

Integrate F5 BIG-IP EventTracker v9.x and later

Publication Date: May 14, 2019

Abstract

This guide provides instructions to configure F5 BIG-IP to send the syslog events to EventTracker.

Scope

The configurations detailed in this guide are consistent with EventTracker version 9.x and later, and F5 BIG-IP (Firmware version 9.x to 14.x).

Audience

F5 BIG-IP users, who wish to forward syslog events to EventTracker manager.

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

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

Netsurion 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 Netsurion, 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.

© 2019 Netsurion. 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
Overview	3
Pre-requisite	3
Configure F5 BIG-IP to forward logs to EventTracker For Version 9.4.5-9.4.8	3 3
For Version 10.0.0-10.2.4	3
For Version 11.x to V14.x	4
EventTracker Knowledge Pack Reports	4 4
Alerts	8
Dashboards	9
Import F5 BIG-IP knowledge pack into EventTracker Categories	12 13
Alerts	13
Token Template	14
Knowledge Object	16
Flex Reports	17
Dashboard	18
Verify F5 BIG-IP knowledge pack in EventTracker Categories	20 20
Alerts	21
Token Template	22
Knowledge Objects	22
Flex Reports	23
Dashboard	24

Netsurion EventTracker

Overview

F5 BIG-IP turns your network into an agile infrastructure for application delivery. It's a full proxy between users and application servers, creating a layer of abstraction to secure, optimize, and load balance application traffic. This gives you the control to add servers easily, eliminate downtime, improve application performance, and meet your security requirements.

EventTracker supports F5 BIG-IP 1600 series and above, it forwards the syslog-ng messages to EventTracker manager. EventTracker generates the alert and report for critical events.

Pre-requisite

- EventTracker v9.x or above should be installed.
- You must have a console with root access to the F5 BIG-IP system.

Configure F5 BIG-IP to forward logs to EventTracker

The mechanism that the F5 BIG-IP uses to log events remotely is the Linux utility syslog-ng which is enabled by default.

For Version 9.4.5-9.4.8

- 1. Use an SSH client to access the F5 Big-IP device.
- 2. Type root and press enter.
- 3. Enter the F5 Big-IP password.
- 4. Type **bpsh**, and press enter.
- To configure the remote syslog server, type the following command: bigpipe syslog remote server <IP_address>
 For example: bigpipe syslog remote server 10.1.1.1
- To save the configuration, type the following command:
 bigpipe save
- 7. Type exit and press enter.

For Version 10.0.0-10.2.4

- 1. Use an SSH client to access the F5 Big-IP device.
- 2. Type **root** and press enter.
- 3. Enter the F5 Big-IP password.
- 4. Type **bpsh**, and press enter.

Netsurion... EventTracker

- 5. To add a single remote syslog server, use the following command syntax:
- 6. bigpipe syslog remote server {<name> {host <IP_address>}}
- 7. For example, bigpipe syslog remote server {server1.net {host 10.1.1.1}}
- 8. To save the configuration, type the following command:
- 9. In versions **10.0.0** through **10.2.1: bigpipe save**
- 10. In versions 10.2.2 and later: bigpipe save all
- 11. Type exit and press enter.

For Version 11.x to V14.x

- 1. Use an SSH client to access the F5 Big-IP device.
- 2. Type **root** and press enter.
- 3. Enter the F5 Big-IP password.
- Log in to the Traffic Management Shell (tmsh) by typing the following command: tmsh
- 5. To add a single remote syslog server, use the following command syntax:

modify /sys syslog remote-servers add { <name> { host <IP address> remote-port <port> }}
For example, to add EventTracker server 172.28.31.40 with port 514 and name ETLog, type the
following command:

modify /sys syslog remote-servers add { ETLog { host 172.28.31.40 remote-port 514 }}

- To save the configuration, type the following command: save /sys config
- 7. Type quit, and press enter.

