



ESP Logs

Technical Note

UPDATED: 27 July 2023

© 2022 Progress Software Corporation and/or one of its subsidiaries or affiliates. All rights reserved.

These materials and all Progress® software products are copyrighted and all rights are reserved by Progress Software Corporation. The information in these materials is subject to change without notice, and Progress Software Corporation assumes no responsibility for any errors that may appear therein. The references in these materials to specific platforms supported are subject to change.

#1 Load Balancer in Price/Performance, 360 Central, 360 Vision, Chef, Chef (and design), Chef Habitat, Chef Infra, Code Can (and design), Compliance at Velocity, Corticon, Corticon.js, DataDirect (and design), DataDirect Cloud, DataDirect Connect, DataDirect Connect64, DataDirect XML Converters, DataDirect XQuery, DataRPM, Defrag This, Deliver More Than Expected, DevReach (and design), Driving Network Visibility, Flowmon, Inspec, Ipswitch, iMacros, K (stylized), Kemp, Kemp (and design), Kendo UI, Kinvey, LoadMaster, MessageWay, MOVEit, NativeChat, OpenEdge, Powered by Chef, Powered by Progress, Progress, Progress Software Developers Network, SequeLink, Sitefinity (and Design), Sitefinity, Sitefinity (and design), Sitefinity Insight, SpeedScript, Stylized Design (Arrow/3D Box logo), Stylized Design (C Chef logo), Stylized Design of Samurai, TeamPulse, Telerik, Telerik (and design), Test Studio, WebSpeed, WhatsConfigured, WhatsConnected, WhatsUp, and WS_FTP are registered trademarks of Progress Software Corporation or one of its affiliates or subsidiaries in the U.S. and/or other countries.

Analytics360, AppServer, BusinessEdge, Chef Automate, Chef Compliance, Chef Desktop, Chef Workstation, Corticon Rules, Data Access, DataDirect Autonomous REST Connector, DataDirect Spy, DevCraft, Fiddler, Fiddler Classic, Fiddler Everywhere, Fiddler Jam, FiddlerCap, FiddlerCore, FiddlerScript, Hybrid Data Pipeline, iMail, InstaRelinker, JustAssembly, JustDecompile, JustMock, KendoReact, OpenAccess, PASOE, Pro2, ProDataSet, Progress Results, Progress Software, ProVision, PSE Pro, Push Jobs, SafeSpaceVR, Sitefinity Cloud, Sitefinity CMS, Sitefinity Digital Experience Cloud, Sitefinity Feather, Sitefinity Thunder, SmartBrowser, SmartComponent, SmartDataBrowser, SmartDataObjects, SmartDataView, SmartDialog, SmartFolder, SmartFrame, SmartObjects, SmartPanel, SmartQuery, SmartViewer, SmartWindow, Supermarket, SupportLink, Unite UX, and WebClient are trademarks or service marks of Progress Software Corporation and/or its subsidiaries or affiliates in the U.S. and other countries. Java is a registered trademark of Oracle and/or its affiliates. Any other marks contained herein may be trademarks of their respective owners.

Please refer to the NOTICE.txt or Release Notes – Third-Party Acknowledgements file applicable to a particular Progress product/hosted service offering release for any related required third-party acknowledgements.

Table of Contents

1 Introduction	4
2 ESP SSO Debug Logs	5
3 ESP Extended Logs	6
3.1 Connection Logs	6
3.2 User Logs	6
4 Security Logs	15
Last Updated Date	16

1 Introduction

This Technical Note provides supplementary information about the Edge Security Pack (ESP) logs in the Kemp LoadMaster. For further information on ESP in general, refer to the ESP Feature Description on the [Kemp Documentation Page](#).

2 ESP SSO Debug Logs

ESP SSO debug logs are extensive. The primary purpose of these logs is to provide deep insight into processing and developer-level debugging information. While these logs are not documented, they are verbose in nature. They can be examined for information and parsed where necessary.

These logs are debug level and are disabled by default under normal operating conditions.

Generally, these logs are only enabled in collaboration with Kemp Customer Support personnel, to provide assistance with troubleshooting problematic flows.

3 ESP Extended Logs

These logs are generated from the L7 layer of the LoadMaster system. They provide insight into ESP and security-related events on the system. The format of these logs rarely change, unless there is a specific request to add extra information (which typically would be new data at the end of the string).

