



ESP Logs

Technical Note

UPDATED: 27 July 2023

Copyright Notices

© 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	8
Last Updated Date	9

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

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.