# SmartApps – TTEC Digital

## Authentication Guide – v1.0

Cloud Version

**Friday, August 9, 2024**

***CX Optimized***

# 1. Table of Contents

# Revision History

| Version | Date Modified (mm/dd/yyyy) | Modifications Made | Author |
|---|---|---|---|
| V1.0 | 01/10/2024 | Initial Draft | TTEC Digital |
| | | | |
| | | | |
| | | | |
| | | | |

# 2. Introduction

The authentication guide provides guidance and information on the authentication processes and related functionality contained in the application. This guide assists in the configuration and maintenance of the authentication and related processes.

The authentication guide is included with all the products that are core-dependent and is an integral part of the system responsible for all the required authentication functions within the organization.

The authentication processes in SmartApps include:

- Member or Customer Authentication within all SmartApps products
- Alternate Member or Customer Identification
- Member Activation
- Force PIN Change
- Collection, Delinquency, and Bankruptcy Settings
- Dormant Account Processing

# 3. Authentication Profiles

The authentication system is structured as a profile-based system. It allows for the creation of an unlimited number of profiles, each of which can be linked to any product requiring authentication. This flexibility enables the customization of authentication settings to cater to various customer types, routing options, or scenarios.

When a new profile is created, the system prompts the selection of a profile type to facilitate the collection of the relevant information required for that specific profile.
SmartApps currently supports following profiles:

- Smart Teller: as many as needed in the cloud.
- Smart Bot
- Proactive Info
- Screen Pop
- Customer Activation
- Force PIN Change

# 4. Global Settings

- **Define Business Rules:** Within the Authentication settings, you can define specific business rules that will be used to authenticate the profiles created for members.
- **Inheritance Across Applications:** The settings defined here are inherited by other applications within SmartApps, including applications such as Teller and Smart Bot. This ensures consistent authentication rules and behavior across the entire suite of applications.
- **Configure Settings:** The image provided below illustrates the various system settings that can be configured. These settings are global and will apply to the entire system.

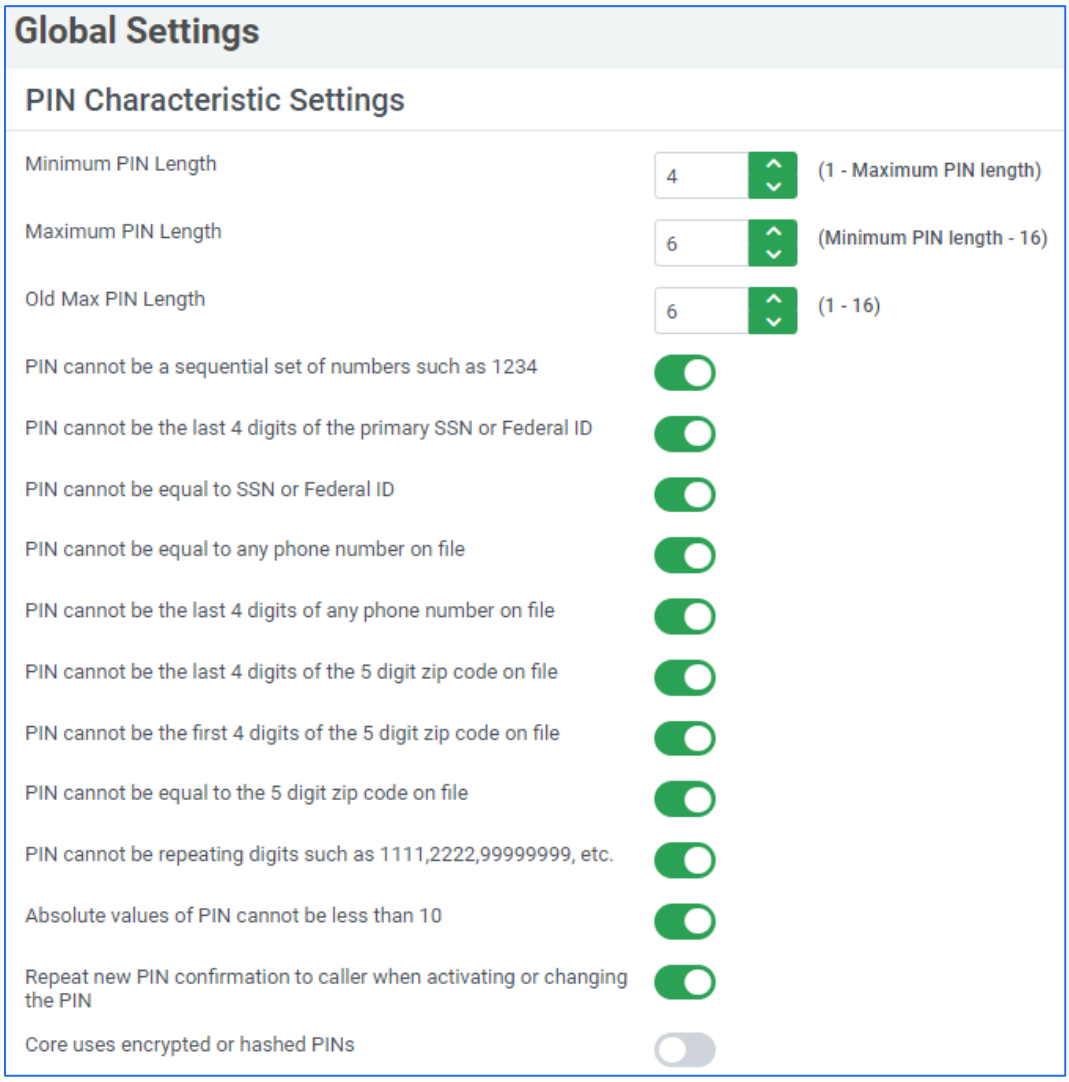



Table:

Describes the different rules that can be set using the Global Settings in SmartApps.

| Settings | Description |
|---|---|
| Minimum PIN Length | This setting controls the required minimum PIN length and is used for new PINs being setup and has no impact on existing PINs. |
| Maximum PIN Length | This setting controls the required maximum PIN length and is used for new PINs being setup and has no impact on existing PINs. |
| Old Maximum PIN Length | This setting controls the maximum old PIN length required previously.<br>**Note:** This setting is only used if the caller requires to change his PIN in case the existing PIN length does not conform to the new maximum length. For example, the old maximum PIN length was 4-digit, and the site is moving to a 5-digit PIN. A caller with a 4-digit PIN will be asked to change the PIN. |
| PIN cannot be a sequential set of numbers such as 1234 | This setting sets a business rule that prevents PINs from containing sequential sets of numbers such as 1234, 5678, etc. |
| PIN cannot be the last 4-digits of the SSN or Federal ID | This setting sets a business rule that prevents PINs from being equal to the last 4-digits of the SSN or Federal ID. |
| PIN cannot be equal to the SSN or Federal ID | This setting sets a business rule that prevents PINs from being equal to the SSN or Federal ID. |
| PIN cannot be equal to any phone number on file | This setting sets a business rule that prevents PINs from being equal to any phone number on file. |
| PIN cannot be the last 4-digits of any phone number on file | This setting sets a business rule that prevents PINs from being equal to the last 4-digits of any phone number on file. |
| PIN cannot be the last 4-digits of the 5-digit zip code on file | This setting sets a business rule that prevents PINs from being equal to the last 4-digit of the 5-digit zip code on file. |
| PIN cannot be the first 4-digits of the 5-digit zip code on file | This setting sets a business rule that prevents PINs from being equal to the first 4-digits of the 5-digit zip code on file. |
| PIN cannot be equal to the 5-digit zip code on file | This setting sets a business rule that prevents PINs from being equal to the 5- digit zip code on file. |
| PIN cannot be repeated digits such as 1111, 2222, 999999, etc. | This setting sets a business rule that prevents PINs from containing repeated digits such as 1111, 2222, 99999, etc. |
| Absolute value of PIN cannot be less than 10 | This setting sets a business rule that prevents a PIN from containing an absolute value of less than 10. |
| Repeat new PIN confirmation to caller when activating or changing the PIN | This setting allows a site to indicate if the new PIN entered should be repeated back to the caller. |
| Core uses encrypted or hashed PINs | This setting indicates if the core uses encrypted or hashed PINs. |

# 5. Member Authentication

Member authentication uses a three-level structure and covers the following topics.

- Authentication structure
- Identifying the member account
- Identifying the individuals on the account
- Additional security
- Authentication options by level
- Authentication options by core
- Authentication failure

## 5.1. Authentication Structure

- **Levels of Authentication:** SmartApps authentication is structured around different levels, which are designed to establish the account owner's identity and ensure that the right individual is using the system.
- **Varying Information and Processes:** The system collects different sets of information and employs distinct processes depending on the specific level of authentication being utilized.
- **Authentication Options:** The options for authentication can vary based on the core application used within the organization. Different applications may offer unique authentication methods and functionalities tailored to their specific purposes.

### 5.1.1. Level 1

- **Mandatory Identification**: Level 1 authentication serves as a mandatory step to identify the member account. It must be completed before proceeding with any further authentication processes.
- **Standard Authentication**: Level 1 offers a standard and essential method for authenticating the caller. It utilizes the features available within the core processing system to establish the caller's identity.
- **Optional Levels**: While Level 1 is mandatory, Levels 2 and 3 are presented as optional methods of authentication, providing flexibility based on specific needs or preferences.

### 5.1.2. Level 2

Level 2 authentication identifies individual users within multi-user accounts and its optional usage depending on account settings.

- **Identify the Individual:** Level 2 authentication is essential to identify the individual associated with the account. It ensures that the system can distinguish between primary and joint users on the same account.
- **Usage in Multi-User Accounts:** Level 2 authentication becomes particularly relevant in accounts that involve multiple users, such as primary account holders and joint account holders. It helps differentiate between these users.
- **Optional Nature:** The use of Level 2 authentication is not mandatory for all accounts. Its application depends on the specific settings and requirements of the organization or system. Some accounts may opt for Level 2 authentication, while others may not, based on their needs.

**Note:** If level 2 authentication is not used or a level 2 question is used that does not determine an individual, the system will assume the primary member is on the phone.

### 5.1.3. Level 3

Level 3 authentication helps in verifying the caller's identity.

- **Additional Verification:** Level 3 authentication is employed to verify extra information provided by the caller. The goal is to ensure that the person accessing the account is indeed the correct and authorized user.

- **Optional Level:** Level 3 authentication is not a mandatory requirement. Its use is at the discretion of the organization or system's policies. It provides an additional layer of security for those who choose to implement it.

### 5.1.4. 3rd Party Authentication (For all Levels)

- **Standard Authentication:** 3rd party authentication offers a standard way to authenticate the caller by utilizing the features within the core processing system. This ensures that the caller is who they claim to be.
- **Optional Alternate Method:** Additionally, 3rd party authentication provides an optional alternative approach for identifying the caller. This flexibility allows organizations to choose the most suitable method for their needs.

**Note:** Level 3 authentication is not utilized in Smart Bot. Instead, the same set of questions available in Level 3 is made available in Level 2 for Smart Bot. This adjustment ensures a consistent and secure authentication process.

## 5.2. Personal Accounts

- Personal Account is linked to memberships.
- With Level 1 authentication, the system can successfully identify the membership as Personal or Business when the correct information is provided.
- The remaining authentication processes will function using the rules for a Personal Account.

## 5.3. Identifying the Member Account

- **Initial Authentication Step:** The first step in the authentication process aims to identify the member account in the system. This is known as Level 1 authentication processing.
- **Verification of Customer ID:** A valid customer ID or member ID is cross-verified with the core processing system. Alternate methods of identification are supported on some cores and include Social Security Number, Account Numbers, and various Card Numbers within the system.
- **Source of Valid ID:** A valid ID can be provided by the caller directly or can be derived from the alternate member or customer authentication component, if utilized. During this stage of the process, the system will either confirm the validity of the provided ID or deny it.
- **Passing Verified ID:** Once a member or customer ID is verified, it is then forwarded to the Level 2 authentication process.

## 5.4. Identifying the individuals on the account

- **Identifying Individuals**: In the Level 2 authentication phase, the system seeks to identify the specific individual associated with the account. For instance, a member account may have a primary member and an unlimited number of joint members.
- **Determining the User:** The Level 2 process aims to determine which person linked to the account is currently using the system.

- **Requesting Specific Information:** During this segment of the authentication process, specific details such as Social Security Numbers (SSN) or dates of birth may be requested to establish the user's identity.
- **Dependency on Core Processing System:** The effectiveness of this authentication level relies on the information provided by the Core Processing System.

**Note:** Although level 2 questions may be answered correctly, the type of questions ask may not allow the system to determine a specific person performing the authentication. In this case, the authentication will proceed but it will be assumed the primary member is performing the authentication.

## 5.5. Additional Security

- **Enhanced Security:** Level 3 processing involves requesting additional security measures to ensure that the person authenticating is indeed the correct individual using the system.
- **Optional Security:** Level 3 security is an optional step in the authentication process.
- **Utilizing Prior Information:** Information gathered during the earlier stages of Level 1 and Level 2 processing may already suffice to authenticate the caller, making Level 3 optional.

## 5.6. Authentication Options by Level

- **Authentication Levels:** The table below specifies the level at which each authentication option is permitted.
- **Information Dependency:** It's important to note that the availability and support of each function are contingent on the information accessible within the core system.

Table: Authentication Options By Level

| Authentication Options by Level | Level 1 | Level 2 | Level 3 |
|---|---|---|---|
| Member Number or Customer Number | X | | |
| Login ID (Keystone Only) | X | | |
| Account Number (DNA Only) | X | | |
| Credit Card Number | X | | |
| ATM Card Number | X | | |
| Debit Card Number | X | | |
| Tax ID or SSN | X | | |
| PIN or Access Code | X | | |
| Choice of Member or Account Number | X | | |
| Choice of Member or Tax ID or SSN | X | | |
| Choice of Account Number or Tax ID or SSN | X | | |
| Choice of Member or Card Number | X | | |
| Card Number | X | | |
| Choice of Login ID or Card Number (Keystone Only) | X | | |
| Choice of Login ID or Tax Id /SSN (Keystone Only) | X | | |
| Choice of Login ID or Card Number (Keystone Only) | X | | |
| Date of Birth | | x | X |
| Last x of SSN | | X | X |
| SSN | | X | X |
| Driver's License | | X | X |
| Last x of Driver's License | | X | X |
| Numeric portion of Driver's License | | X | X |
| Phone Number | | X | X |
| PIN or Access Code | | X | X |
| Choice of PIN or SSN | | X | X |
| Choice of PIN or Federal ID | | X | X |
| X Number of characters of last name | | X | X |
| Zip Code | | | X |
| Federal ID | | X | X |
| Last 4 of Federal ID | | X | X |
| X Number of characters of business name | | | X |
| Choice of PIN or Last x of SSN | | X | X |
| Choice of PIN or Last x of Federal ID | | X | X |

## 5.7. Authentication Options by Core

The following list of authentication options is available within the system. The items listed indicate availability in the core processor.

Each function is dependent on the information available in the core. All information may not be available for all cores. Table on the next page.

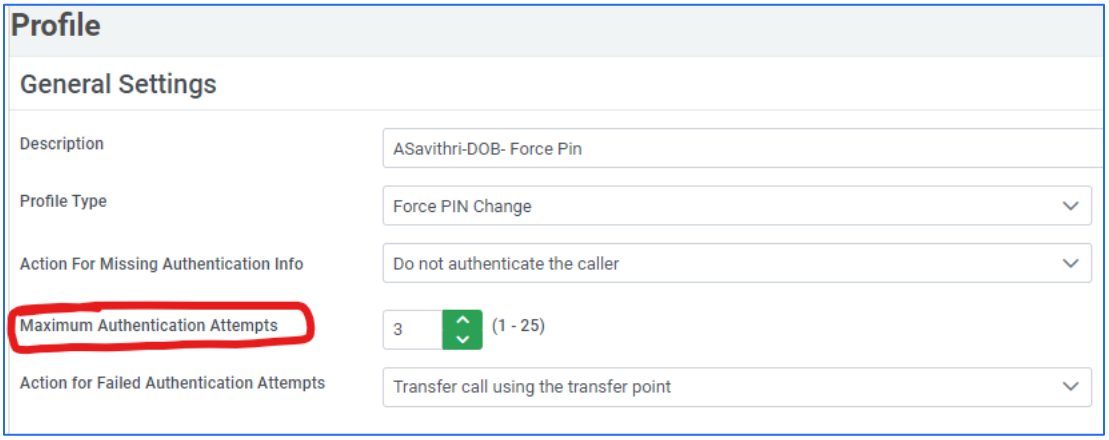
Table: Authentication Options By Core

| Level | Authentication Options by Core | Symitar (SymXchange) | Spectrum | Core API (DNA) | XP2 | Correlation Keystone |
|---|---|---|---|---|---|---|
| 1 | Member Number/Customer Number | X | X | X | X | |
| 1 | Login ID | | | | | X |
| 1 | Account Number | | | X | | |
| 1 | Credit Card Number | X | | | X | X |
| 1 | ATM Card Number | X | | | X | X |
| 1 | Debit Card Number | X | | | X | X |
| 1 | Level 1 Tax ID/SSN | X | X | X | | X |
| 1 | Level 1 PIN1 (In combination with another level 1 item) | | | X | | |
| 1 | Choice of Member or Account Number | | | X | | |
| 1 | Choice of Member or TaxID/SSN | | | X | | X |
| 1 | Choice of Account Number or Tax Id /SSN | | | X | | |
| 1 | Choice of Member or Card Number | X | X | | X | |
| 1 | Card Number | X | X | | X | X |
| 1 | Last x of Tax Number/SSN | | | X | | |
| 1 | Last x of SSN (In combination with another level 1 item) | | | X | | |
| 1 | Date of Birth (In combination with another level 1 item) | | | X | | |
| 2,3 | Date of Birth | X | X | X | X | X |
| 2,3 | Last x of SSN | X | X | X | X | X |

| Level | Authentication Options by Core | Symitar (SymXchange) | Spectrum | Core API (DNA) | XP2 | Correlation Keystone |
|---|---|---|---|---|---|---|
| 2,3 | SSN | X | X | X | X | X |
| 2,3 | Driver's License | X | | X | X | X |
| 2,3 | Last x of Driver's License | X | | X | X | X |
| 2,3 | Numeric portion of Driver's License | X | | X | X | X |
| 2,3 | Phone Number | X | X | X | X | X |
| 2,3 | PIN or Access Code | X | X | X | X | X |
| 2,3 | Choice of PIN or SSN | X | X | X | X | X |
| 2,3 | X Number of characters of last name | X | X | X | X | X |
| 2,3 | Zip Code | X | X | X | X | X |
| 2,3 | Choice of PIN or Last x of SSN | X | X | X | X | X |

## 5.8. Authentication Failure

- **System Settings for Authentication**: The system offers two settings to configure how a failed authentication is defined and how the caller will be informed of the failure.
- **Handling Authentication Failures**: In the case of an authentication failure within Proactive Info and Screen Pop, the call is directed to the caller's initially intended destination.
- **Maximum authentication attempts** : This setting specifies the maximum authentication attempts that will be allowed before assuming an authentication failure has occurred.



