

---

E-Sign in React – Authentication

# FIRELIGHT BASE

---



Platform

**E-SIGN IN REACT – AUTHENTICATION**

**Document Version: 1.1**

**Published: May 25, 2021**

**Insurance Technologies, LLC**

Copyright © 2020 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](mailto:info@insurancetechnologies.com)

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

## Table of Contents

iConnect 243571 Design Approach - E-Sign in React - Authentication .....	4
1 Sign Now Enhancements .....	4
1.1 E-Sign: Client Identification Verification Authentication - SMS Text .....	4
1.2 E-Sign: Client Identification Verification Authentication - Lexis Nexis .....	8

# iConnect 243571 Design Approach - E-Sign in React - Authentication

We are continuing the enhancement the E-signature process within using the APIs in this release, which would include additional authentication. This includes both the SMS Text functionality, and the use of the LexisNexis services. Within the embedded signing ceremony, users will be able to verify users using both of these functionalities, either individually or together. This new enhancement will only impact the embedded users at this time, and will not impact the current signing ceremony that is found within FireLight.

## Impacts:

Client Verification Identification: SMS Text - Adding the ability for embedded users to authenticate clients through the use of SMS text

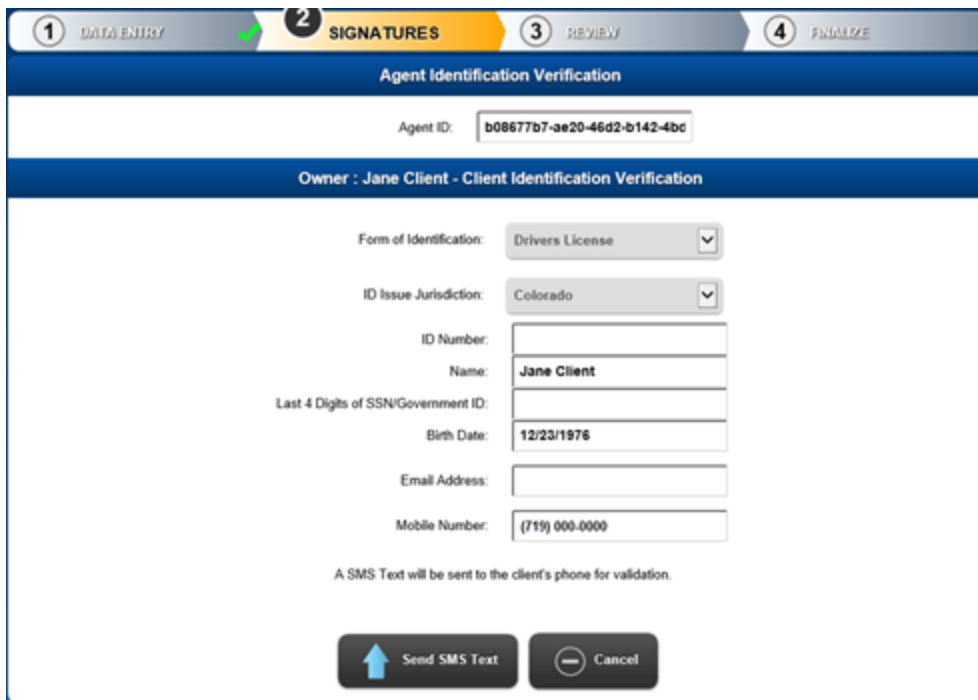
Client Verification Identification: LexisNexis - Adding the ability for embedded users to authenticate clients through the user of the LexisNexis Validation service (InstantID Quiz)

## 1 Sign Now Enhancements

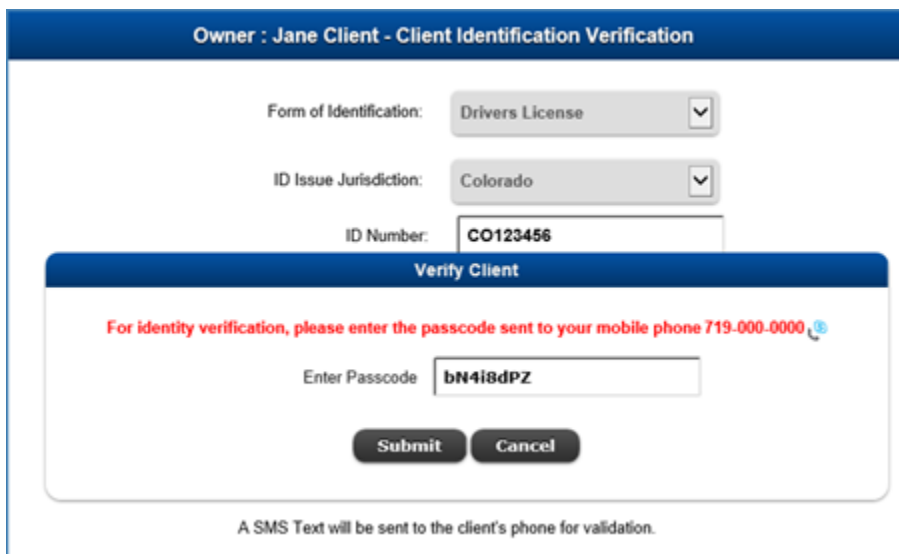
### 1.1 E-Sign: Client Identification Verification Authentication - SMS Text

