Hewlett Packard
Enterprise

HPE Security
Fortify Runtime

Software Version: 17.3
Versions 2017.1.3 (Java) and 2017.1.3 (.NET)

Application Logging Rulepack Kit Guide

Document Release Date: April 2017
Software Release Date: April 2017

Legal Notices

Warranty

The only warranties for Hewlett Packard Enterprise Development products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. HPE shall not be liable for technical or editorial errors or omissions contained herein.

The information contained herein is subject to change without notice.

Restricted Rights Legend

Confidential computer software. Valid license from HPE required for possession, use or copying. Consistent with FAR 12.211 and 12.212, Commercial Computer Software, Computer Software Documentation, and Technical Data for Commercial Items are licensed to the U.S. Government under vendor's standard commercial license.

The software is restricted to use solely for the purpose of scanning software for security vulnerabilities that is (i) owned by you; (ii) for which you have a valid license to use; or (iii) with the explicit consent of the owner of the software to be scanned, and may not be used for any other purpose.

You shall not install or use the software on any third party or shared (hosted) server without explicit consent from the third party.

Copyright Notice

Trademark Notices

Adobe™ is a trademark of Adobe Systems Incorporated.

Microsoft® and Windows® are U.S. registered trademarks of Microsoft Corporation.

UNIX® is a registered trademark of The Open Group.

This product includes an interface of the 'zlib' general purpose compression library, which is Copyright © 1995-2002 Jean-loup Gailly and Mark Adler.

Documentation Updates

The title page of this document contains the following identifying information:

- Software Version number
- Document Release Date, which changes each time the document is updated
- Software Release Date, which indicates the release date of this version of the software

To check for recent updates or to verify that you are using the most recent edition of a document, go to:

https://www.protect724.hpe.com/community/fortify/fortify-product-documentation

You will receive updated or new editions if you subscribe to the appropriate product support service. Contact your HPE sales representative for details.

Contents

Preface

Contacting HPE Security Fortify Support

If you have questions or comments about using this product, contact HPE Security Fortify Technical Support using one of the following options.

To Manage Your Support Cases, Acquire Licenses, and Manage Your Account

https://support.fortify.com

To Email Support

fortifytechsupport@hpe.com

To Call Support

1.844.260.7219

For More Information

For more information about HPE Security software products: http://www.hpe.com/software/fortify

About the Documentation Set

The HPE Security Fortify Software documentation set contains installation, user, and deployment guides for all HPE Security Fortify Software products and components. In addition, you will find technical notes and release notes that describe new features, known issues, and last-minute updates. You can access the latest versions of these documents from the following HPE Security user community website:

https://www.protect724.hpe.com/community/fortify/fortify-product-documentation

You will need to register for an account.

Change Log

The following table lists changes made to this document. Revisions to this document are published only if the changes made affect product functionality.

Software Release / Document Version	Changes
17.3	Updated: Minor edits.
16.12	Updated: Minor edits.
16.8	Updated: Minor edits.

HPE Security Fortify Runtime Application Logging Rulepack Kit

This document describes the capabilities of Fortify Runtime Application Logging (RTAL) Rulepack Kit.

Fortify Runtime Application Logging Rulepack is a special Runtime Kit for the HPE Security Fortify Runtime platform. It provides web application internal activities to HPE Security ArcSight analysis servers so that these events can be correlated with other existing ArcSight events.

A custom configuration file is provided for which:

- Events are dispatched to syslog, and not written to local host
- System log is still logged in local host

Both Java and .NET Taint Rulepacks support the following events.

