INSURANCE TECHNOLOGIES

LexisNexis Upgrade to New Service

FIRELIGHT BASE

FireLight®

Platform

LEXISNEXIS UPGRADE TO NEW SERVICE

Document Version: 1.1

Published: February 14, 2020

Insurance Technologies, LLC

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

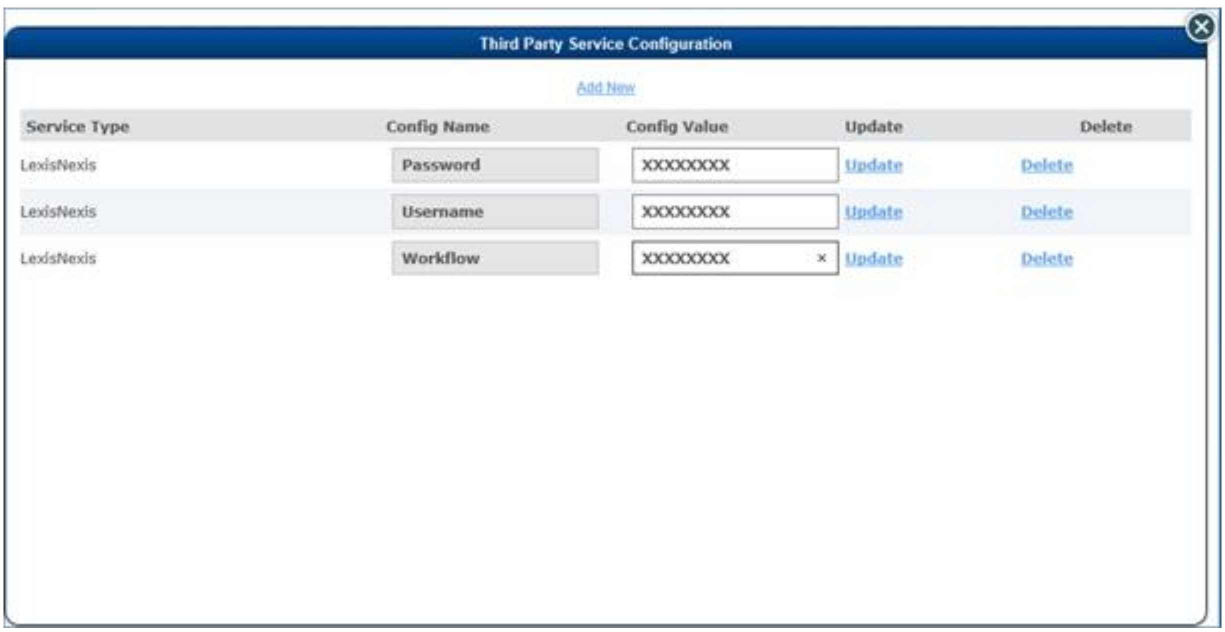
Table of Contents

Design Approach - LexisNexis Upgrade to New Service

The LexisNexis functionality will be upgrading to a new platform, which means that FireLight will need to also engage in this update. For this enhancement, we will need to upgrade to the RDP platform from our current IDM platform, without altering the process for our current clients utilizing this feature.

1.1 Third Party Configuration Credential Update

Currently within Firelight, LexisNexis is set up through the Third Party Service Config, found on the Organization Settings under the Admin tab. If adding for the first time, the user selects the Add new button at the top of the screen, where the username and password is added. Note that the username will contain the account ID that LexisNexis provided, and the password will be added on a separate line within the config.



If the credentials need to be updated or deleted, this can be done at this level as well.

The credentials that FireLight uses are solely of the carriers.

Acceptance Criteria

- Third party config is where the LexisNexis information is entered for the organization
- User will enter username into username section for LexisNexis

- User will enter password into password section for LexisNexis
- User will enter AccountID into AccountID section for LexisNexis
- User will enter workflow into workflow section for LexisNexis
- User's credentials can also be updated or deleted in this config
- Use the credentials to start the LexisNexis Process
- Note: AccountID and workflow are used to create the service endpoint therefore slashes(/) are not allowed

1.2 Use of Mapping and Signature Controls

The following fields need to be mapped in order to allow the LexisNexis service to work:

-First Name
-Last Name
-Street Address
-City
-State
-Zip
-DOB
-SSN
-Phone Number

The application dataitem fields will need to be mapped within the mapping tool to the global data item tags:

-FLI_OWNER_LNAME
-FLI_OWNER_FNAME
-FLI_OWNER_SSN
-FLI_OWNER_BDATE
-FLI_OWNER_PHONENUMBER
-FLI_OWNER_STREETADDRESS
-FLI_OWNER_CITYADDRESS
-FLI_OWNER_STATEADDRESS
-FLI_OWNER_ZIPCODEADDRESS

Within the signature controls, the "Use LexisNexis" checkbox needs to be selected in order to activate the use of the third party organization.

