



MatrixSSL 3.3 Open Source Release Notes



Minutiae
047 018 287
106 021 192
070 023 210
053 024 000
073 032 230
108 032 428
091 033 174
058 039 248
108 054 402
125 059 400
099 060 400
070 061 256
048 068 340
065 070 338
104 071 358
115 075 358
041 077 096
123 079 384
063 083 064
053 091 052
028 097 052
084 100 031
050 102 044
103 106 050
117 111 046
104 118 282

AuthenTec, Inc.
100 Rialto Place, Suite 100
Melbourne, Florida 32901
321.308.1300
[authentec . com](http://authentec.com)

AuthenTec welcomes your input. We try to make our publications useful, interesting, and informative, and we hope you will take the time to help us improve them. Please send any comments or suggestions by mail or e-mail.

Disclaimer of Warranty

AUTHENTEC SOFTWARE, INCLUDING INSTRUCTIONS FOR ITS USE, IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. AUTHENTEC FURTHER DISCLAIMS ALL IMPLIED WARRANTIES INCLUDING WITHOUT LIMITATION ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR OF FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK ARISING OUT OF THE USE OR PERFORMANCE OF THE SOFTWARE AND DOCUMENTATION REMAINS WITH YOU.

IN NO EVENT SHALL AUTHENTEC, ITS AUTHORS, OR ANYONE ELSE INVOLVED IN THE CREATION, PRODUCTION, OR DELIVERY OF THE SOFTWARE BE LIABLE FOR ANY DAMAGES WHATSOEVER (INCLUDING, WITHOUT LIMITATION, DAMAGE FOR LOSS OF BUSINESS PROFITS, BUSINESS INTERRUPTION, LOSS OF BUSINESS INFORMATION, OR OTHER PECUNIARY LOSS) ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE OR DOCUMENTATION, EVEN IF AUTHENTEC HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME STATES OR COUNTRIES DO NOT ALLOW THE EXCLUSION OR LIMITATION OF LIABILITY FOR CONSEQUENTIAL OR INCIDENTAL DAMAGES, THE ABOVE LIMITATION MAY NOT APPLY TO YOU.

U.S. Government Restricted Rights

AuthenTec software and documentation are provided with RESTRICTED RIGHTS. Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 or subparagraph (c)(1) and (2) of the Commercial Computer Software – Restricted Rights 48 CFR 52.227-19, as applicable. Manufacturer is AuthenTec, Inc., Melbourne, Florida 32901. This Agreement is governed by the laws of the State of Florida.

AuthenTec, Inc.
100 Rialto Place, Suite 100
Melbourne, Florida 32901
321-308-1300
www.authentec.com
apps@authentec.com

MatrixSSL 3.3 Open Source Release Notes

The material in this publication is provided for information only. It is subject to change without notice. While reasonable efforts have been made to assure its accuracy, AuthenTec, Inc. assumes no liability resulting from errors or omissions in the document, or from the use of the information contained herein.

Copyright © 2012 by AuthenTec, Inc. All rights reserved. No part of this publication may be reproduced in any form or by any means without prior written permission. Printed in the United States of America.

Table of Contents

FEATURE ADDITIONS	3
LIMITED REHANDSHAKES	3
IMPROVEMENTS	3
SAMPLE SERVER SUPPORTS CHROME FALSE START	3
CIPHER SUITE AND PROTOCOL VERSION DEBUG TRACE	3
CHANGES	4
MATRIX_USE_FILE_SYSTEM DEFINE	4
USE_MATRIX_MEMORY_MANAGEMENT DEFINE	4

Feature Additions

This section highlights the new features that have been added since MatrixSSL 3.2.2

Limited Rehandshakes

Servers now limit how many rehandshakes a client may initiate for each session. SSL rehandshaking allows clients and servers to perform a handshake over an already connected session. There are some use-cases where this functionality is useful to upgrade or modify the security parameters but it also has been demonstrated to be an avenue for DOS attacks on a server. This new feature allows the server to restrict the number of rehandshake requests to prevent this potential threat. It is still possible to disable rehandshaking completely if desired.

The implementation of this feature works on a “handshake credit” mechanism where each client is given **one** credit at the beginning of a new connection (modify `DEFAULT_RH_CREDITS` to change the default credits). A new credit is awarded after a specific amount of data has been exchanged between peers. The default is 20MB and may be set at compile time with the `BYTES_BEFORE_RH_CREDIT` define.

Improvements

This section highlights under-the-hood changes since MatrixSSL 3.2.2

Sample Server Supports Chrome False Start

The sample SSL server now utilizes False Start support within MatrixSSL to allow the Google Chrome browser to connect. Support for False Start has been available in MatrixSSL since version 3.1.4 but the sample server was not taking advantage of this feature.

Cipher Suite and Protocol Version Debug Trace

When `USE_SSL_INFORMATIONAL_TRACE` is enabled in `matrixsslConfig.h` there will be a debug message that displays the SSL version and the cipher suite that has been negotiated. Previous versions would display the completion of the handshake but did not show these connection details.

Changes

This section highlights user interface or configuration changes since MatrixSSL 3.2.2

MATRIX_USE_FILE_SYSTEM define

The PS_USE_FILE_SYSTEM define has been renamed MATRIX_USE_FILE_SYSTEM

USE_MATRIX_MEMORY_MANAGEMENT define

The USE_PEERSEC_MEMORY_MANAGEMENT define has been renamed
USE_MATRIX_MEMORY_MANAGEMENT



AuthenTec, Inc.
100 Rialto Place, Suite 100
Melbourne, Florida 32901
321-308-1300 (voice)
321-308-1430 (fax)
www.authentec.com
apps@authentec.com