

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.

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

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

3.2.1 User Account Control (UAC) Check 10

4 Security Logs **12**

Last Updated Date **13**

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

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.

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

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.

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

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.

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

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"

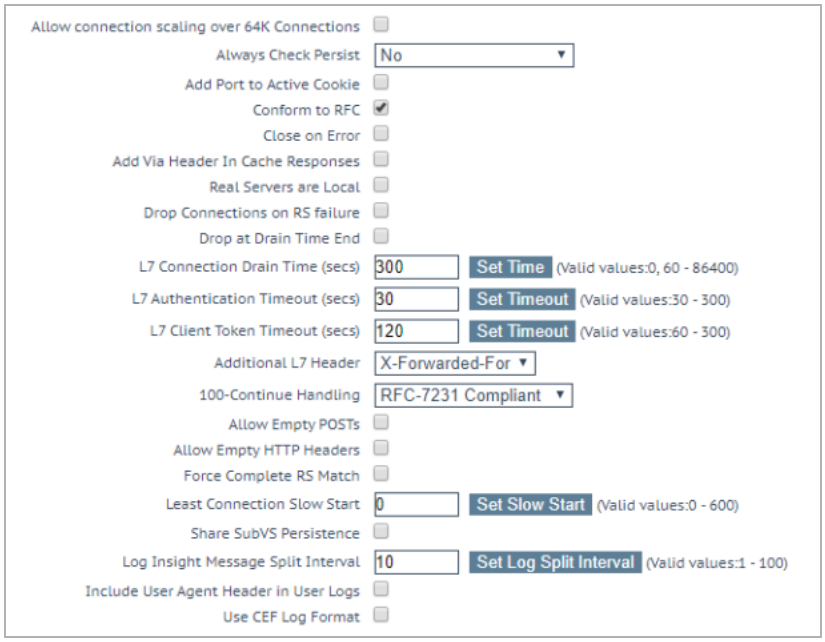
Where the **MESSAGE** can be:

- logged on
- denied access
- blocked access
- requires passphrase

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

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

You can also generate user logs in Common Event Format (CEF). CEF is an open log management standard that improves the interoperability of security-related information from different security and network devices and applications.



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.

The CEF logs are composed of a header and an extension. The header is well defined within the specification and the extension is a key-value pair vendor specific segment. The following log headers appear in the user logs when the CEF format is enabled:

- vs
- event type

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

- source ip
- source port
- user
- user agent
- request method
- request url

For example:

CEF:0|Kemp|LM|1.0|14|Request|1|vs=10.35.46.157:443 event=Request srcip=10.35.2.45 srcport=54548 method=GET url=https://10.35.46.157/ user=mgupta@kempqaesp.net useragent=Mozilla/5.0

In LoadMaster firmware version 7.2.51, ESP user logs were expanded to be more useful and applicable to enterprise customers with extensive logging infrastructure. User Authentication, Authorization, and Accounting (AAA) information is included in the logs, including the time of request, username, domain, AAA server, AAA protocol type, AAA result, and error message.

To view, clear, and save the ESP user logs, go to **System Configuration > Logging Options > Extended Log Files** in the LoadMaster User Interface (UI).

Here is an example of these logs:

2021-09-08T07:34:22-04:00 lb100 ssomgr: vs=10.35.46.240:80 user=mgupta@kpauto.net domain=kempqaesp.net server=172.20.7.170 protocol=LDAP Unencrypted result=0:Success

...

2021-09-08T08:08:40-04:00 lb100 ssomgr: vs=10.35.46.240:80 user=mgupta@kpauto.net domain=KPAUTO.NET msg=Deleted expired user session, start time:1631102854 duration:66 seconds

You can generate these logs in Common Event Format (CEF) by enabling the Use CEF Log Format check box in **System Configuration > Miscellaneous Options > L7 Configuration**. Here is an example of these CEF logs:

2021-09-08T07:17:15-04:00 lb100 ssomgr: CEF:0|Kemp|LM|1.0|100|User AAA|0|vs=10.35.46.240:80 event=User AAA user=mgupta@kpauto.net domain=kempqaesp.net server=172.20.7.170 protocol=LDAP Unencrypted result=0:Success

...

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

2021-09-08T07:32:22-04:00 lb100 ssomgr: CEF:0|Kemp|LM|1.0|101|User session timeout|0|vs=10.35.46.240:80 event=User session timeout user=mgupta@kpauto.net domain=KPAUTO.NET msg=Deleted expired user session, start time:1631099835 duration:906 seconds

In LoadMaster firmware version 7.2.53, the ESP client session logging was further enhanced. The LoadMaster logs:

- The initially created ESP session

  CEF:0|Kemp|LM|1.0|8|Logged on|1|vs=10.35.46.157:443 event=Logged on srcip=10.35.2.45 user=mgupta@kempqaesp.net msg=logged on

- The time when the LoadMaster cleared the session from the cache. Note that if the entire cache is cleared, a single log message is recorded at the time of clearing, which notes that all existing sessions at that time were cleared form the cache.

  CEF:0|Kemp|LM|1.0|104|Flush SSO cache|1|event=Flush SSO cache msg=SSO cache being flushed user sessions:1 cookie sessions:0

- If an ESP session is deleted (when the user logs out from the application, when the session expires, or the user enters invalid credentials). The time of when the LoadMaster cleared the session is also logged.

  CEF:0|Kemp|LM|1.0|101|User session timeout|0|vs=10.35.46.242:443 event=User session timeout user=mohit@parent.net domain=MULLTIDOMAIN msg=Deleted expired user session, start time:1629182393 duration:69 seconds

  CEF:0|Kemp|LM|1.0|102|User session kill|0|vs=10.35.46.235:443 event=User session kill user=mohit@parent.net domain=MULLTIDOMAIN msg=Deleted user session, start time:1629378587 duration:8 seconds

  CEF:0|Kemp|LM|1.0|103|Kill all sessions|0|event=Kill all sessions domain=MULLTIDOMAIN msg=Deleted 1 user session(s) associated with domain

3.2.1 User Account Control (UAC) Check

You can configure the **User Account Control Check** interval value in **Virtual Services > Manage SSO > Modify** for certain authentication protocols. If the UAC check interval value is set to 0 minutes (default value), then UAC is not performed periodically for users after successful login.

When you specify an interval value in the range of 1 to 300 minutes, the periodic UAC check is performed per user for the requests received after the interval expiry.

The UAC detects:

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

- Unknown users
- Disabled accounts
- Locked accounts
- Expired passwords on accounts

Extended ESP user logs provide the results of the UAC check. Additional information is logged for the user such as start session time, total duration, protocol information, KCD information, and blocked user events.

The check may occur on new connection establishment or as part of existing sessions. The **msDS-User-Account-Control-Computed** and **userAccountControl** attributes are used to determine the UAC status.

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

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"
```


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

Last Updated Date

This document was last updated on 27 July 2023.

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