Reference Guide

Strategies for Securing and Controlling Member Access

INSIDE THIS GUIDE:

This guide describes the strategic decisions your credit union should make to secure and control member access to **It's Me 247**.

Last Revision date: December 23, 2025

Find other Reference Materials page on our website: https://www.cuanswers.com/resources/doc/cubase-reference/

Start your online help journey here:
https://help.cubase.org/cubase/Welcome.htm

Table of Contents

Access Terminology to Learn

The following terms explain controls on a member's access to **It's Me 247** that are used within this publication.

Activate / Deactivate / Activation – Refers to the Activate Online Banking box that is turned on to allow a member to access their account through online banking. If turned off, the member cannot use the system at all. This is controlled via the *Update Online Mobile Banking Access* screen. See page 24 for more information.

Complex Passwords – If you have not already done so, your credit union has the option to force your members to make complex passwords. Complex password rules require three of the four following: uppercase letter, lowercase letter, number, and special character. Once you activate this feature, members without complex passwords will need to change their password to be complex the next time they log in. This is activated in the *Online/Mobile Password and Security Settings* screen. (See page 15.)

Custom Password – Your credit union can allow credit union employees to enter a custom password for the member via the *Update Online Mobile Banking Access* screen. (See page 25 for more information on resets.) These passwords are temporary. The member must change the password when they log in. This feature is activated in the *Online/Mobile Password and Security Settings* screen. (See page 15.)

Disable - Refers to when a member tries to access online banking with an incorrect password/security question combination 3 times in a row. In this case, the actual password on the member's record is cleared and must be reset to a temporary password to get back into **It's Me 247**. **This has no effect on the actual Activation flag.** Refer to page 25 for more information on resets.

Expired Due to Non-Use (Stale Password) - Refers to when a member has not used **It's Me 247** for a period, determined by the expiration period (in days) in the *Online/Mobile Password and Security Settings* screen. (See page 15.) The expiration period is evaluated with the member's *Last Logged In Date* every time they attempt to log in. **This has no effect on the password itself or the Activation flag.** Passwords can be set to expire after 1-90 days of non-use. (Or the credit union can set the expiration period to 999 days to never expire passwords due to non-use.)

Hide My Typing – Members can use this option and click an eyeball icon to view asterisks when entering the answer to a security question when logging on to **It's Me 247**. (See following entry on Security Questions.)

Inter-Member Transfers – Inter-Member Transfers allow members to transfer to other members at your credit union. Two options exist for inter-member transfers, and the credit union can select to allow one or both options. See page 40 for more information.

Maximum Password Length/Minimum Password Length – The maximum length a member's password is set by the system at 256 characters. The minimum length is set by the credit union and must be six to ten characters. Activate this feature in the *Online/Mobile Password and Security Settings*. (See page 15.)

Multi-Factor Authentication (MFA) – *Also known as two-factor authentication.* Credit unions can configure that a member enters a code that is texted or emailed to them for authentication to access certain online banking features such as:

- During standard login

- During first-time authentication
- When making Pay Anyone transfer (Person-to-Person transfer services)
- When updating their personal information
- When resetting their password using the "I forgot my password" feature.

Discussion of the various MFA options available to your credit union begins on page 15.

Promotional Campaign - Credit unions can run promotional campaigns to encourage members who fit certain requirements to take it for a "test drive." See promotional campaign section (beginning on page 29) for directions on setting up and running a promotional campaign.

Reset - Refers to having an MSR take the option that changes the member's password to the temporary password setting. The system will require the member to change the password immediately upon login. Perform a reset on the *Update Online Banking Access* screen. This screen allows the employee to reset other credentials such as username and security questions. (See page 25 for a more complete discussion on resets and resetting credentials.)

Jump – Activate this feature and grant the appropriate permissions. Then the member can login to one membership, and from there, the member can "Jump" to another account (with appropriate permissions). See page 39 for details.

Security Questions – Members select these questions and answers the first time they log into online banking. Security question answers can be a maximum of thirty characters, allowing the member to create a phrase as an answer. Then the member answers one of these questions in conjunction with the password request each time they log into **It's Me 247**.

My member is trying to log into online banking and their security question does not work. Why might that be the case?

Special Character – Members must use three of the following: lower case letter, upper case letter, number, and special character to comply with complex password requirements.

Some special characters are not allowed because they are used by certain programming languages. Permitted special characters appear on the password change screen and the screen where the security questions and answers are set up.

Learn more in this knowledge base item: What special characters are allowed in online banking passwords, security question answers, and personalized security questions? Which ones are not allowed?

Temporary Password – Members get a "temporary password" whenever the credit union grants them access, including password reset, new member password, new enrollment with a "# of days," or password for promotional campaign. As a general rule temporary passwords are valid for 24 hours, but the length of time this password is valid depends on the method by which the password is set.

Credit unions have four selections for their temporary password, including:

- Last four digits of SSN
- First four digits of SSN/TIN and last two letters of last name/company name (all CAPS)
- 4-digit birth/charter year and first two letters of last name/company name (all CAPS)

- Last four digits of SSN/TIN and 4-digit birth/charter year

Selection is made on the *Online/Mobile Password and Security Settings* screen. (See page 15.)

Transfer Control List – Transfer control lists can be used to control to which memberships (at your credit union) that a member can transfer to via the Transfer Wizard, as well as the accounts used for ACH Distribution and Automated Funds Transfer (AFTs) set up by the member in online banking. This list also dictates transfers made via Mobile Web Banking; Credit unions control the addition of memberships to this list. See page 40 for more information.

Two-Factor Authentication – See Multi-Factor Authentication.

Username – Members create a username while in **It's Me 247** to use in place of the account number at login. Credit unions can elect to require usernames. In this case, the feature is not optional, and all members must create a username. Usernames can be a maximum of twenty characters.

- Refer to page 28 for more information about usernames.
- Activate required usernames on the *Online/Mobile Password and Security Settings* screen. (See page 15.)
- Refer to page 9 for rules when creating usernames.
- The *Update Online Banking Access* screen allows an employee to reset usernames. (See page 25.)

Security Overview

It's Me 247 is an online banking product designed to safeguard your members' money and privacy by using the latest Internet security technologies. To further ensure security, the system applies these protective technologies in layers to address each phase of the online transaction.

Transmission security is provided by using 2048-bit SSL encryption, ensuring that only the member and the **It's Me 247** systems can read the transaction information as it flows across the Internet. Through our use of digital certification, the system assures the members that they are communicating with the legitimate **It's Me 247** servers and not an imposter.

A combination of segregated network architecture, hardened server configurations, and redundant firewalls provide access security. Our segregated network architecture separates the **It's Me 247** servers from the systems that contain member data. Consequently, these systems exchange member data only using a valid member request following verification of Member Account Number and password. Internet-based attacks (hackers) are stopped using redundant state-of-the-art firewall technology and hardened server configurations.

To ensure that **It's Me 247** security measures continue to meet the ever-changing security threats of the Internet, **It's Me 247** is reviewed on an ongoing basis by regulators and expert security consultants as well as being monitored by CU*Answers network engineers.

Minimum Usage Requirements

Remember that as security requirements and the Internet world change, so will these requirements. If a member is having trouble accessing **It's Me 247** features, the first step is always to upgrade the browser software.

- Supported browsers are the two latest versions of: Chrome, Firefox, Edge, and Safari.

Modern browsers provide features and benefits that older browsers may not:

- CSS3
- HTML5
- Faster Speed
- Safer Protection
- Continued Support from major vendors.

Older/legacy browsers can also cause problems with websites and applications you use frequently. In these older browsers you may have trouble using certain features in **It's Me 247** Online Banking.

- NOTE: Because phones can vary, desktop **It's Me 247** features are not warranted on mobile devices. For best results, use a computer with desktop **It's Me 247**.

Access Security

User account security is furnished using a unique Member Account Number (or username) and a combination of password and security question answer known only to the member. Without this information (account number or username, password, and security question answer), accessing account data and initiating transactions online is impossible.

Passwords

Considering the increasingly security-conscious environment of the Internet, **It's Me 247** Online Banking offers many controls for managing the passwords used by members to gain access to their accounts.

- Online banking passwords can be up to **256 alphanumeric characters**, including special characters.
- Passwords are **case-sensitive** (i.e., Ds443&sld is different from dS443&SLD)
- Passwords can include a blank space.
- You specify a **minimum number of characters** (6 to 10, the configuration requires at least six characters). This is set in the *Online/Mobile Password and Security Settings* screen. (See page 15.)
- If desired, you can force members to follow **complex password** rules (requires three of the four following: uppercase letter, lowercase letter, number, and special character). Activate this feature in the *Online/Mobile Password and Security Settings* screen. (See page 15.)

NOTE: Certain special characters are not allowed because they are used by special programming languages. Permitted special characters appear on the password set up screen. Learn more in Answer Book: What special characters are allowed in online banking passwords, security question answers, and personalized security questions? Which ones are not allowed?

If a member enters an incorrect password three times, the password is deactivated, and the member must contact the credit union for reactivation (see page 25) or use the "I forgot my password" feature to reset their password. Additional access controls are in place to control the length of time a temporary or unused password is available to the member without their logging into **It's Me 247**. If a member fails to log into **It's Me 247** within the allowed time, the member will have their password reset.

Online banking passwords can also be configured to expire after a certain period of non-use. Enter a configured number of days (1-90) or enter 999 days to never expire passwords due to non-use. If a member does not log into online banking during this period, the member's password will expire due to non-use, and the account will be locked from access until a password reset. This is set in the *Online/Mobile Password and Security Settings* screen. (See page 15.)

> ***NOTE:** If a member logs into online banking at least one time during this period, the member's password will never expire.)*

This expiration comes into play only after a member has not logged into **It's Me 247** for a certain period. This provides an extra measure of security for dormant memberships or members who do not choose to use your self-service options. If someone attempts to access the member's account after the expiration period, the application displays a message instructing the user to contact the credit union to reactivate the password. Members can also use the "I forgot my password" feature to reset their password.

Like your credit union's dormancy procedures, we designed this feature to help limit the risk that an unauthorized person could access an unused account.

It's Me 247 monitors authorization every time a member attempts to log in and controls access by comparing the last date the member logged in with the date to the configured expiration period. Remember that you can also choose to disable an individual member's access to these systems completely.

> *NOTE: As covered above, your credit union has the option to set online banking passwords to never expire. With this configuration, members' passwords will never expire due to non-use.*

Security Questions

It's Me 247 *requires* users to answer a **challenge question** in addition to supplying a password each time they login to online banking. When logging into online banking for the first time, members must set up 3 security/challenge questions. These can be used to reset the member's password if they have forgotten their password. To log in to online banking, members must enter their password *and* answer one of the three questions they set up. Answers can be a maximum of thirty characters.

> ***NOTE:** These security question answers and customized security questions cannot have certain special characters in them. Learn more in Answer Book.*

Since answers can be a maximum of 30 characters, this gives the member an opportunity to create a longer, harder to guess passphrase to work in tandem with the password.

> ***A Note About Security Questions:** For maximum security, members can choose to use their security questions as a second, longer "passphrase." A passphrase is essentially a sentence used for the purposes of a password, and due to its length, it is much harder for hackers to guess. "A passphrase is hard to guess!" is exactly 30 characters, and according to some sites, would take a hacker over a billion years to crack! For members concerned about*

password security, recommend that they use their security questions as a secondary passphrase.

Usernames

A member can create an *optional* username while in **It's Me 247** that the member can use *in place of* the account number when they log into online banking. Once the member has set up a username, they can change it at any time in online banking, but they can't clear it. Credit union employees cannot create usernames for members. However, CBX does have a feature to clear the username so that the member is prompted again for a new one.

- **Rules for Usernames:** Usernames can contain all letters or a combination of letters and numbers. They can contain spaces, but not special characters. They are not case-sensitive. Usernames cannot contain the account number nor the member's first or last name. Usernames can be a maximum of twenty characters.

Credit unions can elect to require usernames. In this case all members must create a username (either as part of the initial login process or the next time they login. Then going forward, members log into online banking using their username in place of the account number. Activate required usernames in the *Online/Mobile Password and Security Settings* screen. (See page 15.)

Grant New Member Access to Online Banking

Your credit union has various ways to grant new members access to online banking.

- Your credit union can elect to require a new member to use multi-factor authentication to access online banking. More discussion of this feature is covered in the MFA section of this booklet starting on page 15. This includes a discussion of several uses of MFA codes to access both online banking and online banking features.
- If you decide not to use MFA, your credit union can configure a period **(from one to seven days)** that the new member temporary password is valid (from the membership open date). The number of days is set in the *Online/Mobile Password and Security Settings* screen. (See page 15.)
- You can choose to define a **promotional period** to allow selected active members to try **It's Me 247** for the first time or start up again if their usage has dropped off after a period. Refer to page 29 for more information on the setting up of a promotional campaign.

As a note, you can always block a member from online banking via the Fraud Block List. Learn more in online help Overview: Fraud Block Lists. Access Fraud Block Lists via **Tool #892 *Fraud Block List/Blocked Persons List***. Refer to page 24.

Layered Security through the PIB Profile

As a companion to the security features already available in **It's Me 247**, we also offer an optional layered security approach which can be activated as a companion to **It's Me 247**. A Personal Internet Branch (PIB) Profile lets your members assume only the risks they are comfortable assuming on the Internet and allows for additional layers of security for selected transaction types, such an inter-member transfers, updating personal information, and accessing the online bill pay system.

For complete details about implementing PIB, refer to the **It's Me 247** Personal Internet Branch (PIB) Configuration and User Guide reference guide.

Security Decisions to Make

Whether you are launching **It's Me 247** for the first time or trying to establish a sound strategy for managing member passwords and access to **It's Me 247**, use the following checklist to make sure you have covered all the bases. Configure many of these features on the *Online/Mobile Password and Security Settings* screen. (See page 15.)

