# Common Event Format Configuration Guide

**F5 Networks**
**BIG-IP Application Security Manager (ASM)**
**Date:** Friday, May 27, 2011

ArcSight An HP Company
CERTIFIED **CEF**
COMPLIANT

**CEF Connector Configuration Guide**

This document is provided for informational purposes only, and the information herein is subject to change without notice. Please report any errors herein to ArcSight, LLC. ArcSight does not provide any warranties covering this information and specifically disclaims any liability in connection with this document.

**Certified CEF Compatible:**

The event format complies with the requirements of the ArcSight Common Event Format. The ArcSight CEF connector will be able to process the events correctly and the events will be available for use within ArcSight products.

**Certified CEF Compliant:**

The event format complies with the requirements of the ArcSight Common Event Format. The ArcSight CEF connector will be able to process the events correctly and the events will be available for use within ArcSight products. In addition, the event content has been deemed to be in accordance with standard SmartConnector requirements. The events will be sufficiently categorized to be used in correlation rules, reports and dashboards as a proof-of-concept (POC) of the joint solution

**CEF Connector Configuration Guide**

**F5 BIG-IP Application Security Manager**

**January 10, 2011**

## Revision History

| Date | Description |
|---|---|
| 01/14/2011 | First edition of this Configuration Guide. |
| 03/28/2011 | Sample Reports added to Configuration Guide |
| 05/26/2011 | Big IP Application Security Manger 10.1 Certified CEF Compliant. |

# F5 BIG-IP ASM Configuration Guide

This guide provides information for configuring the F5 BIG-IP Application Security Manager (ASM) to collect syslog events that is based on ArcSight Common Event Format. This document describes the field mappings for the following types of events from F5 BIG-IP Application Security Manager (ASM) messages:

- Anomaly Detection messages
- BF (expand) Attack messages
- Web Scraping Attack messages
- IP Enforcer messages

It also provides the sample content packages for the F5 Dashboard and Reports. This Syslog Connector is supported on [Windows, Linux, and Solaris] platforms. Device versions v10.1 thru v10.1 are supported

## Overview

F5 BIG-IP ASM is an advanced web application firewall that protects critical applications and their data by defending against application-specific attacks that bypass conventional firewalls.

## Configuration

### Configuring a logging profile if using ArcSight logs

If your network uses ArcSight™ logs, you can configure a logging profile that formats the log information for that system. Application Security Manager stores all logs on a remote logging server using the predefined ArcSight settings for the logs.

The log messages are in Common Event Format (CEF). The basic format is:

**CEF:Version|Device Vendor|Device Product|Device Version|Device Event Class ID|Name|Severity|Extension**

**Note**

*This logging profile relies on external systems to perform the actual logging. The configuration and maintenance of the external logging servers is not the responsibility of F5 Networks.*

**To create a logging profile for ArcSight logs**

1. In the navigation pane, expand **Application Security**, point to **Options**, and then click **Logging Profiles**.

The Logging Profiles screen opens.

2. Above the Logging Profiles area, click the **Create** button.

The Create New Logging Profile screen opens.

3. For the **Configuration** setting, select **Advanced**.

The screen refreshes to display additional settings.

4. For the **Profile Name** setting, type a unique name for the logging profile.

5. Check the **Remote Storage** box, and for the **Type** setting, select **ArcSight**.

The screen displays additional settings.

6. If you do not want data logged locally as well as remotely, click to clear the **Local Storage** check box.

7. For the **Protocol** setting, select the protocol that the reporting server uses: **TCP** (the default setting), **UDP**, or **TCP-RFC3195**.

8. For the **Server IP** setting, type the IP address of the remote storage server.

9. For the **Server Port** setting, type a port number or use the default value, **514**.

10. To ensure that the system logs requests for the web application, even when the logging utility is competing for system resources, check the **Guarantee Logging** box.

***Note**: Enabling this setting may slow access to the associated web application.*

11. Optionally, adjust the maximum request, header, and query string size and maximum entry length settings. (Refer to online help for details on the settings.)

12. If you want the system to log details (including the start and end time, number of dropped requests, attacking IP addresses, and so on) about brute force attacks, DoS attacks, IP enforcer attacks, or web scraping attacks, check the **Report Detected Anomalies** box.

13. In the Storage Filter area, make any changes as required. (See *Configuring the storage filter*, following, for details.)

14. Click the **Create** button.

The screen refreshes, and displays the new logging profile.

## Configuring the storage filter

The storage filter of a logging profile determines the type of requests the system or server logs.

**Note**

*The following procedure describes configuring the storage filter for an existing logging profile.*

**To configure the storage filter**

1. In the navigation pane, expand **Application Security**, point to **Options**, and then click **Logging Profiles**.

The Logging Profiles screen opens.

2. In the Logging Profiles area, click the name of an existing logging profile.

The Edit Logging Profile screen opens.

3. For the **Storage Filter** setting, select **Advanced**.

The screen refreshes to display additional settings.

4. For the **Logic Operation** setting, select the manner in which the system associates the criteria you specify. The criteria are the remaining settings in the storage filter.

• **OR**: Select this operator if you want the system to log the data that meets one or more of the criteria.

• **AND**: Select this operator if you want the system to log the data that meets all of the criteria.

5. For the **Request Type** setting, select the kind of requests that you want the system to store in the log.

6. For the **Protocols** setting, select whether logging occurs for HTTP and HTTPS protocols or a specific protocol.

7. For the **Response Status Codes** setting, select whether logging occurs for all response status codes or specific ones.

8. For the **HTTP Methods** setting, select whether logging occurs for all methods or specific methods.

9. For the **Request Containing String** setting, select whether the request logging is dependent on a specific string.

10. Click the **Update** button.

The screen refreshes, and displays the new logging profile on the Logging Profiles screen.

## Setting event severity levels for security policy violations

You can customize the severity levels of security policy violations for application security events that are displayed on the Security Alerts screen, in the request details, and also in the messages logged by the **syslog** utility.