EventTracker Knowledge Pack

Once F5 BIG-IP events are enabled and F5 BIG-IP events are received in EventTracker, Alerts, and Reports can be configured in EventTracker.

The following Knowledge Packs are available in EventTracker to support F5 BIG-IP monitoring.

Reports

• **F5 BIG-IP Login and Logout Activity:** This report provides information related to user logon and logout which includes User Name, Host Address, Logon Attempts, Session Start Time and Session End Time fields.

Netsurion... EventTracker

		Fuentfeuree		Login			
Loglime	Computer	EventSource	userip	attempts	Username	Login Time	Logout Time
05/02/2019 03:49:51 PM	WIN-F5-BIG-IP	SYSLOG	10.140.50.15	1	admin(admin)	Thu Apr 25 15:53:54 2019	
		auth					
05/02/2019 03:49:51 PM	WIN-F5-BIG-IP	SYSLOG	10.140.50.15	1	admin(admin)	Thu Apr 25 15:53:13 2019	Thu Apr 25 15:53:50 2019
		auth					
05/02/2019 03:49:52 PM	WIN-F5-BIG-IP	SYSLOG	10.140.50.15	1	admin(admin)	Thu Apr 25 15:41:41 2019	
		auth					
05/02/2019 03:49:52 PM	WIN-F5-BIG-IP	SYSLOG	10.150.254.234	1	admin(admin)	Wed Apr 24 12:48:46 2019	Thu Apr 25 15:41:41 2019
		auth					
05/02/2019 03:49:52 PM	WIN-F5-BIG-IP	SYSLOG	10.150.254.234	1	admin(admin)	Wed Apr 24 12:40:28 2019	Thu Apr 25 15:41:41 2019
		auth					
05/02/2019 11:29:32 AM	WIN-F5-BIG-IP	SYSLOG	10.140.50.15	1	admin(admin)	Thu Apr 25 15:41:41 2019	Thu Apr 25 15:53:16 2019
		authpriv					
05/02/2019 11:29:32 AM	WIN-F5-BIG-IP	SYSLOG	10.140.50.15	1	admin(admin)	Thu Apr 25 15:42:44 2019	Thu Apr 25 15:53:08 2019
		authpriv					
05/02/2019 11:29:32 AM	WIN-F5-BIG-IP	SYSLOG	10.140.50.15	1	admin(admin)	Thu Apr 25 15:53:13 2019	
		authpriv					
05/02/2019 11:29:35 AM	WIN-F5-BIG-IP	SYSLOG	10.150.254.234	1	admin(admin)	Wed Apr 24 12:40:25 2019	Thu Apr 25 15:42:44 2019
		authpriv					

Figure 1

Sample Logs:

event_category	+- 0
event_computer	+- WIN-F5-BIG-IP
event_datetime	+- 5/3/2019 4:55:12 PM
event_datetime_utc	+- 1556882712
event_description	Apr 24 13:40:28 10.151.37.26 Apr 24 12:40:28 CH-BIG-IP-02 notice httpd[4940]: 01070417:5: AUDIT - user admin - RAW: httpd(mod_auth_pam): user=adm
	in(admin) partition=[All] level=Administrator tty=/bin/bash host=10.150.254.175 attempts=1 start="Mon Dec 10 12:26:17 2018" end="Wed Apr 24 12:40:
	28 2019".
event_id	+- 3230
event_log_type	+- Application
event_source	+- syslog auth

Figure 2

• **F5 BIG-IP Login Failed Activity:** This report provides information related to user logon failure which includes User Name, Host Address, Logon Attempts, Session Start Time and Session End Time fields.