If you would like to make any changes to other of your configuration settings or would like to discuss the options further, contact a Client Service Representative or fill out the **It's Me 247** Configuration Change Request Form available on our website and submit a store order to request.

Decision	*Choices Offered by **It's Me 247** / CBX*	*For configuration…*
Activation Settings		
Will multi-factor authentication (MFA) code be used for access?	Credit unions can select from Temporary Password Reset or MFA to control a member's first-time login experience. The member logs in using their account number and social security number. This prompts them to have a code sent to a phone or email associated with the membership for a multi-factor authentication experience.	This is activated in the *Online/Mobile Password and Security Settings*. (See page 15.) *Pictures of the members' MFA experience shown starting on page 19.*
Would you like to activate all members to start, but then "close" the enrollment period after a period of 1-7 days?	▪ Check to activate all online banking enrollments; also activate all new memberships automatically. ▪ Credit unions can select to have a new member temporary password valid for one to seven days past the creation date of the membership (seven is the default). ▪ The members will not be able to access their online account after a configured period (1 to 7 days with 7 being the maximum allowed). The member logs into online banking, entering their account and temporary password.	This is activated in the *Online/Mobile Password and Security Settings* screen. (See page 15.) To allow a member in after the period, the MSR must <u>reset</u> the password using the *Update Online/Mobile Banking Access* screen. (See page 25.)
Should all existing memberships be activated automatically?	▪ You can elect in the configuration of **OPER Tool #5356 *Online Banking Configuration*** to activate online banking for all new memberships.	Contact a Client Service representative for assistance. For newly converting credit unions, talk to your Conversion Coordinator about the desired setting when your credit union switches to CBX and **It's Me 247.**

Decision	*Choices Offered by **It's Me 247** / CBX*	*For configuration…*
		For existing credit unions, contact Client Services for information about custom programming to "flood" the activation flag setting for all your memberships.
If members are not automatically activated, how do they become activated?	▪ Develop an internal policy and procedure MSRs and phone staff can use to sell online banking and activate the new member's account. ▪ Give staff tips for talking to members - for example, ask members whether they want the option to use online banking whenever they are ready, to sign up now, or to disable the account so it cannot be accessed via **It's Me 247** until requested.	Use the *Update Online/Mobile Banking Access* screen (see page 24) to activate a member's account.
Should new members be activated with a promotional campaign?	While this is not as frequently used, a promotional period may be used to activate new members. ▪ Check to activate all online banking enrollments; also activate all new memberships automatically. ▪ Credit unions can select to have a new member's temporary password valid for one to seven days (seven is the default). ▪ The members will not be able to access their online account after a configured period (1 to 7 days with 7 being the maximum allowed). ***IMPORTANT: Remember** that if you do not activate members, the promotional features will only apply to members who have been activated but then do not use **It's Me 247** actively.* ***IMPORTANT:** Running a promotion will NOT work for the rest of your membership because the member activation flags will have been turned off. Therefore, we recommend you activate all, then control access with new member password controls or deactivate all and only use expiration for controlling inactive members.*	Use **Tool #234 *Config New Online User Promo Campaign*.**
Do you want to market an open enrollment period on a regular basis?	▪ Configure promotional campaign periodically to encourage members who are active but not allowed access due to an expired password, such as once or twice a year. (See above also.)	Use **Tool #234 *Config New Online User Promo Campaign***.

Decision	*Choices Offered by **It's Me 247** / CBX*	*For configuration…*
What if a member misuses the system or requests that no access be allowed to their accounts via online banking?	▪ Any member account can be permanently disabled from online banking.	Use the *Update Online/Mobile Banking Access* screen (see page 24) to change the activation flag to disable an account.
Passwords		
What should the temporary password setting be for the credit union?	If the MFA option for login is not selected, then members get a "temporary password" any time the credit union grants them access without specifically setting a custom password. This can be via regular password reset, new member enrollment activation, or promotional campaign. Credit unions have four configurations to select from for their temporary password, including: • Last four digits of SSN • First four digits of SSN/TIN and last two letters of last name/company name (all CAPS) • 4-digit birth/charter year and first two letters of last name/company name (all CAPS) • Last four digits of SSN/TIN and 4-digit birth/charter year	This is activated in the *Online/Mobile Password and Security Settings* screen. (See page 15.)
Should usernames be required?	Your credit union can elect to require usernames are used in place of account numbers when logging into online banking. ▪ In this case, all members must create a username (either as part of the initial login process or the next time they login). ▪ Then going forward, members logging into online banking use their username in place of the account number. ▪ Members create usernames in online banking. Usernames can be viewed and deleted in CBX but cannot be added for the member.	For newly converting credit unions, talk to your Conversion Coordinator about the desired setting when your credit union switches to CBX and **It's Me 247**. This is activated in the *Online/Mobile Password and Security Settings* screen. (See page 15.) *Refer to page 9 for rules when creating usernames.* *Refer to page 28 for more information about usernames.*

Decision	*Choices Offered by **It's Me 247** / CBX*	*For configuration…*
Do you want to force complex password rules?	▪ Activate the complex passwords flag.	This is activated in the *Online/Mobile Password and Security Settings* screen. (See page 15.)
What should your expiration period be for members who do not use **It's Me 247** regularly?	▪ Configure expiration period by number of days (1-90 days, for example 60 days). (Select 999 for never to expire.) ▪ If expired member tries to log in, they will be notified as follows: **It has been more than xx days since you last logged in. Your password has expired. Please contact the credit union to reactivate your password.**	This is set in the *Online/Mobile Password and Security Settings* screen. (See page 15.) See page 25 for more information on password resets.
What experience should the members have when they initiate their password reset themselves? ("I forgot my password")	▪ Credit unions can elect that when a member uses the "I forgot my password" feature, they are required used two-factor authentication. At that point, the member must log into online banking using the new password and by answering a security question. ▪ Otherwise, the members must answer three security question answers to reset their password.	This is activated in the *Online/Mobile Password and Security Settings* screen. (See page 15.)
Maintenance Tasks		
Do you want to allow your staff to set custom passwords for members who are having trouble setting up their own?	▪ This gives you the option to allow members to have a custom temporary password that is not the temporary password setting configured by your credit union. ▪ Members must still log in and change their password within 24 hours or else they will need to reset their password again. ▪ Develop an internal credit union policy and procedure for your staff.	This is activated in the *Online/Mobile Password and Security Settings*. (See page 15.) Use the *Update Online/Mobile Banking Access* screen (see page 25) to set custom passwords.
How will MSRs validate identity when a member calls to be reactivated after their password has expired?	▪ Develop an internal credit union policy and procedure for your staff.	To allow a member in after the expiration period, the MSR must reset the password using the Update *Online/Mobile Banking Access* screen. (See page 25.)
What if a member loses their password?	▪ Develop an internal policy and procedure MSRs and phone staff should use to verify identity.	Use the *Update Online/Mobile Banking Access* screen to

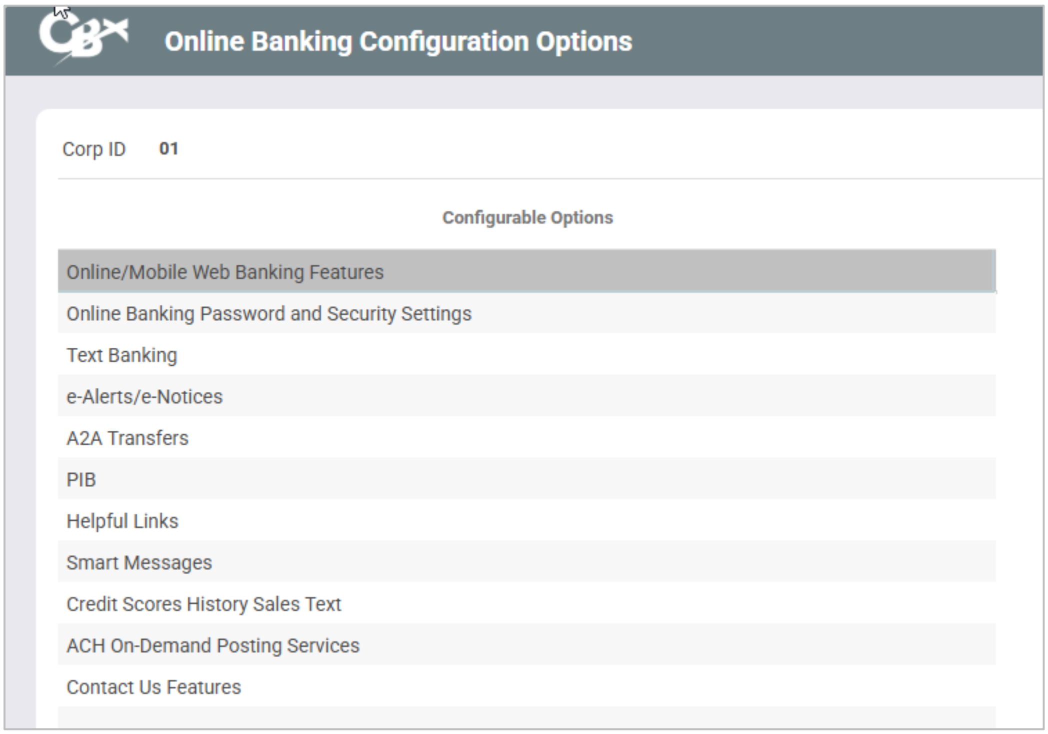
Decision	*Choices Offered by **It's Me 247** / CBX*	*For configuration…*
	▪ Reset the password to the configured credit union temporary password; the member will be required to change it immediately upon logging in.	reset a password. (See page 25.)
What if a member knows their password but forgets the answers to their challenge questions?	▪ Develop an internal policy and procedure MSRs and phone staff should use to verify identity. ▪ Delete the member's challenge questions and answers in CBX; the member will be required to select new questions and answers immediately upon logging in. ▪ NOTE: The credit union employee can see the questions in CBX via Phone Operator, but not the answers.	Use the *Update Online/Mobile Banking Access* screen (see page 25) to reset the security questions.
What if a member forgets their password and forgets the answers to their challenge questions?	▪ Develop an internal policy and procedure MSRs and phone staff should use to verify identity. ▪ Delete the member's challenge questions and answers in CBX as well as the password. ▪ The member will be required to immediately log in using the temporary password and to change their password. ▪ The member will also change the answers to the challenge questions immediately upon logging in. ▪ NOTE: The credit union employee can see the questions in CBX on a separate screen but not the answers. See note in the section starting on page 25	Use the *Update Online Mobile Banking Access* screen (see page 25) to delete the member's questions and answers. Conformation will be required. This access also allows you to separately reset the member's password to the temporary password.
What if a member forgets their username?	▪ There is no "I forgot my username" feature in online banking. If members forget their username, they will need to contact the credit union for assistance, just as members do when they forget their account number. ▪ Develop an internal policy and procedure MSRs and phone staff should use to verify identity. ▪ Either view or delete the member's username. NOTE: The employee can view the member's username prior to deleting it. ▪ Refer to page 9 for rules when creating usernames.	Use the *Update Online/Mobile Banking Access* screen (see page 25) to view or delete the member's username. Confirmation will be required if deleted. The member will then need to create a new username the next time they log into online banking.

Online/Mobile Password and Security Settings/MFA Configuration

Credit unions can set up many of their online and mobile password settings themselves; however, they can also ask a Client Service Representative for assistance. Many of these settings have been covered previously in this booklet.

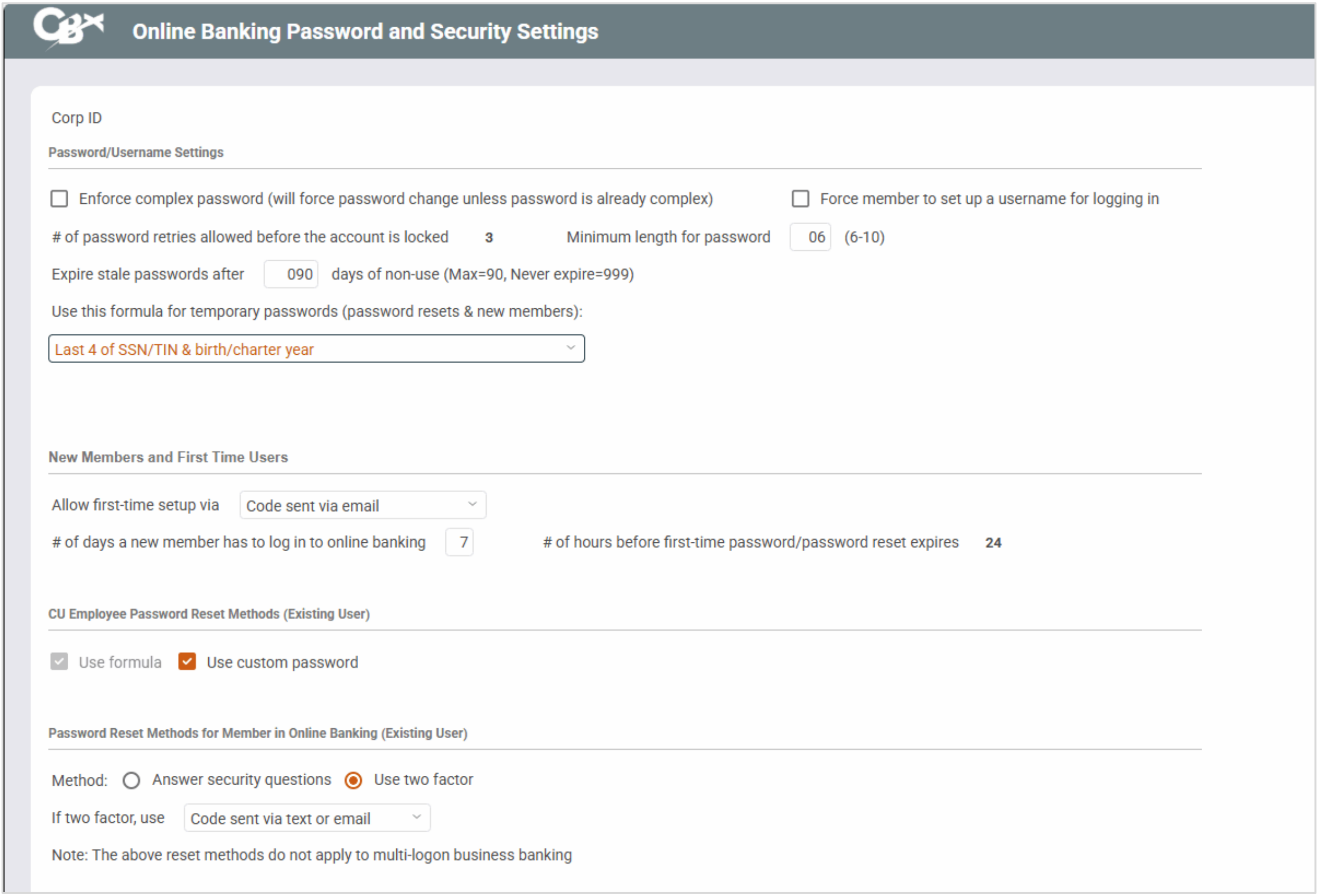
To access the Online/Mobile Password and Security Settings, use **Tool #569 *Online/Mobile/Text Banking VMS Config***.