- HPE Security Fortify System Startup Message
- Web Application Start
- Web Application Stop
- HTTP Session Start
- HTTP Session Stop
- User Logon: Success
- User Logon: Failure
- User Logoff
- Database Query
- General Exception Created
- Security Exception Created (Java only)
- Crypto Exception Created (Java only)
- File Create
- File Delete
- File Read
- File Write
- Network Socket Bind
- Network Socket Connect
- Windows Registry Create (.NET only)
- Windows Registry Read (.NET only)
- Windows Registry Write (.NET only)
- Windows Registry Delete (.NET only)
- Spring/Struts/Dotnet Validation Failure
- Unified Logging: JUL (Java only)
- Unified Logging: Log4j (Java only)
- Unified Logging: JCL (Java only)
- Unified Logging: Slf4j (Java only)
- Unified Logging: NLog (.NET only)
- Unified Logging: Log4Net (.NET only)
- Unified Logging: Enterprise Library (.NET only)
- User Management: Create User
- User Management: Delete User
- User Management: Change User Password
- User Management: Create Group
- User Management: Delete Group
- User Management: Add User to Group

- Network Socket Shutdown
- Network Socket Close
- Command Execution
- User Management: Remove User from Group
- Web AccessLog

Note:

- For Security Exception Created and Crypto Exception Created Events, see General/Security/Crypto Exception Created for a full list.
- x.xx represents the current version of HPE Security Fortify Runtime in all sample Syslog messages in this document.

This section contains the following topics:

ProcessCEF Filter

A custom filter is provided to convert HPE Security Fortify Event Message to ArcSight Common Event Format (CEF).

Basics

The filter is enabled in Fortify RTAL Kit standalone_config.xml as follows:

```
...
<EventHandler propagate="true" description="Convert Fortify Event to CEF Format" label="CEF Format
Filter">
  <Match/>
  <Handle>
    <Filter name="ProcessCEF">
      ...
    </Filter>
  </Handle>
</EventHandler>
...
```

Standard CEF Format is as follows.

```
CEF:Version|Device Vendor|Device Product|Device Version|Signature
ID|Name|Severity|[Extension]
```

CEF Header Fields

The CEF Format Filter in the runtime will fill out the header fields as follows.

CEF Field Name	HPE Security Fortify Field Name
CEF:Version	CEF:0
Device Vendor	Fortify
Device Product	runtime
Device Version	x.xx (replaced by current version of HPE Security Fortify Runtime)
Signature ID	Category
Name	Category
Severity (1-10)	Priority (Critical/High/Medium/Low) Critical »10

CEF Field Name	HPE Security Fortify Field Name
	High » 7 Medium » 4 Low » 1 If this field is not defined, default to 5.

Sample Syslog message:

```
Jun 25 22:22:04 sng2 fortify_runtime: CEF:0|Fortify|runtime|x.xx|Web
Application Start|Web Application Start|1|…
```

CEF Extension Fields

In addition to the standard CEF fields, extensions can be added at the end. When available, the extensions described in the following table are added.

CEF Extension Field Name	HPE Security Fortify Field Name	Only send this to syslog if Request exists?
rt	timestamp	NO
app	request.scheme	YES
src	request.ip	YES
dhost	request.host	YES
dpt	request.port	YES
suser	request.remote_user	YES
requestMethod	request.method	YES
request	Regenerate full URL with querystring	YES
requestClientApplication	request.headers.user-agent	YES
requestCookies	request.headers.cookie	YES
msg	trigger	NO
cs2	SessionId	YES

CEF Extension Field Name	HPE Security Fortify Field Name	Only send this to syslog if Request exists?
cs3	eventType	NO

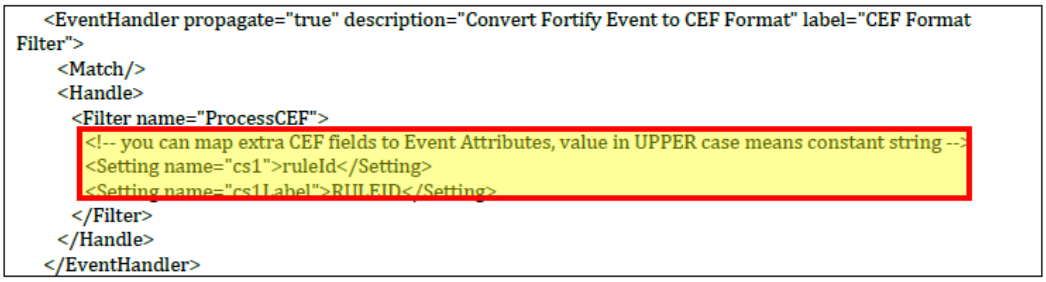
*All strings longer than 256 chars are truncated. The string length for URL is 512.

