INSURANCE TECHNOLOGIES

SHA1 to SHA2 Password Encryption

FIRELIGHT BASE

FireLight®

Platform

SHA1 TO SHA2 PASSWORD ENCRYPTION

Document Version: 1.0

Published: February 03, 2021

Insurance Technologies, LLC

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

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