SMS Text is added by selecting a checkbox in the signature control box. When SMS Text is enabled for the signer, the client identification verification page will show the Verified button as "Send SMS Text" prior to verifying the signer. The page will also show the Mobile number in a read only fashion with the mobile number that is mapped in from the application. The Mobile Number section will be enabled, and show the mapped phone number, but will not allow any edits.

The user can have the option to enter the mobile number in at the Client Verification Identification screen if "Allow Edits to Mobile" is selected in the Signing General section on the Groups Page. If this is enabled, the mobile phone number will be enabled and blank so the user can enter this information.



By selecting this button, a pop-up shows asking for the authentication code to be entered. The Submit button will verify the code, and take the user back to the client identification verification page, where the user can now select Verified or cancel. The cancel button on the pop-up will take the user back to the client identification verification screen again.



**Agent Identification Verification**

Agent ID:

**Annuitant - Client Identification Verification**

Form of Identification:

ID Issue Jurisdiction:

ID Number:

Name:

Last 4 Digits of SSN/Government ID:

Birth Date:

Email Address:

Mobile Number:

A SMS Text will be sent to the client's phone for validation.

**Verified**

**Cancel**

If the user does not have this validation turned on, and a mobile number is not mapped from the application, the user will have to cancel client identification validation, and unlock the application to enter the mobile number.

An audit will be taken of the code being sent to the user and will include the timestamp, and the signer's name and mobile number. It will display as "Agent Sent Passcode to Client"

## History

### Pending Signatures

SMS passcode sent to Julie Henry at mobile number  
+17195554444

### Agent Sent Passcode to Client

3/26/2021 3:58:59 PM EDT

### Pending Signatures

Application lock. Electronic signatures accepted.

