Two-Factor Authentication Implementation Guide

E-Closing

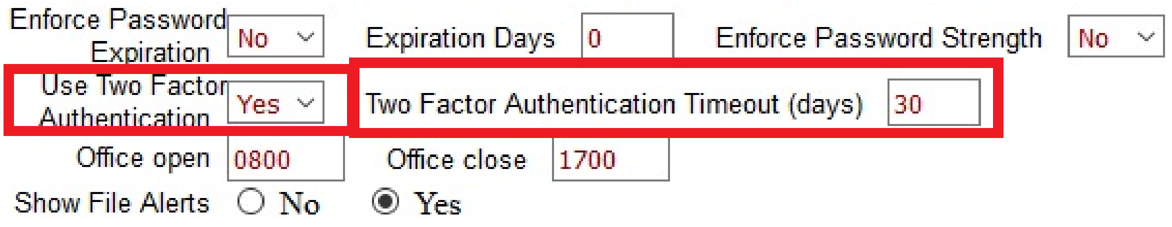
YOUR ONLINE SETTLEMENT HUB

About:

At E-Closing data security and consumer privacy is one of our top priorities. With an increase in cyber-attacks and phishing schemes it has become increasingly important to strengthen the systems that we use to protect NPPI. The first level of defense, or factor, for most systems is a username and password. We can all agree on the importance of implementing strong passwords and regular password resets and within E-Closing we provide you with the tools necessary to enforce these habits. However, in today's day and age a single factor like a username and password combination is not enough to adequately protect the data we collect during financial transactions. That is why we have implemented an added level of security that allows your users to validate their credentials using their mobile phone. This secondary level of protection will require your users to validate their credentials any time they are logging in from an unregistered network and at regular periodic intervals. This implementation guide will walk you through the process of implementing two-factor authentication for your office. While two-factor authentication is currently an optional feature within E-Closing at some point it may not. As always please do not hesitate to contact us by phone (603) 485-7951 or by email support@e-closing.com with any questions.

Enabling Two-Factor Authentication

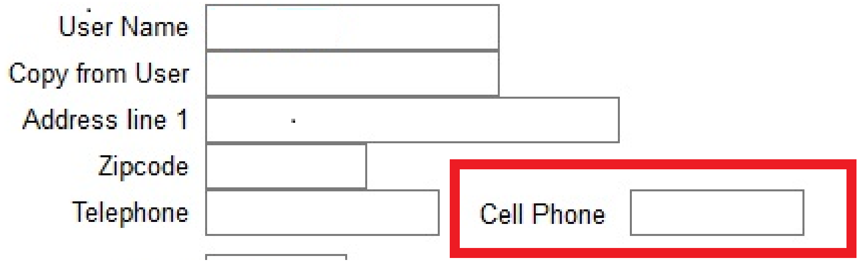
Two-Factor Authentication can be enabled company-wide by going to Back-Office – Rolodex Menu – Manage Rolodex and selecting “This Company” from the business type drop-down menu. Within your companies rolodex record there are two settings that pertain to Two-Factor Authentication. The first is labeled “Use Two-Factor Authentication” which defaults to No and should be switched to Yes to enable this feature. The second setting is labeled “Two Factor Authentication Timeout (days)” which is used to set the number of days that can elapse between credential validations assuming your users are logging in from the same network. If a user logs in from an unknown network they will be required to immediately validate their credentials. Validation occurs when a user receives a unique validation code sent by text message to their mobile device and is entered when prompted to validate credentials.



Enforce Password Expiration: No
Expiration Days: 0
Enforce Password Strength: No
Use Two Factor Authentication: Yes
Two Factor Authentication Timeout (days): 30
Office open: 0800
Office close: 1700
Show File Alerts ○ No ● Yes

User Settings to Receive Text Message Validation Codes

In order for the Two-Factor Authentication to properly protect your account from unauthorized access you will need to store a valid cellphone number for each of your users in their user records. You can access these records by going to Back Office – Misc. Menu – Manage Users and clicking on each of your company users. The field that will need to be filled in is labeled “Cell Phone”.