Sample Syslog message:

```
Jun 25 22:22:04 sng2 fortify_runtime: CEF:0|Fortify|runtime|4.00|Web
Application Start|Web Application Start|1|rt=1372170124737
filePath=C:\\Fortify\\apache-tomcat-6.0.20\\webapps\\riches\\ cs1=/riches
cs1Label=Application Name cs3=audit cs3Label=Application Event Type act=
(none)
```

Customization

Users can send extra fields to syslog by configure the filter as follows, the mapping will only be added if the field is not already added.



The above example will map extra CEF extension field “cs1” to Fortify “ruleID,” and CEF extension field “cs1Label” to constant string “RULEID.”

Sample Syslog message:

```
Jun 25 22:22:04 sng2 fortify_runtime: CEF:0|Fortify|runtime|4.00|Web
Application Start|Web Application Start|1|rt=1372170124737
filePath=C:\\Fortify\\apache-tomcat-6.0.20\\webapps\\riches\\ cs1=/riches
cs1Label=Application Name cs3=audit cs3Label=Application Event Type
cs1=B675C4AB-995A-4BF9-8355-1E3C75C8EED4 cs1Label=RULEID act=(none)
```

System Startup Message

An event is sent when HPE Security Fortify Runtime starts successfully.

Sample Syslog message:

```
25 13:58:39 MMADOU fortify_runtime: CEF:0|Fortify|runtime|4.00|HP Fortify
Runtime Setup Complete|HP Fortify Runtime Setup
Complete|1|rt=1372161519478
```

Command Execution

An event is triggered when a new Process (exec) is created within the execution of a HTTP request.

Sample Syslog message:

```
Jun 25 23:11:03 sng2 fortify_runtime: CEF:0|Fortify|runtime|4.00|Command
Execution|Command Execution|1|rt=1372173063692 app=http src=127.0.0.1
dst=127.0.0.1 spt=64569 dhost=localhost dpt=80 requestMethod=GET
request=http://localhost/test/ProcessStart.aspx
requestClientApplication=Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0)
Gecko/20100101 Firefox/21.0 requestCookies=ASP.NET_
SessionId\=h5hkainzjnz43hj4XXXXXXXX reason=The system cannot find the file
specified cs6=no_such_file.exe /c dir C:\\*.* cs6Label=Command
cs2=h5hkainzjnz43hj4XXXXXXXX cs2Label=SessionId cs3=audit
cs3Label=Application Event Type act=(none)
```

CEF Field Mapping

CEF Field Name	Description
cs6	Fully Executed Command
reason	Error Message (if any)

Database Query

An event is triggered when any database create/read/update/delete is executed. In order to prevent logging sensitive information, by default, the system will only log the normalized SQL query. A normalized query will convert all SQL literal parameters to 'a' and numbers (integers or floating points) to 0. For example:

```
SELECT * FROM tbl_user WHERE name = 'john' and password = 'mysecret' and status = 100
```

```
SELECT * FROM tbl_user WHERE name = 'a' and password = 'a' and status = 0
```

Sample Syslog message:

```
Jun 25 22:24:02 sng2 fortify_runtime: CEF:0|Fortify|runtime|4.00|Database
Query|Database Query|1|rt=1372170242633 app=http src=127.0.0.1
dst=127.0.0.1 spt=29193 dhost=0.0.0.0 dpt=8080 requestMethod=GET
request=http://localhost:8080/riches/login/j_security_check
requestClientApplication=Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0)
Gecko/20100101 Firefox/21.0
requestCookies=JSESSIONID\=B61BC1482C7399BFXXXXXXXXXXXXXXXX cs6=SELECT
password FROM profile WHERE username \= ? cs6Label=Query
cs2=B61BC1482C7399BFXXXXXXXXXXXXXXXX cs2Label=SessionId cs3=audit
cs3Label=Application Event Type act=(none)
```