### Locked

3/26/2021 3:54:41 PM EDT

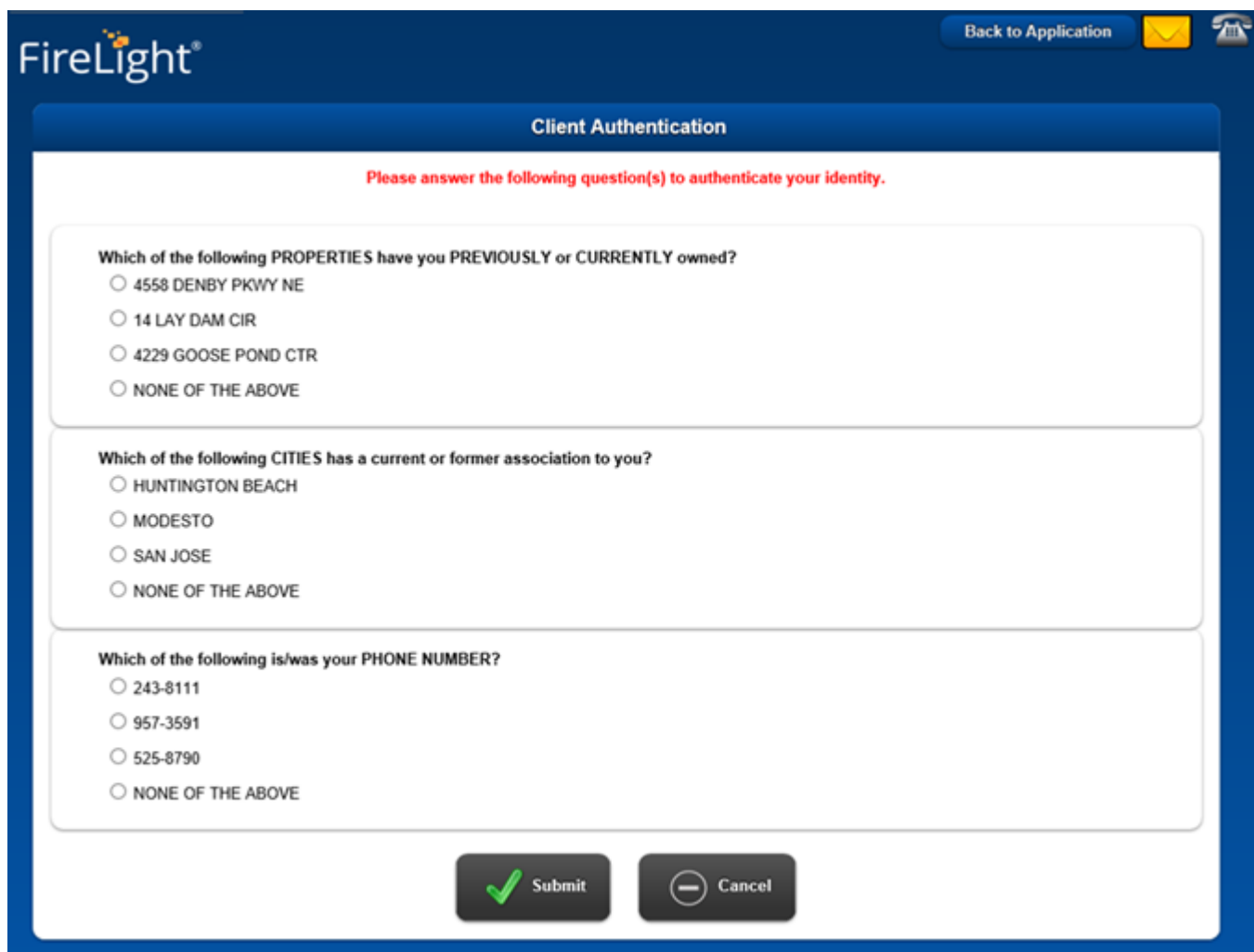
### Acceptance Criteria

- SMS Text is enabled based on the signature control. This is the only way to enable this feature.
- SMS text will add a mobile phone field that is locked and number mapped from the application. A text will be sent to that number where an authentication code will need to be entered.
- A user can also enter the phone number if "Allow Edits to Mobile" is selected in the Signing General section of the Groups page for that specific role code.
- The Verified button will show as "Send SMS Text" prior to sending the code, and verifying the user.
- If the user selects "Send SMS Text", a pop-up will display waiting for the validation code to be entered.
- Once the code is entered, and the user selects OK, the user is taken back to the Client Identification Verification screen where they can select the "Verified" button
- If Cancel is selected on the Pop-up, the user is taken back to the client identification verification screen. The user can then click on the "Resend SMS Text" to re-initiate sending the code.
- If Cancel is selected on the Client Identification Verification screen, the user is taken back to the list of required signers.
- The audit "Agent Sent Passcode to Client" will show the timestamp of the verification, along with the signer's name and mobile number.

## 1.2 E-Sign: Client Identification Verification Authentication - Lexis Nexis

Lexis Nexis is a third party feature that will map client data into the text fields, and will then ask a series of questions verifying the identity of the user. This third party option is added by selecting a checkbox on the signature control. Mapping from the mapping tool needs to occur as well to get the information to map through and engage the Lexis Nexis feature. The following data items need to be mapped to run the service: Party's first name, last name, street address, city, state, zip, date of birth, and SSN.

Once the user verifies the correct information is mapped to the name, SSN, and DOB fields, and they select Verified, then another screen shows a series of questions that will verify this user's identity upon selecting "Submit". If "Cancel" is selected, then the user is taken back to the client identification verification screen.



FireLight®
Back to Application

Client Authentication

Please answer the following question(s) to authenticate your identity.

Which of the following PROPERTIES have you PREVIOUSLY or CURRENTLY owned?

- ☐ 4558 DENBY PKWY NE
- ☐ 14 LAY DAM CIR
- ☐ 4229 GOOSE POND CTR
- ☐ NONE OF THE ABOVE

Which of the following CITIES has a current or former association to you?

- ☐ HUNTINGTON BEACH
- ☐ MODESTO
- ☐ SAN JOSE
- ☐ NONE OF THE ABOVE

Which of the following is/was your PHONE NUMBER?

- ☐ 243-8111
- ☐ 957-3591
- ☐ 525-8790
- ☐ NONE OF THE ABOVE



***Acceptance Criteria***

- The Party's first name, last name, street address, city, state, zip, date of birth, Phone number, and SSN need to be mapped from the mapping tool in order to utilize Lexis Nexis
- LexisNexis is active through the signature control checkbox labeled "Lexis Nexis"
- When user selects "Verified" on Client Identification Verification screen, the user is presented with a series of questions (number of questions differs by client)
- A challenge question could also be added if the user fails the initial questions
- User needs to answer all of the available questions, and click on Submit. This will then make a webservice call to LexisNexis to validate the user.
- By selecting submit, the user will move forward to the Signing ceremony, regardless if user passes or fails the quiz.
- An audit of the LexisNexis Quiz will display in the Audit report. This will show in the Signing Ceremony section of the report, and will show the user that was validated, the amount of questions, and if the user passed or failed the validation.