Online/Mobile/Text Banking VMS Config (Tool #569)



From here, select *Online Banking Password and Security Settings*.

Online Banking Password and Security Settings (Tool #569)



Here you can set online banking password configurations, including your temporary password configuration and minimum password length, without having to contact Client Services to access the controls for you. You can also set your first-time member login experience, including MFA or # of days that the member must log in before their password expires.

To finalize changes on this screen, click **Update** to advance to the second screen shown on page 19.

For more information on the features on the screen above, refer to the Security Decisions to Make section on page 10.

More detailed field descriptions for all the security features on this screen are documented in CBX Online help. Refer to the online help topic: Online/Mobile Password and Security Settings.

Multi-factor (MFA) Access for First Time Users

Included in the settings of the first Online Banking Password and Security Settings screen shown previously is the configuration for first time users' two-factor authentication option.

Configuration

In the **New Members and First-Time Users** section, the field *Allow first time setup via email and/or text message* allows your credit union to activate MFA for first-time users. To use this method, select which delivery method you would like members to use: email, text, or both.

> *NOTE: The alternative using MFA for first-time and new users is to have the member log in with a temporary password and to configure a "# of days a new member has to log in to online banking" on the screen shown previously. Refer to the Security Decisions to Make section on page 10 for more information, as well as the related online help topic.*

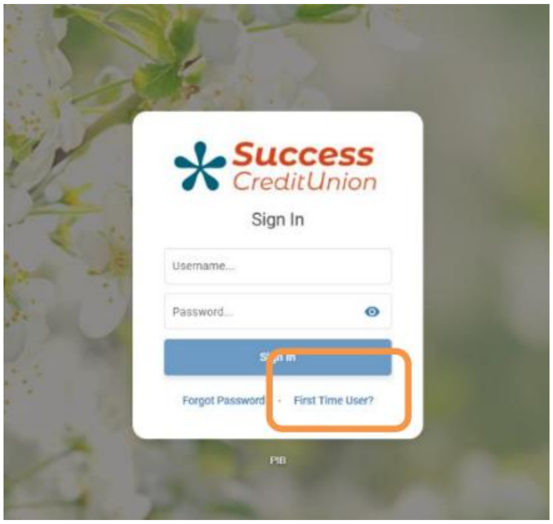
Member Experience

Once this feature is activated, the members will experience a different first-time enrollment flow. The member will then access online banking and select a link labeled "First Time User?." Instead of entering in the temporary password, they will be required to use the code. The email or phone number that the code is sent to must be associated with membership in CBX. The code is active for 24 hours.

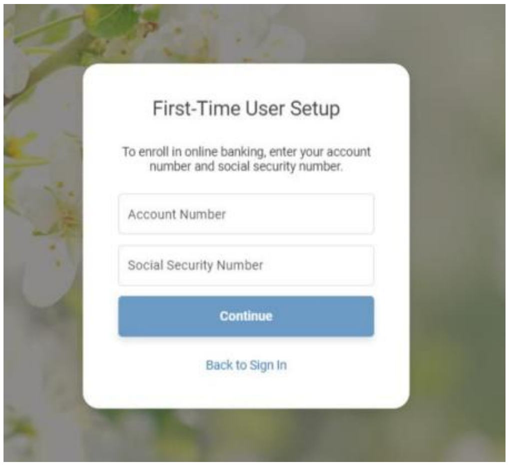
- NOTE: If you do not use the MFA option, your member will simply enter the account and password in the fields provided. A good rule of thumb is not to add the "First Time User?" access point in this interface.

See following screenshots for more details.

First, the member clicks **First Time User**.

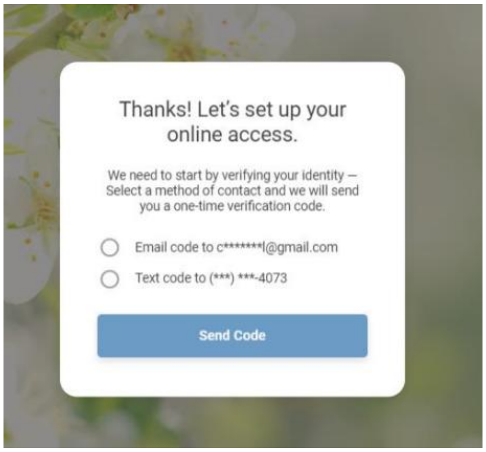


Then the member enters their account number and social security number and clicks **Continue**.

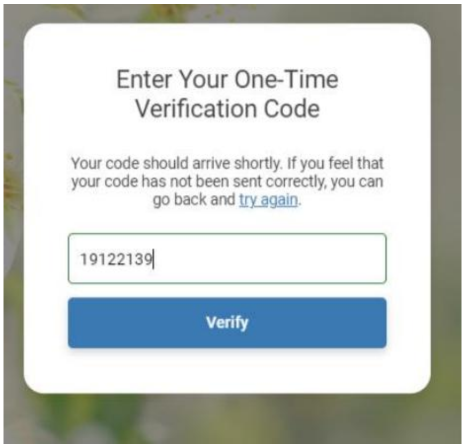


The email and phone numbers presented are already associated with the membership. The member selects where they would like to receive the code and selects **Send Code**.

- This code is active for 24 hours.



The member enters the code and selects **Verify**.

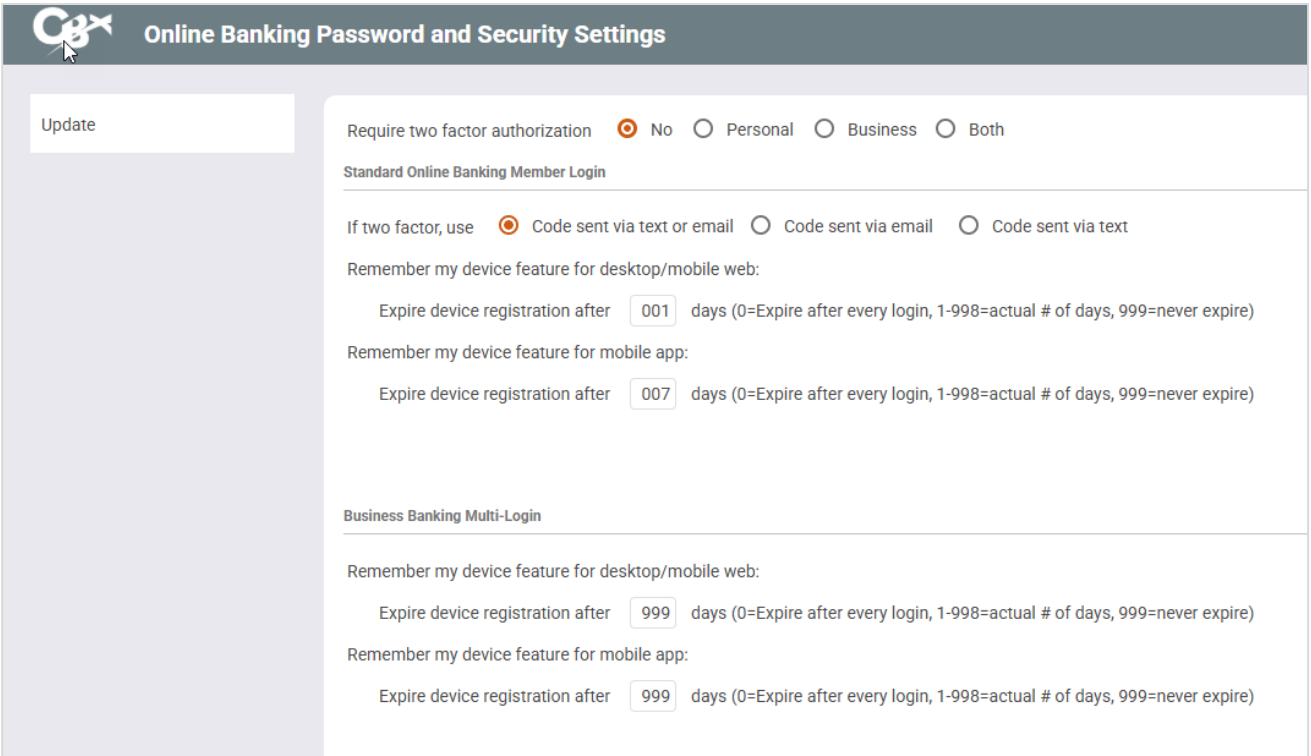


Next, the member sets up their password, username, security questions, etc., as with any first-time login to online banking.

MFA One-time Passcode and Registration at Online Banking Login

The second Online Banking Password and Security Settings screen is shown below. It is accessed by clicking the forward arrow on the first screen shown on page 16.

Second Screen (Tool #569 > Online Banking Password and Security Settings)



Refer to online help for assistance with understanding the fields on this screen. This help topic also includes many informative FAQs.

Configuration

Use the screen above to require that the member request a code for authentication to online banking; these are also referred to as “one-time passcodes” or two-factor authentication. Members can opt to register their device so that authorization isn’t required each time they log in. (See the MFA FAQ below for more details!) Different activations apply to **It’s Me 247** and **BizLink 247**. On this screen, select whether the one-time login passcode will be sent to the members email, phone number, or both.

This is different than first-time MFA covered previously because it could be each time the member logs into online banking.

The number of days before device registration expiration is also configured on this screen. Designate the number of days the device registration will be active for the member’s device before they will need to register via MFA again (999 is never expire). Different settings can also be set for **BizLink 247** business online banking at the bottom of the screen. Additionally, different settings can be configured for desktop/mobile banking versus mobile app banking for each platform.

- Concerned about your members having to use MFA frequently? *Configure a set number of days for the device to be remembered.*
- Concerned your phone database and personal details are not up to date in CBX? *Encourage your members to update their phone number using an online banner, form, or Xtend campaign.*

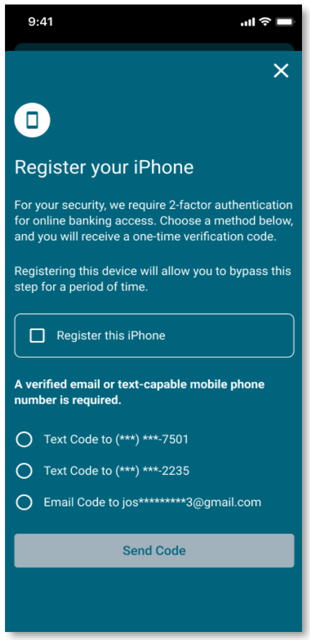
- Interested in having different controls for business banking, standard browser banking, and mobile app? *Set different controls for each in the configuration screen.*

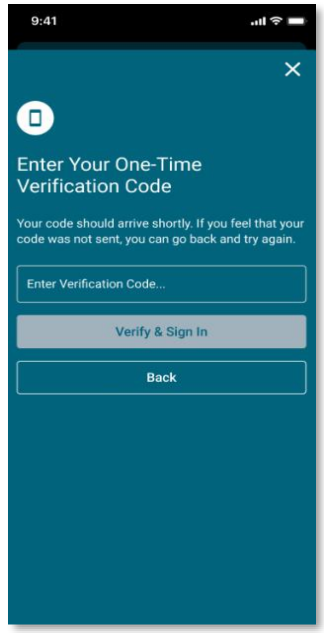
Use **Update** to save the changes. When ready, return to this screen to activate this feature.

Member Experience

The member is presented their options for receiving their MFA code on the first screen. They also have the option to register their device. The second screen allows entry of the code.

- This MFA code is active for 15 minutes.





MFA for Member-Initiated Password Reset

If the member locks themselves out of online banking or otherwise forgets their password, they can use the "I forgot my password" feature to reset their password. Your credit union can optionally elect to require MFA for a member using the "I forgot my password" feature to reset their password. This is like way that members are prompted with first time login and device registration:

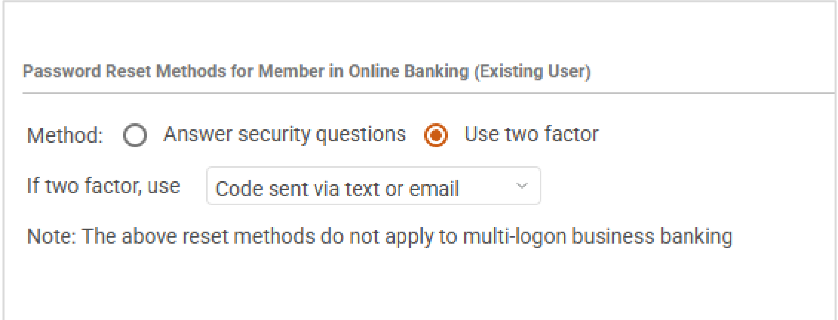
Configuration

This setting is configured at the bottom of the first Online Banking Password and Security screen shown on page 16.