CEF Field Mapping

CEF Field Name	Description
cn1	Query Time
cn2	Affected Row Count
cs6	Query String
cs4	Binding Parameter(s), separated by '|'

Configurable Parameter

Name	Description
DbTraceFullQuery	allows users to specify when full query, instead of normalized query, should be logged. DbTraceFullQuery should be a valid regular expression pattern.

Name	Description
	The pattern is matched against the “normalized” query and if matched, will log the full query string along with all bound parameters.

File Create/Delete/Read/Write

An event is triggered when a new file is created/deleted/read/write within the execution of a HTTP request. By default, we will only monitor file activities in the following folders:

- Create/Delete/Write: anywhere except in the TEMP directory
- Read: anywhere except in the TEMP directory and Context real path
- All file activities during ASPX/JSP compilation are excluded

Sample Syslog message:

```
Jun 25 22:24:02 sng2 fortify_runtime: CEF:0|Fortify|runtime|4.00|File
Write|File Write|1|rt=1372170242458 app=http src=127.0.0.1 dst=127.0.0.1
spt=29193 dhost=0.0.0.0 dpt=8080 requestMethod=GET
request=http://localhost:8080/riches/login/j_security_check
requestClientApplication=Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0)
Gecko/20100101 Firefox/21.0
requestCookies=JSESSIONID\=B61BC1482C7399BFXXXXXXXXXXXXXXXX
fname=riches.properties.new filePath=C:\\apache-tomcat-
6.0.20\\webapps\\riches\\WEB-INF\\database\\riches.properties.new
cs2=B61BC1482C7399BFXXXXXXXXXXXXXXXX cs2Label=SessionId cs3=audit
cs3Label=Application Event Type act=(none)
```

CEF Field Mapping

CEF Field Name	Description
`filePath`	File involved (full path)
`fname`	File involved (file name only)

Configurable Parameter

Name	Description
`FileTraceExclusion`	Allows users to specify the exclusion pattern for `FileTraceMonitor`. It is a comma separated list of ANT style wildcards with the following extra features: • an exclamation mark [!] means inversion (inclusion instead of exclusion) • patterns prefixed with READ|WRITE|CREATE|DELETE followed by two colons [::] means applying the pattern only to File Read|Write|Create|Delete, respectively

<table>
<tr><th>Name</th><th>Description</th></tr>
<tr><td></td><td>

environment variables are supported by the format of %{env.VARIABLE}
%{ContextPath} is a special keyword which resolves to the Context real path

The default exclusion pattern is.
<pre>WRITE|CREATE::*.log, CREATE|DELETE::*.lck, %{env.temp}/**, READ::%{ContextPath}/**</pre>
<table>
<tr><th>Example Pattern</th><th>Explanation</th></tr>
<tr><td><code>WRITE|CREATE::*.log</code></td><td>For File Write and Create, ignore all files with “<code>.log</code>” extension. This pattern will not apply to Read and Delete operations.</td></tr>
<tr><td><code>CREATE|DELETE::*.lck</code></td><td>For File Create and Delete, ignore all files with “<code>.lck</code>” extensions. This pattern will not apply to Read and Write operations.</td></tr>
<tr><td><code>%{env.temp}/**</code></td><td>Ignore all File activities in TEMP directory.</td></tr>
<tr><td><code>READ::%{ContextPath}/**</code></td><td>For File Read, ignore all files inside the Context real path.</td></tr>
</table>
</td></tr>
</table>

General/Security/Crypto Exception Created

An event is triggered when an exception of predefined type is created. Security Exception and Crypto Exception are Java only rules and are further split into the following subtypes.