LogTime	Computer	EventSource	User IP	UserName	Reason
05/02/2019 05:41:57 PM	WIN-F5-BIG-IP	syslog auth	15.105.32.22	gary	Authentication
					failure
05/02/2019 05:41:58 PM	WIN-F5-BIG-IP	syslog auth	15.105.32.22	gary	Authentication
					failure
05/02/2019 05:45:51 PM	WIN-F5-BIG-IP	syslog auth		ETAdmin	password
					check failed
05/02/2019 05:45:53 PM	WIN-F5-BIG-IP	syslog auth	88.65.127.195	karen	authentication
					failure
05/02/2019 05:45:53 PM	WIN-F5-BIG-IP	syslog auth	88.65.127.195	karen	authentication
					failure
05/03/2019 03:26:17 PM	WIN-F5-BIG-IP	syslog auth	162.244.140.179	root	authentication
					failure
05/03/2019 03:26:17 PM	WIN-F5-BIG-IP	syslog auth	40.237.45.82	root	Authentication
					failure
05/03/2019 03:26:17 PM	WIN-F5-BIG-IP	syslog auth		user (root)	password
					check failed

Figure 3

Sample Logs:

event_category	+- 0
event_computer	+- WIN-F5-BIG-IP
event_datetime	+- 5/3/2019 3:26:22 PM
event_datetime_utc	+- 1556877382
event_description	Apr 24 13:45:22 150.230.193.80 Apr 24 12:45:22 CH-BIG-IP-02 err sshd[23153]: error: PAM: Authentication failure for root from 40.237.45.82
event_id	+- 3230
event_log_type	+- Application
event_source	+- syslog auth

Figure 4

• **F5 BIG-IP Global Traffic Management Activity:** This report provides information related to global traffic management.

LogTime	Computer	EventSource	Connection Type	Source IP	Destination IP	Source Port Number	Reason	Connection Status
04/30/2019 12:52:49 PM	WIN-F5-BIG-IP	SYSLOG	tcp	8.45.157.10	50.234.180.27	443	success	DOWN> UP
04/30/2019 12:53:48 PM	WIN-F5-BIG-IP	SYSLOG	tcp	212.250.215.168	50.234.180.27	443	success	DOWN> UP
05/02/2019 03:20:43 PM	WIN-F5-BIG-IP	SYSLOG auth	tcp	8.45.157.10	50.234.180.27	443	success	DOWN> UP
05/02/2019 03:21:44 PM	WIN-F5-BIG-IP	SYSLOG auth	tcp	212.250.215.168	8.45.157.26	443	timeout	UP> DOWN
05/03/2019 03:35:05 PM	WIN-F5-BIG-IP	syslog local2	tcp	8.45.157.10	50.234.180.27	443	success	DOWN> UP
05/03/2019 03:35:05 PM	WIN-F5-BIG-IP	syslog local2	tcp	212.250.215.168	50.234.180.27	443	success	DOWN> UP
05/03/2019 03:35:04 PM	WIN-F5-BIG-IP	syslog local2	tcp	8.45.157.10	50.234.180.27	443	success	DOWN> UP





Sample Logs:

event_category	+- 0
event_computer	+- WIN-F5-BIG-IP
event_datetime	+- 5/3/2019 3:35:04 PM
event_datetime_utc	+- 1556877904
event_description	Apr 26 05:56:11 10.151.37.25 Apr 26 04:56:11 CH-BIG-IP-01 alert gtmd[16956]: 011ae0f2:1: Monitor instance /Common/tcp 212.250.215.168:443 UP> D
	OWN from 8.45.157.26 (state: timeout)
event_id	+- 3230
event_log_type	+- Application
event_source	+- syslog local2

Figure 6

• **F5 BIG-IP Local Traffic Management Activity:** This report will generate a detailed view of local traffic management logs.