These fields allow your credit union to configure whether members must answer their three security questions (*Answer security questions*) or if they should receive an MFA login code (*Use two factor*) for member-initiated password reset.

If two-factor (MFA) is selected, your credit union can select if the member gets to select to receive their MFA via text message, email, or either.

First Online Banking Password and Security Setting Screen (Bottom)

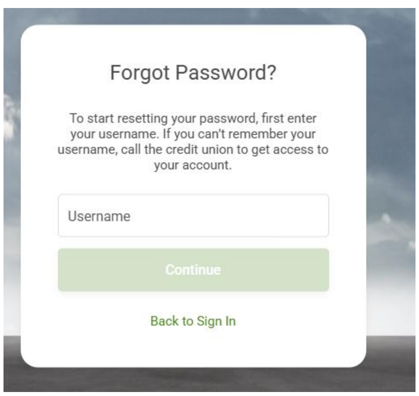


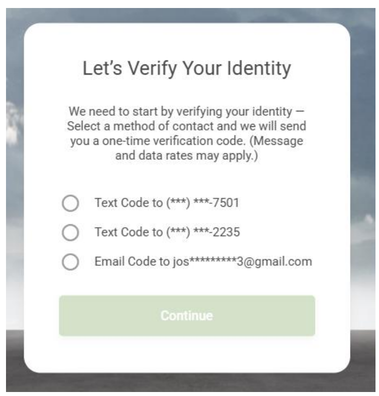
*This feature is only for use with **It's Me 247** and is not for use with **BizLink 247** online banking.*

Member Experience

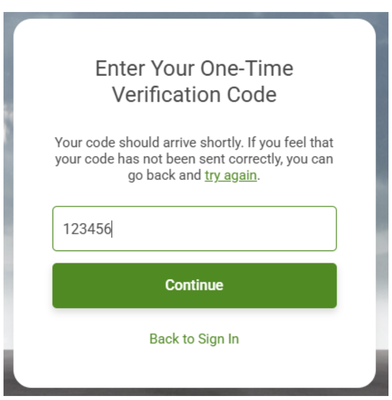
Following is the member experience once they select "I forgot my password":

- Members are prompted to enter their account number or username to request an MFA code via text or email (as allowed by your credit union configuration). They are then asked to select where to send the code.





- They then enter that code in the screen provided.



- The process follows the standard process for updating their password. After resetting their password, the member is then logged off and must log in with a standard password and security question answer.

The member needs to answer a security question when logging into online banking. For this reason, security questions are required. If the member does *not have security question answers already in the system, they will need to contact your credit union for assistance.*

MFA for Pay Anyone or Personal Information Update

Your credit union can also optionally activate MFA to provide even greater security (beyond the initial online banking login) for two member-facing activities (Pay Anyone and personal information updates).

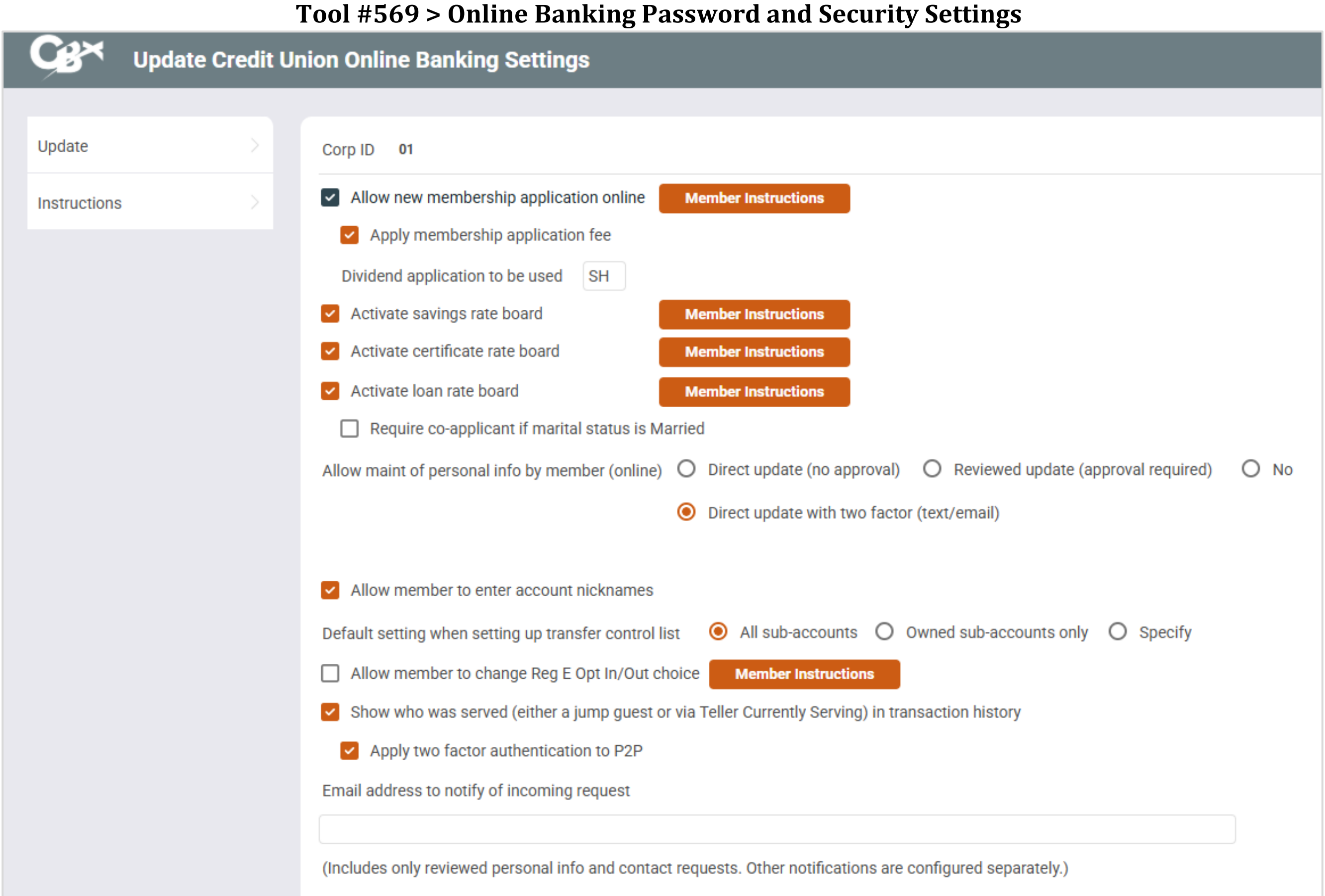
To activate MFA for either of these features, use **Tool #569 *Online/Mobile/Text Banking VMS Configuration*** and then *Update Online Banking Security Settings* to access the screen shown below.

Refer to this help topic for more details.

- **For MFA for personal information changes**, check *Direct update with two factor (text/email)* for *Allow main of personal info by member (online)*.
    - *If you activate this feature for personal information changes, you cannot set the member's changes for review by your credit union. All changes are implemented immediately.*

- **For P2P (Pay Anyone)** check *Apply two factor authentication to P2P*.
    - *This provides MFA to the Pay Anyone module which provides access to enrollment, sending of payments, and unenrollment.*
    - *NOTE: MFA is not supported by the Pay Anyone micro-app. Learn more about the micro app.*

Tool #569 > Online Banking Password and Security Settings

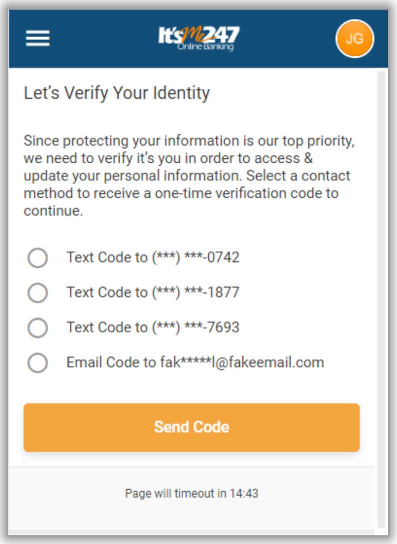


- Use *Direct update with two factor (text email)* as the selection for *Allow maint of personal info by member (online)* to allow direct update of personal information via two-factor authentication.

- Use Apply two factor authentication to P2P to require MFA for P2P transfers.

Once either feature on the previous page is activated, the first MFA pop up window allows the member to indicate whether they want to receive the MFA code via email or text message. The phone numbers and emails presented are configured on the member's membership in CBX.

First MFA Pop Up Window

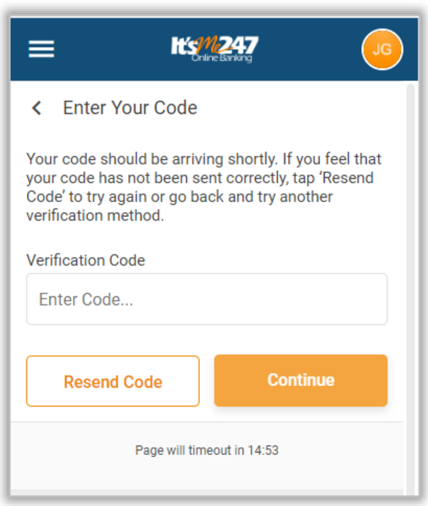


The member selects **Send Code** to receive the code.

- NOTE: This MFA code expires after 15 minutes.

The member then advances to the second pop up window and enters the MFA code in the space provided.

Second MFA Pop Up Window



The member then selects **Continue** to proceed to access the protected feature.

- This access is granted for the entire online banking session. The member does not need to enter a new code until they log off **It's Me 247**. Then, a new code is required the next time they want to access the Pay Anyone module.

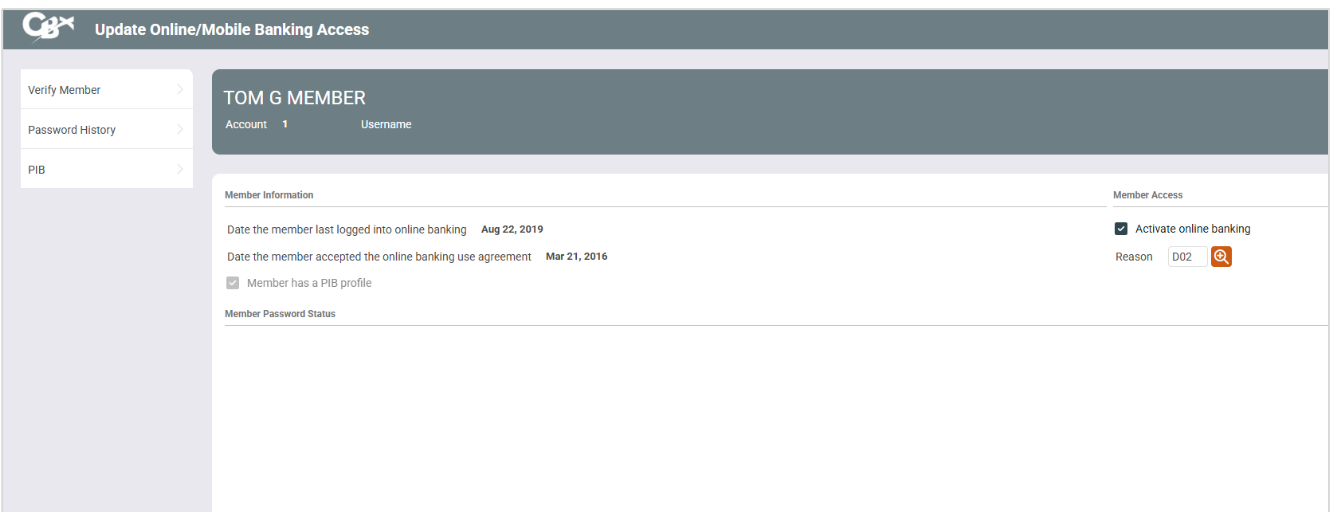
Activating/Deactivating Members Access to Online Banking in CBX

Activation of online banking memberships is configured in the Online Banking controls in OPER. This will typically be activated during conversion to the core. Additionally, your credit union can use a field on this screen to also optionally activate all new memberships to have the *Activate Online Banking* box checked on the screen below upon creating the new membership.

Remember that you can also permanently disable any individual member's account so that access is never granted. See information on disabling the member and fraud lists in this section.

Alternatively, you can activate access for memberships on demand. For example, if a credit union does not activate the member during membership enrollment, it can select to have their MSRs activate the member via this manner. Not only does this method allow you to monitor online banking enrollments, but this method also lets you work directly with a member to ensure they receive the proper training and an introduction to features such as product rates and opening accounts online. On the screen shown below, the MSR checks *Activate Online Banking* and selects a reason code.

Tool #14 > Online Banking > Activate or Deactivate



*Access this screen via Member Personal Banker, during the membership open process (for example via **Tool #3**), or directly via the **OLBPIN** shortcut.*

Additionally, this screen can be used to deactivate a member, for example, to block access for a member by credit union policy or at the member's request. MSRs would simply check or uncheck the activation checkbox. (Unchecked meaning deactivated.)

The MSR will also need to reset the member's password. To view these fields, click the forward arrow. *See the following section on resets.*

If you are just changing the access to online banking, simply click the forward arrow again to finalize the process.

Fraud Block Lists

If a member is already on the fraud block list, you will receive the message, “SSN/TIN appears on block list” and will be unable to check the *Online Banking* box. If there is a match on the block list, follow your credit union policies and procedures. (In order to remove the block, you will need to remove the membership from the appropriate block list.)