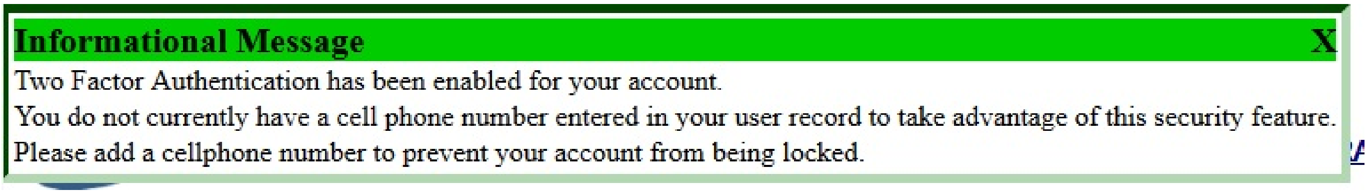


User Name
Copy from User
Address line 1
Zipcode
Telephone
Cell Phone

Two-Factor Authentication in Practice

Now that you have enabled TFA and registered cell phone numbers for each of your users this is how the feature will work to protect your account:

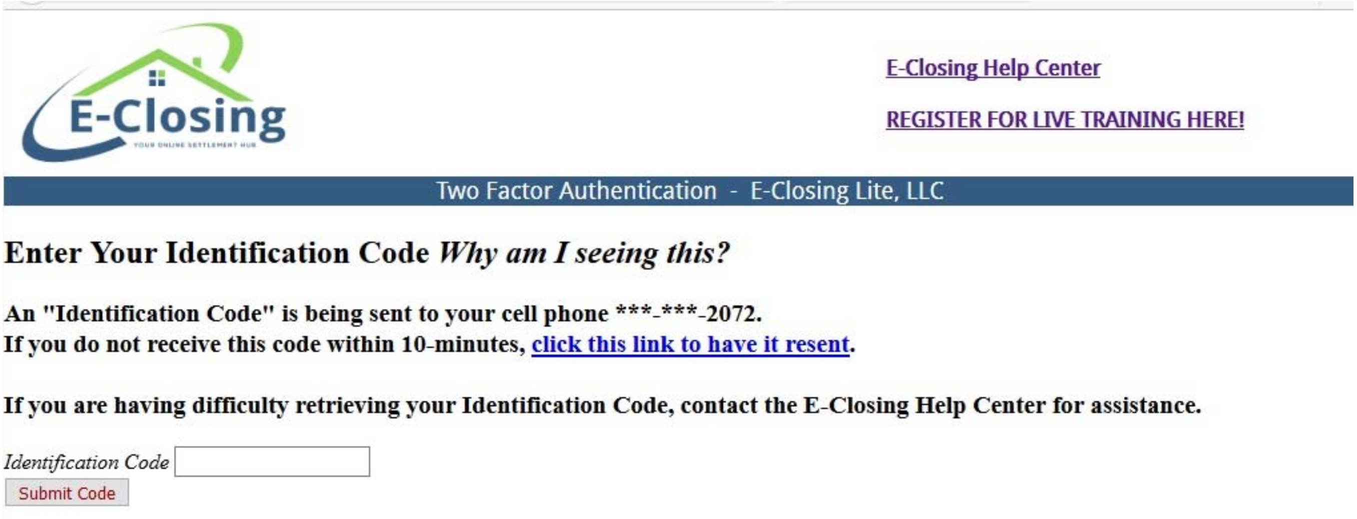
If a user logs in and does not have a registered cell phone entered in their user record they will be presented with the following informational message:



Informational Message

Two Factor Authentication has been enabled for your account.
You do not currently have a cell phone number entered in your user record to take advantage of this security feature.
Please add a cellphone number to prevent your account from being locked.

Users who have valid cell phone numbers entered in their user record will be presented with the following screen upon login and will receive a text message with their one time passcode. This passcode will need to be entered before being allowed access to your account.



E-Closing Help Center

REGISTER FOR LIVE TRAINING HERE!

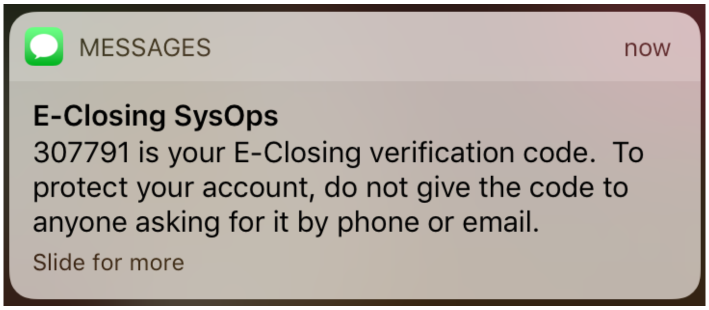
Two Factor Authentication - E-Closing Lite, LLC

Enter Your Identification Code ***Why am I seeing this?***

An "Identification Code" is being sent to your cell phone *-***-2072.**
If you do not receive this code within 10-minutes, click this link to have it resent.

If you are having difficulty retrieving your Identification Code, contact the E-Closing Help Center for assistance.

Identification Code



E-Closing SysOps
307791 is your E-Closing verification code. To protect your account, do not give the code to anyone asking for it by phone or email.
Slide for more