LogTime	Computer	Process	Process ID	Source User	File Path	Status
05/03/2019 03:16:40 PM	WIN-F5-BIG-IP	tmsh[10142]: 01420002:5	10142	root	/Common	Command OK
05/03/2019 03:16:45 PM	WIN-F5-BIG-IP	tmsh[9444]: 01420002:5	9444	root	/Common	Command OK
05/03/2019 03:16:51 PM	WIN-F5-BIG-IP	tmsh[8811]: 01420002:5	8811	root	/Common	Command OK
05/03/2019 03:16:59 PM	WIN-F5-BIG-IP	tmsh[8117]: 01420002:5	8117	root	/Common	Command OK
05/03/2019 03:17:05 PM	WIN-F5-BIG-IP	tmsh[7477]: 01420002:5	7477	root	/Common	Command OK

Figure 7

Sample Logs:

event_log_type	+- Application
event_type	+- Information
event_id	+- 3230
event_source	+- syslog
event_user_domain	+- N/A
event_computer	+- WIN-F5-BIG-IP
event_user_name	+- N/A
event_description	Apr 26 01:20:46 10:151:37:25 Apr 26 00:20:46 CH-BIG-IP-01 notice tmsh[29393]: 01420002:5: AUDIT - pid=29393 user=root folder=/Common module=(t
	mos)# status=[Command OK] cmd_data=save / sys config partitions { Common }

Figure 8



• **F5 BIG-IP SSL Activity**: This report will generate a detailed view on all the SSL related activities as seen on F5 BIG-IP.

LogTime	Computer	Log Info	Source IP	Source Port	Destination IP	Destination port
05/04/2019 04:24:06 PM	WIN-F5-BIG-IP	Connection error				
05/04/2019 04:24:06 PM	WIN-F5-BIG-IP	No shared ciphers between SSL peers	10.151.100.100	993	208.100.26.235	42868
05/04/2019 04:24:06 PM	WIN-F5-BIG-IP	SSL Handshake failed for TCP	10.151.100.100	993	208.100.26.235	42750
05/04/2019 04:24:06 PM	WIN-F5-BIG-IP	Connection error				
05/04/2019 04:24:06 PM	WIN-F5-BIG-IP	No shared ciphers between SSL peers	10.151.100.100	993	208.100.26.235	42868

Figure 9

Sample Logs:

event_computer	+- WIN-F5-BIG-IP
event_datetime	+- 5/4/2019 4:40:22 PM
event_datetime_utc	+ - 1556968222
event_description	Apr 26 05:34:48 10.151.37.26 Apr 26 04:34:48 CH-BIG-IP-02 warning tmm1[21425]: 01260013:4: SSL Handshake failed for TCP 208.100.26.235:42750 -> 1
	0.151.100.100:993
event_id	+- 3230
event_log_type	+- Application
event_source	+- syslog local0



Alerts

- **F5 BIG-IP: ARP entry deleted** This alert is generated when an ARP entry is deleted.
- F5 BIG-IP: Authentication failed This alert is generated when authentication fails.
- F5 BIG-IP: Authentication success This alert is generated when authentication succeeds.
- **F5 BIG-IP: Connection error** This alert is generated when a connection has an error.
- F5 BIG-IP: Monitor removed This alert is generated when a monitor is removed from local traffic management.
- F5 BIG-IP: Packet filtering disabled This alert is generated when packet filtering is disabled.
- **F5 BIG-IP: Packet filtering rule modified** This alert is generated when the packet filtering rule is modified.
- F5 BIG-IP: Pool member status down BIG-IP: Pool member status down.
- **F5 BIG-IP: Root login failure** This alert is generated when the root has authentication failure.
- **F5 BIG-IP: User account deleted** This alert is generated when the user account is deleted.