	Security Exception Created:	**Crypto Exception Created:**
Available subtypes:	Access Control Basic Key Exception CERT Certificate CERT Certificate Revocation List CERT Path Builder CERT Path Validator CERT Store Digest Security Generic KeyStore Exception Illegal Access Invalid Algorithm Parameter Invalid Key Specifications Invalid Parameter Specification Login Exception No Such Provider Privileged Action Signature Unrecoverable KeyStore Entry Unrecoverable KeyStore Key	Bad Padding Exemption Mechanism Illegal Block Size No Such Cryptographic Algorithm No Such Padding Short Buffer

Sample Syslog message:

```
Jun 25 20:09:41 sng2 fortify_runtime: CEF:0|Fortify|runtime|4.00|Security
Exception Created: Illegal Access|Security Exception Created: Illegal
Access|1|rt=1372162181356 reason=Class
```

```
org.apache.catalina.loader.WebappClassLoader can not access a member of
class org.aspectj.runtime.reflect.SignatureImpl with modifiers "private
static" cs5=java.lang.IllegalAccessException cs5Label=Exception API
cs3=audit cs3Label=Application Event Type act=(none)
```

CEF Field Mapping

CEF Field Name	Description
reason	Exception Message
cs5	Exception Class Name

Configurable Parameter

Name	Description
CaptureJavaExceptionType CaptureDotnetExceptionType	A regular expression specifying the types of Java or Dotnet exceptions needs to be recorded. The operation is checked against the exception class name as well as all super classes of the exception. Empty string means not recording any exception. For Java, the exception class has to be an instance of java.lang.Exception (and not java.lang.Error or java.lang.Throwable). Example: `com\.mypackage\..*, .*(Authentication|Authorization).*`
CaptureJavaExceptionWithEmptyMessage CaptureDotnetExceptionWithEmptyMessage	Variable which allows the recording of the Java Exceptions with empty exception message. When the Exception has an empty message, it's very hard to track down where it originated, or how to fix it. Set to “true” to record exceptions with empty messages, default value is “false.”

HTTP Session Start/Stop

An event is triggered when a new Session ID is created, expired or invalidated.

Sample Syslog message:

```
Jun 25 22:23:38 sng2 fortify_runtime: CEF:0|Fortify|runtime|4.00|HTTP
Session Start|HTTP Session Start|1|rt=1372170218029 app=http src=127.0.0.1
dst=127.0.0.1 spt=29193 dhost=0.0.0.0 dpt=8080 requestMethod=GET
request=http://localhost:8080/riches/ requestClientApplication=Mozilla/5.0
(Windows NT 6.1; WOW64; rv:21.0) Gecko/20100101 Firefox/21.0
cs2=B61BC1482C7399BFXXXXXXXXXXXXXXXX cs2Label=SessionId cs3=audit
cs3Label=Application Event Type act=(none)
```

CEF Field Mapping

CEF Field Name	Description
cs2	SessionId

Note: Only first 16 characters of the SessionID are shown, other characters are masked by "X." User can change the number of characters to be displayed by setting the field "${SessionIdMask}" in the config file. Setting the value to "-1" will disable this feature and display the full SessionID in plain text.

Known limitation for .NET:

Session timeout will only be monitored if Global.asax exists and method Session_End() is defined.

Network Socket Bind/Connect/Shutdown/Close

An event is triggered when a network socket is bind/connect/shutdown/close within the execution of a HTTP request.