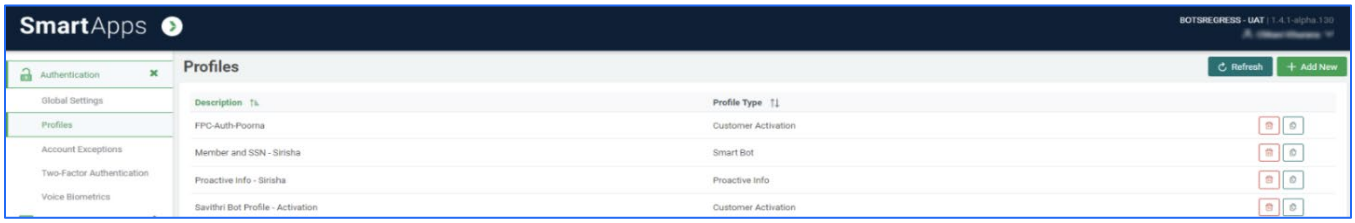
# 6. Profiles

A profile is created to associate with any of the SmartApps products for authentication. When a new profile is created, the system requests a Profile type to display the appropriate screens and collect the necessary information.

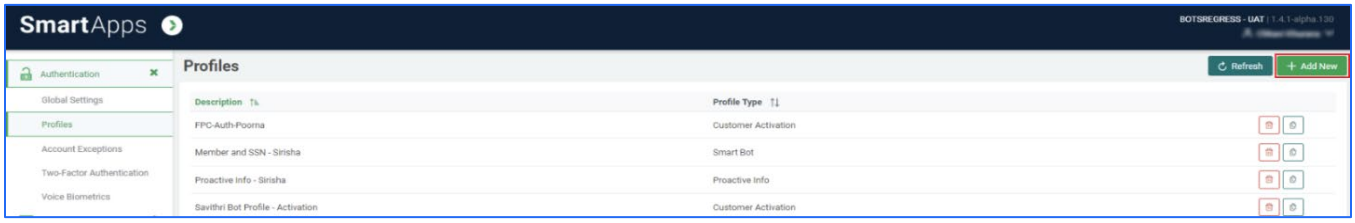
Profile Types that are currently available:

- Customer Activation
- Force PIN Change
- Proactive Info
- Screen Pop
- Smart Bot
- Teller

- Navigate to the **Profiles** under SmartApps **Authentication**.



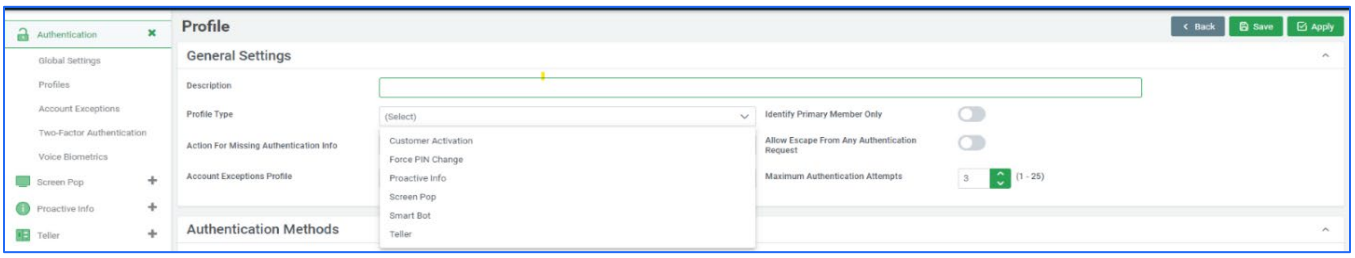

- Click on **Add New** to create a new authentication profile.



- **General Settings** section opens to help create a new profile. Select the required profile from the **Profile Type** drop-down.

**Note:** Since requirements are similar for these groups, the applications are grouped together for simplification:

- Proactive Info, Screen Pop, and Teller

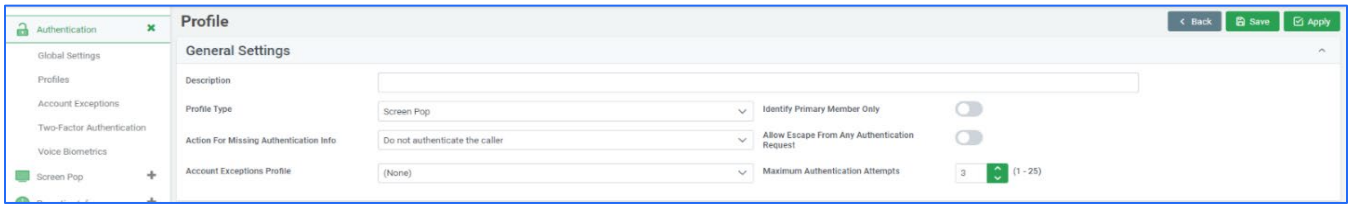



- Customer Activation and Force PIN Change

.

## 6.1. Adding a Proactive Info, Screen Pop Profile

Choose the Proactive Info or Screen Pop profile in the **Profile Type** in the **General Settings** section.




### 6.1.1. General Settings

The settings provided in the General Settings under Profile while creating a proactive Info or Screen Pop profile are explained below. The snapshot represents the General Settings on the Profiles page.


- **Description:** Create a profile with a complete description. The description is displayed in the pull-down lists on other screens.
- **Profile Type:** Choose the profile type from the pull-down menu. The following profile types are currently available:
    - Proactive Info
    - Screen Pop
    - Smart Bot
    - Customer Activation
    - Force PIN Change
    - Teller

- **Action For Missing Authentication Info:** Determines how to handle authentication information needed if the member does not have this information on file. For example, if the driver's license number is chosen as an authentication option. The caller may not have a driver's license number or may not have a driver's license number on file. In this situation, it will cause problems in the authentication process. To handle this issue, an option is provided describing what should occur if this situation is detected.

| Description | Explanation |
|---|---|
| Skip the authentication process for the missing information. | Ignore the authentication option selected. However, the system will never eliminate all authentication requirements. At least one authentication is always required, and level 1 authentication is never excluded. |
| Do not authenticate the caller. | The caller is treated as Failed Authentication completely. |

- **Account Exceptions Profile:** Account Exceptions Profile is a collection of settings related to Delinquency, Collections, Bankruptcy, Frozen & Dormancy that can be applied

to an Authentication Profile to tell the system how to handle each of those types of exceptions.

- **Identify Primary Member Only:** Identify Primary Member Only allows a site to specify that only the primary member on the account will be provided access to the system. If this is set to 'Yes', joint member records will not be considered during authentication.

- **Allow Escape from Any Authentication Request:** Allow Escape from Any Authentication Request, when set to 'Yes' allows the caller to press # if they do not know the information they are asked to complete.

- **Maximum Authentication Attempts:** Maximum Authentication Attempts indicates the maximum number of attempts allowed before the authentication process will consider it as a failure.

### 6.1.2. Authentication Methods

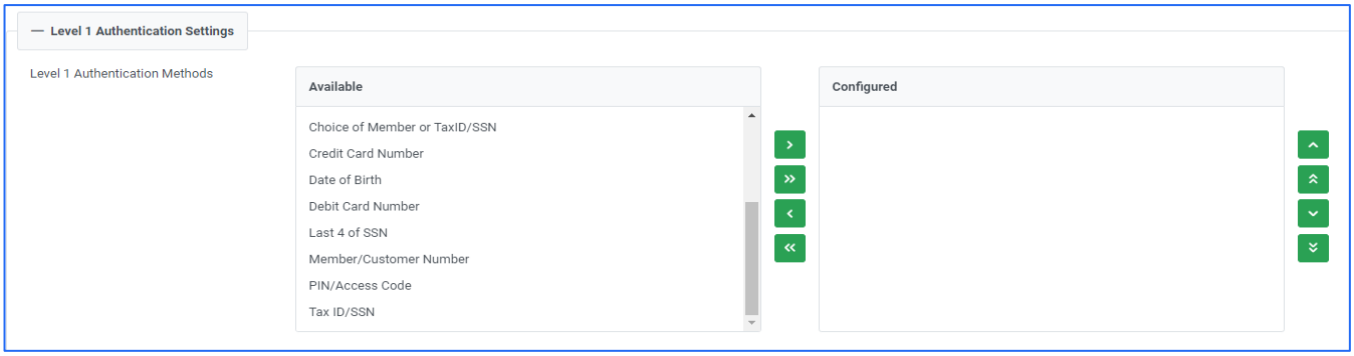
SmartApps provide Authentication Methods for the authentication process at three levels:

- Level 1
- Level 2
- Level 3

- **Level 1** is the first step and a mandatory authentication step.
- **Level 2** and **Level 3** have been identified under the tag *Personal Authentication Settings* and are optional for the Credit Unions.

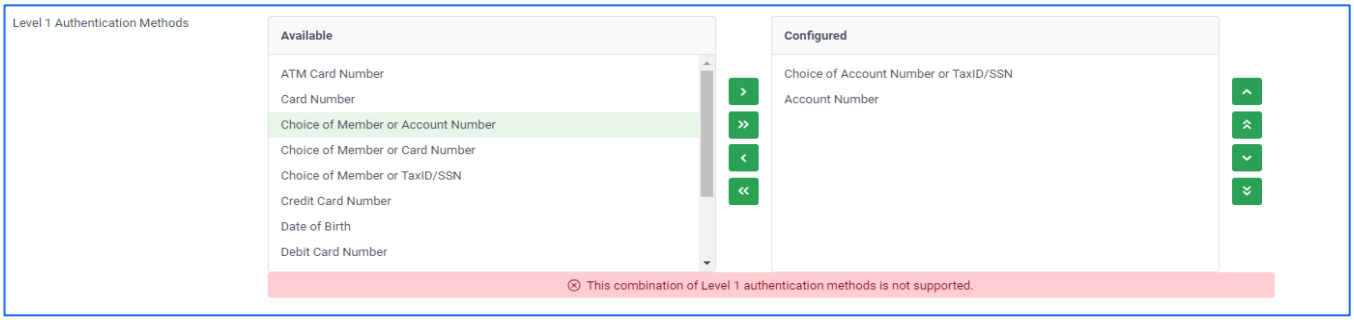
#### 6.1.2.1. Level 1 Authentication Settings

The authentication methods provided in the pull-down list vary based on the implemented active core. One or more options can be chosen and added to this selection, however in most situations, only one item is chosen.

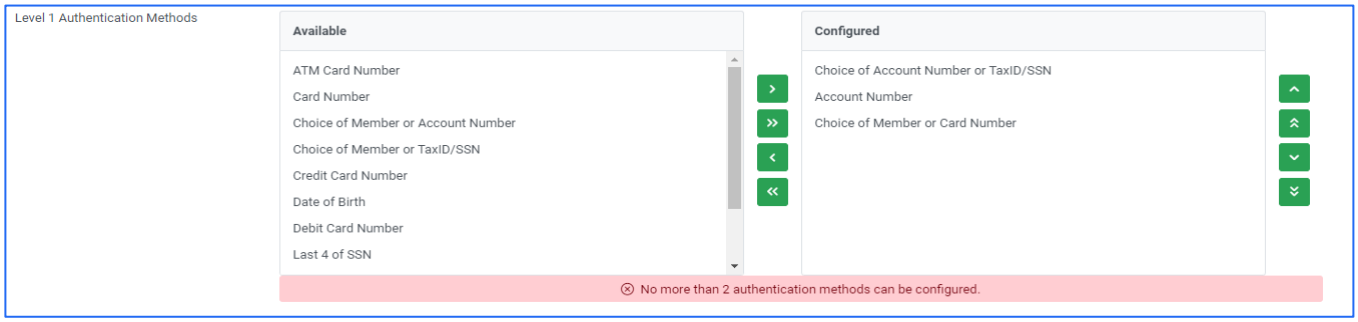



Choose the *Level 1* options in the Available tab and use the arrow buttons to select, deselect or move them up and down.

For a list of available authentication options for level 1 Authentication Options, please see section *Authentication Options by Level*




- Level 1 authentication option does not support more than 1 authentication method.
- Fiserv Core API does support more than one level 1 authentication method and other cores have a limit of maximum 2 options.
- Level 1 authentication option is mandatory for verification and authentication.

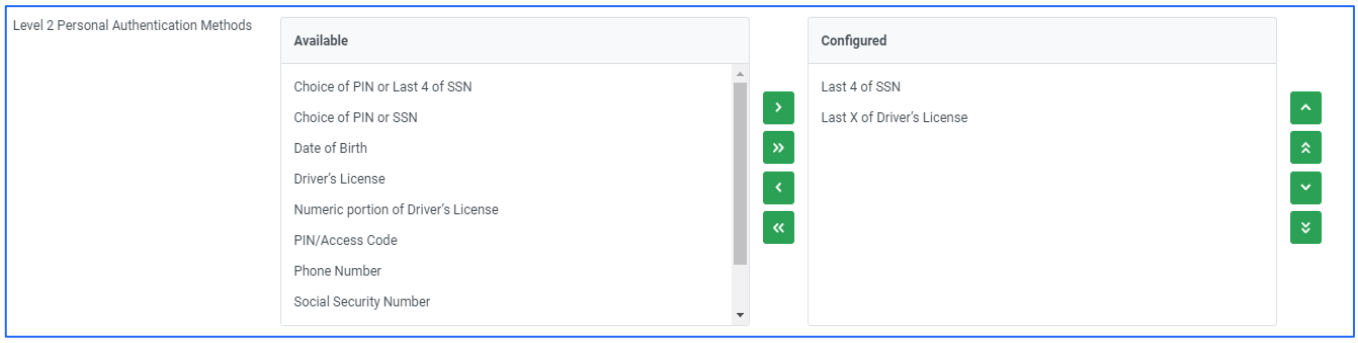



### 6.1.2.2. Personal Authentication Settings

Personal authentication settings allow a site to set up the additional authentication requirements over the *Level 1* requirements defined. Different authentication requirements can be defined for a personal account. Also, the definition of a verified caller and authenticated caller is defined. For a list of available authentication options for level 2 and level 3 of Personal Authentication Options, please see section *Authentication Options by Level*

#### *6.1.2.2.1. Level 2 Personal Authentication Methods*

Level 2 personal authentication method allows a site to choose one or more level 2 authentication options for personal accounts. There is no limit to the options that can be configured.



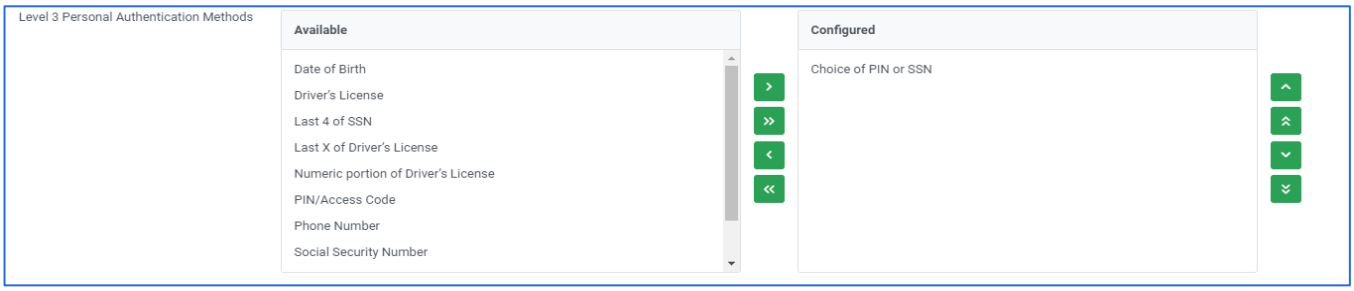

**Adding Level 2 Personal Authentication methods –**

A list of authentication options is provided to choose and add to the profile. The list of options available depends on the core processing system used for the site. For a list of available options for core, please see *Authentication Options by Core*.

- To add an authentication method, choose the authentication method using the pull-down list and click Add arrow.
- To remove a chosen authentication method, choose the authentication method to be removed and, click Remove arrow.
- To control the order of the authentication questions to be presented to the caller, move options up or down using the up or down arrows provided beside the Available authentication methods. The screen-listed order will be the method presented to the caller.

### *6.1.2.2.2. Level 3 Personal Authentication Methods*

Level 3 personal authentication method allows a site to choose one or more level 3 authentication options for personal accounts. There is no limit to the number of options that can be used for authentication.




**Adding Level 3 Personal Authentication Options** :

A list of authentication options is provided to choose and add to the profile. The list of options available depends on the core processing system used for the site. For a list of available options for your core, please see *Authentication Options by Core.*

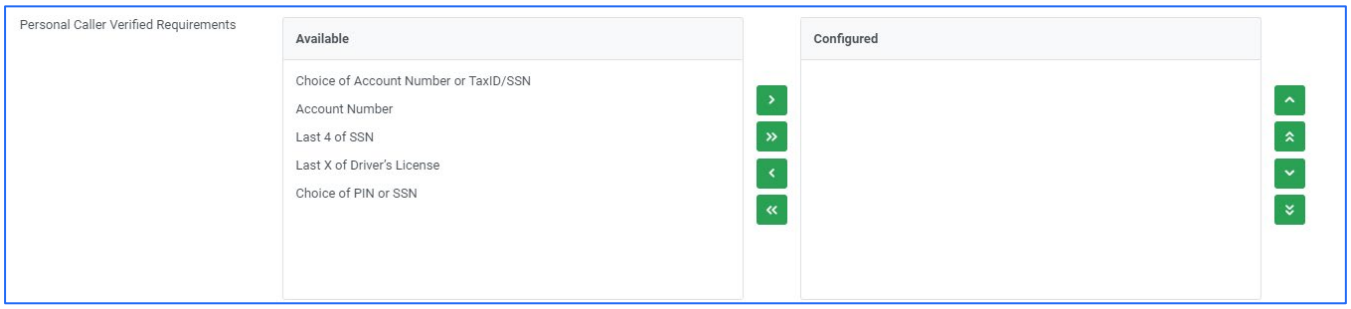
- To add an authentication method, choose the authentication method using the pull-down list and click Add arrow.
- To remove a chosen authentication method, choose the authentication method to be removed and, click Remove arrow.
- To control the order of the authentication questions to be presented to the caller, move options up or down using the up or down arrows provided beside the **Available**

authentication methods. The screen-listed order will be the method presented to the caller.

#### *6.1.2.2.3. Personal Caller Verified Requirements*

The personal caller verified requirements allows the site to determine the authentication methods that must be correct to determine the caller is verified but not authenticated. The list of verified requirements available for selection will be a combination of the authentication methods chosen for *level 2 and level 3*.

- To add an authentication method to the verified list, choose the authentication method using the pull-down list and click Add arrow.
- To remove a chosen authentication method, choose the authentication method to be removed and, click Remove arrow.

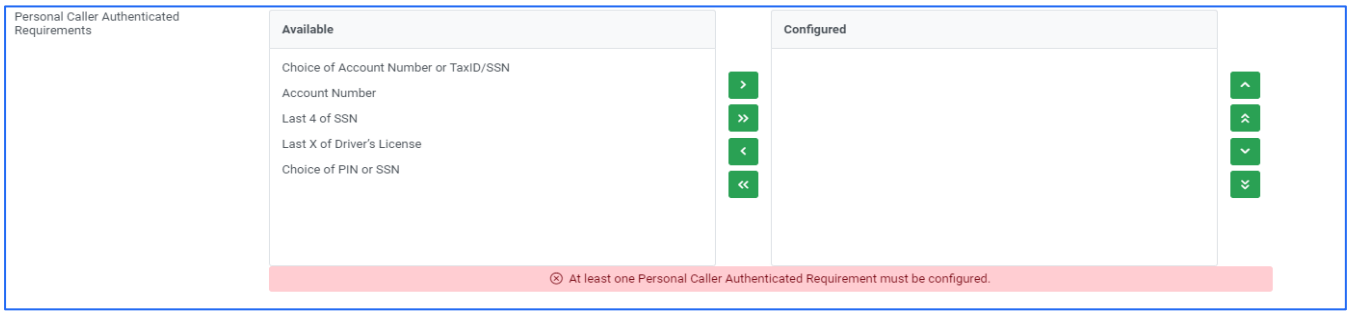



#### *6.1.2.2.4. Personal Caller Authenticated Requirements*

The personal caller authenticated requirements allows the site to determine the authentication methods that must be correct to determine the caller is authenticated. The list of authentication requirements available for selection will be a combination of the authentication options chosen for *level 2 and level 3*.

