
Implement Timeout for Passcode

FIRELIGHT BASE



Platform

IMPLEMENT TIMEOUT FOR PASSCODE

Document Version: 1.0

Published: Oct 11, 2022

Insurance Technologies, LLC

Copyright © 2022 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 269829 Design Approach – Implement Timeout for Passcode	4
1 Admin - Org Setting for Passcode Expiration.....	4
2 Admin - Add New Email Tag for Passcode Timeout.....	6
3 App - Passcode Expiry and Resend	6

iConnect 269829 Design Approach – Implement Timeout for Passcode

Project Overview

This enhancement will allow applying a timeout to the validity of passcode required for external login link to FireLight by clients, agents, and reviewers. Currently, there is no time limitation for the passcode to be valid. To implement a standard practice for passcode (OTP) expiry, this enhancement will allow clients to enforce a timeout using an organization setting. This is an optional feature that can be set by organizations via the Organization Settings.

Impact:

- A new text box "Passcode Timeout" will be added to page FL Admin > Organization Configuration > Organization Settings > Signature (tab).
- A new "Resend Passcode" button will be added to external link login page to resend passcode in case of expiration.

1 Admin - Org Setting for Passcode Expiration

A new org setting "Passcode Timeout" will be added to the "Activity" tab of Organization Settings page in the admin tool. This field will store passcode expiration time in minutes. Default value for the timeout will be "0" mins, which means the passcode will never expire. Organizations can set this value to any integer number between "0" and "180" to denote the timeout in minutes.

The new organization setting "Passcode Timeout" will be added in the Activity tab below the field "Requests Timeout".

Organization
Security
External Integrations
Activity
Signature
Admin

Edit Masks [Add](#)

None

E-Delivery Reminder Frequency

Daily

Expiration Reminder Frequency

Daily

Submit Reminder Frequency

Daily

E-Delivery Expiration Warning Threshold

1

 days (0 for never)

Expiration Warning Threshold

1

 days (0 for never)

Single

Cumulative

Maximum Upload File Size

3

 MB

5

 MB

Requests Timeout

1

 days (0 for never)

Passcode Timeout (between 10 and 180)

10

 mins (0 for never)

Validation Message Style

Inline

Lock Mode

View Forms and Wiz

Allow Client E-Fill ☒
Allow Client Fill & Sign ☒

Allow NIGO Printing ☒
Use DMARC ☐

Prevent Email Editing ☐
Print Submitted Only ☐

Enable Common Tags ☒

Save Organization

There will be min and max limitation applied to the passcode timeout. Min limit for the timeout will be 0 mins and max will be 180 mins. If the client does not want to apply any limits to the timeout, they will enter "0" value.

When value outside this range is entered, an error message shows "Passcode Timeout must be between 0 and 180".

Organization
Security
External Integrations
Activity
Signature
Admin

Edit Masks [Add](#)

None

E-Delivery Reminder Frequency

Daily

Expiration Reminder Frequency

Daily

Submit Reminder Frequency

Daily

E-Delivery Expiration Warning Threshold

1

 days (0 for never)

Expiration Warning Threshold

1

 days (0 for never)

Single

Cumulative

Maximum Upload File Size

10

 MB

15

 MB

Requests Timeout

2

 days (0 for never)

Passcode Timeout (between 0 and 180)

200

 minutes (0 for never)

Validation Message Style

Inline

Lock Mode

View Forms and Wiz

Allow Client E-Fill ☒
Allow Client Fill & Sign ☒

Allow NIGO Printing ☒
Use DMARC ☐

Prevent Email Editing ☐
Print Submitted Only ☐

Enable Common Tags ☒

Passcode Timeout must be between 0 and 180.

Save Organization

Organization saved.

Acceptance Criteria

- Passcode timeout is configured from the Organization Settings in the admin tool.
- Passcode timeout can be configured to allow for it to never expire.
- Passcode expiration can be configured for a limited time in minutes.
- Default value is "0" for no timeout.
- Min timeout limit is 0 mins.
- Max timeout limit is 180 mins.
- Value is deployable from environment to environment.

2 Admin - Add New Email Tag for Passcode Timeout

A new email tag "PASSCODE_TIMEOUT" will be added to be used into the email templates. This data item will record the "Passcode Timeout" value for the organization from Signature tab on Organization Setting page.

Organizations will be able to use this email tag with the email template "Passcode Notification" to mention the expiry of passcode being sent to the users for authentication via email or text.

Sample text of how this might be optionally used in the email template "Passcode Notification":

"The passcode for the recent request is <PASSCODE>. It is valid for <PASSCODE_TIMEOUT> minutes."

Acceptance Criteria

- New data item "PASSCODE_TIMEOUT" is available to be used with email template "Passcode Notification".