Sample Syslog message:

```
Jun 25 23:09:15 sng2 fortify_runtime: CEF:0|Fortify|runtime|4.00|Network
Socket Connect|Network Socket Connect|1|rt=1372172955029 app=http
src=127.0.0.1 dst=127.0.0.1 spt=64569 dhost=localhost dpt=80
requestMethod=GET request=http://localhost/test/SocketConnect.aspx
requestClientApplication=Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0)
Gecko/20100101 Firefox/21.0 requestCookies=ASP.NET_
SessionId\=h5hkainzjnz43hj4XXXXXXXX cs4=smtp.domain.com:25
cs4Label=RemoteEndPoint cs5=<Unknown> cs5Label=LocalEndPoint
cs2=h5hkainzjnz43hj4XXXXXXXX cs2Label=SessionId cs3=audit
cs3Label=Application Event Type act=(none)
```

CEF Field Mapping

CEF Field Name	Description
cs4	Remote End Point (Format in "IP:Port")
cs5	Local End Point (Format in "IP:Port")

Spring/Struts/Dotnet Validation Failed

An event is triggered when the input validation failed. Currently, the following validators and APIs are covered:

Microsoft .NET

- RequiredFieldValidation
- RangeFieldValdiation
- RegularExpressionValidation
- CompareValidator
- CustomValidator

Java

Spring Validation using

- org.springframework.validation.ValidationUtils
- org.springframework.validation.Errors

Struts (1.x) Validation using validation.xml

- org.apache.struts.validator.FieldChecks

Sample Syslog message:

```
Jun 25 23:12:39 sng2 fortify_runtime: CEF:0|Fortify|runtime|4.00|Dotnet
Validation Failure|Dotnet Validation Failure|1|rt=1372173159908 app=http
src=127.0.0.1 dst=127.0.0.1 spt=9900 dhost=localhost dpt=80
requestMethod=POST request=http://localhost/test/Validation.aspx
requestClientApplication=Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0)
Gecko/20100101 Firefox/21.0 requestCookies=ASP.NET_
SessionId\=h5hkainzjnz43hj4XXXXXXXX cs4=18-99 cs4Label=Validation
cs5=Range cs5Label=ValidationType cs6=1000 cs6Label=Input
cs2=h5hkainzjnz43hj4XXXXXXXX cs2Label=SessionId cs3=audit
cs3Label=Application Event Type act=(none)
```

CEF Field Mapping

CEF Field Name	Description	Example
cs4	Validation Setting	1-500

CEF Field Name	Description	Example
cs5	Validation Type	Range
cs	Input	100000
Reason	Error	Weight is not in the range 1 through 500.

Unified Logging: Log4j/Jcl/Jul/Slf4j/Log4net/NLog and Enterprise Library

An event is triggered when the application is logging via the following logging frameworks.

Java	.NET
Log4j	Log4Net
JCL (Apache Common Logging)	NLog
JUL (java.util.logging)	Enterprise Library
Slf4j	

The priority of the HPE Security Fortify Runtime event is dynamically adjusted to the log level in the following order.

Severity	JCL	JUL	Log4j	Slf4j	NLog	Log4net	Enterprise Library
1	TRACE	FINEST	TRACE	TRACE	TRACE		Start/Stop/Suspend/Resume/Transfer/ActivityTracing
2		FINER					
3	DEBUG	FINE	DEBUG	DEBUG	DEBUG	DEBUG	Verbose
4		CONFIG					
5	INFO	INFO	INFO	INFO	INFO	INFO	Information
6							
7	WARN	WARNING	WARN	WARN	WARN	WARN	Warning
8							
9	ERROR	SEVERE	ERROR	ERROR	ERROR	ERROR	Error
10	FATAL		FATAL		FATAL	FATAL	Critical

Sample Syslog message:

```
Jun 25 22:22:18 sng2 fortify_runtime: CEF:0|Fortify|runtime|4.00|Unified
Logging: Log4j|Unified Logging: Log4j|1|rt=1372170138973
cs1=org.springframework.scheduling.quartz.SchedulerFactoryBean
cs1Label=Log Name cs4=Starting Quartz scheduler now cs4Label=Log Message
flexString1=INFO flexString1Label=Log Level cs3=audit cs3Label=Application
Event Type act=(none)
```

CEF Field Mapping

CEF Field Name	Description
`flexString1`	Log Level or Log Severity (.NET Enterprise Library)
`cs1`	Logger Name or Log Category (.NET Enterprise Library)
`cs4`	Log Message
`cs5`	Log Source Class (JUL only)
`cs6`	Log Source Method (JUL only)
`reason`	Log Exception