- To add an authentication method to the authenticated list, choose the authentication method using the pull-down list and click Add arrow.
- To remove a chosen authentication method, choose the authentication method to be removed and, click Remove arrow.

- At least, one Personal Caller authentication requirement must be configured.




**Comparison between Verified Requirements and Authenticated Requirements**

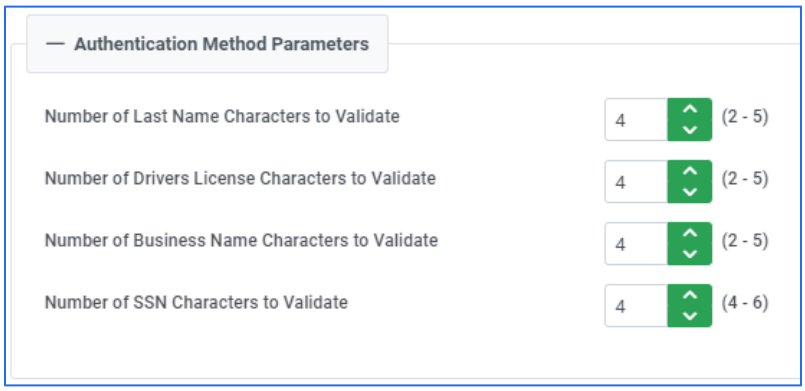
The authentication system allows a site to define the difference between an authenticated caller and a verified caller.

- A V**erified Caller** is a caller that has provided enough correct information to determine who the caller is but has not provided enough information to be considered authenticated.
- An authenticated caller provided all the information required to be considered authenticated. On several products, the configuration will allow the site to indicate if the caller must be authenticated or verified to continue.
- An important reason that a site wants to define the difference between authenticated and verified is for **Screen Pop**. If the caller is verified but not authenticated, the information can still be passed to the agent even if a positive authentication has not been made.
- It should be noted that Teller will always require authentication to continue. Verified is not supported on this type of profile.
- Level 1 authentication options are considered required for verification and authentication.

### 6.1.2.3. Authentication Method Parameters:

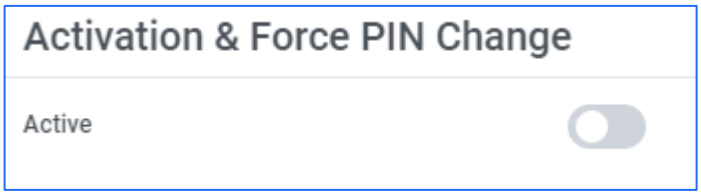
- **Number of Last Name Characters -**allows a site to configure the number of characters needed if the last name authentication option is used**.** The number of characters can range from 2 to 5.
- **Number of Driver's License Characters** – allows a site to configure the number of digits needed if the driver's license authentication option is used. The number of digits can range from 2 to 5.

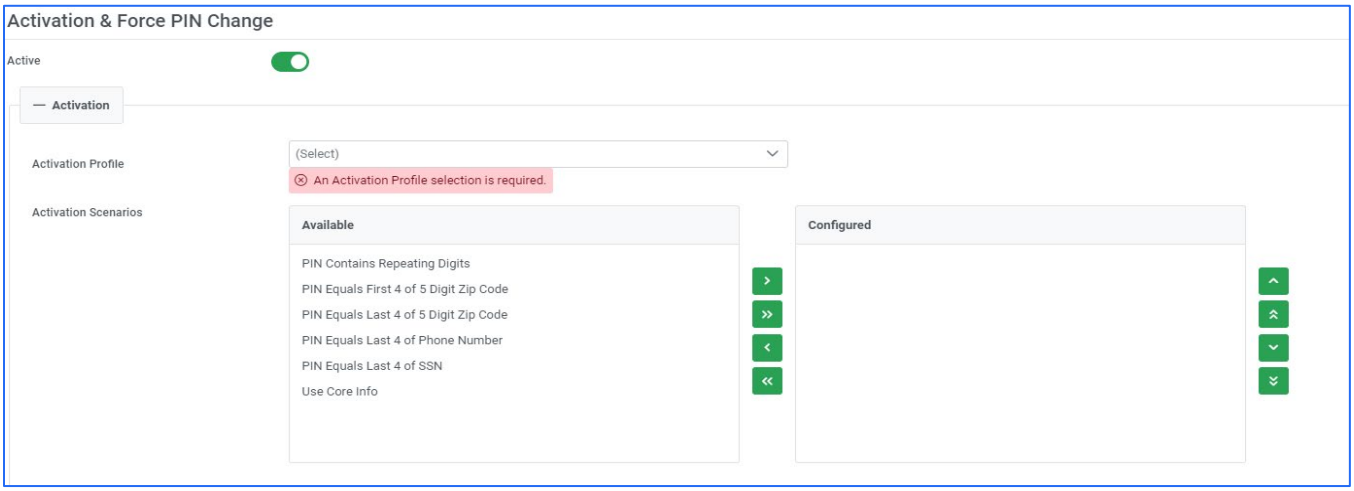
- **Number of Business Name Characters-** A site that configures the number of characters needed if the business name authentication option is used. The number of characters can range from 2 to 5.
- **Number of SSN Characters-** allows a site to configure the number of SSN characters if SSN is used as Authentication option. It ranges from 4 to 6.

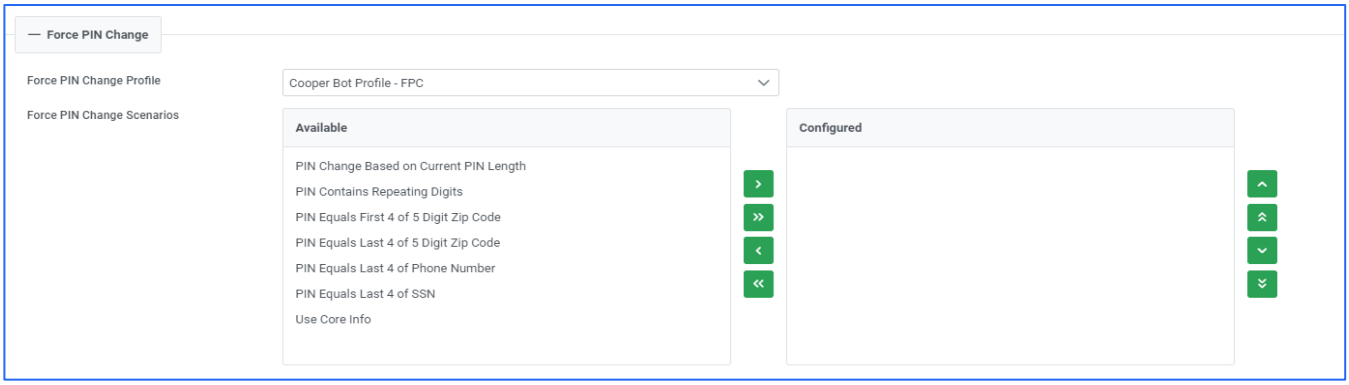


### 6.1.3. Customer Activation & Force PIN Change

If the Activation and Force Pin Change are active



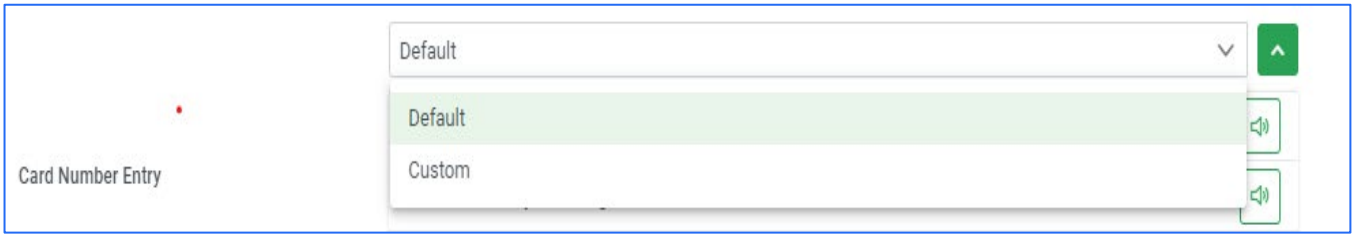
### 6.1.4. Custom Prompts

The authentication system provides default prompts for all authentication methods.

- These prompts can be customized by overriding the default prompts within the Custom Prompts section of an Authentication Profile.
- Each screen is listed below which the default verbiage will be played if not overridden. A sequence of prompts can be chosen. If 'Default' is displayed, the default sequence of prompts will be used.
- The prompts are available in English language .

Default Verbiage

The default touch-tone provided by SmartApps. These prompts can be customized using the **Custom** option in the drop-down menu.




| Custom Prompt | Touchtone |
|---|---|
| Account Number Entry | Please enter your account number followed by the pound sign. |
| ATM Card Number Entry | Please enter your ATM card number followed by the pound sign. |
| Card Number Entry | Please enter your card number followed by pound (#) sign. |
| Account Number or Tax Id/SSN | You can use your Account Number, Federal ID, or Social Security Number to authenticate.<br>To authenticate using Account Number, Press 1.<br>To authenticate using Federal Id or Social Security Number, Press 2. |
| Login ID | Please enter your login-id followed by the pound (#) sign. |
| Login Id or Tax Id/SSN | You can use your Login Id, Tax Id or Social Security Number to authenticate.<br>To authenticate using a Login Id, Press 1.<br>To authenticate using Tax Id or Social Security Number, Press 2. |
| Login Id or Card Number | You can use your Login Id, or Card Number to authenticate.<br>To authenticate using a Login Id, Press 1. |

| | |
|---|---|
| | To authenticate using a Card number, Press 2. |
| Member or Account Number (A variation) | You can use your Member Number or Share to authenticate.<br>To authenticate using a Member Number, Press 1.<br>To authenticate using a Share, Press 2. |
| Member or Account Number (An variation) | You can use your Member Number, or Account Number to authenticate.<br>To authenticate using a Member Number, Press 1.<br>To authenticate using a Account Number, Press 2. |
| Member or Card Number (A variation) | Please enter a Member Number or Card Number followed by # sign. |
| Member or Card Number (An version) | Please enter an Member Number or Card Number followed by the pound (#) sign. |
| Member or Tax ID/SSN | You can use your Member Number, Tax id or Social Security Number to authenticate.<br>To authenticate using a Member Number, Press 1.<br>To authenticate using a Tax id or Social Security Number, Press 2. |
| Credit Card Number Entry | Please enter your Credit Card Number followed by the pound (#) sign. |
| Member Entry | Please enter your Member Number followed by the pound (#) sign. |
| PIN/Access Code Entry | Please enter your Personal Identification Number followed by the pound (#) sign. |
| Tax Id/SSN Entry | Please enter the social security or Tax Id number followed by the pound (#) sign. |
| Debit Card Number Entry | Please enter a Debit Card Number followed by the pound (#) sign. |
| DOB Entry | Please enter a birthdate associated with your account followed by the pound sign. This date must be entered as a 2-digit month, a 2- digit day, and a 4-digit year.<br>For example, January fifth, 1970, would be entered zero-one, zero-five, one-nine-seven-zero. |
| DL Entry | Please enter a driver's license number associated with this account, followed by the pound (#) sign. |
| Last x of SSN | Please enter the last x digits of a Social Security Number associated with the account followed by the pound (#) sign. (Number of digits controlled by a configuration setting) |
| PIN or Last X of SSN | You can use the last 4 digits of a Social Security Number or PIN to authenticate. |

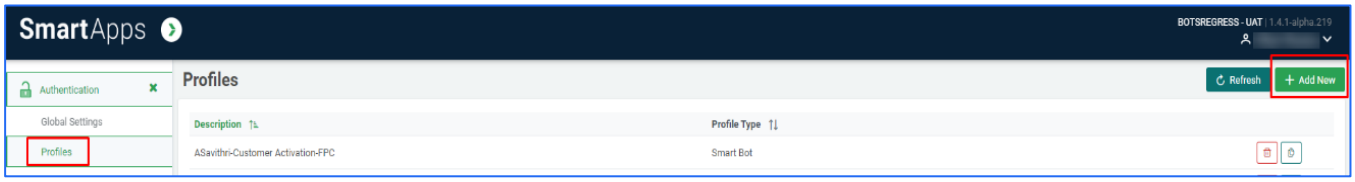
| | |
|---|---|
| | To authenticate using a PIN, press 1<br>To authenticate using the last 4 digits of a Social Security Number on the account, press 2. |
| PIN or SSN | You can use a Social Security Number or PIN to authenticate.<br>To authenticate using a PIN, press 1<br>To authenticate using a Social Security Number on the account, press 2. |
| Last X of DL Entry | Please enter the last {X} digits of the driver's license number associated with your account followed by the pound (#) sign. |
| Numeric DL Entry | Please enter the numeric portion of a driver's license associated with the account followed by the pound (#) sign. |
| Phone Number | Please enter a 10-digit phone number which includes the area code associated with this account followed by the pound (#) sign. |
| PIN Entry | Please enter your PIN associated with your account followed by the pound (#) sign. |
| Full SSN | Please enter a Social Security Number associated with the account followed by the pound (#) sign. |
| X Number of Chars of Business Name | Please enter the first {X} characters of a last name associated with the account followed by the pound (#) sign. |
| X Number of Chars of Last Name | Please enter the first {X} characters of a last name associated with the account followed by the pound (#) sign. |
| Zip Code | EN: Please enter a zip code associated with the account followed by the pound (#) sign. |

## 6.2. Adding a Customer Activation or Force PIN Change profile

Force PIN Change and Customer Activation share a close structural relationship as they both involve situations where a member is prompted to change their PIN during a phone call. The process of Force PIN change and Activation is governed by various aspects. These aspects encompass PIN creation configuration, scenario configuration, PIN change determination, and authentication profiles.

The creation of a valid PIN is guided by multiple business rules. Each credit union may set up its unique set of rules that outline the specific requirements for a valid PIN. The SmartApps Authentication Global Settings screen enables the configuration of PIN characteristics.

1. Click **Add New** on the **Profiles** Page.

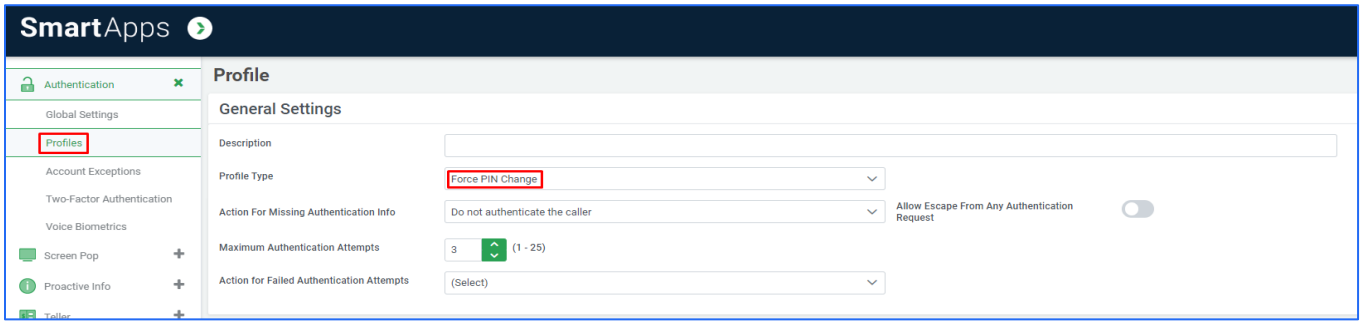



2. Choose the Customer Activation or Force PIN Change profile in the **Profile Type** in the **General Settings** section.
3. For other settings related information, read further description.

### 6.2.1. General Settings

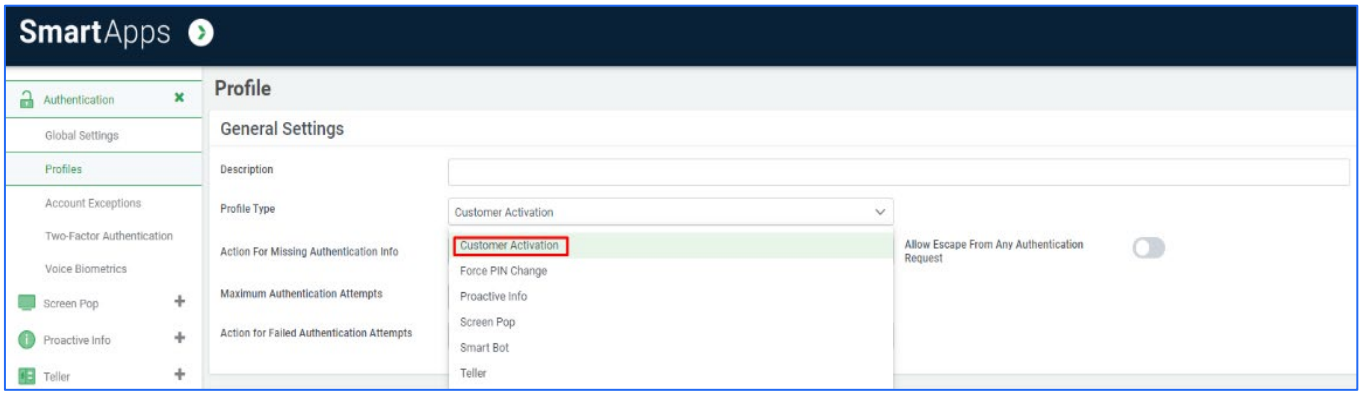
The settings provided in the **General Settings** under **Profile** while creating a Customer Activation or Force PIN Change profile are explained below.

Snapshot: **General Settings** on the **Profiles** page.




#### *6.2.1.1. For Customer Activation*

Customer Activation has similar requirements as Force PIN Change.




- **Description:** Create a profile with a complete description. The description is displayed in the pull-down lists on other screens.

- **Profile Type:** Choose the profile type from the pull-down menu. The following profile types are currently available:

  i) Proactive Info
  ii) Screen Pop

iii) Smart Bot
iv) Customer Activation
v) Force PIN Change
vi) Teller

- **Action For Missing Authentication Info:** Decides how to handle authentication information needed if the member does not have this information on file. For instance, if the driver's license number is chosen as an authentication method. The caller may not have a driver's license number or may not have a driver's license number stored in the records. This can pose challenges during the authentication process. To address this issue, an option is available to specify how to continue when such a situation is detected.

| Description | Explanation |
|---|---|
| Skip the authentication process for the missing information. | Ignore the authentication method selected. However, the system will never drop all authentication requirements. At least one authentication is always needed, and level 1 authentication is never excluded. |
| Do not authenticate the caller. | The caller is treated as Failed Authentication completely. |

- **Maximum Authentication Attempts:** Maximum Authentication Attempts shows the maximum number of attempts allowed before the authentication process will consider it as a failure. This can be set ranging between 1 and 25.