The event severity levels are **Informational**, **Notice**, **Warning**, **Error**, **Critical**, **Alert**, and **Emergency**. They range from least severe (**Informational**) to most severe (**Emergency**).

For more information on how BIG-IP systems use the **syslog** utility, refer to the *Logging BIG-IP System Events* chapter in the ***TMOS® Management Guide for BIG-IP® Systems***.

**Note**

*When you make changes to the event severity level for security policy violations, the changes apply globally to* ***all*** *web applications.*

**To customize event severity level for security policy violations**

1. In the navigation pane, expand **Application Security**, point to **Options**, and then click **Severities**.

The Severities screen opens.

2. For each violation, change the severity level as required.

3. Click the **Save** button to retain any changes.

**Tip**

*If you modify the event severity levels for any of the security policy violations, and later decide you want to use the system-supplied default values instead, click the* ***Restore Defaults*** *button.*

### Specifying the logging profile for a web application

1. In the navigation pane, expand **Application Security** and click **Web Applications**.

The Web Application List screen opens.

2. In the Name column, click a web application name.

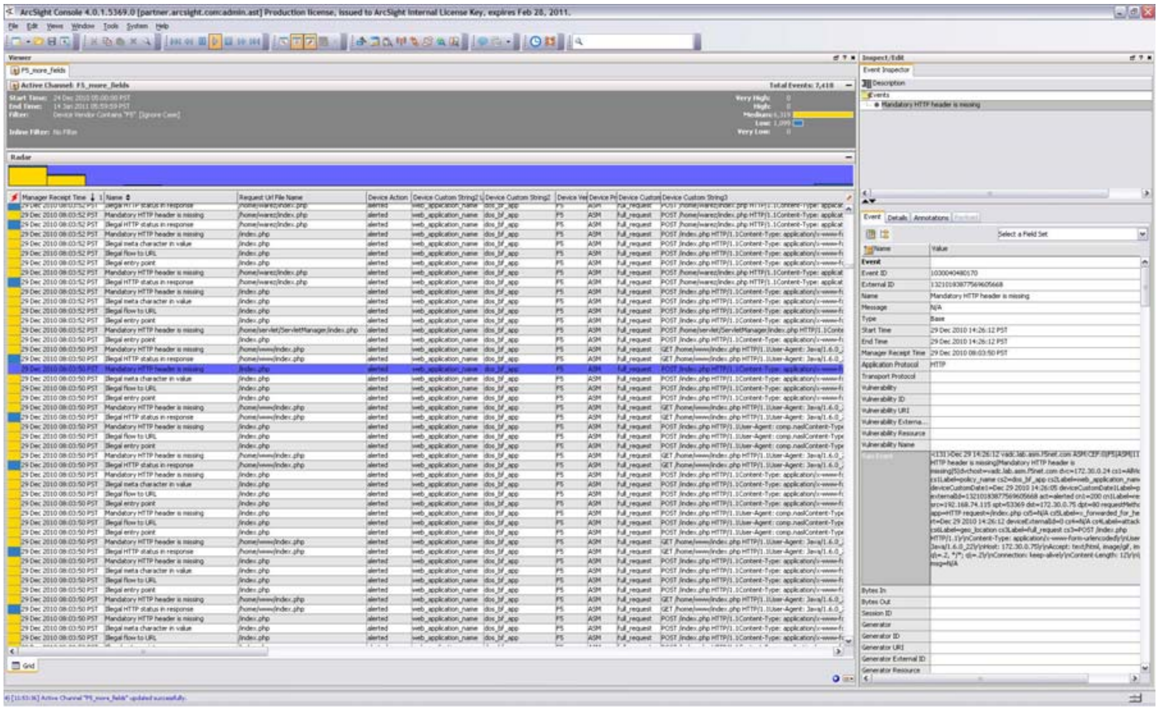
The Web Application Properties screen opens.

3. For the **Logging Profile** setting, select a logging profile.

4. Click the **Update** button.

The system updates the configuration with any changes you may have made.

## Screen Shot



ArcSight Console 4.0.1.5369.0 [partner.arcsight.com:admin.ast] Production license, issued to ArcSight Internal License Key, expires Feb 28, 2011.

Active Channel: F5_more_fields

Start Time: 24 Dec 2010 05:00:00 PST
End Time: 14 Jan 2011 05:59:59 PST
Filter: Device Vendor Contains "F5" [Ignore Case]

Inline Filter: No Filter

Total Events: 7,418

| Name | Value |
|---|---|
| Event | |
| Event ID | 1030040480170 |
| External ID | 13210183877569605668 |
| Name | Mandatory HTTP header is missing |
| Message | N/A |
| Type | Base |
| Start Time | 29 Dec 2010 14:26:12 PST |
| End Time | 29 Dec 2010 14:26:12 PST |
| Manager Receipt Time | 29 Dec 2010 08:03:50 PST |
| Application Protocol | HTTP |
| Transport Protocol | |
| Vulnerability | |
| Vulnerability ID | |
| Vulnerability URI | |
| Vulnerability Externa... | |
| Vulnerability Resource | |
| Vulnerability Name | |
| | <131>Dec 29 14:26:12 vadc.lab.asm.f5net.com ASM:CEF:0\|F5\|ASM\|11... HTTP header is missing\|Mandatory HTTP header is missing\|5\|dvchost=vadc.lab.asm.f5net.com dvc=172.30.0.24 cs1=... cs1Label=policy_name cs2=dos_bf_app cs2Label=web_application_name deviceCustomDate1=Dec 29 2010 14:26:05 deviceCustomDate1Label=... externalId=13210183877569605668 act=alerted cn1=200 cn1Label=... src=192.168.74.115 spt=53369 dst=172.30.0.75 dpt=80 requestMetho... app=HTTP request=/index.php cs5=N/A cs5Label=x_forwarded_for_he... rt=Dec 29 2010 14:26:12 deviceExternalId=0 cs4=N/A cs4Label=attack... cs6Label=geo_location cs3Label=full_request cs3=POST /index.php HTTP/1.1\r\nContent-Type: application/x-www-form-urlencoded\r\nUser... Java/1.6.0_22\r\nHost: 172.30.0.75\r\nAccept: text/html, image/gif, im... q=.2, */*; q=.2\r\nConnection: keep-alive\r\nContent-Length: 12\r\n... msg=N/A |
| Bytes In | |
| Bytes Out | |
| Session ID | |
| Generator | |
| Generator ID | |
| Generator URI | |
| Generator External ID | |
| Generator Resource | |