Three identifiers are used:

- L7_LOG_CONN
- L7_LOG_USER
- L7_LOG_SECURITY

These map to the corresponding files on the system:

- /var/log/userlog/connection
- /var/log/userlog/user
- /var/log/userlog/security

For more information on each of the log types, refer to the sections below.

3.1 Connection Logs

The connection logs provide information relating to the client, Virtual Service, Real Server, and the nature of the connection (if SSL is in use or not).

Format:

SSL accept on "VSIP:Port" from "Client IP:Port"

Format:

Connect from "ClientIP:Port" to "RSIP:Port" using "VSIP:Port"

3.2 User Logs

User logs reflect the activity of the user. The logs have the following format.

Format:

"VSIP:Port" ("RSIP:Port") User "USERNAME" requested|attempted "HTTP METHOD"
"URI" "USERAGENT"

Where:

USERNAME reflects the user

The log indicates what the user requested OR attempted

HTTP METHOD reflects the HTTP method used, for example, GET or POST

URI comprises of http or https, the host being accessed, and the path and query as presented

USERAGENT is the User Agent header from the HTTP request (if enabled to be included). To enable this, go to **System Configuration > Miscellaneous Options > L7 Configuration** in the LoadMaster Web User Interface (WUI) and tick the **Include User Agent Header in User Logs** check box.

The user logs also explicitly shows log off activity.

Format:

"VSIP:Port": User "USERNAME" logged off

For common activity events (for example, log on and access denied), or if a dialogue is required between the client and LoadMaster (for example, for two-factor authentication), the user logs capture this detail in a simple user log message.

Format:

"VSIP:Port": User "USERNAME" "MESSAGE" from "HOST"

Where the **MESSAGE** can be:

- logged on
- denied access
- blocked access

3 ESP Extended Logs

- requires passphrase
- requires re-enter passphrase
- requires pin
- requires re-enter pin
- requires password reset

You can also generate user logs in Common Event Format (CEF).

Allow connection scaling over 64K Connections	<input type="checkbox"/>
Always Check Persist	<input type="text" value="No"/>
Add Port to Active Cookie	<input type="checkbox"/>
Conform to RFC	<input checked="" type="checkbox"/>
Close on Error	<input type="checkbox"/>
Add Via Header In Cache Responses	<input type="checkbox"/>
Real Servers are Local	<input type="checkbox"/>
Drop Connections on RS failure	<input type="checkbox"/>
Drop at Drain Time End	<input type="checkbox"/>
L7 Connection Drain Time (secs)	<input type="text" value="300"/> <input type="button" value="Set Time"/> (Valid values:0, 60 - 86400)
L7 Authentication Timeout (secs)	<input type="text" value="30"/> <input type="button" value="Set Timeout"/> (Valid values:30 - 300)
L7 Client Token Timeout (secs)	<input type="text" value="120"/> <input type="button" value="Set Timeout"/> (Valid values:60 - 300)
Additional L7 Header	<input type="text" value="X-Forwarded-For"/>
100-Continue Handling	<input type="text" value="RFC-7231 Compliant"/>
Allow Empty POSTs	<input type="checkbox"/>
Allow Empty HTTP Headers	<input type="checkbox"/>
Force Complete RS Match	<input type="checkbox"/>
Least Connection Slow Start	<input type="text" value="0"/> <input type="button" value="Set Slow Start"/> (Valid values:0 - 600)
Share SubVS Persistence	<input type="checkbox"/>
Log Insight Message Split Interval	<input type="text" value="10"/> <input type="button" value="Set Log Split Interval"/> (Valid values:1 - 100)
Include User Agent Header in User Logs	<input type="checkbox"/>
Use CEF Log Format	<input type="checkbox"/>

To enable the CEF log format, go to **System Configuration > Miscellaneous Options > L7 Configuration** and select the **Use CEF Log Format** check box. CEF log format is easily consumable for Security Information and Event Management (SIEM) tools, such as; Splunk, SolarWinds, LogRhythm, AlienVault, and so on.