Configurable Parameter:

Name	Description

`[default], package1=level1, package2=level2`	There is a corresponding log level for each supported frameworks, namely: Jdk14LogLevel, Log4jLogLevel, JclLogLevel, Slf4jLogLevel, NLogLogLevel, Log4NetLogLevel and EntLogLogLevel. These parameters are used in HPE Security Fortify Runtime only and will not affect the logging frameworks. If the parameter value is empty, the system will log according to the log level defined in the logging framework. Otherwise, the parameter should be in the following format:
	`[default], package1=level1, package2=level2`
	For example, the following example means capturing logs with log level INFO or above, but for package com.fortify.runtime.*, log DEBUG or above.
	`INFO, com.fortify.runtime.=DEBUG`
	Note that in this example, the "." after "`com.fortify.runtime`" is required. Otherwise, the package "`com.fortify.runtime2`" will also be matched.

User Logon/Logoff

An event is triggered when user logon or logoff to the web application. Currently, the following authentication mechanisms are supported:

- .NET Form authentication using standard MembershipProvider (logon and logoff)

  Java container authentication using Form and HTTP basic authentication (logon only)

For User Logon, the event is further split into:

- User Logon: Success
- User Logon: Failure

The suffixes (Success or Failure) are generated inside the monitor and therefore, disabling rules using category name will not match the suffix.

Sample Syslog message:

```
Jun 25 22:24:02 sng2 fortify_runtime: CEF:0|Fortify|runtime|4.00|User
Logon: Success|User Logon: Success|1|rt=1372170242642 app=http
src=127.0.0.1 dst=127.0.0.1 spt=29193 dhost=0.0.0.0 dpt=8080
requestMethod=GET request=http://localhost:8080/riches/login/j_security_
check requestClientApplication=Mozilla/5.0 (Windows NT 6.1; WOW64;
rv:21.0) Gecko/20100101 Firefox/21.0
requestCookies=JSESSIONID\=B61BC1482C7399BFXXXXXXXXXXXXXXXX suser=admin
cs2=B61BC1482C7399BFXXXXXXXXXXXXXXXX cs2Label=SessionId cs3=audit
cs3Label=Application Event Type act=(none)
```

CEF Field Mapping

CEF Field Name	Description
suser	User Involved

User Management: Create/Delete User/Group, Add/Remove User to/from Group, Change Password

An event is triggered when a user management activity is observed. Currently, the following frameworks or APIs are supported:

- ASPX.NET: MembershipProvider
- IBM WebSphere and Oracle WebLogic
  - User Management activities via admin console

Sample Syslog message:

```
Jun 25 22:38:44 sng2 fortify_runtime: CEF:0|Fortify|runtime|4.00|User
Management: Create User|User Management: Create User|1|rt=1372171124522
app=http src=127.0.0.1 dst=127.0.0.1 spt=6825 dhost=localhost dpt=80
requestMethod=POST request=http://localhost/MyWebSite/register.aspx
requestClientApplication=Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0)
Gecko/20100101 Firefox/21.0 duser=user01 cs2=2agmigmbe4itdr45XXXXXXXX
cs2Label=SessionId cs3=audit cs3Label=Application Event Type act=(none)
```

CEF Field Mapping

CEF Field Name	Description
duser	User Involved
cs6	Group Involved

Web AccessLog

Every web page access will trigger a log to be sent to HPE Security ArcSight analysis server. Web AccessLog category is supported in the following application servers:

- Apache Tomcat
- JBoss
- IBM WebSphere
- Oracle WebLogic
- .NET applications running on Microsoft IIS server