# Events

## ASM Remote Log Messages

### General enforcement samples

### Typical Violation is triggered

```
Sep  2 17:50:25 172.30.0.130 ASM:CEF:0|F5|ASM|10.1.0|Illegal query string
length|Illegal query string length|6|dvchost=3600.lab.asm.f5net.com
dvc=172.30.0.20 cs1=new_app_default cs1Label=policy_name cs2=new_app
cs2Label=web_application_name deviceCustomDate1=Sep 02 2009 15:09:20
deviceCustomDate1Label=policy_apply_date externalId=416829024209663345
act=alerted cn1=200 cn1Label=response_code src=172.30.0.126 spt=37446
dst=172.30.0.32 dpt=80 requestMethod=GET app=HTTP
request=/phpauction/search.php?\=&q\=%3Cscript%3E%3C%2Fscript%3E&\=Go%21 cs5=
cs5Label=x_forwarded_for_header_value rt=Sep 02 2009 17:09:25
deviceExternalId=0 cs4=Buffer Overflow cs4Label=attack_type cs6=N/A
cs6Label=geo_location cs3Label=full_request cs3=GET
/phpauction/search.php?\=&q\=%3Cscript%3E%3C%2Fscript%3E&\=Go%21
HTTP/1.1\r\nHost: 172.30.0.32\r\nUser-Agent: Mozilla/5.0 (X11; U; Linux i686
(x86_64); en-US; rv:1.8.1) Gecko/20061023 SUSE/2.0-30 Firefox/2.0\r\nAccept:
text/xml,application/xml,application/xhtml+xml,text/html;q\=0.9,text/plain;q\=0
.8,image/png,*/*;q\=0.5\r\nAccept-Language: en-us,en;q\=0.5\r\nAccept-Encoding:
gzip,deflate\r\nAccept-Charset: ISO-8859-1,utf-8;q\=0.7,*;q\=0.7\r\nKeep-Alive:
300\r\nConnection: keep-alive\r\nReferer:
http://172.30.0.32/phpauction/help.php?\r\nCookie:
PHPAUCTION_SESSION\=lhuqakkdn6icm9vv33p9nepcm0lga6rd;
TS2ea638\=1c1e60b9764bace0c13f1829c93d009ec4b6e3e4598e3bb14a9f12c67b46979e7faa5
254\r\n\r\n
```

### Attack Signature is triggered

```
Sep  3 16:06:16 172.30.0.20 ASM:CEF:0|F5|ASM|11.0.0|200000098|XSS script tag
(Parameter)|5|dvchost=3600.lab.asm.f5net.com dvc=172.30.0.20
cs1=maui_app_default cs1Label=policy_name cs2=maui_app
cs2Label=web_application_name deviceCustomDate1=Sep 03 2010 15:56:49
deviceCustomDate1Label=policy_apply_date externalId=2922246059721752663
act=alerted cn1=200 cn1Label=response_code src=192.168.74.216 spt=52793
dst=172.30.0.30 dpt=80 requestMethod=GET app=HTTP
request=/xss/xss.php?param\=<script cs5=N/A
cs5Label=x_forwarded_for_header_value rt=Sep 03 2010 16:06:15
deviceExternalId=0 cs4=Cross Site Scripting (XSS) cs4Label=attack_type cs6=N/A
cs6Label=geo_location cs3Label=full_request cs3=GET /xss/xss.php?param\=<script
HTTP/1.1\r\nAccept: */*\r\nAccept-Language: en-US\r\nUser-Agent: Mozilla/4.0
(compatible; MSIE 8.0; Windows NT 6.1; WOW64; Trident/4.0; SLCC2; .NET CLR
2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729; Media Center PC 6.0;
InfoPath.2; MS-RTC LM 8)\r\nAccept-Encoding: gzip, deflate\r\nHost:
172.30.0.30\r\nConnection: Keep-Alive\r\nCookie:
Super_Secret_Session_Cookie\=123456789;
TS49b723\=5dc5319219c48503ae788c666bc08a1fbf81f2c754f2bc3b4c817eec\r\n\r\n
```

**Fields description**

Prefix:

**CEF:Version|DeviceVendor|DeviceProduct|DeviceVersion|deviceEventClassId|ViolationName|Severity|**

**NOTE: we duplicate violation name in deviceEventClassId field in case of general violations and we put ASM internal signature ID to this field in case an Attack Signature was triggered.**

**IMPORTANT: A single CEF format log message is generated for every security event (violation)**

| CEF format field name | Meaning |
|---|---|
| dvchost | Host name of the BIG-IP machine |
| dvc | IP of the management interface of the BIG-IP machine |
| externalId | Unique id given for a blocked transaction |
| act | Action performed on a transaction: blocked, alerted |
| src | IP address of the client for ASM |
| spt | Remote port, client side |
| dst | Destination IP (Virtual Server IP of the device) |
| dpt | Local port, client side |
| requestMethod | HTTP method of the request |
| app | HTTP/HTTPS |
| request | **In case of CEF format**: the full URL, URI +QS of the HTTP request<br>**In case of key/value format:** uri without the query string |
| deviceExternalId | ID of the blade receiving the traffic when using the VIPRION hardware |
| rt | Timestamp of the transaction |

| CEF key name | Meaning |
|---|---|
| cs1 | Name of the security policy |
| cs2 | Web application name for ASM |
| cs3 | Full request |
| cs4 | Attack Type |
| cs5 | IP or domain name of clients going via proxies |
| cs6 | A string indicating the geographic location from which the request has arrived |
| cn1 | HTTP response code |
| deviceCustomDate1 | Timestamp of the last time the policy was applied |