> *NOTE: If a member has already logged in to their account, block further access to the account. Uncheck “Activate Online Banking” (and give a reason code).*
>
> *Being on the block list does not affect access made prior to the addition to the block list. If the member enrolled already in online banking, the addition to the block list will not prevent the member from logging into that account with the already created access points. If a member on the block list has already logged into online banking, is subsequently added to the block list, and then tries to login using mobile banking (a new method of login they haven’t used before), the member will be blocked from logging in via Mobile Banking.*

Resetting Online Banking Credentials

Besides activating a member in online banking, as covered previously, the MSR can reset the password, delete the security questions, and delete the username from the Update Online/Mobile Banking *Access* screen.

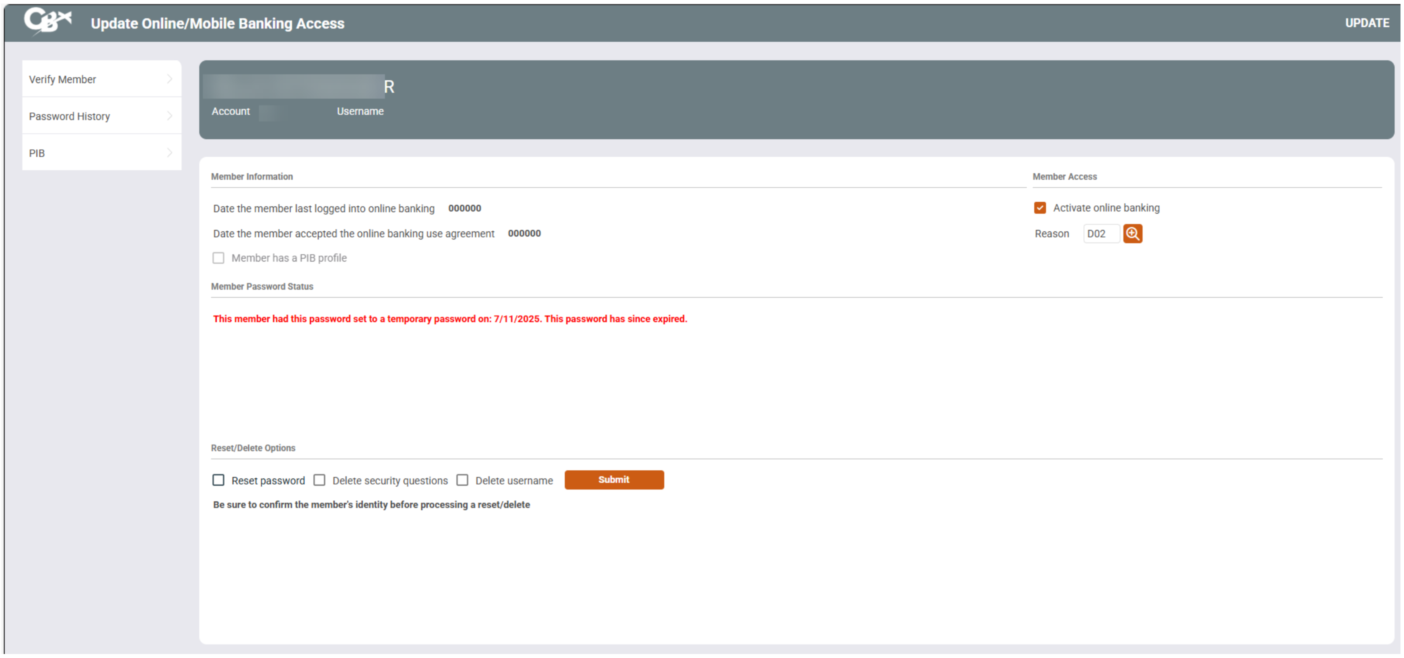
Access Points

Access the *Update Online/Mobile Banking Access* screen to perform a reset via the following routes:

- Enter an account number on **Tool #72** (Shortcut: **OLBPIN**).
- Select "Online Banking (activate, change PIN/password; view password history)" on the initial Member Personal Banker screen (**Tool #14**),
- Click **Reset Password** on the Online Banking Usage screen (when accessed from the **Online Banking** button from **Phone Operator** and **Standard Teller**).

> ***Learn more about the Update Online/Mobile Banking Access screen in online help.***

Update Online/Mobile Banking Access Screen

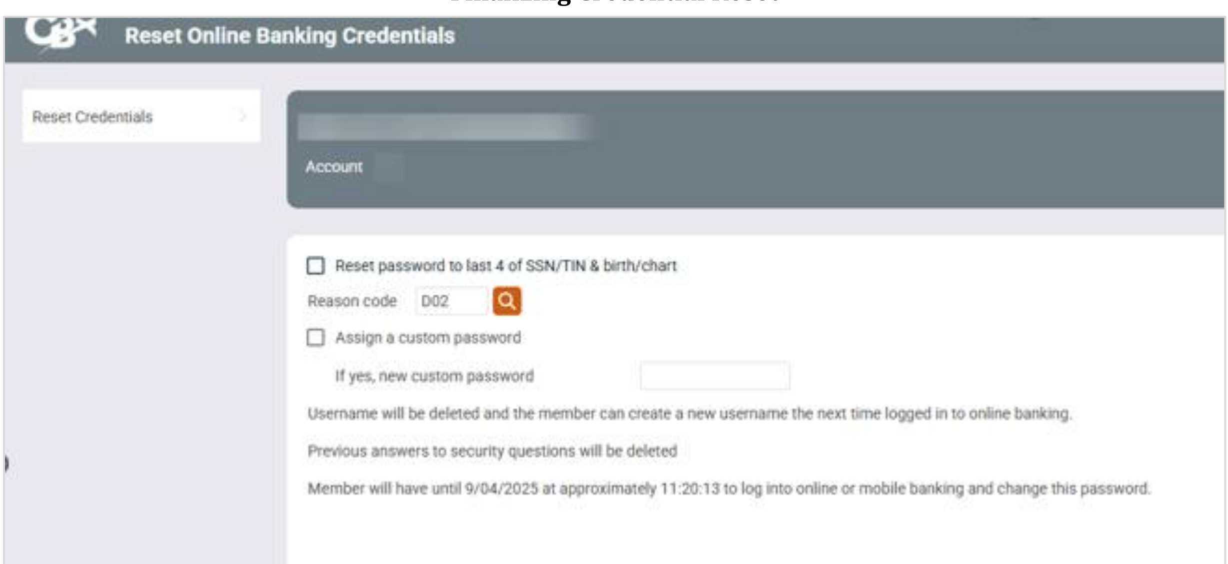


Always follow credit union policies and procedures when resetting a member's online banking credentials.

To reset the credentials, the MSR selects them from the *Reset/Delete Options* section of the screen. (See following screen example.) Then the MSR selects **Submit**. This advances the member to the next screen. The second screen confirms that the password is being reset as well as any other credentials (username, security questions) that were selected on the previous screen. If a password reset is included, the configured temporary password will appear on the screen.

To finalize the reset, the MSR clicks **Reset Credentials**.

Finalizing Credential Reset



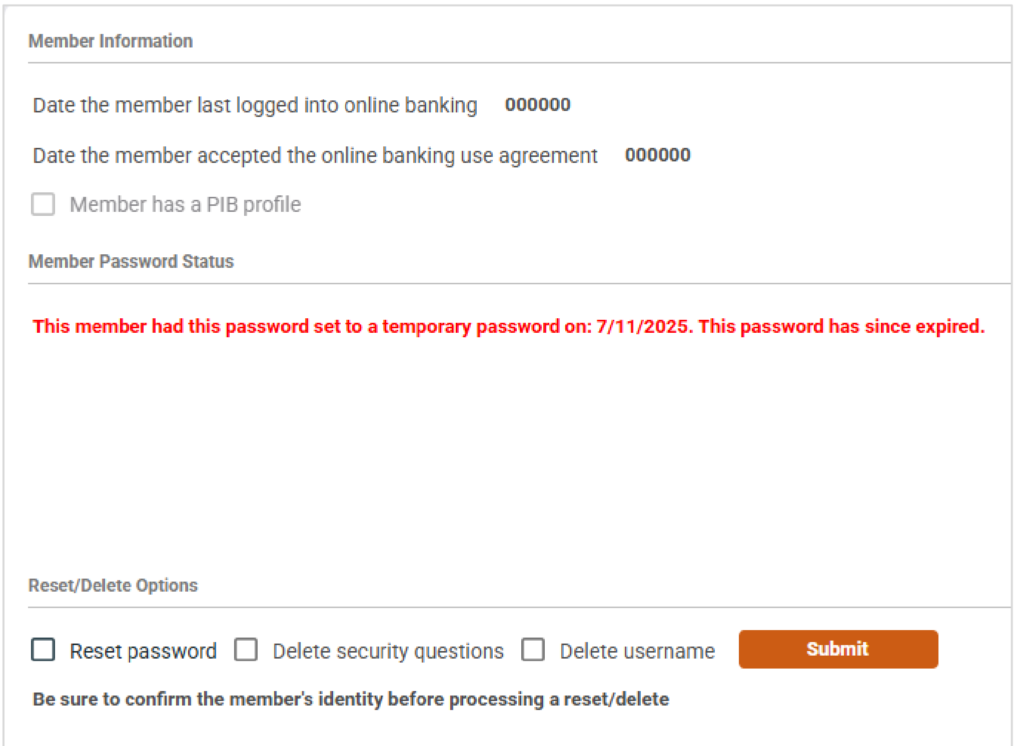
- If allowed by your credit union, the MSR can also reset the password to a custom password requested by the member.

Generally temporary password only will be valid for 24 hours. An instance where this does not apply is with new members at credit unions who do not use MFA for first time user login. Refer to the **Security Decisions to Make** section at the front of this document for more information.

Messaging Explains Reason Member Needs Reset

The *Member Password Status* section of the first Reset screen alerts the MSR the reason the member is locked out of their account, including three incorrect password attempts, expired password due to not use, or expired temporary password.

Messaging on Update Online/Mobile Access Screen



Temporary Password Expiration

When a member receives a password reset on the screen shown in this section, the password is valid for only 24 hours. If the member fails to log in during this period, the member will need to contact the credit union or use the "I forgot my password" feature to reset their password.

Password Expired Due to Non-Use

In the *Online/Mobile Password and Security Settings* screen (covered on page 15), there is a setting for expired password days (maximum 90 days). If a member fails to log into online banking for a length of time greater than this range, the member's password will expire due to non-use. Members can contact the credit union or use the "I forgot my password" feature to reset their password.

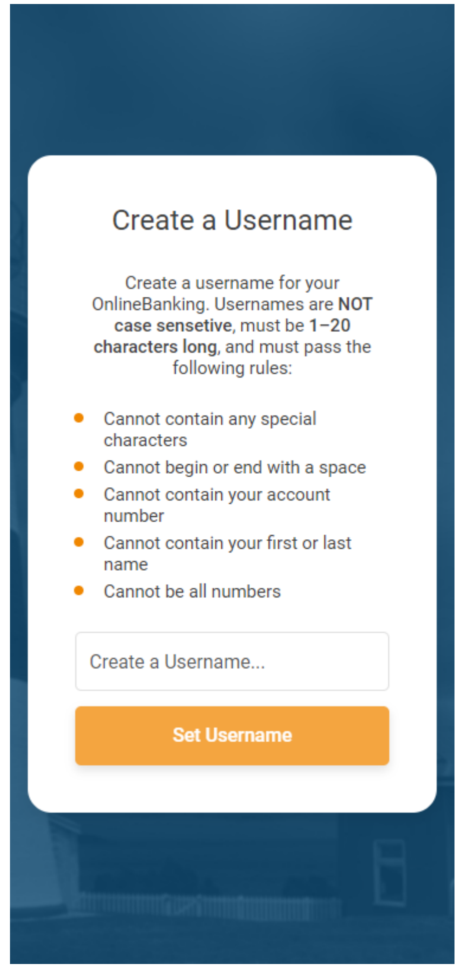
Three Incorrect Password Attempts

Members can only enter their passwords/security question combination three times before they are locked from their account. Then the system clears the security questions from the system, and the password then requires a reset.

In this instance, the password will need to be reset by an MSR since a security question answer is required at login (and the member does not have any since they are cleared). When the member logs in after the credential reset, the member will be required to set up a new password and new security question answers.

Usernames

More information on usernames is on page ***9.***



Members have the option of creating a username in **It's Me 247**. They then use this username in place of their account number when they log into online banking. Usernames are intended to help keep the account number more private. Usernames can be a maximum of twenty characters.

If your credit union does not require usernames, a member can create an *optional* username. Once the member has set up a username, they can change it at any time in **It's Me 247**. However, once they have a username, they can't clear it.

If the member forgets their username, they'll need to contact your credit union, just as they do if they forget their account number. A credit union employee can view and clear the member's username. In this case, the member is prompted to set up a new one the next time they login.

Required Usernames

Your credit union can require usernames. In this case, all members without a username must create one the next time they log into online banking. They will then automatically advance to the username setup screen and will be prompted to create one. They cannot advance until they set a username.

*This feature must be activated by your credit union. To change your settings, you will need to fill out an "**It's Me 247** Configuration Change Request form.*

- Brand new members will log on with their account number. They will be asked to set up a username after accepting the Online Use Agreement (and before they set their password and challenge question answers).

Assisting a Member with a Username in CBX

There might be occasions when the member forgets their username and contacts the credit union. The credit union will need to develop a policy for managing these situations. On the *Update Online Mobile Banking Access* screen, the employee can view the username and clear it. (Refer to page 25.)

Promotional Campaigns for First Time Users

This section covers promotional campaigns, which were used more widely before the MFA feature was available. For example, select January as your promotional period. During this month, you can allow members who do not have access to online banking (with for example, an expired password due to non-use or a temporary password past its reset time window) to access online banking for a “try it out” period. This allows you *to sell* online banking services as a special value your members receive from belonging to the credit union. You can even send these members targeted marketing to encourage them to sign on and become new online banking users. It requires very little time on the part of your staff—members can log in at any time that is convenient for them during the promotional period.