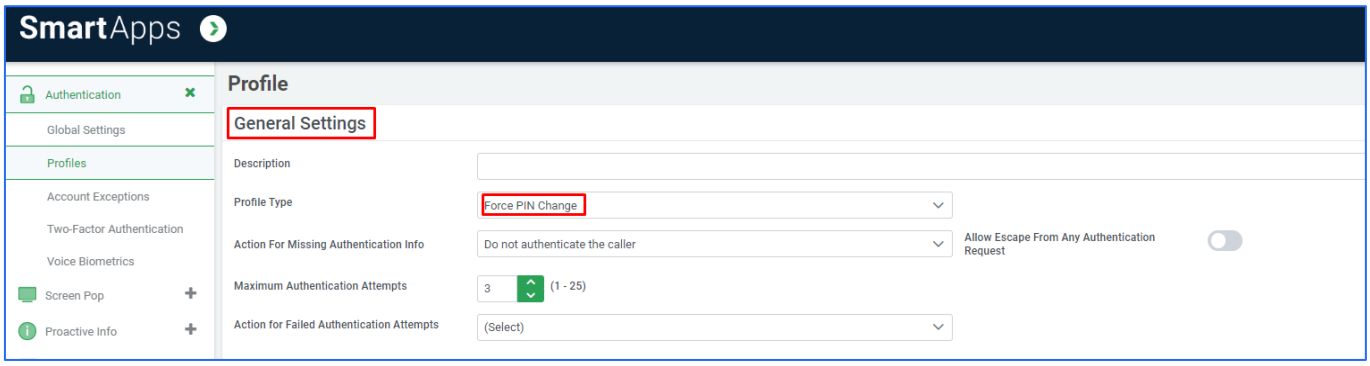
- **Action for Failed Authentication Attempts:** The below table describes the available action parameters.

| Action | Explanation |
|---|---|
| Disconnect the call. | The caller will be disconnected with no message. |
| Play authentication failure message and disconnect. | A message will be played saying the authentication failure has occurred then the call will be disconnected |

| | |
|---|---|
| Transfer call using the transfer point | A message will be played saying the authentication failure has occurred and the caller will be transferred to an agent. The call is then transferred to the transfer point FPCH – Force PIN Change. |

- **Allow Escape from Any Authentication Request:** When the setting "Allow Escape from Any Authentication Request" is set to 'Yes', it grants the caller the ability to press the '#' key if they are unable to supply the requested information during the authentication process.

### *6.2.1.2. For Force PIN Change*




- **Description:** Create a profile with a complete description. The description is displayed in the pull-down lists on other screens.

- **Profile Type:** Choose the profile type from the pull-down menu. The following profile types are currently available:
  i) Proactive Info
  ii) Screen Pop
  iii) Smart Bot
  iv) Customer Activation
  v) Force PIN Change
  vi) Teller

- **Action For Missing Authentication Info:** Decides how to handle authentication information needed if the member does not have this information on file. For example, if the driver's license number is chosen as an authentication method. The caller may not

have a driver's license number or may not have a driver's license number on file. In this situation, it will cause problems in the authentication process. To handle this issue, an option is supplied describing what should occur if this situation is detected.

| Description | Explanation |
|---|---|
| Skip the authentication process for the missing information. | Ignore the authentication method selected. However, the system will never drop all authentication requirements.<br><br>At least one authentication is always needed, and level 1 authentication is never excluded. |
| Do not authenticate the caller. | The caller is treated as Failed Authentication completely. |

- **Maximum Authentication Attempts:** Maximum Authentication Attempts shows the maximum number of attempts allowed before the authentication process will consider it as a failure. This can be set ranging between 1 and 25.

- **Action for Failed Authentication Attempts:** The below table describes the available action parameters.

| Action | Explanation |
|---|---|
| Disconnect the call. | The caller will be disconnected with no message. |
| Play authentication failure message and disconnect. | A message will be played saying the authentication failure has occurred then the call will be disconnected |
| Transfer call using the transfer point | A message will be played saying the authentication failure has occurred and the caller will be transferred to an agent. The call is then transferred to the transfer point FPCH – Force PIN Change. |

- **Allow Escape from Any Authentication Request:** When the setting "Allow Escape from Any Authentication Request" is set to 'Yes', it grants the caller the ability to press the '#'

key if they are unable to supply the requested information during the authentication process.

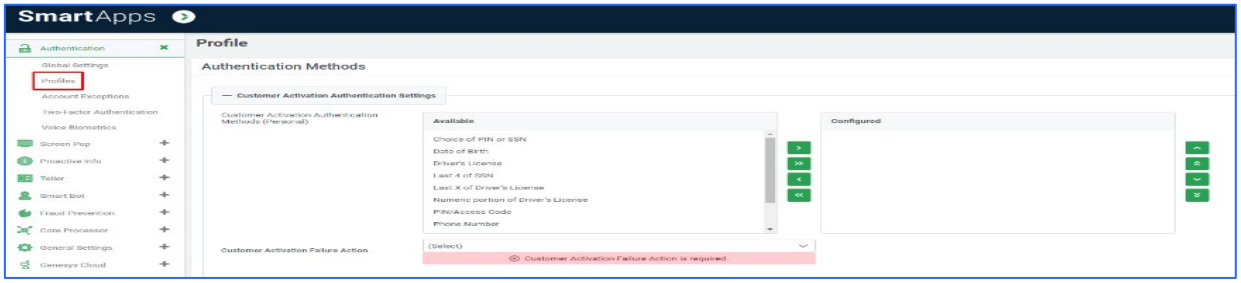
## 6.2.2. Authentication Methods

### *6.2.2.1. For Customer Activation*

Once it is confirmed that customer activation is needed, they will be directed to a preconfigured authentication profile designed specifically for handling customer activations.

A list of authentication methods is supplied and can be added to the profile. The list of options available varies depending on the core processing system used for the site.

- To add an authentication method, choose the authentication method from the **Available** list and press single right *arrow (>).*
- To remove a chosen authentication method, choose the authentication method from **Configured** list and press single left arrow *(<).*
- Double arrow moves all the options from the **Available** list to the **Configured** list and vice versa.
- To control the order in which the authentication questions will be presented to the caller, move options up or down using the up or down arrows provided to the right of the **Configured** authentication methods box.
- The order listed on the screen will be the order options are presented to the caller.



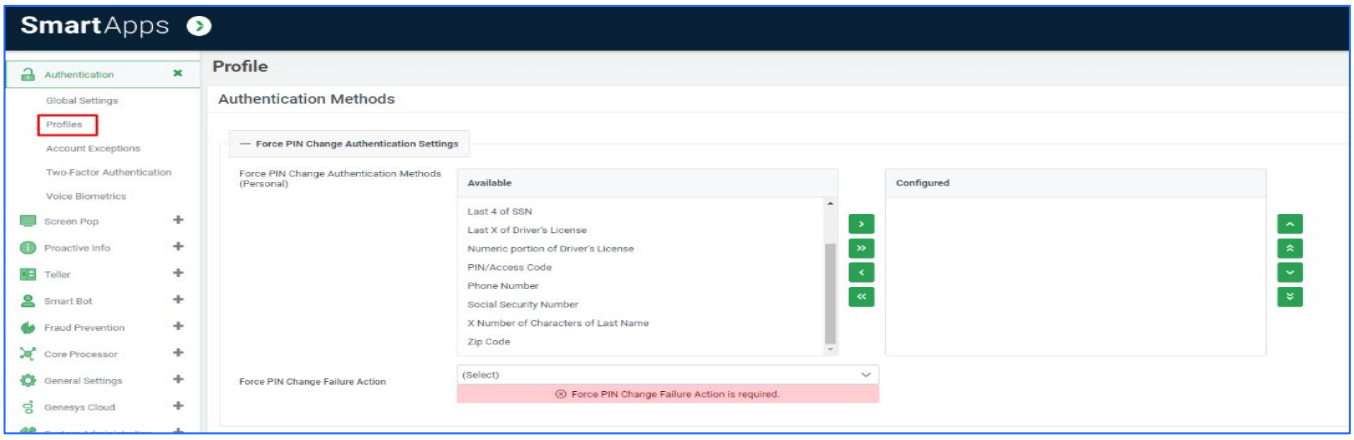

**Activation Failure Options:** The table below the list of available messages played to the caller in case of Activation failure.

| Action | Explanation |
|---|---|
| Disconnect | The caller will be disconnected with a “Thank you for calling, Goodbye.” message. |

| | |
|---|---|
| Play authentication failure message and disconnect | A message will be played saying the authentication failure has occurred then the call will be disconnected |
| Transfer the caller based on the Customer Activation Transfer Point | A message will be played saying the authentication failure has occurred. If the smart apps product is Teller, the caller will be transferred to transfer point 0235. If the smart apps product is Screen Pop or Proactive Info, the call will continue to its destination. |

### *6.2.2.2. For Force PIN Change*

Once it is confirmed that Force PIN Change is needed, they will be directed to a preconfigured authentication profile designed specifically for handling Force PIN Changes.




A list of authentication methods is supplied and can be added to the profile. The list of options available varies depending on the core processing system used for the site.

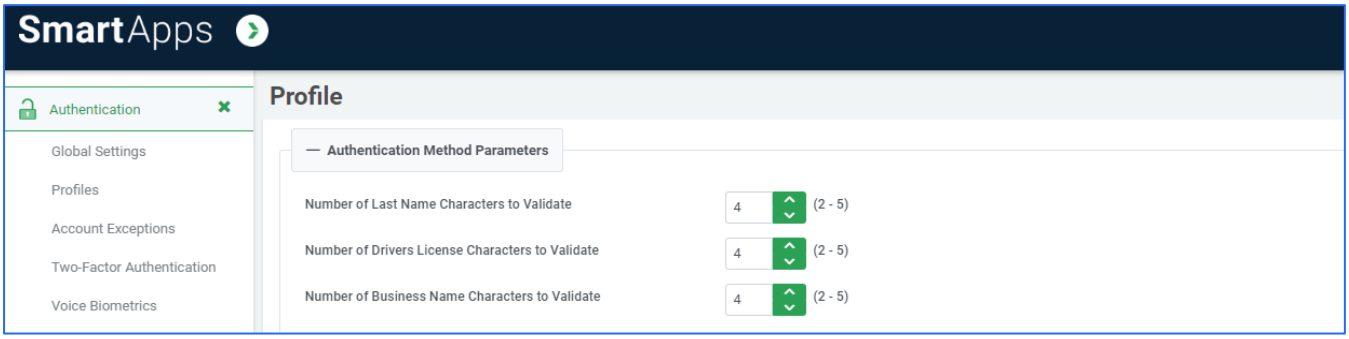
- To add an authentication method, choose the authentication method from the **Available** list and press single right *arrow (>*.
- To remove a chosen authentication method, choose the authentication method from **Configured** list and press single left arrow *(<)*.
- Double arrow moves all the options from the **Available** list to the **Configured** list and vice versa.
- To control the order in which the authentication questions will be presented to the caller, move options up or down using the up or down arrows provided to the left of the **Configured** authentication methods box.
- The order listed on the screen will be the order options are presented to the caller.

**Force PIN Change Failure Actions:** The table below the list of available messages played to the caller in case of Activation failure.

| Action | Explanation |
|---|---|
| Disconnect | The caller will be disconnected with a "Thank you for calling, Goodbye." message. |
| Play authentication failure message and disconnect | A message will be played saying the authentication failure has occurred then the call will be disconnected |
| Transfer the caller based on the Force PIN Change Transfer Point | If the smart apps product is Teller, the caller will be transferred to transfer point FPCH. If the smart apps product is Screen Pop or Proactive Info, the call will continue to its destination. |

### 6.2.3. Authentication Method Parameters

**For both Customer Activation and Force PIN Change:** The below snapshot displays the Authentication Method Parameters both for Customer Activation and Force PIN Change.




- **Number of Last Name Characters** allows a site to configure the number of characters needed if the last name authentication method is used**.** The number of characters can range from 2 to 5.

- **Number of Driver's License Characters** – Number of Driver's License allows a site to configure the number of digits needed if the driver's license authentication method is used. The number of digits can range from 2 to 5.

- **Number of Business Name Characters:** A site that configures the number of characters needed if the business name authentication method is used. The number of characters can range from 2 to 5.

### 6.2.4. Custom Prompts

The authentication system provides default prompts for all authentication methods. These prompts can be customized by overriding the default prompts within the **Custom Prompts** section of an **Authentication Profile**.

#### *6.2.4.1. For Customer Activation*

**Default Verbiage:** Your "Credit Union Name" credit union welcomes you as a new member or a new caller to our automated system. This process will help you activate your account. Once activated, you can log in to the system to access your account information.


#### *6.2.4.2. For Force PIN Change*

**Default Verbiage:** Your "Credit Union name" credit union is always concerned about the security of your account. To protect your security, you will need to change your PIN.

# 7. Account Exceptions

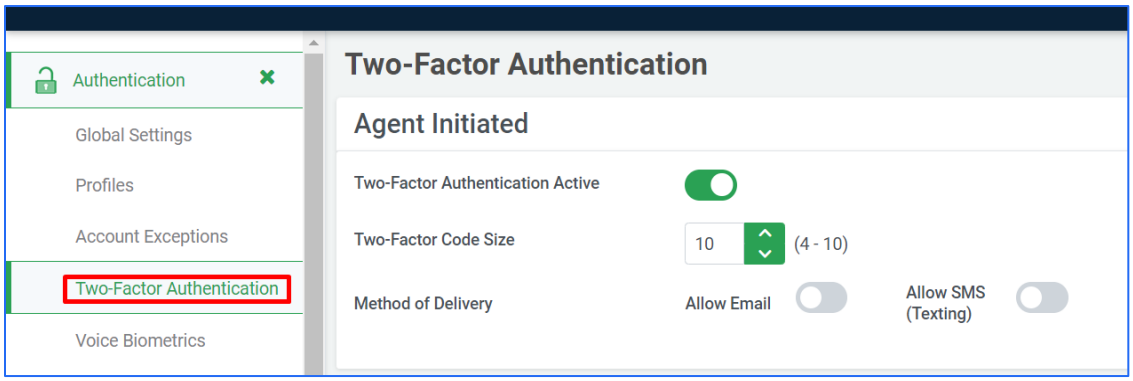
# 8. Two-Factor Authentication

## 8.1. Overview

- SmartApps Cloud includes sending SMS or Emails to members with a temporary code for verification and authentication.
- This approach enhances security by keeping the process within the member's account and ensuring delivery only to registered contact addresses.
- The Two-Factor Authentication section manages the method and specifics of how communications, including the temporary codes, are sent.

## 8.2. Setting up Two-Factor Authentication

The **Agent Initiated** section helps configure Two-Factor Authentication for members.




The table below describes the parameters of the setting.

Table: Two -factor Authentication parameters

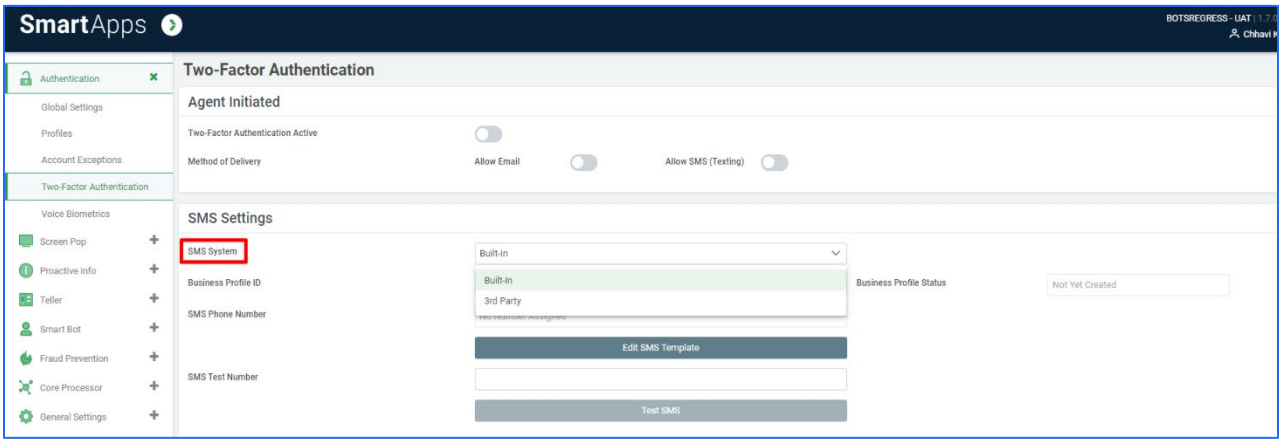
| Parameter | Description |
|---|---|
| Two-Factor Authentication Active | Enables Two-Factor authentication for the platform |
| Two-Factor Code Size | Controls the number of digits used when the temporary code is generated. The range lies between 4 to 10. |
| Method of Delivery | Enables the ways in which the generated code can be sent, via Email and/or SMS. |

# 8.3. SMS Settings

The SMS settings allow Credit Unions to send SMS messages securely, either through SmartApps Cloud's built-in SMS system or using Genesys Cloud as a 3rd Party provider, with detailed configuration options for business profiles, phone number assignment, and message templates.

The SMS setting in the Two-Factor Authentication provides two SMS systems:

- Built-In
- 3rd Party




## 8.3.1. SMS System – Built-in( SmartApps Cloud)

- The SMS settings allows to procure a phone number for sending SMS messages and assign the phone number to your organization.
- In this process, the Credit Union must provide a contact within the organization to ensure the company exists and confirm the employment status of the requested employee.

### Prerequisite

a) **Create Business Profile:** All US carriers now mandate that businesses register each phone number used for sending automated SMS. This form guides the Credit Union through the process of registering its organization with the carriers. Once all the required information is provided, the Credit Union can submit the business profile for review.

Table: Create Business Profile parameters

| Parameter | Description |
|---|---|
| Legal Business Name | Enter the legal name for the registering business. |
| Profile Friendly Name | The system will automatically generate the profile name. |
| Business Type | Specify the type of business; for Credit Unions, it should be Non-Profit. |
| EIN Number | Provide the Business EIN Number, which can be searched for here. |
| Website URL | Share the business home website, ensuring the format is https://website.com. |
| Status Email | Enter the email address to receive updates on the registration process. Details about the application's status—whether in process, declined, or completed—will be sent to this email address. It doesn't necessarily have to be an email from the business applying. |
| Business Address Information | Provide the business headquarters address. |
| Person to Contact | Share contact information for an employee working for the business. This person must be verifiable on sites like LinkedIn and may be contacted through the provided information for verification purposes.<br>**Note:** For the Job Position field, choose the closest position or select "other" if none match. |

**b) Assign Phone Numbers:**

1. Upon creating a business profile:
    a. Actively assign a phone number for Two-Factor authentication messages.
    b. No approval is needed for the assignment and testing of the phone number.
2. The process is facilitated through the "Assign Phone Number" form:
    a. Explore available numbers based on area code or locality (City/State).
    **b. Search by Number:**
        i. Choose **Number** from the Search Criteria dropdown.
        ii. In the Search Criteria textbox, enter desired starting numbers for the phone number (three digits of the area code or more, including the exchange).
        iii. Initiate the search by clicking the Search button to display available phone numbers and their respective localities.
    **c. Search by Locality:**

i. Choose **Locality** from the Search Criteria dropdown.
ii. Input the City and State in the corresponding textbox.
iii. Click the **Assign** button upon pinpointing the desired phone number to trigger the procurement and assignment to the SmartApps Cloud organization.

3. If there is a decision to change the assigned phone number later repeat the process to release the previous phone number.
4. Select and assign the new phone number to assign to the Smart Apps Cloud organization.

**Note:** After the prerequisites are completed the below table describes the SMS system parameters and their functionality that can be used to set up the desired Built-in settings.