Sample Syslog message:

```
Jun 25 22:24:05 sng2 fortify_runtime: CEF:0|Fortify|runtime|4.00|Web
AccessLog|Web AccessLog|1|rt=1372170245760 app=http src=127.0.0.1
dst=127.0.0.1 spt=29193 dhost=0.0.0.0 dpt=8080 requestMethod=GET
request=http://localhost:8080/riches/auth/AccountSummary.action
requestClientApplication=Mozilla/5.0 (Windows NT 6.1; WOW64; rv:21.0)
Gecko/20100101 Firefox/21.0
requestCookies=JSESSIONID\=B61BC1482C7399BFXXXXXXXXXXXXXXXX; authType\=0
suser=admin cs5=/riches/auth/AccountSummary.action cs5Label=Request Path
out=6133 outcome=200 cs2=B61BC1482C7399BFXXXXXXXXXXXXXXXX
cs2Label=SessionId cs3=audit cs3Label=Application Event Type act=(none)
```

CEF Field Mapping

CEF Field Name	Description
cs5	Request Path
cs6	Post Parameters (in standard URL encode format)
out	Number of byte sent
outcome	HTTP response code

Note: The application server needs to have Web AccessLog enabled in order for this rule to work. Please refer to the application server manual for how to enable web accesslog.

Configurable Parameter

Name	Description	Default Value
WebAccessLogMaxPostLen	Max HTTP POST parameter value length to be included in Web AccessLog. This is per item string length. POST parameter value long than this length is truncated.	50
WebAccessLogIgnorePostParamNames	A regular expression matching against POST parameter names. Matched POST parameter (s) will NOT be excluded in Web AccessLog	__*

Web Application Start/Stop

An event is triggered when a web application starts and shuts down.

Sample Syslog message:

```
Jun 25 22:22:04 sng2 fortify_runtime: CEF:0|Fortify|runtime|4.00|Web
Application Start|Web Application Start|1|rt=1372170124737
filePath=C:\\Fortify\\apache-tomcat-6.0.20\\webapps\\riches\\ cs1=/riches
cs1Label=Application Name cs3=audit cs3Label=Application Event Type act=
(none)
```

CEF Field Mapping

CEF Field Name	Description
`cs1`	Application Name
`filePath`	Application RealPath

Note:

- For WebLogic: The RealPath is the path of the WAR/EAR if it is a WAR/EAR deployment.
- For .NET: Web Application starts will only be triggered when the application is accessed for the first time. And by default, an application is stopped if it has been idle for 20 minutes. And in some rare cases, if the application is configured to run with more than one worker process (Web Garden mode), it is expected to see multiple start/stop for the same context.

Windows Registry Create/Delete/Read/Write

An event is triggered when the application is reading/writing Windows registry within the execution of a HTTP request. Registry activities directly/indirectly triggered by the following functions are excluded:

- Performance Counter
- ASPX Compilation

Sample Syslog message:

```
Jun 25 22:41:03 sng2 fortify_runtime: CEF:0|Fortify|runtime|4.00|Windows
Registry Read|Windows Registry Read|1|rt=1372171263056 app=http
src=127.0.0.1 dst=127.0.0.1 spt= dhost=127.0.0.1 dpt=80 requestMethod=GET
request=http://localhost/riches/ fname=RuntimeVerificationBehavior
filePath=HKEY_LOCAL_
MACHINE\\Software\\Microsoft\\ASP.NET\\4.0.30319.0\\RuntimeVerificationBeh
avior fileType=Registry Key cs3=audit cs3Label=Application Event Type act=
(none)
```

CEF Field Mapping

CEF Field Name	Description
`filePath`	Registry Key
`fname`	Registry Key Name
`fileType`	“Registry Key” (constant)

Note: This is a .NET-only rule.

Send Documentation Feedback

If you have comments about this document, you can contact the documentation team by email. If an email client is configured on this computer, click the link above and an email window opens with the following information in the subject line:

Feedback on Application Logging Rulepack Kit Guide (HPE Security Fortify Runtime 17.3)

Just add your feedback to the email and click send.

If no email client is available, copy the information above to a new message in a web mail client, and send your feedback to HPFortifyTechPubs@hpe.com.

We appreciate your feedback!