Dashboards



• F5 BIG-IP: Login failed - By city



• F5 BIG-IP: Login and Logout - By source IP



Figure 12



• F5 BIG-IP: Global Traffic Management

F5 BIG IP : Global Traffic Management						
dest_ip_address	log_status	src_ip_address	<pre>src_port_no</pre>			
8.45.157.26	timeout	212.250.215.168	443			
8.45.157.26	timeout	212.250.215.168	443			
50.234.180.27	success	212.250.215.168	443			
50.234.180.27	success	8.45.157.10	443			
50.234.180.27	success	212.250.215.168	443			
212.250.215.190	timeout	8.45.157.10	443	<>		
50.234.180.27	success	8.45.157.10	443			
50.234.180.27	success	212.250.215.168	443			
212.250.215.190	timeout	8.45.157.10	443			
50.234.180.27	success	8.45.157.10	443			
Apr 30 12:05 PM - May 07 12:06 PM						



• F5 BIG-IP: Login failed - By source IP



Figure 14



• F5 BIG-IP: Login failed - By user name





• F5 BIG-IP: Login and Logout - By user name



Figure 16



Import F5 BIG-IP knowledge pack into EventTracker

NOTE: Import knowledge pack items in the following sequence:

- Categories
- Alerts
- Token Values
- Knowledge Objects
- Flex Reports
- Dashboard
- 1. Launch the EventTracker Control Panel.
- 2. Double click Export Import Utility.



Figure 17

Export Import Utility							
Export Import							
1. Provide the path and 2. Click the Import butto	file name of the Categories file. Use the '' button to n.						
Options	Location						
Category							

Figure 18



3. Click the **Import** tab.

Categories

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

ŋ,	Export Import Utility	_		×
E	Export Import			
	1. Provide the path and file n 2. Click the Import button.	ame of the Categories file. Use the '' button to browse and locate the import file.		
	Options Category	Location		
	⊖ Filters			
	⊖ Alerts			
	O Systems and Groups	Source :		
	O Token Value			
	⊖ Reports			
	O Behavior Correlation			
		Import	Close	

button.

Figure 19

- 2. Navigate to the location having a file with the extension ".iscat" and then click "Import" button.
- 3. EventTracker displays a success message:



Alerts

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



💺 Export Import Utility		- 0	×
Export Import			
 Provide the path and file nan Click the Import button. 	ne of the Alerts file. Use the '' butt	on to browse and locate the import file.	
Options	Location		
 Category 	Import E-mail settings		
 Filters Alerts 	 Set Active Only if notifications set By default 	This setting is applicable only for imports from Legacy (v6x) Alert files. For v7, the active status will be set based on "Active" key available in the configuration section.	
 Systems and Groups 	Watchlist Configuration		
◯ Token Value	This setting is applicable only f	on or alerts which have Advanced watchlist configured.	
Reports	on the console where the alert	s are imported.	
O Behavior Correlation			
	Source :		
	E:\NetS_Projects\F5 BIG IP	LTM\KP Items - New\Alerts_F5 BIG IP LTM.isalt	
		Import	e

Figure 21

2. Navigate to the location having a file with the extension ".isalt" and then click "Import" button.

Token Template

1. Click **Parsing Rules** under the **Admin** option in the EventTracker manager page.





2. Next, click the "Template" tab and then click the "Import Configuration" button.



Parsing Rules	5			
Parsing Rule	Template			
Groups			+ **	Group :
Default			A	
Azure Intune		Ē	0	Templa



†	/ Admin / Parsing Rules
	C 1 I
Active	Import configuration

Figure 24

3. Now, click "**Browse**" button and navigate to the folder where ".ettd" file is located. Wait for few seconds, as templates will be loaded. Once you see the templates, click desired templates and click "Import" button:

Iı	Import								
	selec	ted file is: Token_Template_F5 BIG IP LTM.ettd		1 🖙 Browse 📮 2					
		Template name	Separator	Template description					
		F5 BIG IP LTM SSL Events	\n	Apr 26 05:34:48 10.151.37.26 Apr 26 04:34:48 CH-BIG-IP- 1[21425]: 01260013:4: SSL Handshake failed for TCP 208. -> 10.151.100.100:993					
		F5 BIG IP LTM Traffic Management	\n	Oct 20 15:12:40 192.168.1.64 Oct 20 02:42:40 BIG notice i 70417:5: AUDIT - user admin - transaction #139343-3 - o ete { ltcfg_instance { ltcfg_instance_name "/Common/rem stance_class_name "remoterole" ltcfg_instance_instance_ ommon" ltcfg_instance_instance_leaf_name "remoterole"					