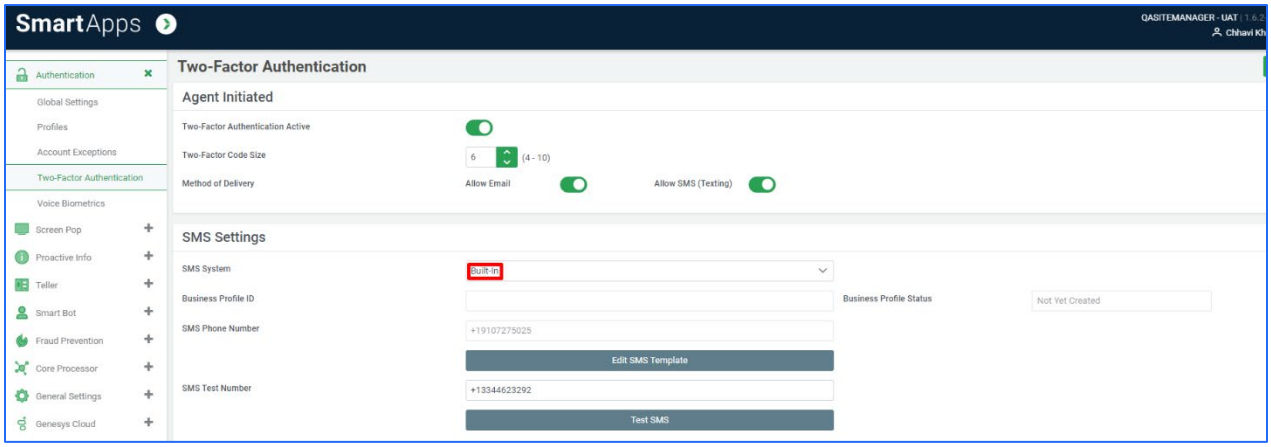



Table: SMS System – Built-in( SmartApps Cloud) parameters

| Parameter | Description |
|---|---|
| SMS System | SmartApps Cloud platform's Built-In feature actively utilizes its ability to procure and send SMS through an integrated SMS broker. |
| | |
| Business Profile ID | To acquire an SMS phone number, the carriers require information about the company procuring the number to link it to that organization. Clicking the **Create Business Profile** button initiates the process of crafting a business profile for the Credit Union using SmartApps. Detailed information on the Business Profile creation process is provided in |

| Parameter | Description |
|---|---|
| | Prerequisite(a). Upon completing the process, a unique identifier becomes visible in the text box. |
| SMS Phone Number | Assigning the phone number to send SMS messages to the member is accomplished using SmartApps. The Credit Union, when procuring the SMS number through SmartApps, can search for available numbers in proximity to their location. After selecting **Assign Phone Number**, the form guides through the process of assigning the desired phone number. Further details on the assignment process are provided in Prerequisite(b).<br><br>**Note:** If toll-free numbers are desired, it is advised to contact SmartApps Cloud support for additional details. The creation of a Business Profile is still necessary to acquire the toll-free number. |
| Edit SMS Template (Button) | Enables the editing of the SMS message sent to the member. The SMS message is subject to a character limit of 160. The **SecurityCode** replacement tag is the location where the temporary generated code is substituted when the message is generated. |
| SMS Test Number | There is a test phone number available to send a test message, ensuring the correct functionality of outbound messages. |
| Send Test SMS (Button) | The system will actively attempt to send an SMS from the SMS Phone Number to the SMS Test Number using the current SMS Template message details when utilizing the SMS Test Number field. |

### 8.3.2. SMS Settings – 3rd Party(Genesys Cloud)

- Enables configuration of the phone number used for sending SMS messages through Genesys Cloud.
- Involves purchasing the SMS number separately from SmartApps Cloud.
- The sending process is executed by Genesys Cloud.
- Whenever SmartApps needs to send a Two-Factor message, it actively sends the request through a Genesys Cloud workflow.

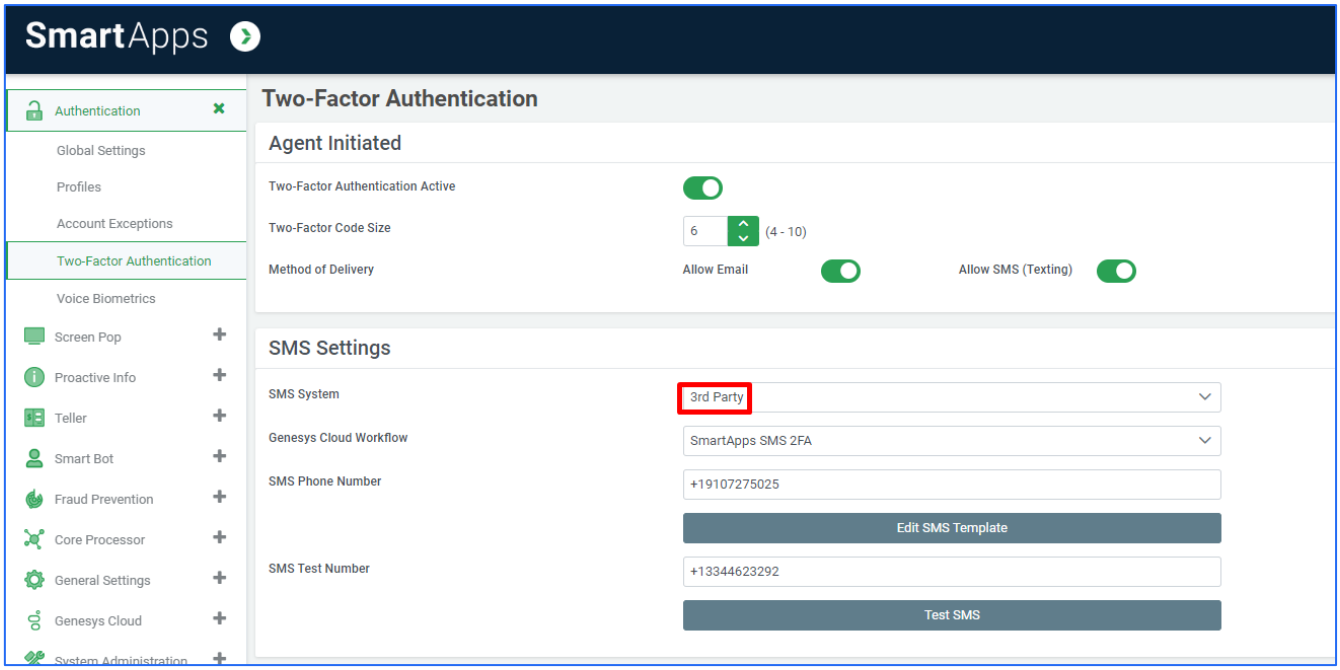


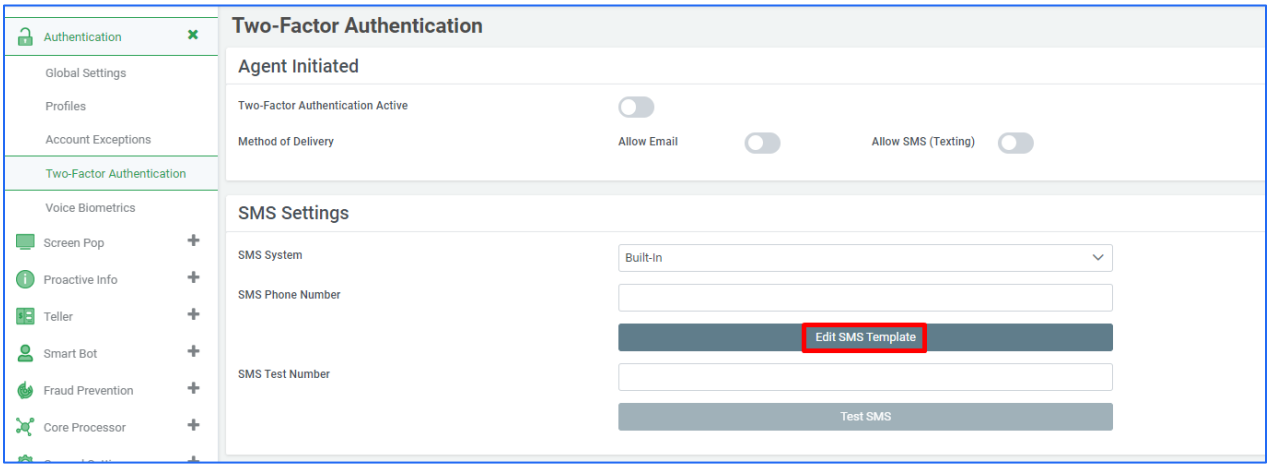

Table: SMS System – 3rd Party( Genesys Cloud) parameters

| Parameter | Description |
|---|---|
| SMS System | 3rd Party uses Genesys Cloud to send the outbound SMS through a configured SMS procured number. |
| Genesys Cloud Workflow (3rd Party) | The list comprises Genesys Cloud workflows configured within your Genesys Cloud environment. The workflow actively seeks four parameters to be sent into it:<br>• Body – Text of the SMS message<br>• To – Phone number to deliver SMS<br>• From – From number to deliver SMS from<br>• Code – Temporary SMS code |
| SMS Phone Number | The system assigns a phone number to send SMS messages from to the member. |
| Edit SMS Template (Button) | Enables the editing of the SMS message sent to the member. The SMS message is subject to a character limit of 160. The **{Security Code}** replacement tag is the location where the temporary generated code is substituted when the message is generated. |
| SMS Test Number | There is a test phone number available to send a test message, ensuring the correct functionality of outbound messages. |

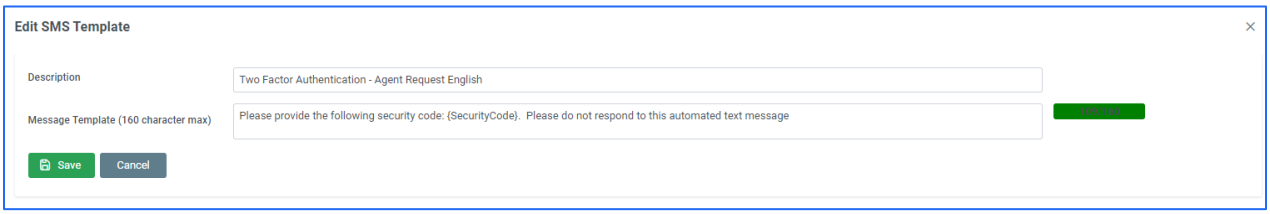
| Parameter | Description |
|---|---|
| Send Test SMS (Button) | The system will actively attempt to send an SMS from the SMS Phone Number to the SMS Test Number using the current SMS Template message details when utilizing the SMS Test Number field. |

**Edit SMS Template (Button)**

1. Click on Edit SMS Template to edit the SMS template.




2. Click Save to save the custom SMS message.



## 8.4. Email Settings

The Email settings enables the Two-factor Authentication security codes to be sent over email to the members to their registered email-ids.


Table: Email- settings parameters

| Parameter | Description |
|---|---|
| Edit Email Template (Button) | Enables editing of the email message sent to the member. The email message has a limit of 160 characters. The {**Two Factor Security Code**}replacement tag is the location where the temporary generated code is substituted when the message is generated. |
| Email Test Address | Utilize a test email address to send a test message and ensure the outbound email messages are functioning correctly. |
| Send Test Email (Button) | Using the Email Test Address field, the system will actively attempt to send an email from the configured sender address to the specified Email Test Address, employing the current Email Template message details. |

# 9. Voice Biometrics

5.1.1 Prerequisites

5.1.2 Supported Vendors

5.1.3 Configuration Steps

# 10. Cores

# 10.1.Symitar

## 10.1.1. Force PIN Change/Activation

- **All PIN-Related Scenarios Supported:** Symitar supports various scenarios related to force pin changes.
- **Core Method and Symitar Design:** When selecting the core method, Smart Apps follows the Symitar design. In this approach, a member's PIN is initially set to 0.
- **Triggering Force Pin Change or Activation:** When using the core method, the system checks for a PIN value of 0. If it finds a PIN set to 0, it triggers a force pin change or activation.

Considerations for Using Core Method:

a) The credit union must set the PIN to 0 to trigger this method.
b) The core method is effective only in environments where hashed PINs (encrypted PINs) are not activated.
c) In environments with hashed PINs, only force pin change scenarios related to PINs are supported.

Timing of Force PIN Change or Activation:

d) The "Use Core Method" scenario is examined after level 1 authentication questions are presented to determine when force pin change or activation is triggered.
e) For all other scenarios, the evaluation is performed after all questions are presented.

Alternative Methods for Force PIN Change or Activation: If you choose not to use the Core Method and select one of the other methods provided, you must include PIN as one of the questions within level 2 authentication.

**Note:**

- PINs within this core are shared across all individuals on the account and are stored at the member level.
- Smart Apps references the PIN using the field **AUDIOACCESS** in the preference record for the account.
- Although the PIN is shared across all individuals on the account, the questions asked during force pin change or activation are validated across all persons on the account, ensuring security and accuracy.

### 10.1.2. Dormancy

This section describes how the system determines dormancy in Symitar core. Dormancy is typically defined as a state of inactivity or non-usage. This process helps the system identify accounts that have been inactive for a certain period, which can be useful for managing and categorizing accounts based on their activity status.

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 263 | Dormant account threshold | This field will indicate the inactivity period allowed before an account is considered dormant. This field is expressed in days. |

**Evaluation Process:**

- To determine inactivity, the system uses two fields **ACTIVITYDATE** and **CORRESPONDDATE**, both located on the **Account** record within the core for evaluation.
- The system first evaluates the **ACTIVITYDATE** to determine if the number of days since the last activity surpasses the threshold configured within the **Dormant account threshold** setting.
- If the number of days since the last activity exceeds the threshold, the system then evaluates the **CORRESPONDDATE** to determine if the number of days since the last correspondence (communication) surpasses the same threshold.
- If both the **ACTIVITYDATE** and **CORRESPONDDATE** exceed the configured threshold, the account is considered dormant.

**Criteria for Dormancy:**

- If only the **ACTIVITYDATE** surpasses the threshold while the **CORRESPONDDATE** does not, the account is not considered dormant.
- In summary, for an account to be considered dormant, both the **ACTIVITYDATE** and **CORRESPONDDATE** must exceed the threshold set in the **Dormant account threshold** configuration.

### 10.1.3. Account Frozen

This section describes the process of account freezing in the Symitar system, particularly in the context of PIN-based authentication and its implications for Smart Apps.

**Account Freezing in Symitar:**
Symitar provides a flag to determine when a member account is frozen. When an account is frozen, it must be unfrozen by the credit union before the member can use Smart Apps.

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 729 | Symitar – Invalid attempts before freezing | Indicates the number of times a caller can enter valid account number with other invalid authentication information before the system freezes the account.<br>This parameter should be synced with the INV ATTEMPTS BEFORE FROZEN within the SymXchange client parameters. Symitar will only freeze accounts that use PINs in the authentication process. This parameter enables the SmartApps applications to freeze the account if authentication information other than PIN is entered incorrectly.<br>0 = Do not freeze<br>1 – 999 Number of attempts allowed |

**Variability of Invalid Attempts**:
The number of invalid PIN attempts within the Smart Apps system may vary. This is because the count of invalid attempts includes those both outside and within Smart Apps for the member, as analyzed by the system.

**Notification of Frozen Account:**
The core system notifies the Smart Apps system of an account frozen condition after the level 1 authentication if the account is frozen upon entry. However, it could also occur within other parts of the authentication process.

**Controlled Indicator:**

The account frozen indicator is controlled by the field FROZENMODE within the Account record. This field determines whether the account is frozen or not.

An account may become frozen in one of two possible ways:

- When the Lock Count in the Preference record reaches the "Inv Attempts Before Frozen" parameter (for invalid security answers).
- When the Invalid Attempt Count reaches the "Inv Attempts Before Frozen" parameter, and the "Pw Reset Probation" in the Preference record is set to "Yes" (for invalid logins with the temporary password).

**Increment of Invalid Attempts:**

Symitar increments the invalid attempts count only when a PIN is being evaluated during authentication. However, Smart Apps has been designed to manually update the attempts count on other non-PIN questions if the member incorrectly answers the security questions.

**Site Parameter for Manual Freezing:**

A site parameter is used to control when Smart Apps manually freezes the account. Once an account is manually frozen, the credit union must unfreeze it. If this parameter is set to 0, callers will not be limited in the number of times they can incorrectly answer a security question across multiple sessions. They will be limited based on the number of times allowed for authentication, but if they disconnect and call back, they will be allowed to answer the questions again.

### 10.1.4. Delinquency, Collections, and Bankruptcy

The Smart Apps system has been designed to support the identification of a member account that has a delinquency, is in collections, and is in a bankrupt status. The following general terms are applied to these conditions:

#### 10.1.4.1. Bankruptcy

- Bankruptcy is the most serious condition among three possible conditions i.e. Delinquency, Collections and Bankruptcy.
- It takes priority over accounts marked as delinquent or in collections. This means that if an account falls into bankruptcy, it is treated with higher urgency and importance.
- Bankruptcy typically indicates that a legal action has been initiated. This legal action usually pertains to a loan, mortgage, or credit card account within the credit union. It signifies that a formal legal process has been initiated against the debtor.
- Unlike other conditions like delinquency, bankruptcy cannot be determined solely based on the number of days past due. It hinges on the occurrence of a legal action, meaning that a legal procedure or event must have transpired for bankruptcy to be considered.
- **Detection Using Warning Codes:** Smart Apps employs warning codes to identify instances of bankruptcy.
- **Placement of Bankruptcy Warning Code:**
    - A bankruptcy warning code can be assigned at either the member account or loan level.
    - Typically, it is assigned at the member account level.
- **System Configuration:** After defining and configuring the bankruptcy warning code in Smart Apps, the system actively searches for this designated code.
- **Flagging Bankruptcy Accounts:** When the system detects the bankruptcy warning code on an account, it marks the account as being in bankruptcy.
- **Treatment Based on Configuration:**
    - Bankruptcy-flagged accounts are processed according to predefined configurations within the Account Exceptions section of Site Manager.
    - The treatment of these flagged accounts follows rules and settings established in this section.
- **Respect for Warning Code Expiration:** The system respects the expiration date set for warning codes, provided it is configured within the Symitar system.
- **Option for Suppressing Loans:** Credit unions have the flexibility to suppress loans associated with bankruptcy accounts.

- **Configuration Parameter for Suppressing Loans:** The suppression of loans related to bankruptcy accounts is managed using the specific configuration parameter shown in the table below within the Smart Apps system.

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 599 | Symitar Bankruptcy Statement Codes | This field will contain a delimited list of statement codes that will be used to suppress any share or loan with this code. |

### 10.1.4.2. Collection

This condition is considered serious, where the credit union has been forced to place a loan, mortgage, or credit card in collections. This usually indicates the member is seriously past due, and the credit union is attempting to collect amounts due. This condition takes precedence over an account that may also be flagged as delinquent. This condition can be determined by looking at days past due or using the warning code system, but it is typically done using the warning code system.

Smart Apps has two methods that can be used to detect collections. Below is a description of these two methods:

1. **Days Past Due:**

- The Days Past Due method is supported when the system is configured to assess the past due status of a loan, mortgage, or credit card account, based on the parameters set within the Site Manager Exceptions screen.
- In this method, the system examines the account to determine if it meets specific criteria, including having a current balance greater than 0, a payment amount due, and a due date in the past.
- The number of days between the current date and the due date is calculated and compared against the configured threshold for days past due, which is set up within Site Manager.
- If the number of past due days is equal to or greater than the configured threshold, the loan, mortgage, or credit card is considered to be in collections.

- The Days Past Due method can be configured individually and separately across three product classes within Smart Apps, which include loans, mortgages, and credit cards. Each of these classes has its own unique configuration parameters.
- It's worth noting that internal mortgages and credit cards, although initially recognized as loans within the Symitar core, are reclassified to more specific product classes within Smart Apps. For example, an internal mortgage may be stored in the core as a loan, but within Smart Apps, it's reclassified and treated as a mortgage. Therefore, collection settings should be configured with this reclassification in mind.

