MatrixSSL 3.3 Open Source Release Notes

AuthenTec, Inc.
100 Rialto Place, Suite 100
Melbourne, Florida 32901
321.308.1300
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.

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

Table of Contents

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 utilities 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