3 ESP Extended Logs

The following log headers appear in the user logs when the CEF format is enabled:

- vs
- event type
- source ip
- source port
- user
- user agent
- request method
- request url

For example:

```
=====
===
files:
user-20200313.gz
=====
===
<133>1 2020-03-12T09:08:26-0400 JWTest 17log - - [meta sequenceId="0"]
10.0.70.141:80: User ruth logged on from 10.0.11.113
<133>1 2020-03-12T09:08:26-0400 JWTest 17log - - [meta sequenceId="0"]
10.0.70.141:80: (10.0.11.113:52896) User 'ruth' requested GET
http://10.0.70.141/ (User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36
Edge/18.17763)
<133>1 2020-03-12T09:08:29-0400 JWTest 17log - - [meta sequenceId="0"]
10.0.70.141:80: (10.0.11.113:52897) User 'kempqaesp\ruth' requested GET
http://10.0.70.141/ (User-Agent: Mozilla/5.0 (Windows NT 10.0; Win64; x64)
AppleWebKit/537.36 (KHTML, like Gecko) Chrome/64.0.3282.140 Safari/537.36
Edge/18.17763)
2020-03-12T11:17:00-04:00 JWTest 17log: 10.0.70.141:80: User ruth logged on
from 10.0.11.113
2020-03-12T11:17:00-04:00 JWTest 17log: 10.0.70.141:80: (10.0.11.113:57532)
User 'ruth' requested GET http://10.0.70.141/ (User-Agent: Mozilla/5.0
(Windows NT 10.0; Win64; x64) AppleWebKit/537.36 (KHTML, like Gecko)
Chrome/64.0.3282.140 Safari/537.36 Edge/18.17763)
2020-03-12T11:29:55-04:00 JWTest 17log: CEF:0|Kemp|LM|1.0|9|Access
Denied|6|vs=10.0.70.141:80 event=Access Denied srcip=10.0.11.113 user=ruth
msg=denied access
2020-03-12T11:29:59-04:00 JWTest 17log: CEF:0|Kemp|LM|1.0|8|Logged
on|1|vs=10.0.70.141:80 event=Logged on srcip=10.0.11.113 user=ruth msg=logged
on
2020-03-12T11:29:59-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.141:80 event=Request
srcip=10.0.11.113 srcport=57703 method=GET url=http://10.0.70.141/ user=ruth
2020-03-12T11:31:38-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.133:443 event=Request
srcip=10.0.11.113 srcport=57782 method=GET url=https://mail.kempqaesp.net/
2020-03-12T11:31:38-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.133:443 event=Request
```

3 ESP Extended Logs

```

srcip=10.0.11.113 srcport=57783 method=GET
url=https://mail.kempqaesp.net/owa/
2020-03-12T11:31:38-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.133:443 event=Request
srcip=10.0.11.113 srcport=57785 method=GET
url=https://mail.kempqaesp.net/owa/prem/15.1.544.27/scripts/boot.0.mouse.js
2020-03-12T11:31:38-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.133:443 event=Request
srcip=10.0.11.113 srcport=57787 method=GET
url=https://mail.kempqaesp.net/owa/prem/15.1.544.27/scripts/boot.2.mouse.js
2020-03-12T11:31:38-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.133:443 event=Request
srcip=10.0.11.113 srcport=57786 method=GET
url=https://mail.kempqaesp.net/owa/prem/15.1.544.27/scripts/boot.3.mouse.js
2020-03-12T11:31:38-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.133:443 event=Request
srcip=10.0.11.113 srcport=57784 method=GET
url=https://mail.kempqaesp.net/owa/prem/15.1.544.27/scripts/boot.1.mouse.js
2020-03-12T11:31:38-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.133:443 event=Request
srcip=10.0.11.113 srcport=57788 method=GET
url=https://mail.kempqaesp.net/owa/prem/15.1.544.27/resources/styles/fonts/of
fice365icons.woff
2020-03-12T11:34:35-04:00 JWTest 17log: CEF:0|Kemp|LM|1.0|9|Access
Denied|6|vs=10.0.70.134:443 event=Access Denied srcip=10.0.11.113
user=administrator msg=denied access
2020-03-12T11:34:40-04:00 JWTest 17log: CEF:0|Kemp|LM|1.0|8|Logged
on|1|vs=10.0.70.134:443 event=Logged on srcip=10.0.11.113 user=administrator
msg=logged on
2020-03-12T11:34:40-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=57868 method=GET url=https://mail.kempqaesp.net/owa
user=kempqaesp\\administrator
2020-03-12T11:34:41-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=57869 method=GET
url=https://mail.kempqaesp.net/owa/prem/15.1.544.27/scripts/boot.1.mouse.js
user=kempqaesp\\administrator
2020-03-12T11:34:41-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=57870 method=GET
url=https://mail.kempqaesp.net/owa/prem/15.1.544.27/scripts/boot.0.mouse.js
user=kempqaesp\\administrator
2020-03-12T11:34:41-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=57871 method=GET
url=https://mail.kempqaesp.net/owa/prem/15.1.544.27/scripts/boot.3.mouse.js
user=kempqaesp\\administrator
2020-03-12T11:34:41-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=57872 method=GET
url=https://mail.kempqaesp.net/owa/prem/15.1.544.27/scripts/boot.2.mouse.js
user=kempqaesp\\administrator
2020-03-12T11:34:41-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=57873 method=GET
url=https://mail.kempqaesp.net/owa/prem/15.1.544.27/resources/images/0/sprite
1.mouse.png user=kempqaesp\\administrator
2020-03-12T11:46:27-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=58249 method=POST