Figure 25



Knowledge Object

1. Click **Knowledge objects** under the **Admin** option in the EventTracker manager page.

		🔎 🛛 Admin -	Tools 🕶 📀
Active Watch Lists	Event Filters	🧭 Parsing Rules	🔒 / Da
Alerts	Second Eventvault	Report Settings	
Behavior Correlation Rules	FAQ Tile Configuration	Systems	
🗞 Behavior Correlation Settings	Group Management	Q Users	
mi pr sc 🚺 Casebook Configuration	Q IP Lookup Configuration	T Weights	since the last 24 hours
Category	·☆· Knowledge Objects	Windows Agent Config	
Diagnostics	Manager		



2. Next, click the "import object" icon:



Figure 27

3. A pop-up box will appear, click "**Browse**" in that and navigate to the file path with the extension ".etko" and then click "upload button":

Import	
KO_F5 BIG IP LTM.etko	1 Growse 2

Figure 28

4. A list of available Knowledge objects will appear. Select the relevant files and click the "**Import**" button.



Import			×
Select file			Frowse Upload
	Object name	Applies to	Group name
	F5 BIG IP	F5 BIG IP	F5 BIG IP
			Import Close

Figure 29

Flex Reports

1. In EventTracker control panel, select "Export/ Import utility" and select the "Import tab". Then, click Reports option, and choose "New (*.etcrx)":

💺 Export Import Utility		_		×
Export Import				
1. Provide the path and file (2. Click the Import button Note : If report(s) contains te	name of Schedule Report file. Use the '' button to browse and locate the import file. mplate, first import template and proceed with exportimport utility.			
Options	Location			
Category				
⊖ Filters				
◯ Alerts	 Legacy (*.issch) New (*.etcrx) 			
O Systems and Groups	Source : *Jssch			
O Token Value				
Reports				
Behavior Correlation				
	Impo	t	Clos	e

Figure 30



- 2. Once you have selected "New (*.etcrx)", a new pop-up window will appear. Click "Select File" button and navigate to the file path with a file having extension ".etcrx".
- 3. Select all the relevant files and then click **Import** button.

£	🚼 Reports Import									
	Note : If report(s) contains template, first import template and proceed with report import process.									
	Select file E:\NetS_Projects\F5 BIG IP LTM\KP Items - New\Reports_F5 BIG IP LTM.etcrx Select file									
Г	Availa	ble repo	ts							
١.	Title			Frequency Show all	- Q Q					
			Title	Sites	Groups	Systems	Frequency			
		EDIT	F5 BIG IP GTM Reports	NTPLDTBLR48	Default	WIN-F5-BIG-IP	Undefined			
		<u>EDIT</u>	F5 BIG IP LTM Login and Logout Rep	NTPLDTBLR48	Default	WIN-F5-BIG-IP	Undefined			
		<u>EDIT</u>	F5 BIG IP LTM Login Failed Reports	NTPLDTBLR48	Default	WIN-F5-BIG-IP	Undefined			
		<u>EDIT</u>	F5 BIG IP LTM SSL Activity	NTPLDTBLR48	Default	WIN-F5-BIG-IP	Undefined			
I		<u>EDIT</u>	F5 BIG IP LTM Traffic Management R	NTPLDTBLR48	Default	WIN-F5-BIG-IP	Undefined			







EventTracker displays a success message:



Figure 33

Dashboard

- 1. Logon to EventTracker Enterprise.
- 2. Navigate to **Dashboard** \rightarrow **My Dashboard**.





3. In "My Dashboard", click Import Button:





4. Select the **Browse** button and navigate to file path where dashboard file is saved.





- 5. Once completed, click "**Upload**" button.
- 6. Next, select all the relevant dashboards for F5 BIG-IP and click "**Import**" button.