**Fields Used in LOAN Records for Determining Days Past Due:**

```
Current Balance = BALANCE
Payment Due Amount = PAYMENTDUE
Payment Due Date = DUEDATE
```

2. **Warning Codes:**

- A collection warning code can be assigned at either the member account or loan level when configuring collections within the Symitar system.
- Once defined and configured within Smart Apps, the system actively searches for the designated collection warning code.
- If the code is found, the associated account is flagged for collections and is processed as configured within the Account Exceptions section of Site Manager.
- The system respects the warning code's expiration date if configured within Symitar.

### 10.1.4.3. Delinquency

This is the least serious of the three possible conditions and generally indicates the payment for the loan, mortgage, or credit card is past due but is not considered a serious condition. This condition can be determined by looking at days past due or using the warning code system, but it is typically done using the days past due method.

Smart Apps has two methods that can be used to detect delinquency. Below is a description of these two methods:

1. **Days Past Due:**

- The Days Past Due method is supported when the system is configured to assess the past due status of a loan, mortgage, or credit card account based on the parameters set within the Site Manager Exceptions screen.
- In this method, the system examines the account to determine if it meets specific criteria, including having a current balance greater than 0, a payment amount due, and a due date in the past.
- The number of days between the current date and the due date is calculated and compared against the configured threshold for days past due, which is set up within Site Manager.
- If the number of past due days is equal to or greater than the configured threshold, the loan, mortgage, or credit card is considered to be in delinquency.
- The Days Past Due method can be configured individually and separately across three product classes within Smart Apps, including loans, mortgages, and credit cards. Each of these classes has its own unique configuration parameters.
- It's worth noting that internal mortgages and credit cards, although initially recognized as loans within the Symitar core, are reclassified to more specific product classes within Smart Apps. For example, an internal mortgage may be stored in the core as a loan, but within Smart Apps, it's reclassified and treated as a mortgage. Therefore, collection settings should be configured with this reclassification in mind.

**Fields Used in LOAN Records for Determining Days Past Due:**

```
Current Balance = BALANCE
Payment Due Amount = PAYMENTDUE
Payment Due Date = DUEDATE
```

**2. Warning Codes:**

- A delinquency warning code can be assigned at either the member account or loan level when configuring delinquency within the Symitar system.
- Once defined and configured within Smart Apps, the system actively searches for the designated delinquency warning code.
- If the code is found, the associated account is flagged for delinquency and is processed as configured within the Account Exceptions section of Site Manager.
- The system respects the warning code's expiration date if configured within Symitar.

### 10.1.5. Employee Accounts

Smart Apps recognizes members who are employees of the credit union. The method for determining employee accounts employs two evaluation methods.

1. The system compares the account type configured on the member account record within the core to a list of employee account types in Smart Apps. When configuring the employee account types in Smart Apps, you use the following site parameter, which allows you to add all employee account types that may exist.

2. The employee account types configured within this site parameter are compared against the **TYPE** field within the **ACCOUNT** record in Symitar. When a match is found, the system flags the member as an employee, and Smart Apps initiates all relevant employee-related processing.

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 794 | Symitar Employee Account Types | This field will contain a delimited list of Employee Account Types that can be used to determine the members that are employees.<br>Example: 49\|33\|67 |

**Note:** If employee accounts are not configured or a match is not found, a secondary check is performed by examining the **RESTRICT** field on the **ACCOUNT** record to make this determination. If the **RESTRICT** field contains a value of 3, 4, 5, or 6, the member is flagged as an employee account.

### 10.1.6. Business Accounts

In the Symitar system, Smart Apps offers two methods to identify Business Account's. To determine the preferred method, please refer to the following site parameter:

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 910 | Symitar Business Account Determination | This field will indicate how the system determines a business account from a personal account within a Symitar system.<br>Valid options are:<br>N = Name Format<br>A = Account Type |

**1. Name Format (N):** With the name format method, Smart Apps examines the value of the **NAMEFORMAT** field in the **NAME** record. If the value is **1**, the account is categorized as a Business Account. Conversely, if the value is **0**, the account is designated as a Personal Account.
**Note:** When a member has multiple name records, the primary member's name record is used for determination.

**2. Account Type (A):** When opting for the account type method, Smart Apps reviews the **TYPE** field within the **ACCOUNT** record to verify if it matches any of the configured account types in the site parameter. If a match is identified, the account is treated as a Business Account. In the absence of a match, the account is classified as a Personal Account.

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 910 | Symitar Business Account Determination | This field will indicate how the system determines a business account from a personal account within a Symitar system.<br>Valid options are:<br>N = Name Format<br>A = Account Type |

### 10.1.7. Core Account Type Specifications

Core account types are codes that define specific products and encompass various configurations associated with those products. Each product retrieved from the core system has an assigned core account type, and most product classes can be derived from these core account types.

The account product class are derived as follows:

| Product | Received from Core as: | Reclassified as and other notes |
|---|---|---|
| Checking | Checking | N/A |
| Savings | Savings | N/A |
| IRAs | Savings | Must be reclassified as an IRA |
| Certificate | Certificate | N/A |
| Loan – Open end | Loan | Loan – Open end; Must be assigned a subclass of open-end |
| Loan – Closed end | Loan | Loan – Closed end; Must be assigned a subclass of closed-end |
| Loans – Open End External | Loan | Loan – Open end; Must be assigned a subclass of open-end and the External indicator should be turned on |
| Loans – Closed End External | Loan | Loan – Closed end; Must be assigned a subclass of closed-end and the External indicator should be turned on |
| Mortgage – Internal | Loan | Must be reclassified as a Mortgage |
| Mortgage – External | Mortgage | N/A; External mortgages do not have a core account type from the core and a core account type must be created on Smart Apps. |
| Credit Card- Internal | Loan | Credit Card |
| Credit Card - External | Credit Card | N/A; External credit cards do not have a core account type from the core and a core account type must be created on Smart Apps. See determining core account types for external cards below |

**Determining core account types for external cards:**

When determining core account types for external cards, there are two approaches to consider.

1. The first method involves creating a core account type within Smart Apps and linking it to the external record definition (see External Accounts). However, this approach doesn't accommodate situations where multiple card types originate from the same

external source. For example, if a credit union deals with both Visa and Visa Gold cards from the same external source, separate core account types for Visa and Visa Gold are required using this method.

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 405 | External Credit Card Type Determination | This field will specify the method that will be used to determine the type of credit card for external cards. Valid Values are:<br>**1=Record Type/Card Code**<br>**2=Card Pattern (BIN)** |

2. Alternatively, core account types can be dynamically determined based on the card's BIN (Bank Identification Number). By specifying the BIN for each card, a core account type can be automatically assigned using the BIN number. This dynamic determination of core account types is configured using the following site parameter:

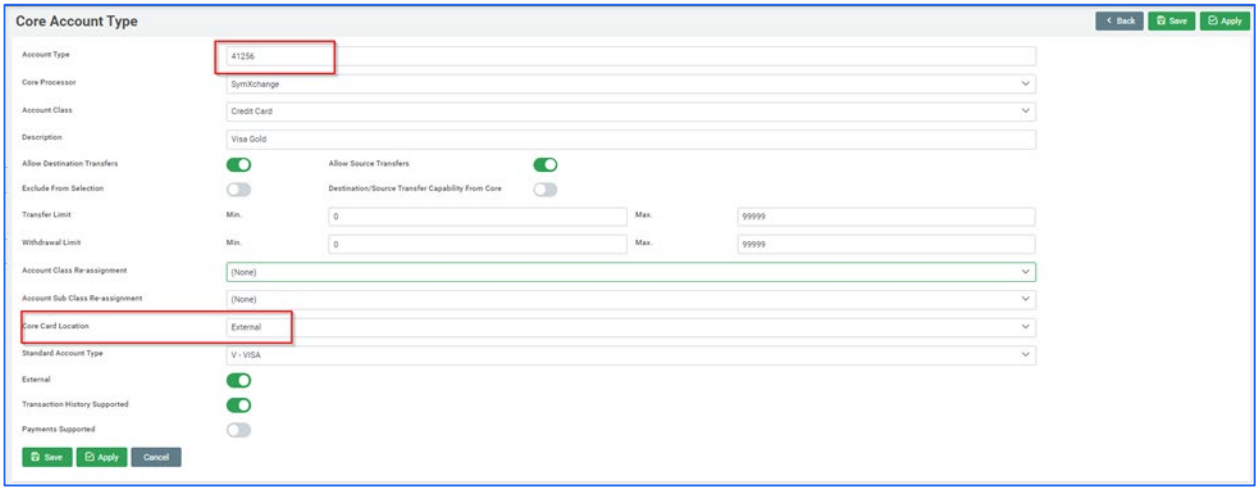
**Option 1:** With this parameter, the system utilizes the core account type assigned on the External Tracking Record or External Loan configuration screen within Site Manager.

**Option 2**: Choosing this option indicates that the system should dynamically determine the core account type based on the card number retrieved. This is the preferred choice when dealing with multiple types of cards from the same external source.

To configure dynamic core account type selection, follow these steps:

1. Determine the credit card **BIN**s that need to be handled.
2. Create a core account type for each BIN within the core account type screen, with the Core Card Location set to External.
3. Establish a standard core account type record for each **BIN**.
4. Associate each core account type record with the corresponding standard account type record.
5. Continue this process for every credit card BIN that requires processing.

The sample screen below illustrates the setup for a Visa Gold card with a credit card **BIN** of 41256 and a core card location set to External:




This setup ensures that Smart Apps can accurately determine and assign core account types to external cards based on their **BIN**s, offering a flexible solution for handling multiple card types from the same source.

### 10.1.8. Notes on Products

#### 10.1.8.1. Loans

Loans can be identified and represented different ways within the core and the Smart Apps system. Loan is generally classified and identified as:

1. Open-end loan
2. Closed-end loan

These categories are used by Smart Apps to identify the loan. However, Symitar has additional information that will allow the system to identify loans more accurately for their actual use. This information is the **loan type** field within the core. This allows the system to not only identify Open-end loans, but it can also identify subcategories of Open-end loans such as line of credit and Credit Cards. The following parameter can be used to specify if Smart Apps should use the generic form of identification or use the loan type from the core:

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 326 | Speak Loan Type instead of sub classification if available | This parameter will indicate whether the loan code description should be spoken when identifying accounts to IVR callers. |

To enable Smart Apps to determine if an open-end loan is draft-capable, a configuration parameter is utilized to identify the core account codes that should be considered as draft-capable. Without this parameter, all open-end loans will be automatically regarded as non-draft capable.

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 539 | Symitar Loan Draft Types | This field will identify all loan types that have draft capability.<br>The format is: xx\|xx\|xx\|xx |

#### 10.1.8.2. Mortgages

Symitar can collect additional information when a member is making a mortgage payment. This allows the collection of information related to the person making the payment to determine if they are the borrower or co-borrower. The following parameter will indicate if this information should be collected when processing a mortgage payment:

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 208 | Collect payer type on mortgage payment | This option will indicate if the system should request that the person making the mortgage payment indicate if they are the borrower or co-borrower.<br>NOTE: This function is only available for the Symitar core processor |

### 10.1.8.3. Miscellaneous Settings

The following parameter allows the credit union to specify where the nickname for the share or loan is stored. This field is typically named **NICKNAME**, but another field name can be specified.

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 547 | Symitar Nickname Field | This field will identify the field name to be used where retrieving the nickname information from Symitar |

When retrieving payroll transactions, the system must attempt to request them based on how they were posted within the system. In many cases, the credit union cannot determine if the transaction is a payroll transaction, as it may be posted as an ACH transaction. If the credit union knows that payroll transactions can be identified, then they will be retrieved as payroll transactions. This parameter will control the method that Smart Apps uses when retrieving this information.

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 556 | Symitar Payroll Deposit Options | This field will indicate the method used in retrieving payroll deposits. Valid options are:<br>P = Use Transaction source of P<br>A = Use transaction source of E (ACH)<br>B = Use both transaction source P and E |

Symitar provides special functionality to enable a member to retrieve a balance from a share or loan on a specific date. This functionality is governed by a core-provided function known as Repgen or PowerOn. The following site parameter allows the credit union to specify the name of the Repgen that offers this functionality. It's typically named IVB.INQUIRY, but it can be any name provided by the credit union.

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 597 | Symitar - Repgen to be used in Balance on a specific Day | This field will indicate the name of the RepGen that will be used in the routines that calculate balance on a specific date. |

### 10.1.8.4. Check Stop Payments

There are two configuration parameters that can be used to control the information posted to the core when processing a check stop payment request. The following parameters control the information posted regarding stop payment fees.

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 804 | Symitar Stop Payment Fee Verbiage | This field will contain the verbiage that will be posted to the core when a stop payment fee is charged against the share. This setting will work in conjunction with parameter 805 – Symitar Stop Payment Fee Include Check Number(s) to determine if the check or checks will be appended to the end of the verbiage. |
| 805 | Symitar Stop Payment Fee Include Check Number (s) | This field will indicate if the check or check range will be appended to the end of the |

| | | |
|---|---|---|
| | | Symitar Stop Payment Fee verbiage listed in parameter 804. |
| 548 | Symitar Post Stop Check Fee to core | This field will indicate if the IVR should post the stop check fee to the core processor. T/F |

### 10.1.8.5. Withdrawals/ Loan Advances

When processing withdrawals and loan advances via checks, the following parameters are provided to allow a credit union to control how the withdrawal is processed and what information is posted to the core for the transaction:

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 557 | Symitar Check Processor Code for withdrawals | This field will indicate how the checks are processed when performing withdrawals and loan advances. Valid values are :<br>• S = server or Symitar (Default)<br>• C = client system<br>T = third party |
| 596 | Symitar – Check Request Reference Data | This field will specify the verbiage that will be inserted in the check reference field when a check withdrawal is processed. 40 Character maximum. |

### 10.1.9. System Access

Symitar allows the credit union to suppress online access to information through an indicator within the system. Smart Apps follows this indicator and restricts information access when it has been suppressed. When the credit union disables online access, they make modifications to the following information within the core:

- HBMODE within the PREFERENCE record:

A 0 in this field indicates that no access should be allowed.
A 1 in this field indicates that access should be allowed. It's important to note that this field is shared between the home banking and audio systems, and Symitar does not currently provide a method to grant access to one system while restricting it for another.

**Member Experience:**
The following table describes the member experience when access is not allowed:

| Product | Experience |
|---|---|
| Smart Screen Pop | The member experience is not impacted |
| Smart Info | The member will be provided the opportunity to authenticate but will not receive any information prior to be transferred to the call center. |
| Smart Teller | The member will be presented with a message indicating the access is not allowed and will be transferred to the call center. The following message will be presented:<br>*Your account is not setup for IVR access. Please remain on the line for the next available...{Agent, Member Services Rep, etc}* |

### 10.1.10. Joint Account Determination

Joint account holders are supported and can be determined within Smart Apps. Symitar permits a joint member to be assigned at one of the following levels or a combination of these levels:

- Member/Account Level
- Share Level
- Loan Level

Joint members assigned at the member/account level are assumed to have access to all shares and loans under the membership. Those assigned at the share or loan levels are specific to the share or loan they are assigned to within the system. Joint accounts are identified by examining the associated **NAME** record. The **NAME** record is typically linked to a person for assignment purposes. Unless configured otherwise, Smart Apps considers all **NAME** record associations when identifying joint accounts.

To restrict or configure specific **NAME** records for joint processing, two site parameters enable a site to specify the name types to be considered. Once configured, any **NAME** record with a type not on the configured list will be excluded. Smart Apps allows a site to configure the **NAME** types to be considered from both an agent's viewpoint and an authentication viewpoint, which may differ. The field used for this analysis within the **NAME** record is **TYPE.** The following parameters serve this purpose:

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 753 | Symitar – Joint Name Types for Smart Screen Pop Display<br><br>(Agent viewpoint) | This field will contain a list of name types that should be retrieved when building the joint accountholder lists to be displayed within Smart Screen Pop. This will be a delimited list using \| as the delimiter. If this field is blank, only primary, and joint (name types 0 and 1) will be retrieved. Example: 0\|3 |
| 797 | Symitar – Joint Name Types<br><br>(Authentication viewpoint) | This field will contain a list of name types that should be retrieved when building the joint accountholder lists. This will be a delimited list using \| as the delimiter. If this field is blank, only primary, and joint (name types 0 and 1) will be retrieved. Example: 0\|3 |

### 10.1.11. Joint Consideration During Authentication

When determining joint account holders for authentication, the site should only include name types that they wish to allow for authentication purposes. Assuming the authentication system is configured to authenticate joint accounts, the authentication questions in level 2 must be designed to elicit responses that enable the system to identify a joint account. Data elements that can be used to identify individuals include SSN, date of birth, driver's license, and so on.

It's important to note that the PIN within Symitar will not allow the system to identify the joint account since all individuals on the account share the same PIN. When questions are asked during authentication, the responses to these questions are compared against all individuals associated with the account. When a unique individual is identified through their responses, the authentication is completed, and the joint account holder is recognized.

#### 10.1.11.1. Joint Account Review for Agents

When identifying joint account holders for agent review, the site should include only the name types they want to make available for agents' viewing purposes. This setting can vary from the criteria used for authentication, as there may be joint accounts that agents need to access but do not necessarily need to authenticate. The joint members will be displayed on the agent screens.

#### 10.1.11.2. Authentication Limited to Primary Members

A site can choose to limit authentication to the primary member exclusively. In such instances, the system will solely consider the **NAME** record with **TYPE** equal to 0 for authentication. It's essential to understand that even if a joint member correctly answers all authentication questions for their demographic information, they will not be able to authenticate in this restricted environment.

#### 10.1.11.3. Determining Access for Joint Members

When it comes to determining access to shares and loans in Smart Apps, there are two distinct approaches a site can choose:

- **Unrestricted Access for All Joint Members:**

Under this configuration, all joint members will have access to all shares and loans, regardless of their specific associations with a particular share or loan.

**Restricted Access Based on NAME Record Associations:**

In this setup, access is strictly determined by the NAME record associations configured within the core. Members will only have access to the shares and loans they are explicitly associated with in the core.

Please note that the primary member will always have access to all shares and loans on the account. Additionally, joint members associated at the member/account level will also have access to all shares and loans.

To implement one of these methods, the following site parameter should be configured:

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 995 | Symitar/Keystone Joint Member Accounts Restricted | This field will indicate the method used by the system to handle share/loan access based on the primary versus joint indication.<br>Value T/F (Default = F)<br>True = Joint members will only have access to Shares/Loans where they are listed on the name record<br>False = Joint members have access to ALL Shares/Loans, External Loans, Mortgages, and Credit Cards on the account. |

### 10.1.12. Preferences

**Interaction Mode:**

Interaction Mode specifically impacts the Smart Teller product and signifies the preferred mode of operation while using Smart Teller. It supports two modes:

- **Menu Mode:** Provides navigation menus.
- **Expert Mode:** Allows a member to navigate using a predefined coding system tied to features within Smart Teller.

The preference for this mode is stored in Symitar at the following location: **`INTERACTIONMODE`** within the **`PREFERENCE`** record

- If this field contains a 0, the member's preference is Expert Mode.
- If this field contains a 1, the member's preference is Menu Mode.

It's important to note that this setting is not automatic within Smart Teller, and both navigational menus and expert mode associations must be configured for the modes to be accessible.