Acceptance Criteria

- On the signature control, "Use LexisNexis" will need to be selected to engage LexisNexis
- The First Name, Last Name, Street Address, City, State, Zip, DOB, SSN, and Phone number will need to be mapped into the Mapping Tool using the dataitems from the application. These will replace the Global Dataitems
- As an option, use the data groups and data group properties within the dataitems

1.3 Creation of Quiz

The creation of the quiz will occur during the initial call to LexisNexis, after the client verification identification page. The call will contain the application ID/DTI number and the data to be validated—the client's name, address, date of birth, and SSN.

LexisNexis will respond with questions and answer options for FireLight to present to the user.

The user will be able to answer these questions through Firelight. The questions and responses will not be retained by FireLight. The responses along with the question IDs will be sent with the customer reference number in a web service call to LexisNexis.

If the user logs out at this point and then logs back in, FireLight will reinitiate the LexisNexis authentication process, sending another web service request. LexisNexis will then respond as configured, with another set of authentication questions.

If the user is unable to pass and continue to retry to enter data for the client, LexisNexis will send a message that the client has "reached maximum number of attempts" or "they have timed out".

The organization will set the number of questions, timeout, and retry settings at LexisNexis.

Acceptance Criteria

- After the client verification identification page, the call to LexisNexis will be initiated, creating the quiz
- A series of questions with various answers will be displayed to the user
- The number of questions, timeout, and retry settings will be determined by the user through LexisNexis and FireLight will display what is sent.

1.4 Response from Quiz - Challenge Question

LexisNexis will respond with the LexID, the pass/fail status, and the score for the authentication questions. The Passing score will be determined by the client through LexisNexis. If the user has failed the authentication, LexisNexis may respond with a bonus question. In this case, FireLight will display the question and possible responses to the user. The question id and the selected response will be sent in a web service call to LexisNexis.

FireLight will save the final authentication score, status and number of questions, along with the LexID. These values will be included in the application audit report and will be available for use within the provider. Additional detailed information also can be obtained using the LexID at LexisNexis. FireLight will only retain an audit record for the initial call to the LexisNexis web service and the final results of the authentication at the conclusion of the web service calls.

After the LexisNexis authentication process, the signer will continue on the signing ceremony process. If the authentication process returns a failed score, the signer will still be allowed to complete the signing process, but the failure will be logged within the Audit history for further review. As a result, if the authentication process returns false positives, the application process is not restricted.

Acceptance Criteria

- LexisNexis will respond with the LexID, the pass/fail status, and the score.
- If user fails the initial quiz, a bonus question may be presented to the user. This answer will be sent via a web service call to LexisNexis
- FireLight saves the LexID, final authentication score, status, and the number of questions asked.
- If the user fails the quiz, it will be noted within the Audit history, but will let the user continue on to submit the application

1.5 Storage of response in Audits

Firelight currently stores the following returned values from the LexisNexis Instant Identity and Instant Authentication responses:
o The LexID value, the identifier assigned by LexisNexis for use within their system.
o The CVI (Comprehensive Verification Index) value that is returned in the LexisNexis response indicating the level of risk for identity theft.
o The NAS (Name Address SSN) value which indicates the level at which these inputs can be linked to the signer, as well as the NAP (Name Address Phone) value—both of which are used to determine the CVI value.

The CVI, NAS, NAP, status, score, and diversionary values will be included in the application audit report within the Identity Authentication section.

? FireLight will create an audit record for the initial web service call to LexisNexis and a second audit at the conclusion of the authentication process. The first audit will include a timestamp for the request and the agent, signer type, and application number for the request. The second audit will contain a timestamp, the values for the CVI, final score, and status. These will be listed within the signing ceremony section of the audit report.

Acceptance Criteria

- FireLight will store the LexID, CVI, NAS, NAP, status, score and diversionary values.
- An audit record will be created for the initial web service call, and a second audit record will be created at the conclusion.
- The first audit will contain a timestamp for the request, the agent, signer type, and application ID
- The second audit will contain the values for the CVI, final score, and the status of the call

1.6 Update Third Party Credentials during 2.17 Production Move

The code will update automatically to remove the IDM credentials during the Production Weekend

Acceptance Criteria