3 App - Passcode Expiry and Resend

Passcode required to login FL using 3rd party links will now be expired based on the timeout set by the organization under their org setting. Passcode expiration time will be determined by the minutes set

under "Passcode Timeout" field on Signature tab on Org Settings page. This timeout will be applied for all the requests that use passcode for authentication.

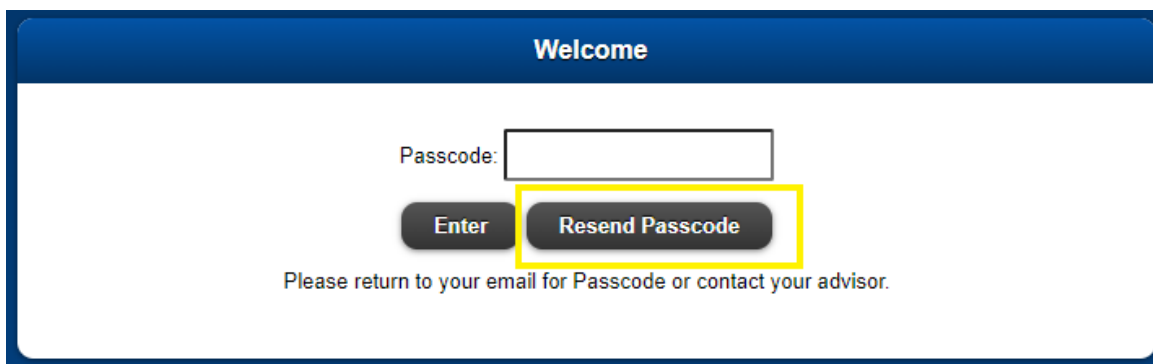
1. Request Client to Fill App
2. Request Client to Fill & Sign
3. Send Email Request to Agent for Signature
4. Send Email Request to Client for Signature
5. Send Review Request to Reviewer
6. Generate Link Without Email
7. SMS Text Authentication
8. Client Verification

When passcode timeout is set as "0" in the org setting, passcode will never expire.

If the passcode has expired, but the link/request is active, the user can send a request to resend/regenerate the passcode and send via email or text (as applicable). When the user enters an expired passcode, an error message appears, and the "Resend Passcode" button gets enabled to allow user to regenerate and send their passcode. The error message that appears is "Passcode has expired or invalid.".

Example: External login that allows authentication via passcode

A "Resend Passcode" button will be placed on this screen to allow user to send a request to resend/regenerate the passcode. This button will appear/enable after the passcode timeout.



Welcome

Passcode:

Please return to your email for Passcode or contact your advisor.

Welcome

Last 4 Digits of SSN/Government ID:

Birth Date (MM/DD/YYYY):

Enter

OR

Passcode:

Enter

Resend Passcode

Please return to your email for Passcode or contact your advisor.

Clicking "Resend Passcode" button will regenerate the passcode for the request and send it to the user via email or SMS text (as applicable).

When the request is valid and the passcode has expired, the pending request dialog will show "Expired" in place of the passcode value currently displayed. The user can click "Resend Passcode to <Recipient>'s Cell Phone" or "Resend Passcode to <Recipient>'s email" links to regenerate the passcode for that external request.

Pending Requests

Request Type: Client Fill Application Owner

Recipient: Valued Client

Email Sent To: KChoubisa@insurancetechnologies.com

Create Date: 9/12/2022

Passcode: Expired

Documents Required:

Outside Illustration: In progress

Voided Check: In progress

[Send Reminder to Valued Client](#)

[Resend Passcode to Peter Hynes's Cell Phone](#)

[Resend Passcode to Peter Hynes's email](#)

[Cancel Request](#)

Close

Pending request dialog appears:

1. As a pop-up dialog when an activity loads.
2. Other Actions > Requests.
3. All Activities page (displays "(Pending Requests!)" under the activity name if there is a pending request).
4. All Activities page > Requests (button) - button is enabled for an activity if that activity has a pending request.

Acceptance Criteria

- Passcode expires after the time (in minutes) configured in Organization Settings.
- If the organization has set unlimited ("0") time for passcode timeout, the passcode never expires and allows user to use the passcode while the request is active.
- Authentication screen allows users to "Resend" request to regenerate the passcode.
- On the pending request dialog, when the passcode has expired, agent is able to resend it to their email or cell phone.
- When the passcode has expired, and the request is active, "Expired" appears on the pending request dialog.
- When the user enters the passcode on external request page and the passcode has expired, "Resend Passcode" button displays.
- When the user enters the passcode on external request page and the passcode has expired, alert message appears. [Error Message]
- New field in InterestedParty object to hold passcode expiry value