The following site parameters are used to determine if these options are available:

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 319 | Allow IVR Interaction Mode | This field will indicate if the IVR Interaction Mode feature will be available to callers. IVR Interaction Mode allows callers to select Menu Mode or Expert Mode navigation settings. Menu Mode will present instructional navigation menus to callers. Expert Mode will allow callers to enter or select pre-defined service codes for specific IVR features and functions. T/F |
| 320 | Enable New User Interaction Mode Setup | This parameter will indicate if a first time IVR user should be prompted to setup their Interaction Mode. T/F |

When site parameter 319 is set to true, the system reads the core to determine the member's established setting. The system will function in the mode selected until the member changes

modes. If it is determined that the member is using the system for the first time, and site parameter 320 is true, then the system will prompt the member to select their preferred mode of operation. Their selection is stored in the core. It's important to note that the interaction mode is only checked after a successful authentication. There is a feature that can be added to any Smart Teller navigational menu or included in the Expert mode selections that allows a member to change this preference within a session.

### 10.1.13. External Accounts

Smart Apps support the external processing of loans, mortgages, and credit cards. These methods come from Symitar and include two components: Tracking Records and External Loan Records.

1. **External Loan Records:** Symitar offers predefined records for the storage and processing of external accounts, such as loans, mortgages, and credit cards. These external accounts get stored within the **external loan** records. The setup for **external loan** records requires defining them with an external loan record number in the Smart Apps system. Within Smart Apps, these records use several fields:

| External Loan Record | SmartApps Mapping Options |
|---|---|
| `BALANCE` | `current balance` |
| `PAYMENTDUE` | `payment amount due` |
| `DUEDATE` | `payment due date` |
| `LATEFEE` | `late fee` |
| `LASTUPDATEDATE` | `as-of date` |

2. **Tracking Records:** Tracking records are versatile, freeform records that allow credit unions to define and use more than 120 fields as needed. These records also have a **tracking record ID** that identifies different tracking records in the system. To use tracking records in Smart Apps, you'll need to configure a tracking record in the system, specifying the **external tracking record ID**, and map the fields within the tracking record to the fields required in Smart Apps. This mapping can be based on product type, enhancing customization and adaptability.

   Both of these methods provide valuable tools for efficiently managing and processing external accounts through the Smart Apps platform.

**For Mortgages:**

| External Loan Record | SmartApps Mapping Options |
|---|---|
| BALANCE | Any tracking amount field |
| Late Fee | Any tracking amount field |
| Interest Rate | Any tracking rate field |
| Payment Due Date | Any tracking amount field |
| Escrow Balance | Any tracking amount field |
| Payment Due | Any tracking amount field |
| Account Number | Any tracking character field |
| As of Date | Any tracking date field |

**For Credit Cards:**

| External Loan Record | SmartApps Mapping Options |
|---|---|
| BALANCE | Any tracking amount field |
| Payment Due Date | Any tracking date field |
| Available Credit | Any tracking amount field |
| Credit Limit | Any tracking amount field |
| Payment Due | Any tracking amount field |
| Account Number | Any tracking character field |
| As of Date | Any tracking date field |
| Last Payment Date | Any tracking date field |
| Last Payment Amount | Any tracking amount field |

**For Loans:**

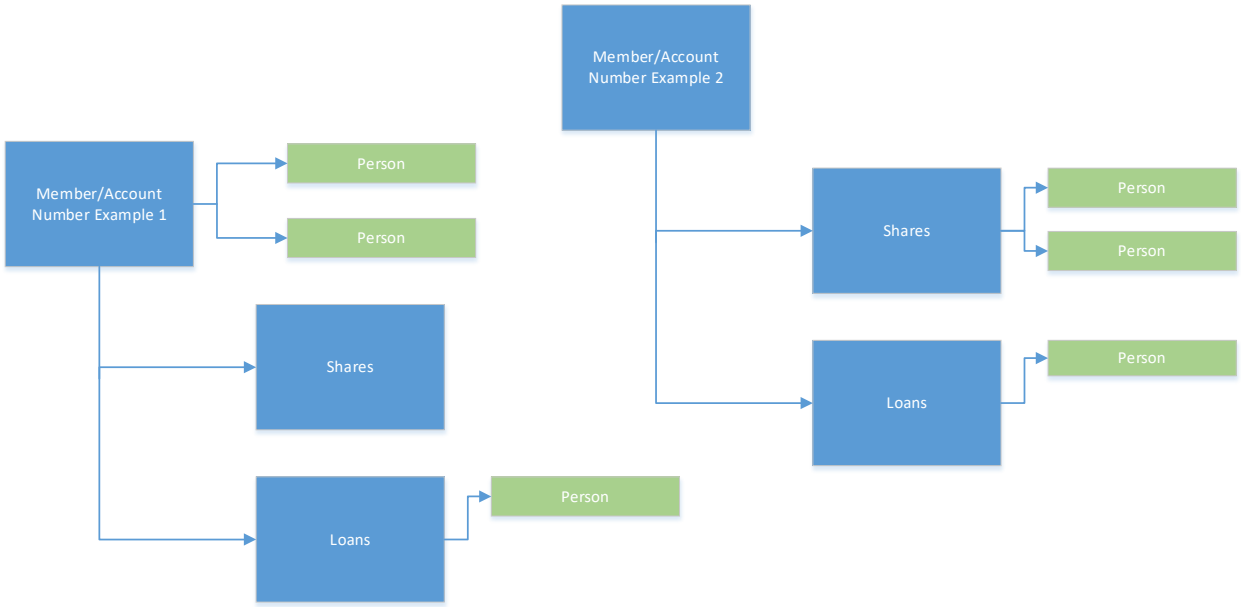
| External Loan Record | SmartApps Mapping Options |
|---|---|
| BALANCE | Any tracking amount field |
| Late Fee | Any tracking amount field |
| Interest Rate | Any tracking rate field |
| Payment Due Date | Any tracking date field |
| Payment Due | Any tracking amount field |
| Account Number | Any tracking character field |
| As of Date | Any tracking date field |

**Core Account Type Assignment:**

Smart Apps assigns a core account type to each loan, mortgage, and credit card because the core doesn't provide core account types for external accounts. The method of assigning core account types varies based on the product type. When dealing with mortgages and loans, core account types are assigned on the configuration screen used for setting up tracking records or external loan records. As for credit cards, core account types can be determined from the card number on the tracking record or external loan record, and they can also be assigned from the configuration screen. For more details on how core account types are assigned, please refer to the *Core Account Type specifications*.

### 10.1.14. Account Centric vs. Person/Member Centric

Symitar operates as an account-centric core processing system. The system features an account record that includes a member/account number with associated shares and loans. Individuals can be added at the account level, share level, or loan level, or at any combination of these levels. There is no linkage between different member accounts.
For instance, a member with both a personal account and a business account must authenticate separately to access their respective information. When logging into their personal account, they can only access shares and loans associated with that account and won't have visibility into shares and loans within their business accounts. The same principle applies when logging into the business account.




- Symitar and Smart Apps allow member/account identification using social security numbers.
- Members can use their social security numbers to link themselves to specific accounts.
- While Symitar doesn't inherently interconnect member accounts, Smart Apps offer the functionality for members to associate their social security number with an account.
- If a site enables the use of social security numbers for level 1 authentication questions:

Members can access their accounts using their social security numbers.
However, this approach may reveal multiple member accounts associated with the same social security number. In such cases, the system presents a list of accounts for the member to choose from during their session.

- This method doesn't replace a member-centric model with a single central account.
- Instead, it provides flexibility to members, allowing them to select the account they want to use for a particular session, even if multiple accounts are tied to their social security number.

### 10.1.15. Loan/Mortgage Payoff Availability

Symitar enables the retrieval of loan or mortgage payoffs. This feature is exclusively available for internally processed loans and mortgages. However, the system's native functionality restricts payoffs to the current day only, and it does not currently support future payoffs.

### 10.1.16. Card Management Capabilities

Smart Apps can support card management functions using the Symitar core system. You can perform card management activities on credit cards, debit cards, and ATM cards, including:

- Card Inquiry
- Card blocking (Lost/Stolen)
- Card Activation
- Authentication by Card Number
-

These functions rely on the existence of card information stored and maintained within CARD records in the core system. You can perform card management on both internal and external cards, provided the credit union maintains the card records for each card.

#### 10.1.16.1. Identifying Card Types

When creating card records, the record includes a card type. Smart Apps requires the following configuration information to identify the specific card type being managed:

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 522 | Symitar Debit Card Types | This field contains a delimited list of account types associated with debit cards.<br>The format is: xx\|xx\|xx\|xx |
| 540 | Symitar ATM Card Types | This field contains a delimited list of card types associated with ATM cards.<br>The format is: xx\|xx\|xx\|xx |
| 629 | Symitar Credit Card Types | This field contains a delimited list of account types associated with credit cards.<br>The format is: xx\|xx\|xx\|xx |

#### 10.1.16.2. Blocking Cards

Smart Apps has three configuration parameters that enable a site to determine how the system records a blocked card within the core.

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 713 | Symitar – Card Block code | Block code to be used in card block features. If this field is blank, the block code will not be updated. |
| 714 | Symitar – Card Reissue code | Reissue code to be used in card block features. If this field is blank, the reissue code will not be updated. Valid values 0 – 4. |
| 715 | Symitar – Card Block Status Reason Code | Card block status reason to be used in card block features. If this field is blank, the status reason code will not be updated. Valid values 0 – 199. |

### 10.1.17. Fund Transfers/Payments/Withdrawal Capabilities

Symitar support a full set of capabilities for processing fund transfers and payments. The following features are supported within Symitar:

| Feature | Description/Note |
|---|---|
| Transfer funds within your own account | |
| Transfer funds to another member of the credit union | Controlled using the access preferences entries on the core |
| Transfer funds from another member of the credit union (This feature is a future enhancement and is not currently available) | Controlled using the access preferences entries on the core |
| Loan Payments | Supported for all internal loans and external loans if supported by the site. The ability to determine if a specific loan type can support payments is indicated within the Core Account Type screen. |
| Mortgage Payments | Supported for all internal mortgages and external mortgages if supported by the site. The ability to determine if a specific mortgage type can support payments is indicated within the Core Account Type screen. |
| Credit Card Payments | Supported for all internal credit cards and external credit cards if supported by the site. The ability to determine if a specific credit card type can support payments is indicated within the Core Account Type screen. |
| Scheduled Payments | Supported for all loan, mortgage, or credit card payments that an on-demand payment is supported |

#### 10.1.17.1. Access Preference Entries

Smart Apps fully adheres to the access preference entries within the core. However, the system does have the capability to restrict activity within Smart Apps even if it's configured within the core system. There are also methods to handle conflicting preferences that may arise within the core. The following provides a brief explanation of how access preferences are interpreted:
Record Name: **PREFERENCE ACCESS**

| Access Type | Description |
|---|---|
| **ACCESSTYPE 0** | Member can transfer funds to the member specified within this access preference record. This is considered an explicit definition. It may include specific shares or loans. If none are listed, it applies to any share or loan for the member. |
| **ACCESSTYPE 1** | Member can transfer funds from the member specified within this access preference record. This is considered an explicit definition. It may include specific shares or loans. If none are listed, it applies to any share or loan for the member. |
| **ACCESSTYPE 3** | Member can transfer funds to anyone in the credit union if they know the member number of the destination member and can answer the additional security questions if configured. |
| **ACCESSTYPE 2** (with **ENABLEDEPOSIT** and **ENABLEWITHDRAWAL** flags) | Member can transfer funds to the member specified within this access preference record. This is considered an explicit definition. |
| **ACCESSTYPE 2** (with **ENABLEWITHDRAWAL** flag) | Member can transfer funds from the member specified within this access preference record. This is considered an explicit definition. |

In certain cases, conflicts may arise in access preferences. For instance, a situation could occur where there's an access type 3 record, but one or more access type 0 records also exist. This raises questions: Which one takes precedence? Can the member transfer funds to any member in the credit union, or are they restricted to the members specified in the type 0 records? To address and resolve such conflicts, the following parameter can be employed:

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 380 | Cross Account conflict handling | This parameter will specify the method used to handle accounts that have transfer specific preference records for accounts and (or) shares but also have an indication that any account can be used for a destination transfer. Valid values are:<br>1 = Ignore ability to transfer to any account |

| | | |
|---|---|---|
| | | 2 = Ignore account specific transfer preferences<br>3 = Handle both situations with a menu selection |

As previously mentioned, Symitar offers various fund transfer and payment options. However, each site can manage these features using configuration parameters. These parameters have the ability to suppress features, even if the core system supports them. For instance, access preference records may be configured in the core to permit members to transfer money from one member to another. Nevertheless, the credit union might opt not to facilitate this kind of activity within Smart Apps. In such cases, suppression is possible. The following parameters are available for such configuration

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 128 | Allow Cross Account funds transfers | This option will indicate if cross account transfers will be allowed. T/F |
| 237 | Allow Scheduled Transfers | This option will indicate if the system allows the caller to process a scheduled transfer if the core supports this capability. T/F |
| 238 | Allow Scheduled Payments | This option will indicate if the system allows the caller to process a scheduled payment if the core supports this capability. T/F |
| 329 | Allow Member to Member Account transfers for Checking to Loan Transfers | This parameter will indicate if the system should offer a member-to-member account transfer on the Checking to Loan Transfer feature. T/F |
| 330 | Allow Member to Member Account transfers for Savings to Loan Transfers | This parameter will indicate if the system should offer a member-to-member account transfer on the Savings to Loan Transfer feature. T/F |
| 331 | Allow Member to Member Account transfers for Loan to Checking Transfers | This parameter will indicate if the system should offer a member-to-member account transfer on the Loan to Checking Transfer feature. T/F |
| 332 | Allow Member to Member Account transfers for Loan to Savings Transfers | This parameter will indicate if the system should offer a member-to-member account transfer on the Loan to Savings Transfer feature. T/F |

| | | |
|---|---|---|
| 333 | Allow Member to Member Account transfers for Checking to Savings Transfers | This parameter will indicate if the system should offer a member-to-member account transfer on the Checking to Savings Transfer feature. T/F |
| 334 | Allow Member to Member Account transfers for Savings to Checking Transfers | This parameter will indicate if the system should offer a member-to-member account transfer on the Savings to Checking Transfer feature. T/F |
| 335 | Allow Member to Member Account transfers for Loan to Deposit Transfers | This parameter will indicate if the system should offer a member-to-member account transfer on the Loan to Deposit Transfer feature. T/F |
| 336 | Allow Member to Member Account transfers for Deposit to Loan Transfers | This parameter will indicate if the system should offer a member-to-member account transfer on the Deposit to Loan Transfer feature. T/F |
| 337 | Allow Member to Member Account transfers for Deposit-to-Deposit Transfers | This parameter will indicate if the system should offer a member-to-member account transfer on the Deposit-to-Deposit Transfer feature. T/F |
| 463 | Allow Member to Member transfers for Savings to Savings Transfers | This parameter will indicate if the system should offer a member- to-member transfer on the Savings to Savings Transfer feature. T/F |
| 464 | Allow Member to Member transfers for Checking-to-Checking Transfers | This parameter will indicate if the system should offer a member-to-member transfer on the Checking- to- Checking Transfer feature. T/F |
| 475 | Suppress fund transfers from another account | This option will indicate that fund transfers from another member's account will be suppressed even if the transfer preferences support this function. |

### 10.1.17.2. Service Codes

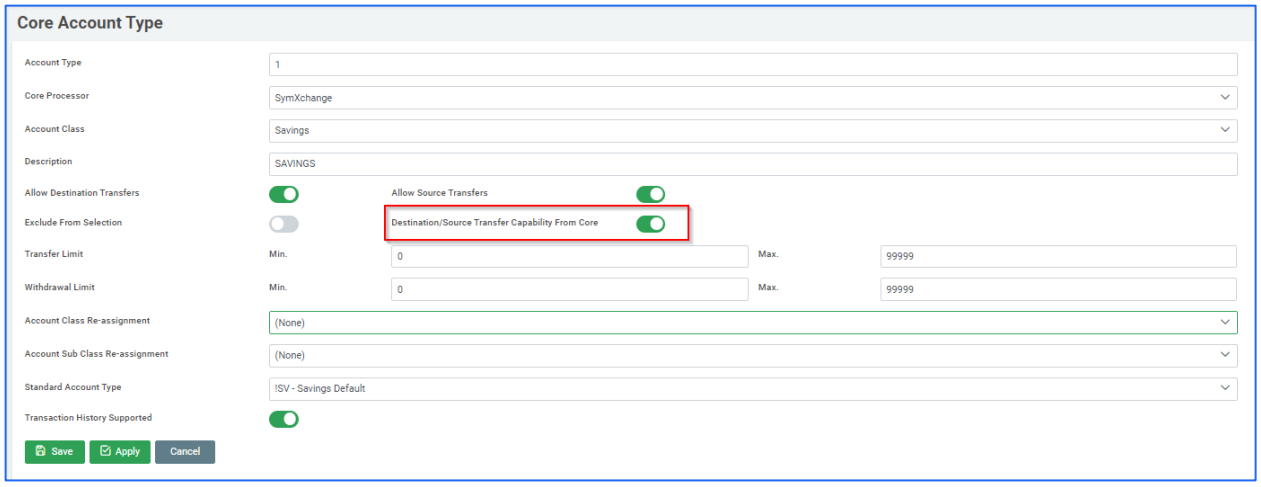
Determining whether a share or loan can be used as a source of funds or a destination for funds is achievable by configuring the core account type screen in Smart Apps. However, managing this access directly from the core account type screen results in a global setting where all members with that type of core account inherit the same settings. Symitar introduces the

concept of Service Codes, which can be used to define the source for a transfer, destination for a transfer, or source for a withdrawal.

- Using Service Codes, a credit union can establish a list of service codes along with their respective meanings.
- For example, a service code may be created to signify that a share or loan can be used as a source of funds, while another service code may indicate that the share or loan can be used for withdrawal purposes.
- These service codes are then applied to each share or loan for a member as required.
- Smart Apps reads these service codes and applies logic to ensure that the Smart Teller system adheres to the intended use of these service codes.

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 380 | Cross Account conflict handling | This parameter will specify the method used to handle accounts that have transfer specific preference records for accounts and (or) shares but also have an indication that any account can be used for a destination transfer. Valid values are:<br>1 = Ignore ability to transfer to any account<br>2 = Ignore account specific transfer preferences<br>3 = Handle both situations with a menu selection |

The use of service codes is trigger by a setting within the core account type screen as shown below:




When this setting is activated, the system will attempt to use service codes to determine the capabilities of this core account type for the member. If a service code is not found within the member's account, the system will default to the settings on this screen.

### 10.1.18. System Restriction Overrides

Symitar does not allow for the establishment of any system restriction overrides.

