



# LoadMaster with FIPS 140-2 Level 1

## Addendum to LoadMaster Manual Software Version 6.0

**Version 1.4**

Revised: January 2012

**World Headquarters:**

KEMP Technologies, Inc.  
12 Old Dock Road  
Yaphank , NY 11980  
U.S.A.

+1 (631) 345 5292

**EMEA Headquarters:**

KEMP Technologies Ltd  
Mary Rosse Centre  
Holland Road, National Tech. Park  
Limerick, Ireland

+353 (61) 260 101

## **Copyright Notices**

Copyright © 2002-2011 KEMP Technologies, Inc.. All rights reserved.. KEMP Technologies and the KEMP Technologies logo are registered trademarks of KEMP Technologies, Inc..

KEMP Technologies, Inc. reserves all ownership rights for the LoadMaster product line including software and documentation. The use of the LoadMaster Exchange appliance is subject to the license agreement. Information in this guide may be modified at any time without prior notice.

Microsoft Windows is a registered trademarks of Microsoft Corporation in the United States and other countries. All other trademarks and service marks are the property of their respective owners.

**Limitations:** This document and all of its contents are provided as-is. KEMP Technologies has made efforts to ensure that the information presented herein are correct, but makes no warranty, express or implied, about the accuracy of this information. If any material errors or inaccuracies should occur in this document, KEMP Technologies will, if feasible, furnish appropriate correctional notices which Users will accept as the sole and exclusive remedy at law or in equity. Users of the information in this document acknowledge that KEMP Technologies cannot be held liable for any loss, injury or damage of any kind, present or prospective, including without limitation any direct, special, incidental or consequential damages (including without limitation lost profits and loss of damage to goodwill) whether suffered by recipient or third party or from any action or inaction whether or not negligent, in the compiling or in delivering or communicating or publishing this document.

Any Internet Protocol (IP) addresses, phone numbers or other data that may resemble actual contact information used in this document are not intended to be actual addresses, phone numbers or contact information. Any examples, command display output, network topology diagrams, and other figures included in this document are shown for illustrative purposes only. Any use of actual addressing or contact information in illustrative content is unintentional and coincidental.

Portions of this software are; copyright (c) 2004-2006 Frank Denis. All rights reserved; copyright (c) 2002 Michael Shalayeff. All rights reserved; copyright (c) 2003 Ryan McBride. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE ABOVE COPYRIGHT HOLDERS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE ABOVE COPYRIGHT HOLDERS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The views and conclusions contained in the software and documentation are those of the authors and should not be interpreted as representing official policies, either expressed or implied, of the above copyright holders..

Portions of the LoadMaster software are copyright (C) 1989, 1991 Free Software Foundation, Inc. -51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA- and KEMP Technologies Inc. is in full compliance of the GNU license requirements, Version 2, June 1991. Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Links to the source files are located on the [Product Matrix](#) page and the [Support](#) page of the KEMP website.

Portions of this software are Copyright (C) 1988, Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms are permitted provided that the above copyright notice and this paragraph are duplicated in all such forms and that any documentation, advertising materials, and other materials related to such distribution and use acknowledge that the software was developed by the University of California, Berkeley. The name of the University may not be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED ``AS IS" AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

Portions of this software are Copyright (C) 1998, Massachusetts Institute of Technology

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Portions of this software are Copyright (C) 1995-2004, Jean-loup Gailly and Mark Adler

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.
2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.
3. This notice may not be removed or altered from any source distribution.

Portions of this software are Copyright (C) 2003, Internet Systems Consortium

Permission to use, copy, modify, and/or distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS" AND THE AUTHOR DISCLAIMS ALL WARRANTIES WITH REGARD TO THIS SOFTWARE INCLUDING ALL IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY SPECIAL, DIRECT, INDIRECT, OR CONSEQUENTIAL DAMAGES OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE.

## **Contents**

<b>KEMP LoadMaster with FIPS 140-2 Level 1 Compliant Software .....</b>	<b>5</b>
<b>Operation.....</b>	<b>5</b>
Enabling FIPS 140-2 Level 1.....	5

## KEMP LoadMaster with FIPS 140-2 Level 1 Compliant Software

### Operation

Thank you for purchasing the KEMP Technologies LoadMaster. This model incorporates FIPS 140-2 Level 1 compliant software. There are some significant operational differences between the standard model and this model with respect to SSL handling, which will be explained in this addendum to the v6.0 manual.

FIPS 140-2 Level 1 is applicable to all currently available LoadMaster models.

Security Level 1 provides the lowest level of security. Basic security requirements are specified for a cryptographic module where no specific physical security devices are used beyond the basic requirement for production-grade components. An example of a Level 1 cryptographic module is a personal computer (PC) encryption board.

The LoadMaster does not use a specific board and uses memory allocation instead –this is within the Level 1 specification. The unmodified OpenSSL FIPS Object Module v. 1.2 is used for all SSL and SSH processing. Per NIST Special Publication 800-52, RC4, MD5, and SSL v3 are all specifically disallowed when the LoadMaster is placed in FIPS 140-2 Level 1 operational mode.

### Enabling FIPS 140-2 Level 1

From the Home screen, navigate to: System Configuration > Logging Options > Log Files and click on the Debug Options button. This will bring up the screen shown below.

The screenshot shows a web-based configuration interface with a yellow background. At the top left is a '<-Back' button. Below it is a table of configuration options:

Disable All Transparency	Disable Transparency
Enable L7 Debug Traces	Enable Traces
Perform an I7adm	I7adm
Enable IRQ Balance	Enable IRQ Balance
Enable FIPS 140-2 level 1 Mode	Enable FIPS mode
Perform a PS	ps
Display Meminfo	Meminfo
Display Slabinfo	Slabinfo
Perform an Ifconfig	ifconfig
Ping Host	Host: <input type="text"/> Ping
Kill VM Instance: 210600	<input type="text"/> Kill VM

Below the table is a section titled 'TCP dump' with the following controls:

Interface: eth0 | Address:  | Port:  | Start: Start | Stop: Stop | Download: Download

Of note here is the **Enable FIPS 140-2 Level 1 Mode** button. Clicking this button will turn on FIPS encryption. After turning this option on, the machine will require a reboot before proceeding.



Turning on FIPS forces the LoadMaster to use FIPS 140-2 Level 1 software for all secure traffic. Once the LoadMaster has been switched to FIPS it cannot be reversed and all protocols specifically disallowed by FIPS 140-2 will no longer function.