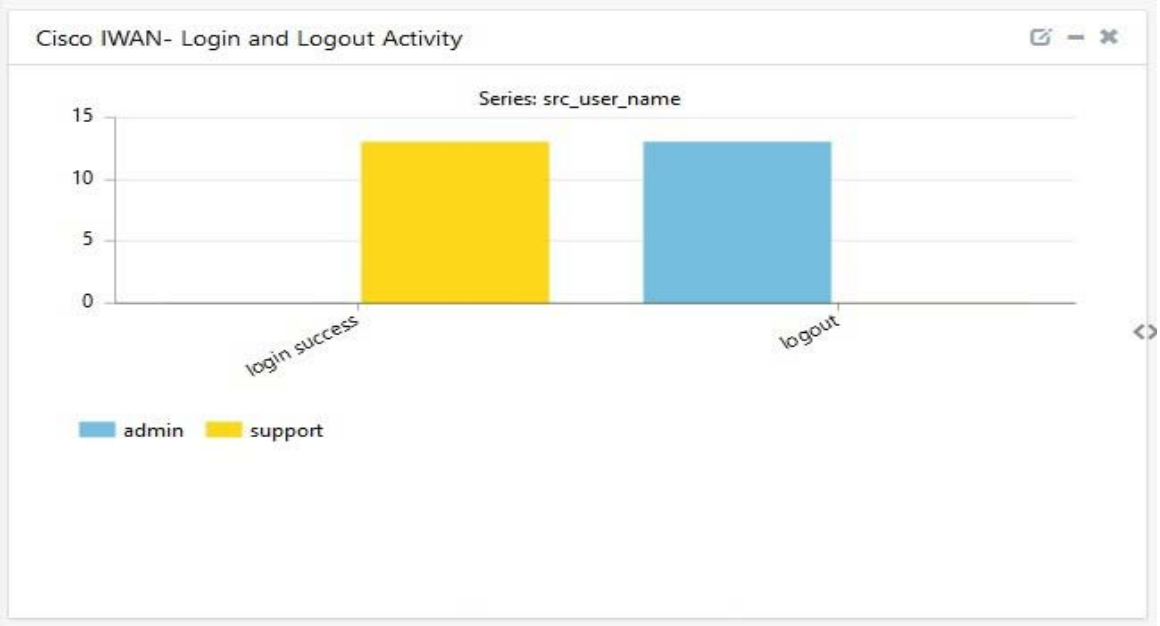

Figure 47

2. **Cisco IWAN- SSL VPN Authentication**: This dashboard provides information related to SSL VPN authentication.

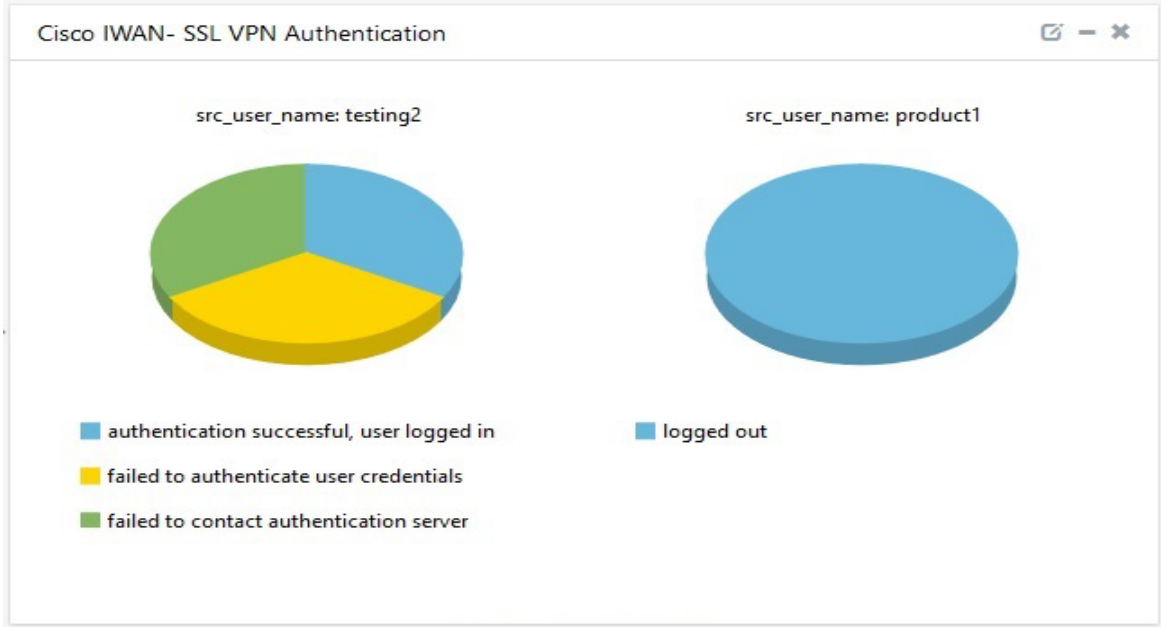

Figure 48

3. **Cisco IWAN- Website Access Allowed and Blocked**: This dashboard provides information related to website access allowed and blocked.