These members would otherwise have to call your credit union to get access.

Your marketing team can manage promotional campaigns on their own and configure their own program via **Tool #234 *Config New Online User Promo Campaign***. From the promotional software, they can select which members they want to include in the promo (excluding, for example, members without an email address) and view a listing of these members to monitor progress with the program. CBX even allows the printing of reports and creation of a Member Connect database file for targeted email campaigns.

- Only members who are activated for online banking are included in promotional campaigns. If your credit union does not activate members (when they open a membership), these (non-activated) members will not be included in the promotional campaign.

Once the period has expired, any members who have not logged in at least once during the promotional campaign period will automatically be instructed to contact the credit union for activation if they attempt to log in.

Who Qualifies for a Promotional Campaign?

Below are the members who are by default allowed in a promotional campaign:

- Members who are activated to use online banking, members who are not activated will not be included.
- Members who have entered their password incorrectly three times.
- Members whose password has expired. (They have not logged in during the number of days before a password expires.)
- Members who just joined the credit union and missed the configured range for new members to log in.
- Members who had their password reset by an MSR and missed the window to log in.
- Members who entered an invalid security question three times.

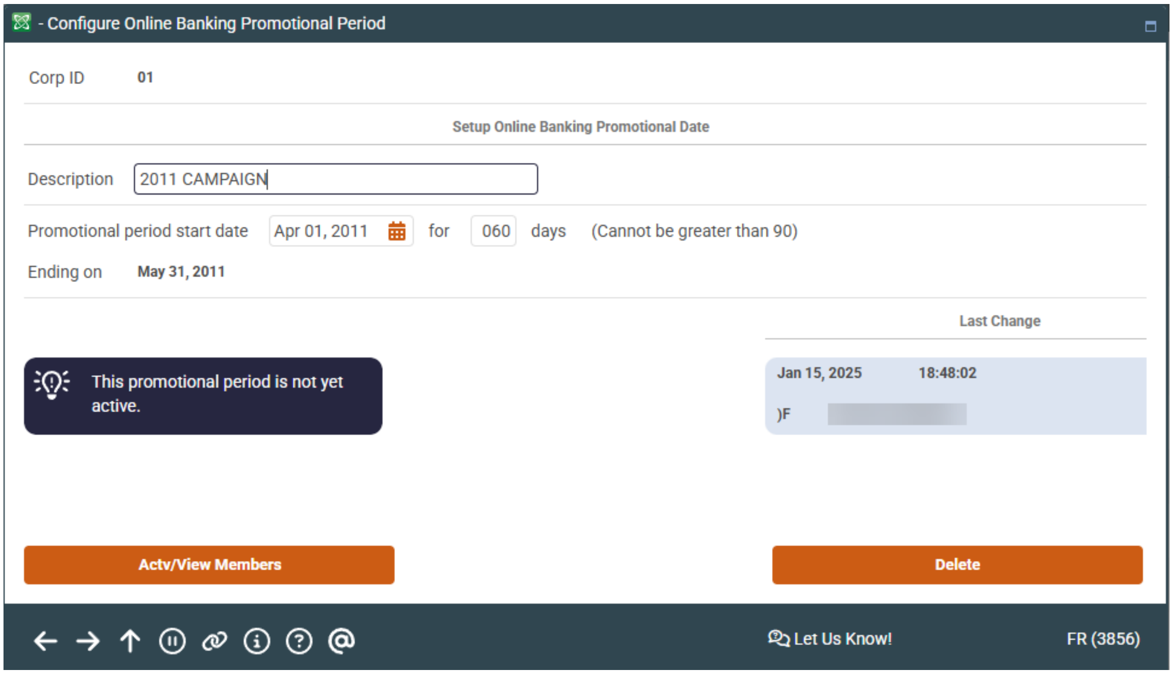
The promotional campaign software allows you to select to exclude some of these members based on the following criteria:

- Members who do not have email addresses.
- Members who have never logged in or have not logged in since a certain period.

Promotional Campaign Configuration

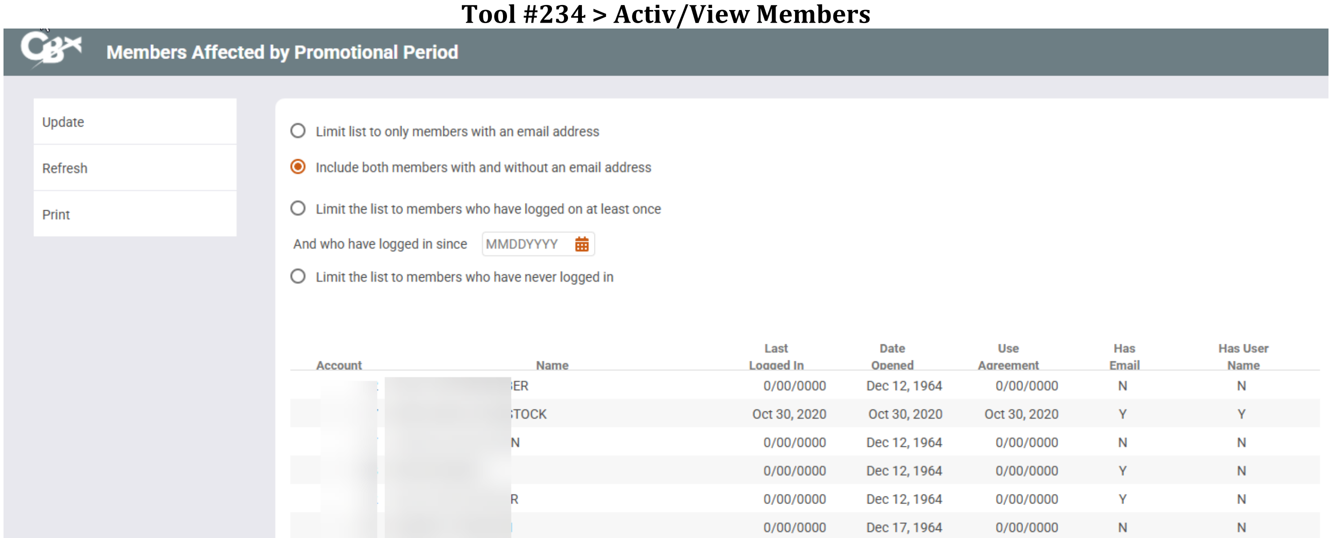
The entry screen of the promotional campaign feature allows you to name your promotional campaign and set the date range of the campaign. Once you use Enter, the end date will be calculated.

Tool #234 Configure Online Banking Promotion Period (Date Selected)



Then use **Activ/View Members** to select the members who will be included in the campaign.

Tool #234 > Activ/View Members



This screen allows you to filter to exclude:

- Members without an email address. (Defaults to include members with and without one.)
- Members who have either never logged in or who have not logged in since a certain date. (Defaults to include both members who have logged in and never logged in.)

Use **Refresh** or use Enter to refresh your list to exclude (or include) members based on these selections.

This screen includes the last log in date, membership open date, the date the member accepted the Online Banking Use Agreement, whether the member has an email account and whether the member has a username for online banking access.

To create a file for Member Connect, use **Print** to view the screen below. Check the *Export to file* checkbox and enter the file name. Then use the forward arrow (Enter) to generate the file.

- NOTE: During a campaign, you can return to this screen to print updated results to a file for further analysis in Report Builder.

Tool #324 > Activ/View Members > Print

To activate the promotional campaign, use **Update** from the entry screen.

Confirmation of Activation

Then use **Add/Update** to complete the activation.

You will then return to the original screen where you can see the date the promotional campaign will begin. Once the campaign is activated, use **Actv/View Mbrs** to view the members in the campaign.

There, you can then see the progress of your campaign, by individual member (last column), as well as with a promotional campaign total at the bottom of the screen. The bottom of the screen lists the number of members in the promotional campaign that have logged into online banking.

Statement Security

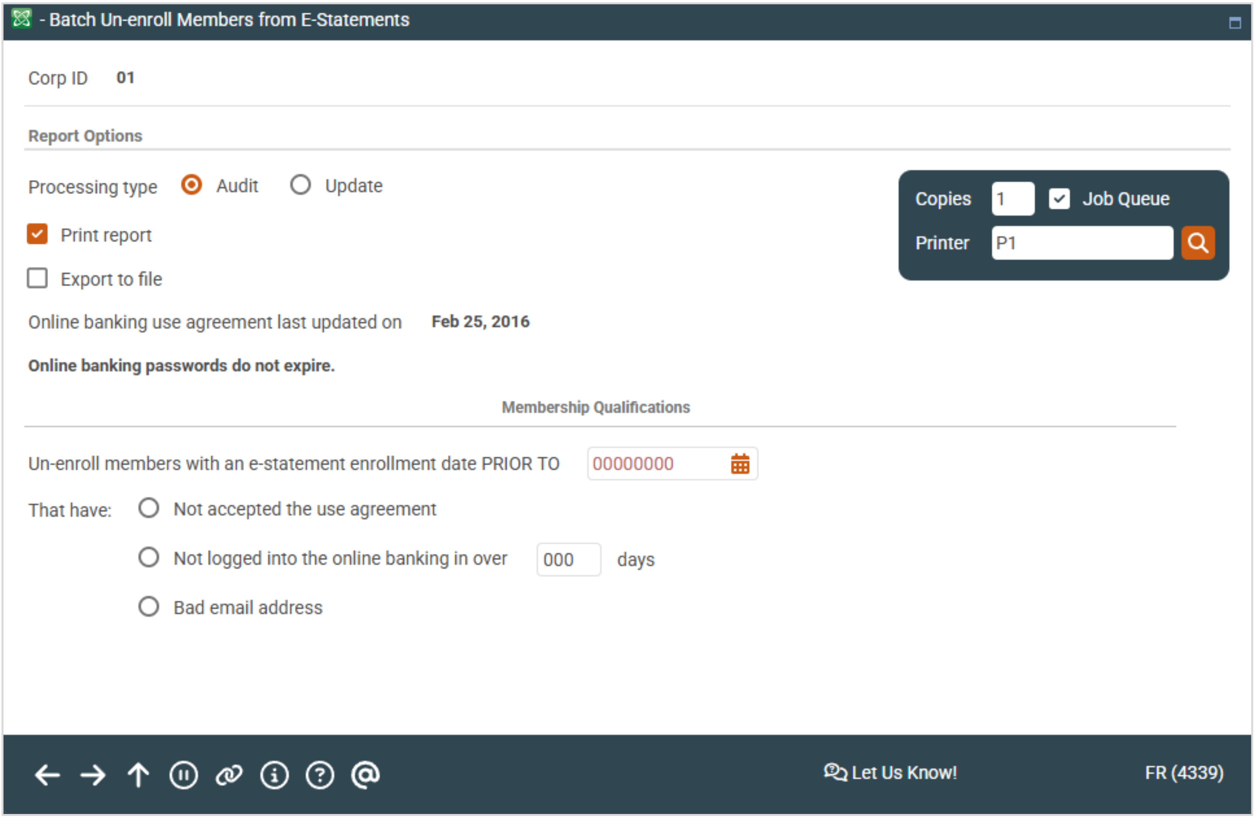
Online Banking Indemnification Not Required for eStatements

Once a member is enrolled in eStatements, the system begins generating eStatements for the member. The member does not need to log into online banking and accept the Online Banking Use Agreement to generate eStatements. To audit the creation of eStatements to only members who have logged into online banking, use the batch unenroll feature covered in the next section of this booklet.

Batch Member Un-enrollment

You can unenroll members from eStatements using the feature below. This feature lets you gather a batch of members according to their e-Statement enrollment status, compared to either their Use Agreement acceptance date, their last logged in date, or even the status of their email address, and then elect to un-enroll them from e-Statements at the same time. This screen allows you to run an audit and prints a corresponding report. After evaluation, select the Update Processing type.

Tool #365 e-Statement Batch Un-enrollment

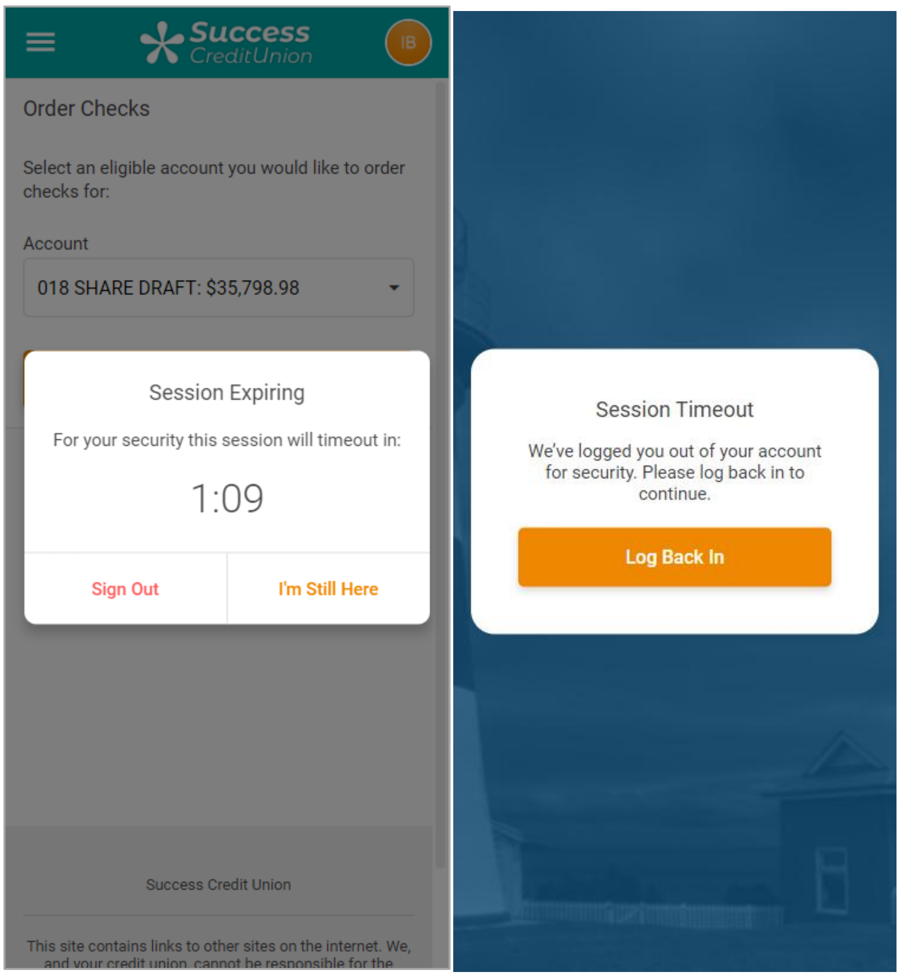


Timeout Notification

As a security feature, members are automatically logged out of **It's Me 247** after fifteen minutes of inactivity or page refresh. (The login and security screens are the only exceptions. Members are logged out of them after five minutes of inactivity.)

