
SHA1 to SHA2 Password Encryption

FIRELIGHT BASE



Platform

SHA1 TO SHA2 PASSWORD ENCRYPTION

Document Version: 1.0

Published: February 03, 2021

Insurance Technologies, LLC

Copyright © 2021 Insurance Technologies, LLC, all rights reserved.

Insurance Technologies, ForeSight® and FireLight® are registered or unregistered trademarks of Insurance Technologies, LLC (IT) in the USA and/or other countries.

ACORD, ACORD ObjX, ACORD OLifE, AL3, ACORD Advantage, ACORD XML, and "Association for Cooperative Operations Research and Development" are registered or unregistered trademarks of ACORD Corporation in the USA and/or other countries.

Microsoft, Microsoft SQL Server, Microsoft Internet Information Server, Windows, and other Microsoft names and logos are either registered or unregistered trademarks of Microsoft Corporation in the U.S.A. and/or other countries.

All other trademarks are the property of their respective owners.

The information contained in this document is current as of the date of the publication. Because Insurance Technologies, LLC must respond to changing market conditions and technology advances, Insurance Technologies, LLC cannot guarantee the accuracy of any information presented after the date of publication.

INSURANCE TECHNOLOGIES, LLC MAKES NO WARRANTIES, EXPRESSED OR IMPLIED, IN THIS DOCUMENT AND HEREBY DISCLAIMS ANY AND ALL SUCH WARRANTIES.

The material contained in this document is considered confidential and the intellectual property of Insurance Technologies, LLC. The recipient is given access to this material on the condition that the recipient (1) will keep the information confidential at all times, and (2) will not copy or modify or share the materials, except as expressly authorized by Insurance Technologies, LLC. The recipient should limit its disclosure of the information and materials only to its employees who have a clear business purpose and need to receive such information and materials and who are bound by confidentiality obligations to the recipient that are at least as protective of such information and materials as those contained herein.

Insurance Technologies, LLC

Two South Cascade Avenue
Colorado Springs, CO 80903
USA

Phone: 719.442.6400

FAX: 719.442.0600

Internet E-Mail: info@insurancetechnologies.com

Website: <http://www.insurancetechnologies.com>

Table of Contents

iConnect Design Approach - SHA1 to SHA2 Password Encryption	4
1 SSO Security: SHA1 to SHA2 password encryption (207828)	4

iConnect Design Approach - SHA1 to SHA2 Password Encryption

Project Overview

Passwords will be enhanced to store as SHA2 version instead of the previous SHA1 version. This enhancement will protect FireLight users with longer, more complex passwords, reducing the risk of password hacks.

1 SSO Security: SHA1 to SHA2 password encryption (207828)

MDE and STS need to be modified to support the following:

Check to see if we can add a way to enable/disable this feature via config or other setting.

1. Storing of passwords in SHA-2 format
3. Ability to transition from SHA-1 to SHA-2
4. All new passwords use SHA-2, old passwords can be transitioned when expired. Verification of historical passwords will contain a check for both SHA-1 and SHA-2.

Note: Historical Passwords were originally built as being independent from the normal ASP Identity passwords and was built using SHA-2. They do not need to support SHA-1 hashes, so that requirement is being removed.

Acceptance Criteria

- MDE and STS are modified to support
 - Storing of passwords in SHA-2 format
 - Transition ability from SHA-1 to SHA-2
 - Passwords use SHA-2
 - Old passwords can be transitioned from SHA-1 to SHA-2 when expired
 - Verification of historical passwords contain a check for both SHA-1 and SHA-2