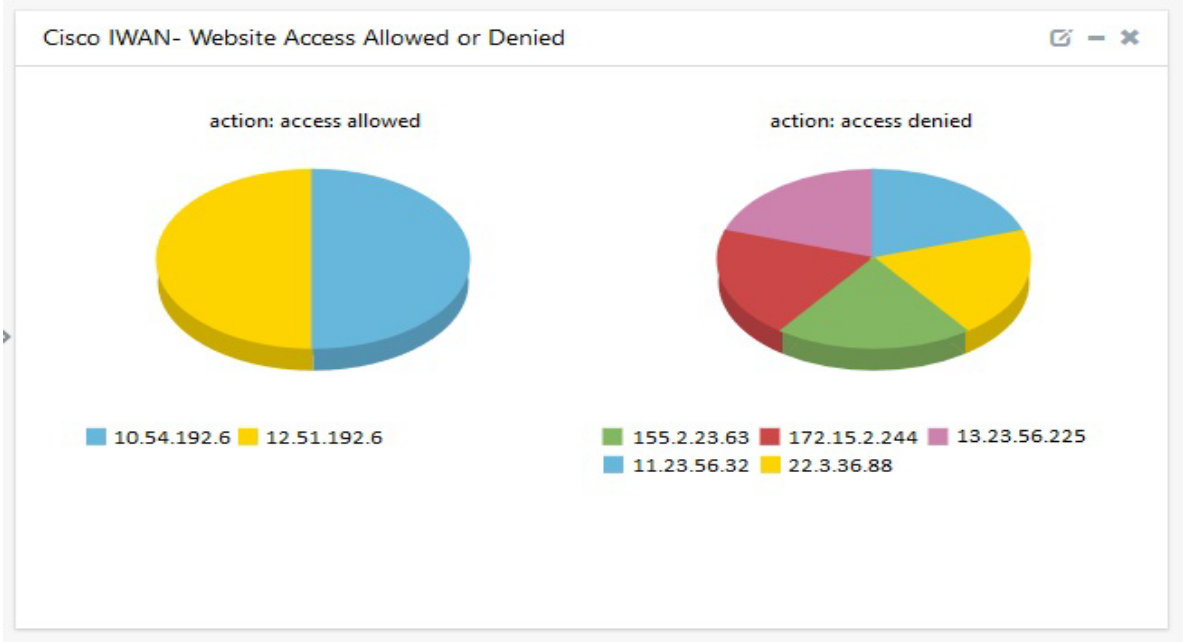

Figure 49

4. **Cisco IWAN- User Authentication Failure**: This dashboard provides information related to user authentication failure.

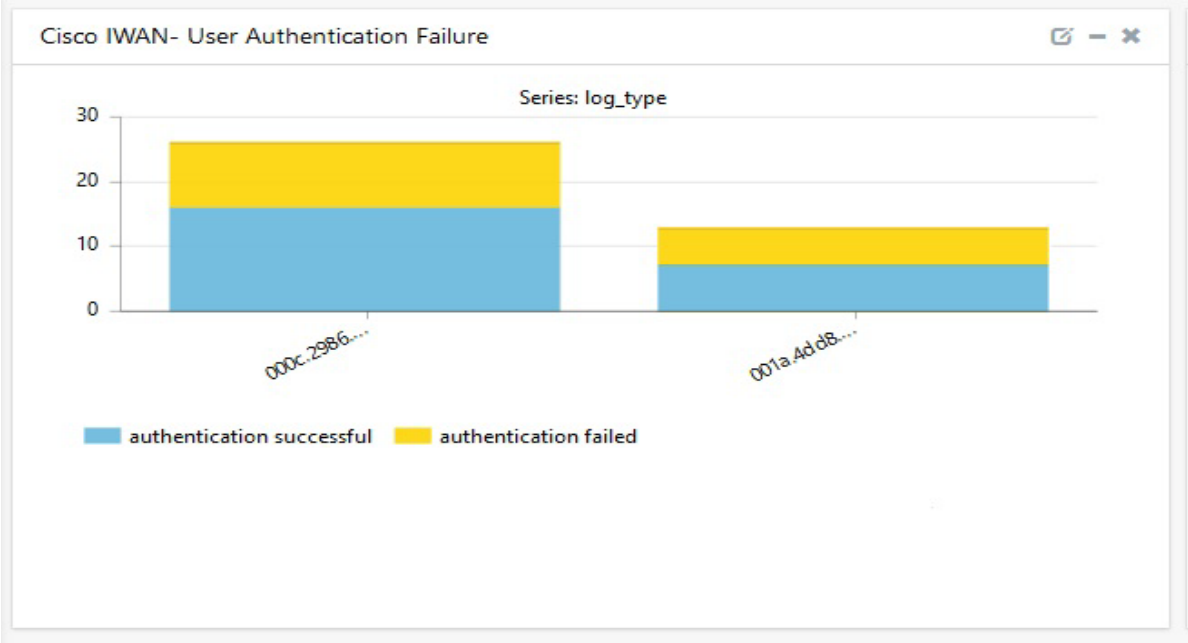

Figure 50