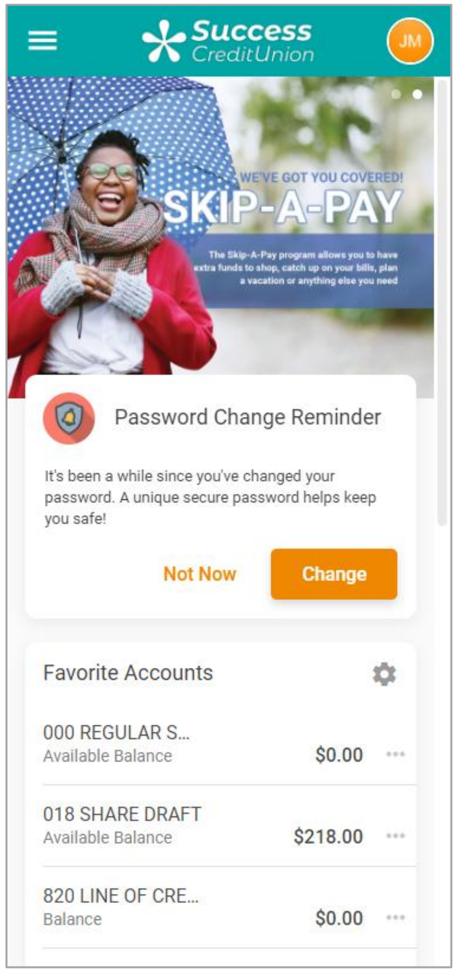
Members are alerted after twelve minutes of inactivity with a pop-up window that counts down the remaining three minutes. If the member selects **I'm Still Here**, the timer will be reset, and the page will not be refreshed (so the member will not lose anything they have done on the page). If the user does not respond or selects **Sign Out**, they are automatically logged out of **It's Me 247**.

"It's Me 247" Timeout Notification



Password Change Reminders

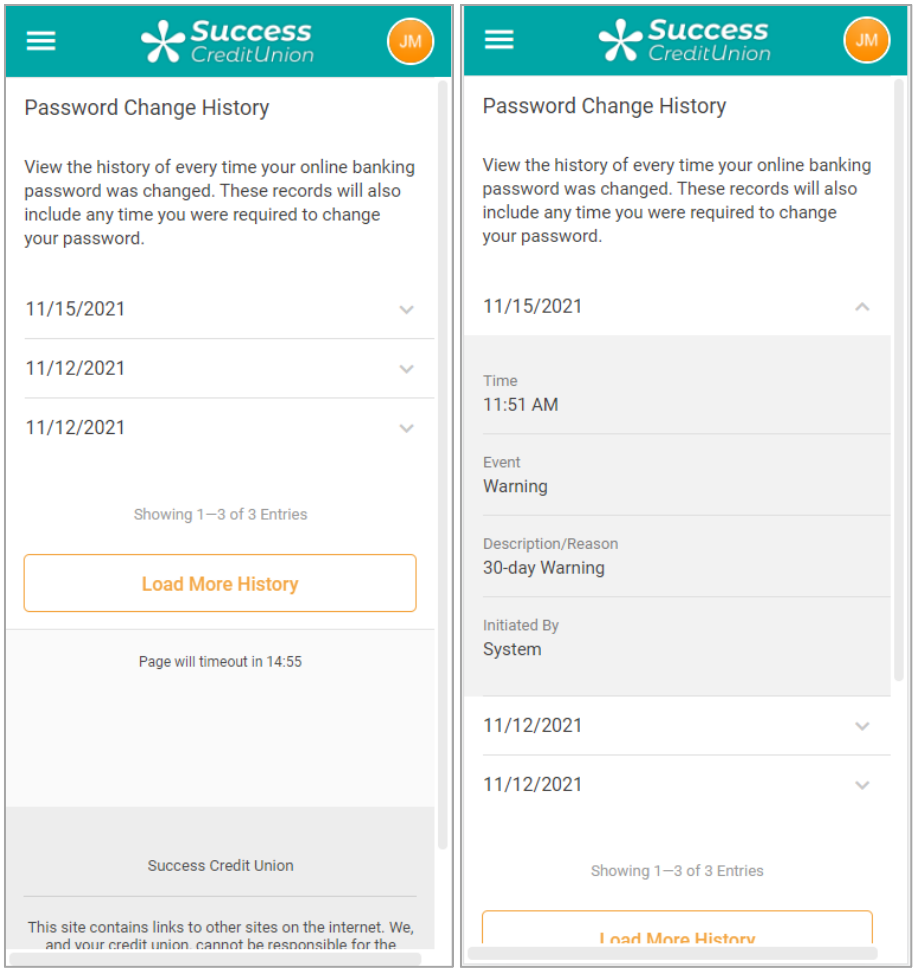
It's Me 247 displays automated "soft" warning messages to members to encourage them to change their password on a regular basis, without making it mandatory. These soft warning messages appear when a member has not changed their password in over thirty days.



Members can select **Change** which navigates them directly to the screen where they can change their password. They can also select **Not Now**. In this case, the warning disappears for thirty days. If they do nothing, the warning will remain at the top of the page.

Members can view their selections on a Password Change History page available from the "Personal Info & Settings" section in online banking. If they select the dropdown arrow, the detail of the password change appears.

Password Change History and Detail



Members changes are recorded in CBX on the PIN/Password change dashboard. **See Page 41.**

Personal Information Change Notifications

To comply with Red Flag requirements to monitor things like address changes, **It's Me 247** and CBX provide alerts to both the credit union and the member when changes are made to a member's personal information to provide an extra layer of security against fraudulent activity.

Note on Credit Union Review of Change

Credit unions can configure that member personal information changes in **It's Me 247** are automatic or they need review through **Tool #13 *Work Online Banking Apps/Req***. If the credit union selects to review the changes, the change confirmation emails and online banking messages (mentioned in the next section) will not be sent until the credit union accepts the change.

Credit unions can require that changes made by members in the Personal Information page in online banking be approved before they are updated in the system. What special conditions do not require an email address to be reviewed?

Changes to Online Banking Password and Email

Both an online banking message and email confirmation are sent (to the email address on file for the member) whenever they change their online banking password, either via **It's Me 247** or with the help of a credit union employee via CBX. These messages and emails are sent automatically. This is a security feature that is intended to warn members if someone else initiates a password change on their accounts without their knowledge. An online banking confirmation message is also sent.

The system generates two confirmation emails any time an employee makes a change to their email address in **It's Me 247** (one to the old email address and one to the new email address).

An example of the email confirmation messages sent is shown below. This is the content of the email sent if a member changes their online banking password. The text changes slightly if the change was made in CBX.

```
Your online banking password was changed 08/04/10. For your protection we are sending
this message as confirmation to verify that this change was made according to your
instructions.

If you did not initiate this change, please contact your credit union immediately.
Remember that if you have more than one membership at the credit union, the change may
only have affected one of these accounts.

ABC Credit Union
616-555-1212
www.abccreditunion.com
```

This email contains the credit union's Signature Line (SL) message to further confirm the message has come from the credit union. This is configured in the Master Message Center. (Refer to the *Marketing Campaigns with Member Connect* reference guide for details.)

HINT: This is another reason it is so important for staff to carefully verify a member's identity when resetting passwords and to have extra controls in place if someone wants them to update both an email address AND reset a password at the same time. The requester could be a bad guy!

If an employee changes the information via CBX, the member will receive a similar message with slightly different wording. The online banking confirmation message the member receives has wording like the email message.

Personal Information Changes

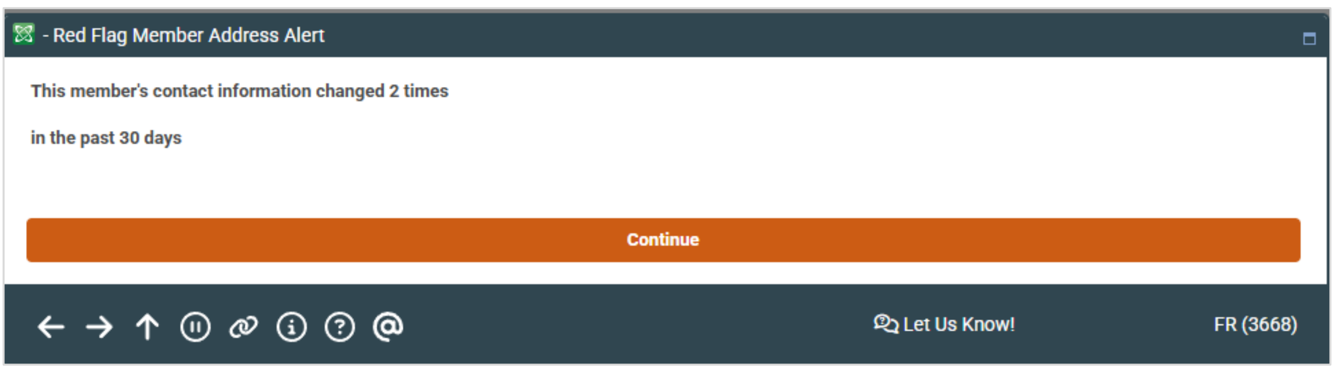
If the member makes any changes to the other information included on the *Personal Information* page in **It's Me 247**, the system generates an online banking confirmation message. These messages are sent both if the change is made by the member online or by an employee in CBX.

Personal Information changes that receive an online baking confirmation include:

- Address Line 1
- Address Line 2
- City
- State
- ZIP code
- County
- Home Phone
- Work Phone
- Other Phone
- Fax Phone
- Code Word

Red Flag Warnings in CBX for Employees

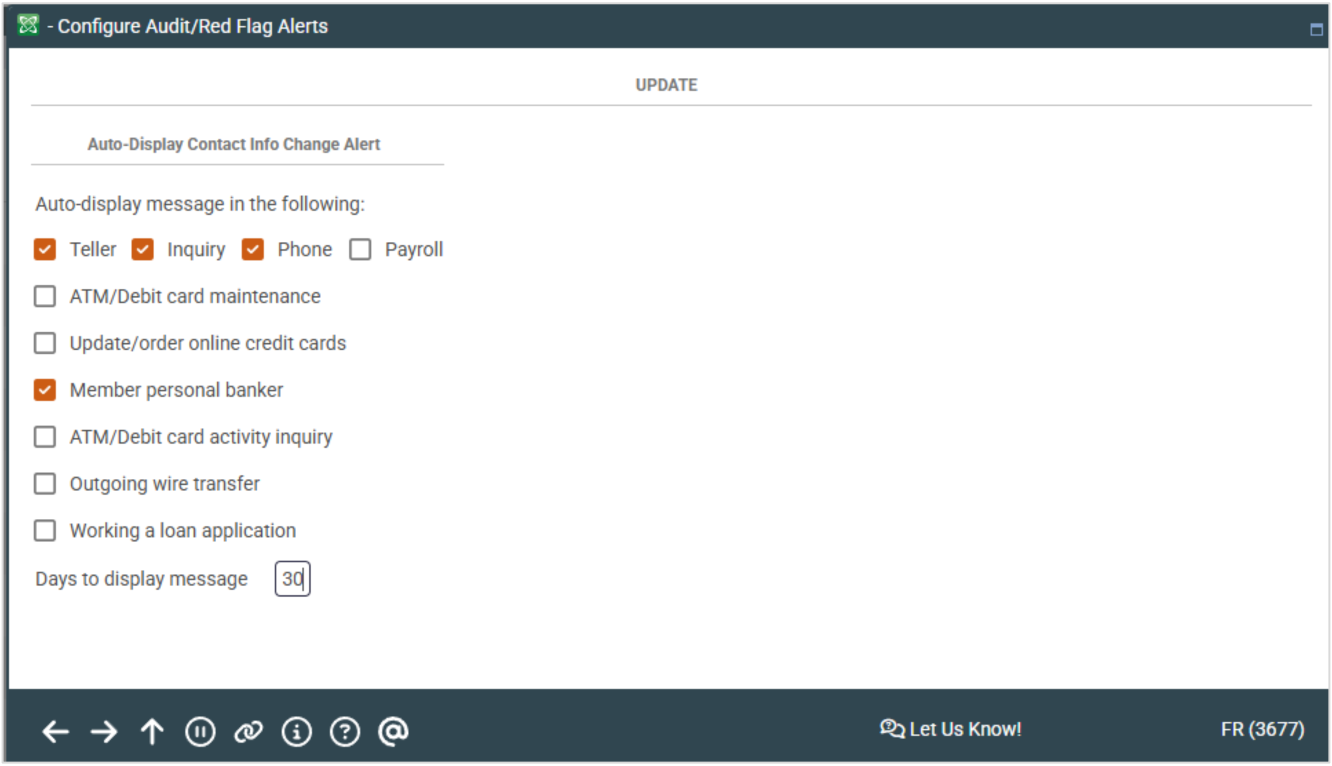
When credit union employees enter select screens (such as Teller, Inquiry, and Phone Operator), they receive a warning message noting how many changes have been made to these personal information items in the last 30 days.