## Anomaly detection features format

### DoS Attack message sample

```
Sep 10 15:19:01 172.30.0.20 ASM:CEF:0|F5|ASM|11.0.0|DoS Attack|URL-Based Rate
Limiting|8|dvchost=3600.lab.asm.f5net.com dvc=172.30.0.20 cs1=maui_app_default
cs1Label=policy_name cs2=maui_app cs2Label=web_application_name
deviceCustomDate1=Sep 10 2010 15:00:40 deviceCustomDate1Label=policy_apply_date
act=Blocked cn3=3263585817 cn3Label=attack_id cs4=Ongoing
cs4Label=attack_status request=/dos/dos3.php src= cs6=N/A cs6Label=geo_location
cs5=Latency Increased cs5Label=detection_mode rt=Sep 10 2010 15:19:00 cn1=21
cn1Label=detection_average cn2=20665 cn2Label=dropped_requests
```

**Field description**

**CEF:Version|DeviceVendor|DeviceProduct|DeviceVersion|AttackType|MitigationType|Severity|**

**AttackType** can be one of: **DoS Attack**, Brute Force Attack, IP Enforcer Attack or Web Scraping Attack

**MitigationType** can be one of: **Source IP-Based Client Side Integrity Defense, URL-Based Client Side Integrity Defense, Source IP-Based Rate Limiting, URL-Based Rate Limiting** or **Transparent**

| **CEF key name** | **Meaning** |
|---|---|
| dvchost | Host name of the BIG-IP machine |
| dvc | IP of the management interface of the BIG-IP machine |
| act | Action performed on a transaction: blocked, alerted or passed |
| request | The URI |
| src | IP address of the client for ASM |
| rt | Timestamp of the transaction |

| **CEF key name** | **Meaning** |
|---|---|
| cs1 | Name of the security policy |
| cs2 | Web application name for ASM |
| cs4 | Attack status: Can be one of the following: **Started, Ongoing** and **Ended** |
| cs5 | Reason for attack detection. Can either be **Latency Increased** or **TPS Increased** |
| cn1 | Detected anomaly in ms in case of Latency Increased, in TPS in case of TPS increased |
| cn2 | Dropped request counter. Each consequent request will report deltas: how many requests were dropped since the last log message for a given attack. |
| cn3 | Attack ID |
| deviceCustomDate1 | Timestamp of the last time the policy was applied |
| cs6 | A string indicating the geographic location from which the request has arrived |

## BF Attack message sample

```
Sep 11 00:12:00 172.30.0.20 ASM:CEF:0|F5|ASM|11.0.0|Brute Force
Attack|Transparent|8|dvchost=3600.lab.asm.f5net.com dvc=172.30.0.20
cs1=maui_app_default cs1Label=policy_name cs2=maui_app
cs2Label=web_application_name deviceCustomDate1=Sep 11 2010 00:05:11
deviceCustomDate1Label=policy_apply_date act=Alerted cn3=3263585820
cn3Label=attack_id cs4=Ongoing cs4Label=attack_status request=/bf/login1.php
src=120.20.20.120 cs6=AU cs6Label=geo_location cs5=Number of Failed Logins
Increased cs5Label=detection_mode rt=Sep 11 2010 00:12:00 cn1=109
cn1Label=detection_average cn2=0 cn2Label=dropped_requests
```

**Field description**

**Field description**

**CEF:Version|DeviceVendor|DeviceProduct|DeviceVersion|AttackType|**
**MitigationType|Severity|**

**AttackType** can be one of: **DoS Attack**, Brute Force Attack, IP Enforcer Attack or Web Scraping Attack

**MitigationType** can be one of: **Source IP-Based Client Side Integrity Defense, URL-Based Client Side Integrity Defense, Source IP-Based Rate Limiting, URL-Based Rate Limiting** or **Transparent**

| CEF key name | Meaning |
|---|---|
| dvchost | Host name of the BIG-IP machine |
| dvc | IP of the management interface of the BIG-IP machine |
| act | Action performed on a transaction: blocked, alerted or passed |
| request | The URI |
| src | IP address of the client for ASM |
| rt | Timestamp of the transaction |

| CEF key name | Meaning |
|---|---|
| cs1 | Name of the security policy |
| cs2 | Web application name for ASM |
| cs4 | Attack status: Can be one of the following: **Started, Ongoing** and **Ended** |
| cs5 | Reason for attack detection |
| cn1 | Detected anomaly. Number of failed login attempts |
| cn2 | Dropped request counter. Each consequent request will report deltas: how many requests were dropped since the last log message for a given attack. |
| cn3 | Attack ID |
| deviceCustomDate1 | Timestamp of the last time the policy was applied |
| cs6 | A string indicating the geographic location from which the request has arrived |

## Web Scraping Attack message sample

```
Sep 10 16:03:01 172.30.0.20 ASM:CEF:0|F5|ASM|11.0.0|Web Scraping Attack|Web
Scraping Attack|8|dvchost=3600.lab.asm.f5net.com dvc=172.30.0.20
cs1=maui_app_default cs1Label=policy_name cs2=maui_app
cs2Label=web_application_name deviceCustomDate1=Sep 10 2010 15:58:23
deviceCustomDate1Label=policy_apply_date act=Blocked cn3=3263585818
cn3Label=attack_id cs4=Ongoing cs4Label=attack_status src=192.168.74.216 cs6=N/A
cs6Label=geo_location rt=Sep 10 2010 16:03:00 cn2=0 cn2Label=dropped_requests
cnt=0
```