```

3 ESP Extended Logs

```
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T11:51:47-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=58669 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T11:57:07-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=58696 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T12:02:27-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=58719 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T12:07:47-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=58927 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T12:13:07-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=59160 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T12:18:27-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=59282 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T12:23:47-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=59305 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T12:29:08-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=59645 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T12:34:28-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=59761 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T12:39:48-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=59808 method=POST
```

3 ESP Extended Logs

```
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T12:45:08-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=59881 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T12:50:28-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=60146 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T12:55:48-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=60245 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T13:01:08-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=60542 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T13:06:28-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=60633 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T13:11:48-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=60655 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T13:17:08-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=60738 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T13:22:28-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=60876 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T13:27:48-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=61044 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T13:33:08-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=61155 method=POST
```

3 ESP Extended Logs

```
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T13:38:28-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=61174 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T13:43:49-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=61494 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T13:49:09-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=61697 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T13:54:29-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=61937 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T13:59:49-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=62238 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T14:05:09-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=62262 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T14:10:29-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=62388 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T14:15:49-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=62704 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T14:21:09-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=62770 method=POST
url=https://mail.kempqaesp.net/owa/ev.owa2?ns\=PendingRequest&ev\=FinishNotif
icationRequest&UA\=0&cid\=e9236b6b-ebbf-4688-be49-fe8c57437e37
user=kempqaesp\\administrator
2020-03-12T14:26:05-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=62840 method=GET
url=https://mail.kempqaesp.net/owa/ user=kempqaesp\\administrator
```


3 ESP Extended Logs

```
2020-03-12T14:26:05-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=62843 method=GET
url=https://mail.kempqaesp.net/owa/prem/15.1.544.27/scripts/boot.1.mouse.js
user=kempqaesp\\administrator
2020-03-12T14:26:05-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=62845 method=GET
url=https://mail.kempqaesp.net/owa/prem/15.1.544.27/scripts/boot.0.mouse.js
user=kempqaesp\\administrator
2020-03-12T14:26:05-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=62842 method=GET
url=https://mail.kempqaesp.net/owa/prem/15.1.544.27/scripts/boot.2.mouse.js
user=kempqaesp\\administrator
2020-03-12T14:26:05-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=62844 method=GET
url=https://mail.kempqaesp.net/owa/prem/15.1.544.27/scripts/boot.3.mouse.js
user=kempqaesp\\administrator
2020-03-12T14:26:05-04:00 JWTest 17log:
CEF:0|Kemp|LM|1.0|11|Request|1|vs=10.0.70.134:443 event=Request
srcip=10.0.11.113 srcport=62846 method=GET
url=https://mail.kempqaesp.net/owa/userspecificresourceinjector.ashx?ver\=15.
1.544.27&appcacheclient\=1&layout\=mouse user=kempqaesp\\administrator
```

4 Security Logs

These logs are generated when configuration on the LoadMaster prevents access to a service, or the LoadMaster detects something malicious regarding the request.

Format:

Attempted XSS attack on "VSIP:Port" from "ClientIP:Port" (dtcode "INTERNAL DETECTION CODE")

Blocked access to invalid "TARGET" "HOST" from "ClientIP:Port" to "VSIP:Port"\n

Where:

- **TARGET** is the directory or host
- **HOST** is the host information from HTTP request or **[No host specified]**

Blocked SMTP access to "MAIL ADDRESS" from "ClientIP:Port" to "VSIP:Port"
SMTP parse failure of data from "ClientIP:Port" to "VSIP:Port"

Last Updated Date

This document was last updated on 27 July 2023.