Each time a change is made to the member's personal information, a Tracker entry is made on the Audit Tracker that records the old and new values. The Tracker also notes the Employee ID of the person who made the change in CBX. If the change was made in online banking, the Employee ID is noted as 96.

- NOTE: CASS Certification does not trigger this red flag feature.

This feature is activated using **Tool #750 *Red Flag Controls***.



This configuration allows the credit union to select which CBX tools will display the message in CBX, including:

- Teller
- Inquiry
- Phone Operator
- Payroll (**Tool #504 *Member Payroll Inquiry***)
- ATM/Debit card maintenance (**Tool #11 *ATM/Debit Card Maintenance***)
- Updating/ordering credit cards (**Tool #12 *Update/Order Online Credit Cards***)
- Member Personal Banker (**Tool #14 *Member Personal Banker***)
- ATM/Debit card activity (**Tool #156 *ATM/Debit Cards & Activity Inquiry)***
- Outgoing wire transfers (**Tool #73 *Post Wire Transfer to Member Account***)
- Loan application creation/maintenance (**Tool #2 *Work/View Loan Application Status*** and **Tool #53 *Process Member Applications***)

Additionally, the configuration allows the credit union to configure the number of days that the warning message will appear in CBX.

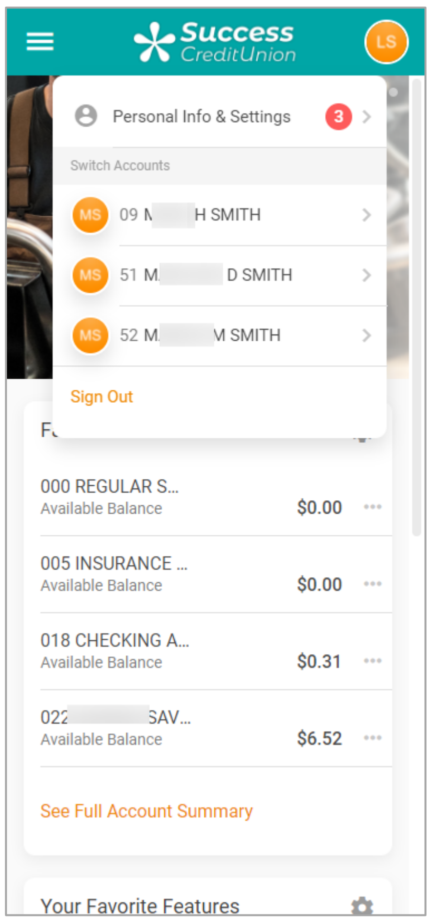
- NOTE: When introducing this feature, be sure to provide your staff with training on what to do if they see the Red Flag message. Should they ask for photo identification to confirm the address?

Jump Access Controls

To learn more about this feature, be sure to check out the Jump Controls reference guide, located on the **It's Me 247** reference page.

Briefly, once this feature is activated and the appropriate permissions are given, the member can "jump" to another account. Your biggest user of Jump will probably be a member with multiple memberships at your credit union.

Jump allows a member to log into one of their memberships and then jump to another of their memberships (same SSN) without additional authentication. Members can also grant Jump permissions to any other joint owner on their base (000) account, such as a spouse, who also has a credit union membership. From here, with a few exceptions such as applying for a loan, viewing checks, or changing a password, it is as if they logged into this second account; they can make transfers, schedule AFTs, change preferences, and more.



For a more in depth look at this discussion, which forms the basis for the decision to only give access to owners via Jump, refer to Answer Book.

Inter-Member Transfer Controls

Inter-Member Transfers allow members to transfer to other members at your credit union. These transfers are done via the Transfer Wizard in online banking. Two options exist for inter-member transfers: transfer control lists and direct account input.

Overview

You credit union can select to activate either one or both inter-member transfer options. To activate this feature, fill out an **It's Me 247** Configuration Change Request and submit a store order. *Self-Processors: This setting is in* **OPER Tool #5356 *Online Banking Configuration***.

Transfer Control Lists

Transfer Control lists are used to control which of your credit union memberships a member can transfer to via the Transfer Wizard. These accounts are the only accounts a member can use when setting up an ACH Distribution or Automated Funds Transfer (AFT) in online banking or when making a transfer in Mobile Banking. The benefit of the Transfer Control lists for members is that these memberships appear in a handy list for them to choose from, so they don't need to remember their friends' and family's account numbers.

The benefit of Transfer Control lists for credit unions is that they control the addition of memberships to the member's Transfer Control list. Credit unions add memberships to a member's Transfer Control list via **Tool #883 *Update ARU/Online Banking Transfer Ctrl***. A member cannot add an account to their Transfer Control List while in online banking.

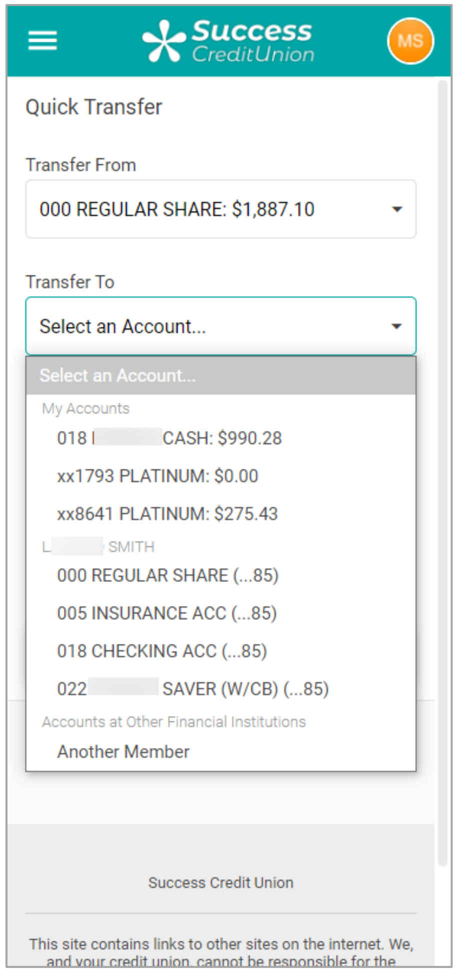
Direct Account Input

Direct Account Input allows the member to enter the account and suffix directly on the Transfer Wizard page when making the transfer. They are also required to enter the first three letters of the last name of the member they are transferring to prevent incorrect entry. This might be used by the member for transfers to accounts they do not transfer to frequently or that they do not want to add to their Transfer Control list.

Inter-Member Transfers: What the Member Sees in Online Banking

Below is an example of what a member might see if a credit union activated both Inter-Member Transfer options. Credit unions can select to offer either one or both options.

- In the example below, Lisa Smith is on this member's Transfer Control list.



Evaluating the Reason for a Password Change

Maybe you want to pinpoint why a member's password has changed in **It's Me 247**.

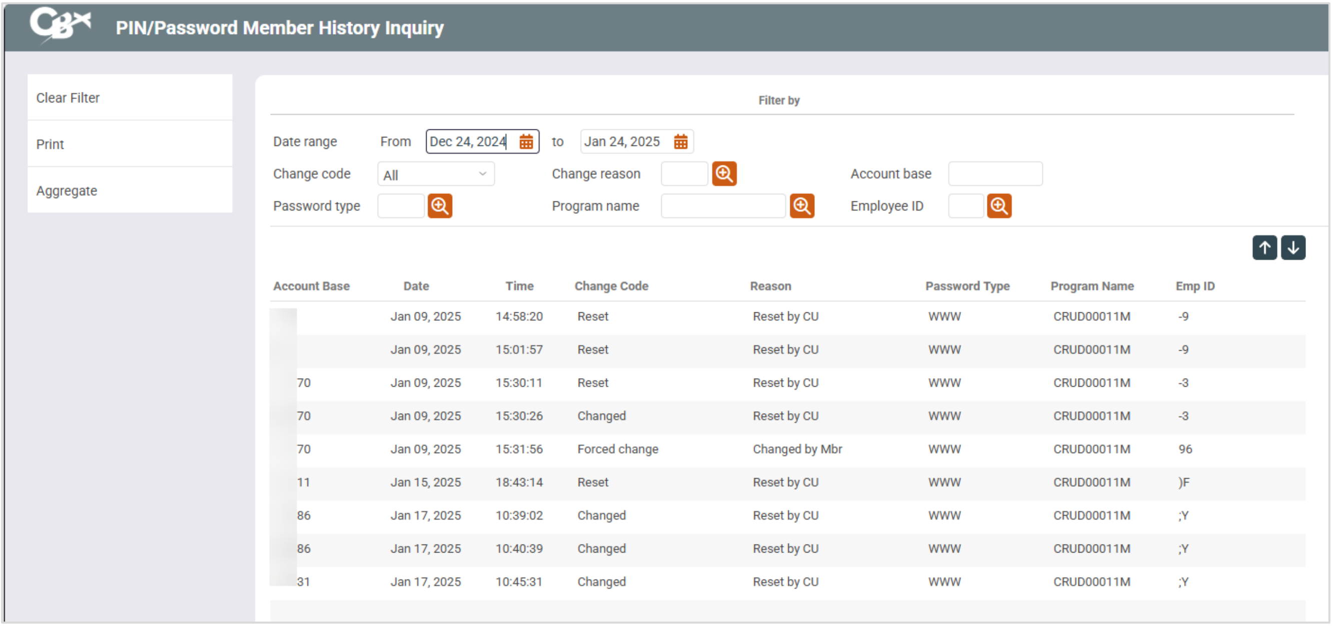
- Did the member change the password or ask an MSR to change it to a specific password?
- Was the account disabled because the member entered an incorrect password too many times?
- Did an MSR change the password temporarily to the last four digits of the member's social security number?
- Did the member follow that action by changing the password to one they chose?

Answer these questions using the Member PIN Password Change online report via **Tool #505 *Member PIN/Password Change History***. Select a Password Type of WWW (online banking), and the online report shows how many times and why a member's online banking password was changed.

This dashboard also records the warnings the member receives to remind them to periodically change their password as well as if they choose to ignore the warning. See **page 34** for details and what the member sees in online banking.

Use **Print** to print a report of the items.

Tool #505 Member PIN/Password Change History



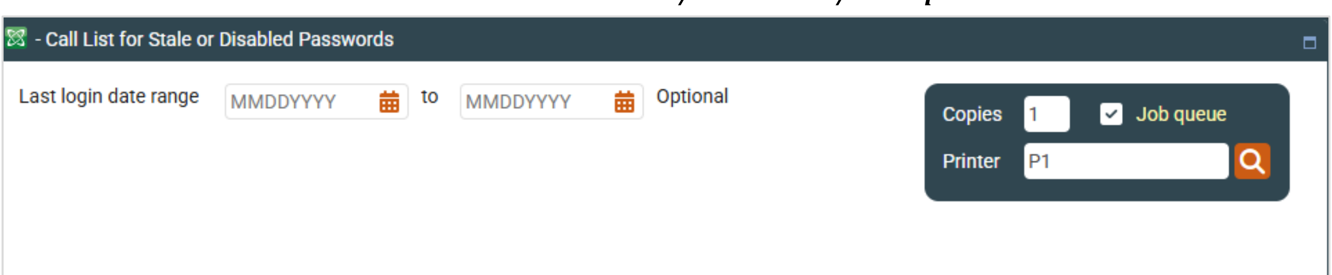
Evaluating Your Memberships Without Activity

You may choose to track your members who have logged into online banking at one time but have not logged in again during the period you have configured for non-use expiration.

- NOTE: The longest period a member might appear on this list would be 90 days, which is the maximum period you can set for password expiration due to non-use. The length of the expiration days is set in the *Online/Mobile Password and Security Settings*. (See page 15.)

To keep an eye on members who are activated but have not logged into **It's Me 247** in a while use **Tool #161 *Audit Disabled/Inactive PIN/PWs Rpt***. The report allows you to specify a range of "last login dates" and view the members who are active but have not used online banking during that time. For example, you might pull a list of all accounts with a last logged in date greater than two months ago. You may decide to set up a personal contact or direct mail campaign to encourage them to try online banking again.

Tool #161 *Audit Disabled/Inactive PIN/PWs Rpt*



Report Sample (LPWDCALLST)

9/24/25 11:26:54 ABC CREDIT UNION LPWDCALLST PAGE 1

DISABLED ONLINE BANKING MEMBER CONTACT LIST USER

LAST LOG ON BEGINNING DATE: 9/24/2024 TO LAST LOG ON ENDING DATE: 9/24/2025

ORDERED BY DAYS SINCE LAST LOGIN

ACCOUNT BASE	MEMBER NAME	PHONE NUMBERS	LAST LOG-IN DATE	LAST CHANGED DATE	DAYS SINCE LAST LOG-IN	STALE PASSWORD	DISABLED PASSWORD	CHALLENGE QUSTN/ANS
		Home:	12/18/2024	12/18/2024	19		Y	Y
				@yahoo.com				N
		Home:	2/27/2025	5/12/2025	209	Y		Y
				@gmail.com				Y
		Home:	11/16/2024	4/10/2025	312	Y		Y
		Work:		@gmail.com				Y
		Home:	5/28/2025	5/30/2025	119	Y		Y
		Work:		@yahoo.com				N
		Home:	1/03/2025	1/03/2025	264	Y		Y
				@gmail.com				Y

Review Your Credit Union Plan and Procedures

Regardless of which CBX and **It's Me 247** tools you choose to use, the point is to make sure your credit union has a *plan* and procedures in place to monitor and control your members' access to online banking. Contact Client Services if you would like assistance in setting up some custom reports or inquiries or in changing any of your existing configuration settings.

Appendix A: Online Banking Use Agreement

Following is the verbiage of the Online Banking Use Agreement.