**Field description**

**CEF:Version|DeviceVendor|DeviceProduct|DeviceVersion|AttackType|AttackType|Severity|**

**AttackType** can be one of: DoS Attack, Brute Force Attack, IP Enforcer Attack or **Web Scraping Attack**

| CEF key name | Meaning |
|---|---|
| dvchost | Host name of the BIG-IP machine |
| Dvc | IP of the management interface of the BIG-IP machine |

| | |
|---|---|
| Act | Action performed on a transaction: blocked, alerted |
| request | The URI |
| Src | IP address of the client for ASM |
| Rt | Timestamp of the transaction |

| CEF key name | Meaning |
|---|---|
| cs1 | Name of the security policy |
| cs2 | Web application name for ASM |
| cs4 | Attack status: Can be one of the following: **Started, Ongoing** and **Ended** |
| cs6 | A string indicating the geographic location from which the request has arrived |
| cn2 | Dropped requests counter. Each consequent request will report deltas: showing how many requests were dropped since the last log message for a given attack. Reported in case a bot is detected. |
| cn3 | Attack ID |
| flexNumber1 | Blocked requests counter. Each consequent request will report deltas: showing how many requests were blocked since the last log message for a given attack. |
| deviceCustomDate1 | Timestamp of the last time the policy was applied |

## IP Enforcer

```
Sep 10 23:54:51 172.30.0.20 ASM:CEF:0|F5|ASM|11.0.0|IP Enforcer Attack|IP
Enforcer Attack|8|dvchost=3600.lab.asm.f5net.com dvc=172.30.0.20
cs1=maui_app_default cs1Label=policy_name cs2=maui_app
cs2Label=web_application_name deviceCustomDate1=Sep 10 2010 23:52:32
deviceCustomDate1Label=policy_apply_date act=Blocked cn3=18446744072678170139
cn3Label=attack_id cs4=Ended cs4Label=attack_status src=192.168.74.169 cs6=N/A
cs6Label=geo_location cn2=0 cn2Label=dropped_requests rt=Sep 10 2010 23:54:50
```

**Field description**

**CEF:Version|DeviceVendor|DeviceProduct|DeviceVersion|AttackType|AttackType|Severity|**

**AttackType** can be one of: DoS Attack, Brute Force Attack, **IP Enforcer Attack** or Web Scraping Attack

| CEF key name | Meaning |
|---|---|
| dvchost | Host name of the BIG-IP machine |
| dvc | IP of the management interface of the BIG-IP machine |
| act | Action performed on a transaction: blocked, alerted |
| request | The URI |
| src | IP address of the client for ASM |
| rt | Timestamp of the transaction |

| CEF key name | Meaning |
|---|---|

| | |
|---|---|
| cs1 | Name of the security policy |
| cs2 | Web application name for ASM |
| cs4 | Attack status: Can be one of the following: **Started, Ongoing** and **Ended** |
| cn2 | Dropped request counter. Each consequent request will report deltas: how many requests were dropped since the last log message for a given attack. |
| cn3 | Attack ID |
| deviceCustomDate1 | Timestamp of the last time the policy was applied |
| cs6 | A string indicating the geographic location from which the request has arrived |

# Device Event Mapping to ArcSight Data Fields

Information contained within vendor-specific event definitions is sent to the ArcSight SmartConnector, then mapped to an ArcSight data field.

The following table lists the mappings from ArcSight data fields to the supported vendor-specific event definitions.

### F5 BIG-IP ASM Connector Field Mappings

| Vendor-Specific Event Definition | ArcSight Event Data Field |
|---|---|
| unit_hostname | dvchost |
| Management_ip_address | deviceTranslatedAddress |
| support_id | externalId |
| request_status | act |
| ip_client | src |
| source_port | spt |
| destination_port | dpt |
| method | requestMethod |
| protocol | app |
| Uri | request |
| slot_number | deviceExternlId |
| date_time | rt |
| server_ip | dst |
| web_application_name | cs2 |
| vs_name | cs2 |
| policy_name | cs1 |
| request | cs3 |
| x_forward_for_header_value | cs5 |

| Vendor-Specific Event Definition | ArcSight Event Data Field |
|---|---|
| attack_type | cs4 |
| response_code | cn1 |
| policy_apply_date | deviceCustomDate1 |
| geo_location | cs6 |

# F5 *“Sample Content”* Reporting Package

As part of the integration effort between ArcSight and F5, a small reporting package was developed for use in ArcSight ESM to provide some sample functionality. The following section outlines how to install the package and its contents.

**Note:**

*This content package was developed as a sample proof of concept to demonstrate functionality with the ArcSight – F5 integration. The content is not supported by ArcSight and is not delivered as part of any officially released product. You can access and download this content as a member of Protect 724 or from F5’s Dev Central.*

## Installing a Content Package in ArcSight ESM

1 Log into the ArcSight ESM Console with an account that has administrative privileges.

**2** Click the **Packages** tab in the Navigator panel.

**3** Click **Import** ( ).

**4** In the Open dialog, browse and select the package bundle file and select **Open**.

The progress of the import of the package bundle is displayed in the Progress tab of the Importing Packages dialog.

**5** When the import is complete, the Results tab of the Importing Packages dialog is displayed as well as the Packages for Installation dialog.

**6** Leave the checkbox selected, and in the Packages for Installation dialog click **Next**.

The progress of the install is displayed in the Progress tab of the Installing Packages dialog. When the install is complete, the Results tab of the Installing Packages dialog displays the Summary Report.

**7** In the Installing Packages dialog, click **OK**.

**8** In the Importing Packages dialog, click **OK**.

You should see the package now installed:

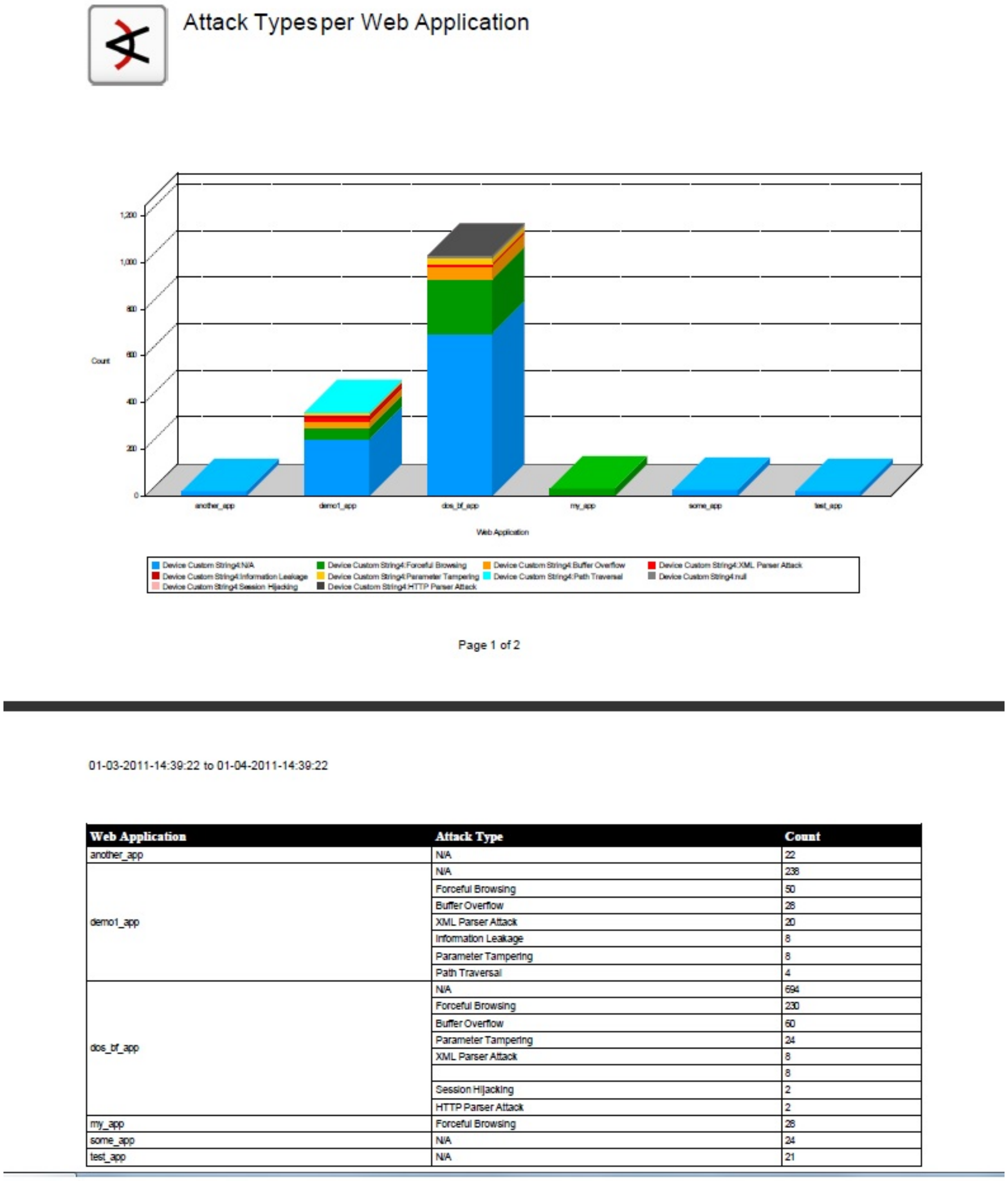
**9** To verify that the installation was successful navigate to the Resources tab of the Navigator panel and select Reports from the drop down menu. Navigate to the “ArcSight Partner Sample Content” folder and open the F5 group.

## Included Content

The following reports are included in the package:

- AlertedViolationsPerWebApp
  - Displays the violations alerted on per web application in a bar chart and table format
- AttackTypesPerWebApp
  - Displays the attacks detected per web application in a stacked bar chart and table format
- BlockedViolationsPerWebApp
  - Displays the blocked violations per web application in a stacked bar chart format
- HTTPAttackSeverityPerWebApp
  - Displays the HTTP attacks detected by their severity levels per web application in a stacked bar chart and table format
- HTTPRequestStatusPerWebApp
  - Displays the HTTP request status per web application in a line chart and table format
- TopAttackers
  - Displays the top source IP Addresses detected in a pie chart and table format

Sample Reports:



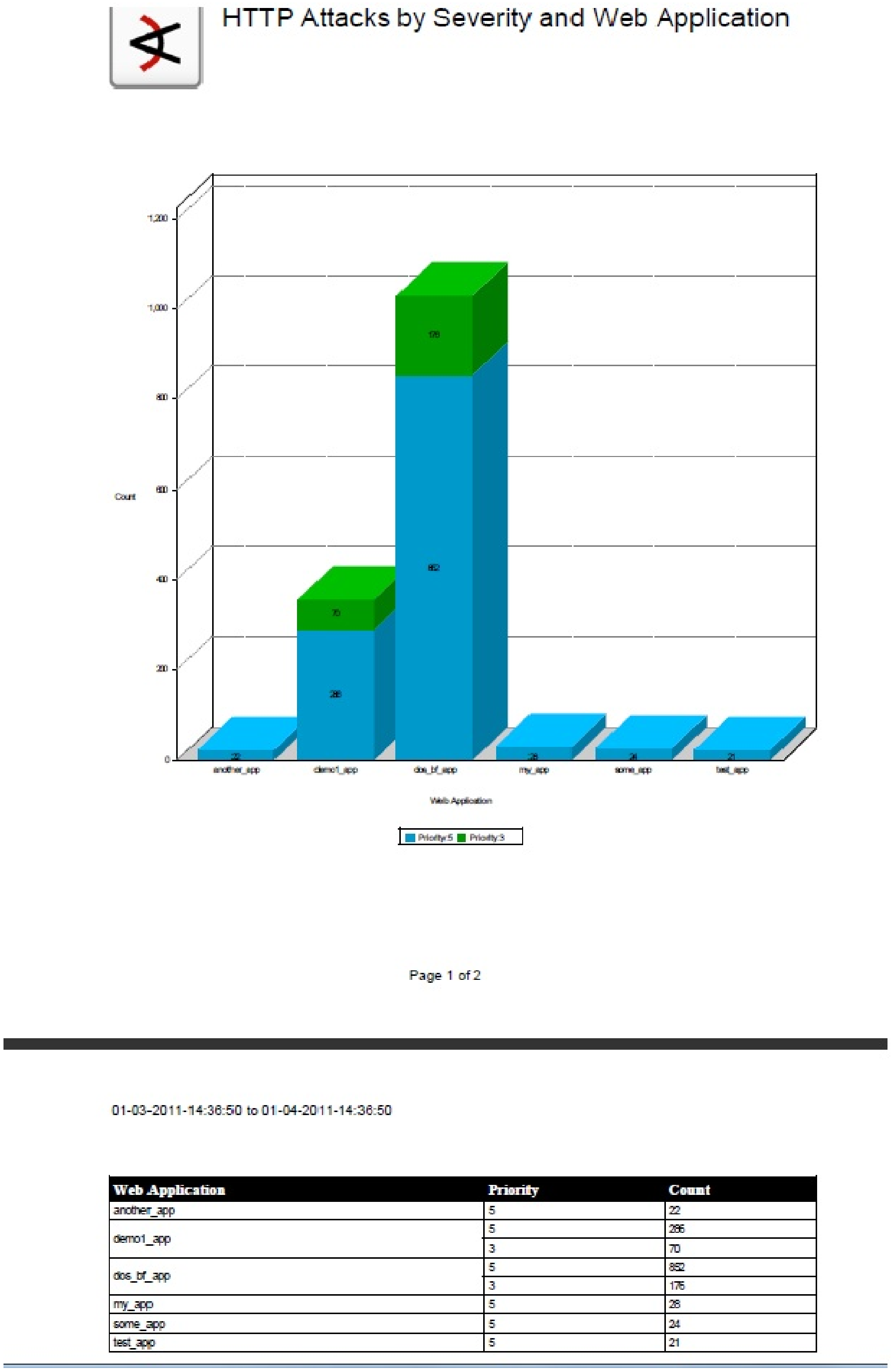
Attack Types per Web Application

1,200
1,000
800
600
400
200
0
Count
another_app
demo1_app
dos_bf_app
my_app
some_app
test_app
Web Application
🟦 Device Custom String4:N/A
🟩 Device Custom String4:Forceful Browsing
🟧 Device Custom String4:Buffer Overflow
🟥 Device Custom String4:XML Parser Attack
🟥 Device Custom String4:Information Leakage
🟨 Device Custom String4:Parameter Tampering
🟦 Device Custom String4:Path Traversal
⬛ Device Custom String4:null
🟥 Device Custom String4:Session Hijacking
⬛ Device Custom String4:HTTP Parser Attack

Page 1 of 2

01-03-2011-14:39:22 to 01-04-2011-14:39:22

| Web Application | Attack Type | Count |
|---|---|---|
| another_app | N/A | 22 |
| demo1_app | N/A | 238 |
| | Forceful Browsing | 50 |
| | Buffer Overflow | 28 |
| | XML Parser Attack | 20 |
| | Information Leakage | 8 |
| | Parameter Tampering | 8 |
| | Path Traversal | 4 |
| dos_bf_app | N/A | 694 |
| | Forceful Browsing | 230 |
| | Buffer Overflow | 60 |
| | Parameter Tampering | 24 |
| | XML Parser Attack | 8 |
| | | 8 |
| | Session Hijacking | 2 |
| | HTTP Parser Attack | 2 |
| my_app | Forceful Browsing | 28 |
| some_app | N/A | 24 |
| test_app | N/A | 21 |