Figure 37

Verify F5 BIG-IP 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 **F5 BIG-IP LTM** group folder to view the imported categories:





Figure 38

Alerts

- 1. In the EventTracker Enterprise web interface, click the Admin dropdown, and then click Alerts.
- 2. In search box enter **F5 BIG-IP** and then click the **Search** button. EventTracker displays alert of **F5 BIG-IP**.

Alerts							🔶 / Admin / Alerts
Show All					Search by	Alert name 🔻	F5 BIG IP 🔍 🍳
117 Available Alerts Total number of alerts available	26 Active Alerts Total number of active alerts		117 System/Use Count for system	System User r Defined Alerts a and user defined ali	105 12 serts	117 Alerts by Count of aler	Critical 10 High 68 Medium 19 Serious 16 Threat Level ts by threat level
Activate Now Click 'Activate Now	w' after making all changes						Total: 1 Page Size 25 V
Alert Name A	Threat	Active E-mail	Forward as SNMP	Forward as Syslog	Remedial Action at Console	Remedial Action at Agent	Applies To
🔲 🙀 F5 BIG IP Login Failed	•						F5 BIP IP v11.x and above





Token Template

- 1. In the **EventTracker Enterprise** web interface, click the **Admin** dropdown, and then click **Template**.
- 2. On the **Template** tab, click on the **F5 BIG-IP LTM** group folder to view the imported Token Templates.

Parsing Rules							
Parsing Rule Template							
Groups		(+)	Group : F5 BIG IP LTM				
Default		-					
Azure Intune	Ī	0	Template Name				
Cisco		0	F5 BIG IP LTM SSL Events				
EventTracker		0	F5 BIG IP LTM Traffic				
F5 BIG IP		0	Management				
F5 BIG IP LTM	Ī	0	F5 BIG IP LTM: GTM Activities				
JumpCloud		1	F5 BIG IP LTM: Login and				
McAfee ePO		0	Logout				
Figure 40							

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 **F5 BIG-IP LTM** group folder to view the imported Knowledge objects.



Event Tracker #				
Knowledge Objects				
Search objects	Q Q Activate Now			
Groups	Object name F5 BIG IP GTM Activity Applies to F5 BIG IP LTM			
F5 BIG IP GTM Activity F5 BIG IP LTM Login Fail F5 BIG IP LTM Login Lo F5 BIG IP LTM Login Lo F5 BIG IP LTM Session A F5 BIG IP LTM SSL Activit	Rules			
	Title			
	F5 BIG IP GTM Activity			
F5 BIG IP LTM Traffic M., Ø	Message Signature: CH\-BIG\-IP\-			
	Message Exception:			

Figure 41

Flex Reports

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



- 2. In **Reports Configuration** pane, select the **Defined** option.
- 3. Click on the F5 BIG-IP LTM group folder to view the imported F5 BIG-IP LTM reports.



Report Configuration							
Scheduled Queued Optimed							
Report Groups		+	Reports configuration: F5 BIG IP LTM				
f: Security			Ð	Ē 2 ,	•		
🕄 Compliance					Title		
Coperations				£ 3 5	F5 BIG IP LTM Traffic Management Reports		
{} Flex				2	F5 BIG IP LTM SSL Activity		
Azure Intune		0		£3	F5 BIG IP LTM Login and Logout Reports		
Cisco		0		213	F5 BIG IP LTM Login Failed Reports		
EventTracker		1	_	~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~	E5 BIG IP GTM Reports		
🕞 🛛 F5 BIG IP LTM	Ē	0		52	is seen or mapping		
F5 BIG IP Test		0					

Figure 43

Dashboard

1. In the EventTracker Enterprise web interface, click on Home Button and select "My Dashboard"





2. In "F5 BIG-IP" dashboard you should be now able to see something like this:





Figure 45