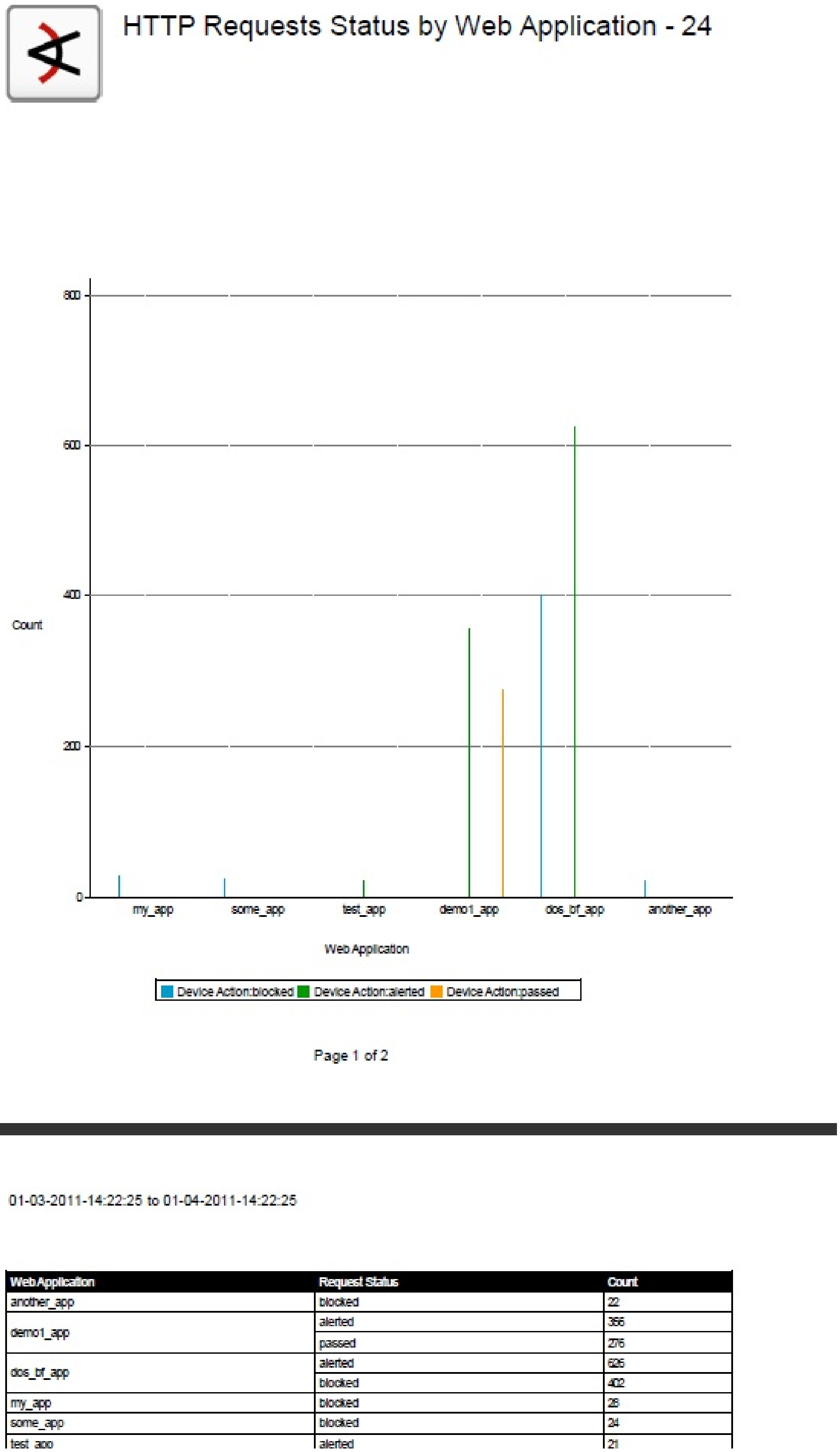


HTTP Attacks by Severity and Web Application

Page 1 of 2

01-03-2011-14:36:50 to 01-04-2011-14:36:50

| Web Application | Priority | Count |
|---|---|---|
| another_app | 5 | 22 |
| demo1_app | 5 | 286 |
|  | 3 | 70 |
| dos_bf_app | 5 | 852 |
|  | 3 | 176 |
| my_app | 5 | 28 |
| some_app | 5 | 24 |
| test_app | 5 | 21 |



HTTP Requests Status by Web Application - 24

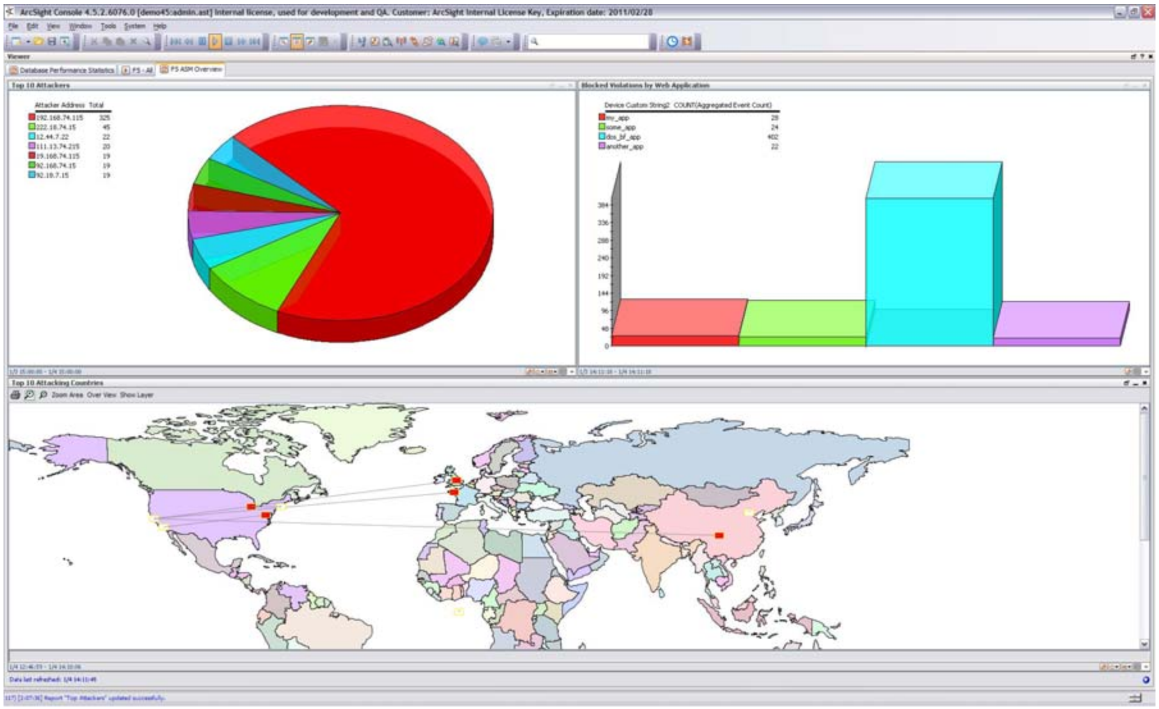
Page 1 of 2

01-03-2011-14:22:25 to 01-04-2011-14:22:25

| Web Application | Request Status | Count |
|---|---|---|
| another_app | blocked | 22 |
| demo1_app | alerted | 356 |
| | passed | 276 |
| dos_bf_app | alerted | 626 |
| | blocked | 402 |
| my_app | blocked | 28 |
| some_app | blocked | 24 |
| test_app | alerted | 21 |

The Package also includes a dashboard made of of the following Data Monitors and Query Viewers:

- Top 10 Attackers (Pie chart)
- Blocked Violations by Web Application (Bar chart)
- Top 10 Attacking Countries (Event graph)



ArcSight Console 4.5.2.6076.0 [demo45:admin.ast] Internal license, used for development and QA. Customer: ArcSight Internal License Key, Expiration date: 2011/02/28

| Attacker Address | Total |
|---|---|
| 🟥 192.168.74.115 | 325 |
| 🟩 222.18.74.15 | 45 |
| 🟦 12.44.7.22 | 22 |
| 🟪 111.13.74.215 | 20 |
| 🟥 19.168.74.115 | 19 |
| 🟩 92.168.74.15 | 19 |
| 🟦 92.18.7.15 | 19 |

| Device Custom String2 | COUNT(Aggregated Event Count) |
|---|---|
| 🟥 my_app | 28 |
| 🟩 some_app | 24 |
| 🟦 dos_bf_app | 402 |
| 🟪 another_app | 22 |

Data last refreshed: 1/4 14:11:49

117) [2:07:36] Report "Top Attackers" updated successfully.