# 10.2. Correlation Keystone

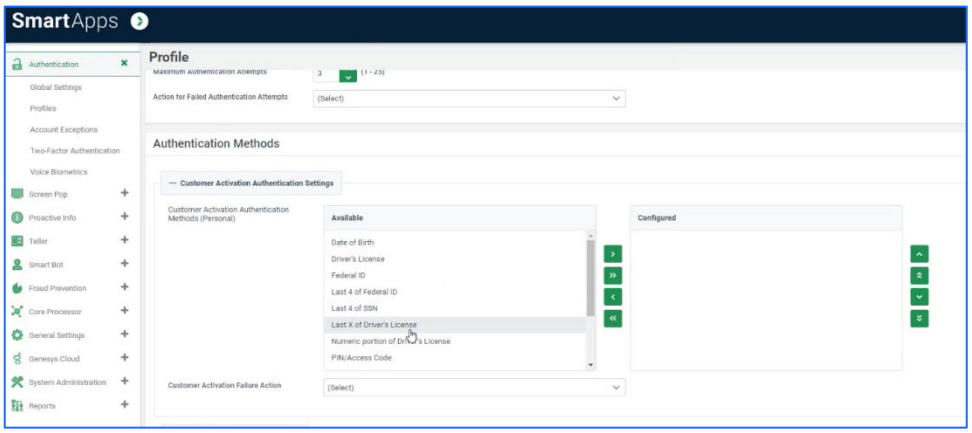
## 10.2.1. Force PIN Change/Activation

All PIN related force pin change scenarios are supported for this core. The following should be considered when using core method for this core:

- To use this method, the credit union must create a LOGIN and a LOGIN_PASSWORD record for the member and the LOGIN_PASSWORD record must have CHANGE_REQUIRED set to "Y".
- The Use Core Info method is configured in Profile in Authentication to trigger Force PIN Change or Activation. The Use Core Info method scenario is examined after Level 1 authentication and questions are presented while determining Force PIN Change or Activation. For all other scenarios, the evaluation is performed after all questions are presented.
- If not using the Use Core Info method for Force PIN Change or Activation and selecting one of the other methods provided, you must use PIN as one of the questions within level 2 authentication.

**Note:**

- PINs within this core are shared across all people on the account. PINs are stored at the member level.
- PINs within this core are stored at the LOGIN record level. A LOGIN can be Account or Person centric.
- Although the PIN is shared across all people on the account, the questions asked during force pin change or activation are validated across all persons on the account. Additional Layer of security to Customer Activation and Force PIN Change. This logic applies only to Account centric logins.



### 10.2.2. Dormancy

To determine dormancy within this core, the system relies on a site parameter setting to determine the inactivity period for the evaluation. Retrieve the dormant threshold value from Site Parameter 263.

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 263 | Dormant account threshold | This field will indicate the time period of inactivity allowed before an account is considered dormant. The field is expressed in days. |

**Fields for Evaluation:**

- The system evaluates two fields on the Account record: `LAST_ACTIVITY_DATE` and `CORRESPONDENCE_DATE`.

**Dormancy Evaluation Process:**

- The system checks if the number of days since the last activity (`LAST_ACTIVITY_DATE`) surpasses the threshold configured within the dormant account threshold configuration.
- If the above condition is met, the system then checks if the number of days since the last correspondence (`CORRESPONDENCE_DATE`) surpasses the threshold configured within the dormant account threshold configuration.
- If both `LAST_ACTIVITY_DATE` and `CORRESPONDENCE_DATE` exceed their respective thresholds, the account is considered dormant.

**Specific Scenarios:**

- If `LAST_ACTIVITY_DATE` surpasses its configured threshold, but `CORRESPONDENCE_DATE` does not, the account is not considered dormant.
- Both `LAST_ACTIVITY_DATE` and `CORRESPONDENCE_DATE` must exceed their respective thresholds for the account to be classified as dormant.

**Dormant Account Labeling:**

- If the Account `LAST_ACTIVITY_DATE` or `CORRESPONDENCE_DATE` surpasses its threshold (according to SP 263), the account is considered dormant.
- The core service should return an `AuthenticationModel` from `AuthValidateByMember` with `DormantAccount` set to True when an account is dormant.

**Non-Dormant Account Handling:**

- If neither of the above scenarios is encountered, the core service should return an `AuthenticationModel` from `AuthValidateByMember` with `DormantAccount` set to **False**.

In summary, the system uses a two-step evaluation process based on **`LAST_ACTIVITY_DATE`** and **`CORRESPONDENCE_DATE`** to determine if an account is dormant. Both dates must individually surpass their thresholds for an account to be considered dormant, and the core service responds accordingly by setting the **`DormantAccount`** flag in the **`AuthenticationModel`**.

### 10.2.3. Account Frozen

**`LOGIN_LOCK` Flag:** Keystone provides a **`LOGIN_LOCK`** flag on a login record to determine if a member account or login is frozen.

**Unlocking Process:** Once an account is frozen (**`LOGIN_LOCK`** set to **`true`**), the credit union must unfreeze the login before the member can use Smart Apps.

**Freezing Triggers:**

- Account freezing can occur manually by the credit union locking out the member's login account.
- Automatic freezing occurs when an invalid login is detected, based on a threshold set in Site Parameters 513 and 514. If the number of failed logins exceeds this threshold, a function is called against the core to set the **`LOGIN_LOCK`** flag to **`true.`**

**SmartApps Implementation:**

- SmartApps implements its own freezing policy at its site, based on the setting in Site Parameter 514.
- Credit unions can have their own Site Parameters (513 and 514) to validate the number of failed logins against the set value.

**Credit Union-Specific Policies:**

- Credit unions can have their own login lockout policies in effect, which work with Site Parameters 513 and 514.
- The policy is evaluated in the core and not in SmartApps.

**Site Parameters 513 and 514:** When set to true, these parameters validate the number of failed logins against the set value.

**Invalid Attempt Count and Pw Reset Probation:** If the Invalid Attempt Count reaches the set threshold (Site Parameter 514) and Pw Reset Probation in the Preference record is set to **`Yes`** (for invalid logins with temporary passwords), the account may be frozen.

**Lock Count in Preference Record:** If the Lock Count in the Preference record reaches the set threshold (Inv Attempts Before Frozen parameter) for invalid security answers, the account may be frozen.

**Incrementing Invalid Attempts:**

- Keystone increments the invalid attempts count only when a PIN is being evaluated during authentication.
- Smart Apps can manually update the attempts count on other non-PIN questions if the member incorrectly answers the security questions, controlled by a specific site parameter.

In summary, Keystone's **`LOGIN_LOCK flag`**, along with configurable Site Parameters and credit union-specific policies, govern the freezing of member accounts or logins based on invalid login attempts and other criteria. The freezing process is managed at the core level, and SmartApps implement their own policies based on site parameters.

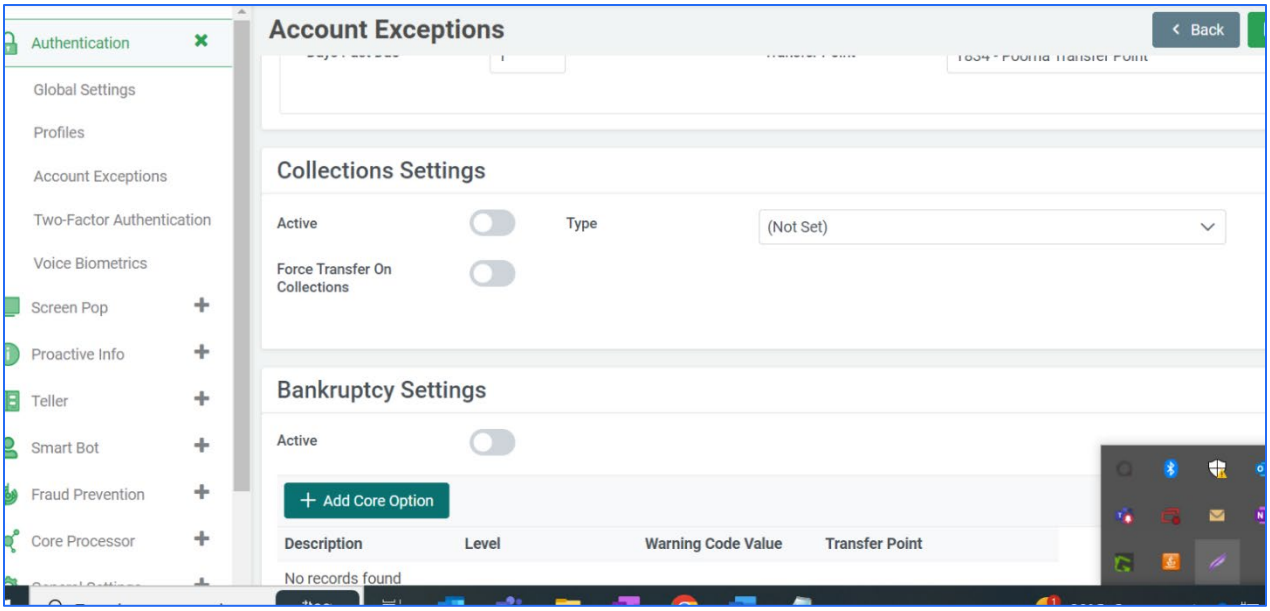
| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 513 | Keystone – Set Lock Flag to Disable Logins | Keystone has the capability to automatically disable further login attempts when a failed login attempts threshold is met. When this site parameter is set to true, SmartSuite applications will assume that the login disable failed threshold setting is turned off and will manually set the locked flag on a Login record when the failed attempts threshold et in Site Parameter 514 is reached. |
| 514 | Keystone – Invalid Attempts Before disabling Logins | Indicates the number of times the caller can enter a valid login id with other invalid authentication information before the system locks the login/disables the login. Keystone out of the box only has the capability of locking out members if PIN Authentication is used. This parameter is used for 2 purposes - locking out a login record when authentication information other than PIN is used as well as in conjunction with Site Parameters 513 to manually set the lock flag if the credit union prefers to use the lock flag.<br>0 = Do not lock/disable |

| | | |
|---|---|---|
| | | 1-999 = Number of attempts allowed. |

This parameter will determine when Smart Apps manually freezes the login. Once frozen, the credit union must unfreeze the login. Warning: if this parameter is set to 0, the caller will not be limited to the number of times they can incorrectly answer a security question across multiple sessions. They will be limited based on the number of times allowed for authentication but if they disconnect and call back, they will be allowed to answer the questions again.

### 10.2.4. Delinquency, Collections and Bankruptcy

The Smart Apps system has been designed to support the identification of a member account that has a delinquency, is in collections, and is in a bankrupt status. The following general terms are applied to these conditions:




**Bankruptcy** – This condition is considered the most series of the three types of conditions and takes precedence over an account that may also be flagged as delinquent or in collections. This indicates a legal action has been taken which applies to a loan, mortgage, or credit card within the credit union. It cannot be calculated with days past due because a legal action must have occurred for this to be in effect.

**Collection** – This condition is considered serious where the credit union has been forced to place a loan, mortgage, or credit card in collections. This usually indicates the member is seriously past due and the credit union is attempting to collect amounts due. This condition takes precedence over an account that may also be flagged as delinquent. This condition can be determined by looking at days past due or using the alerts/notes system, but it is typically done using the alerts/notes system.

**Delinquency** – This is the least serious of the three conditions and indicates the payment for the loan, mortgage, or credit card is past due but is not considered a serious condition. This

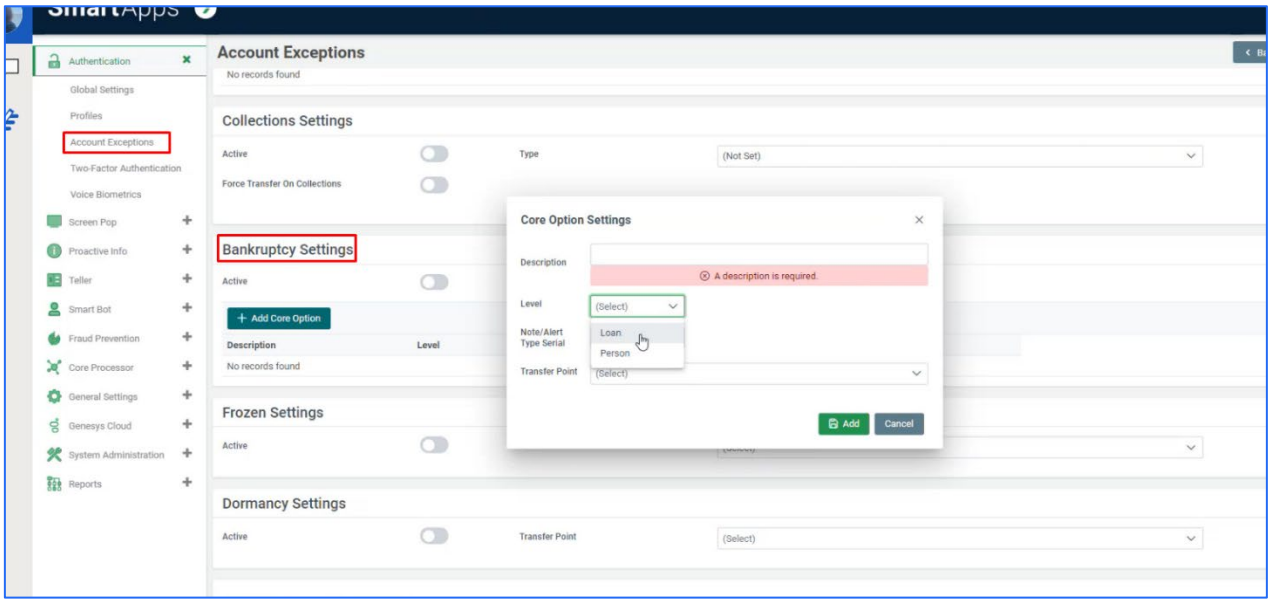
condition can be determined by looking at days past due or using the alerts/notes system, but it is typically done using the days past due method.

The following provides more detail descriptions of each condition and how it is handled:

### 10.2.4.1. Bankruptcy

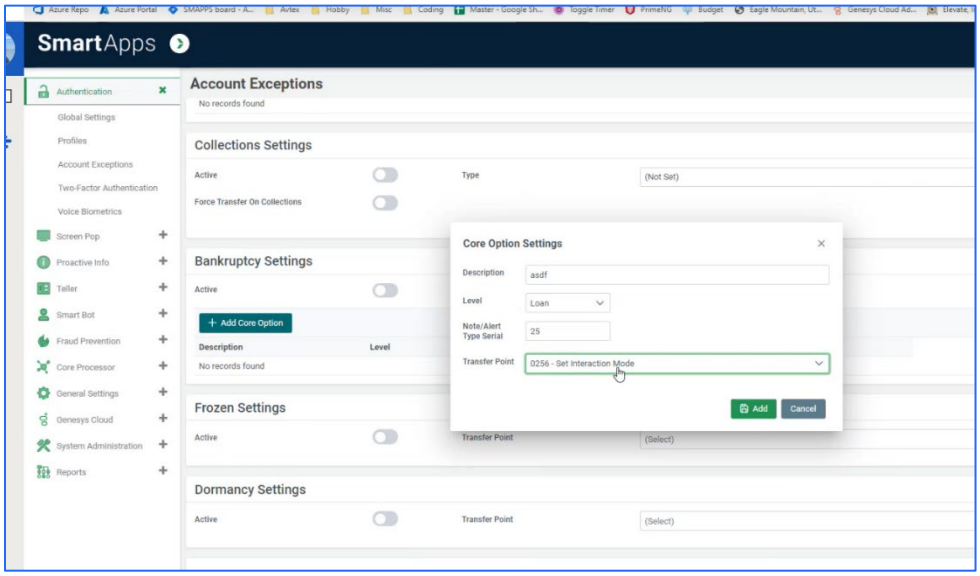
Smart Apps use alerts/ notes codes to detect bankruptcy. A bankruptcy alert/note code can be placed at the member account or loan level although it is typically placed at the member account level. Once defined and configured within Smart Apps, the system will look for the designated bankruptcy alert/note type serial and if found, the account will be flagged for bankruptcy and will be treated as configured within the Account Exceptions section of Site Manager. The system honors the alert/note code expiration date if configured within Keystone.

You can come in here and say if, if there's a note type of 25 on at the you know associated with a loan, then we. You know, then we're considering this bankruptcy, and we would want to transfer the caller to a particular transfer point.



### 10.2.4.2. Collections

Smart Apps have two methods that can be used to detect collections. Below is a description of these two methods:




1. **Days Past Due**

The Days Past Due method is supported where the system is configured to look at the loan, mortgage, or credit card account to determine if the account is past due based on the configured parameters within the Site Manager Exceptions screen. When this method is used, the system will check the loan, mortgage, or credit card to determine if it has a current balance greater than 0, has a payment amount due, and has a due date in the past. The number of days between the current date and the due date is calculated and compared against the configured threshold for days' pay due configured within Site Manager. If the past due days are equal to or greater than the configured threshold, the loan, mortgage, or credit card is considered in collections. The Days Past Due method can be configured individually and separately across three product classes within Smart Apps. Loans, mortgages, and credit cards can be configured individually with each having its own configuration parameters. It should be noted that internal mortgages and credit cards are recognized within the Keystone core as loans but are reclassified to more specific product classes within Smart Apps. For example, an internal mortgage will be stored in the core as a loan but upon retrieval into Smart Apps, it is reclassified and treated as a mortgage. The collection settings should be configured with this reclassification in mind.

The following Posting Status fields are used within the LOAN records when determining days past due:

```
Current Balance = balance
Payment Due Amount = PaymentsDue -> totalDuePayment
Payment Due Date = paymentDueDate
```

2. **Alerts**

Collection alerts can be placed at the member account or loan level when configuring collections within the Keystone system. The note type used for the Alert must be set with **ALERT_OPTION** set to **Y** in Keystone. Once defined and configured within Smart Apps, the system will look for the designated collection alert and if found, the account will be flagged for collections and will be treated as configured within the Account Exceptions section of Site Manager.

### 10.2.4.3. Delinquency

Smart Apps have two methods that can be used to detect delinquency. Below is a description of these two methods:

1. **Days Past Due :**

The Days Past Due method is supported where the system is configured to look at the loan, mortgage, or credit card account to determine if the account is past due based on the configured parameters within the Site Manager Exceptions screen. When this method is used, the system will check the loan, mortgage, or credit card to determine if it has a current balance greater than 0, has a payment amount due, and has a due date in the past. The number of days between the current date and the due date is calculated and compared against the configured threshold for days' pay due configured within Site Manager. If the past due days are equal to or greater than the configured threshold, the loan, mortgage, or credit card is considered delinquency. The Days Past Due method can be configured individually and separately across three product classes within Smart Apps. Loans, mortgages, and credit cards can be configured individually with each having its own configuration parameters. It should be noted that internal mortgages and credit cards are recognized within the Keystone core as loans but are reclassified to more specific product classes within Smart Apps. For example, an internal mortgage will be stored in the core as a loan but upon retrieval into Smart Apps, it is reclassified

and treated as a mortgage. The collection settings should be configured with this reclassification in mind.
The following fields are used within the LOAN records when determining days past due:

```
Current Balance = balance
Payment Due Amount = PaymentsDue -> totalDuePayment
Payment Due Date = paymentDueDate
```

2. **Alerts**

A collection alert can be placed at the member account or loan level when configuring delinquency within the Keystone system. Once defined and configured within Smart Apps, the system will look for the designated delinquency alerts and if found, the account will be flagged for delinquency and will be treated as configured within the Account Exceptions section of Site Manager.

**Employee Accounts**

Smart Apps have been designed to recognize members that are employees of the credit union. Employe accounts are identified by the **ACCOUNT -> ACCESS_RESTRICTION** field where the value is set to **'E'** (Employee).
If a match is found, the member is flagged as an employee and all appropriate employee related processing will occur within Smart Apps.

**Business Accounts**

Smart Apps has two methods that can be chosen to identify business accounts within a Keystone system.

if the primary person on the account has a Tax ID number type with the field **TIN_TYPE** of (E) for EIN.
The second type would be the other one we looked at, which is if the account. if the (Table name) Account Type, Category (column name) has a value of (C) Commercial. That's the 2nd way, then an account is determined to be a business.
If a match is found, the account is assumed to be a business account. If no match is found, the account is assumed to be a personal account.

### 10.2.5. Core Account Type Specifications

Core account types are codes that define a specific product and many configurations associated with the product. Each product retrieved from the core has an associated core account type and most product classes can be derived from the core. Within Keystone, the account product class are derived as follows:

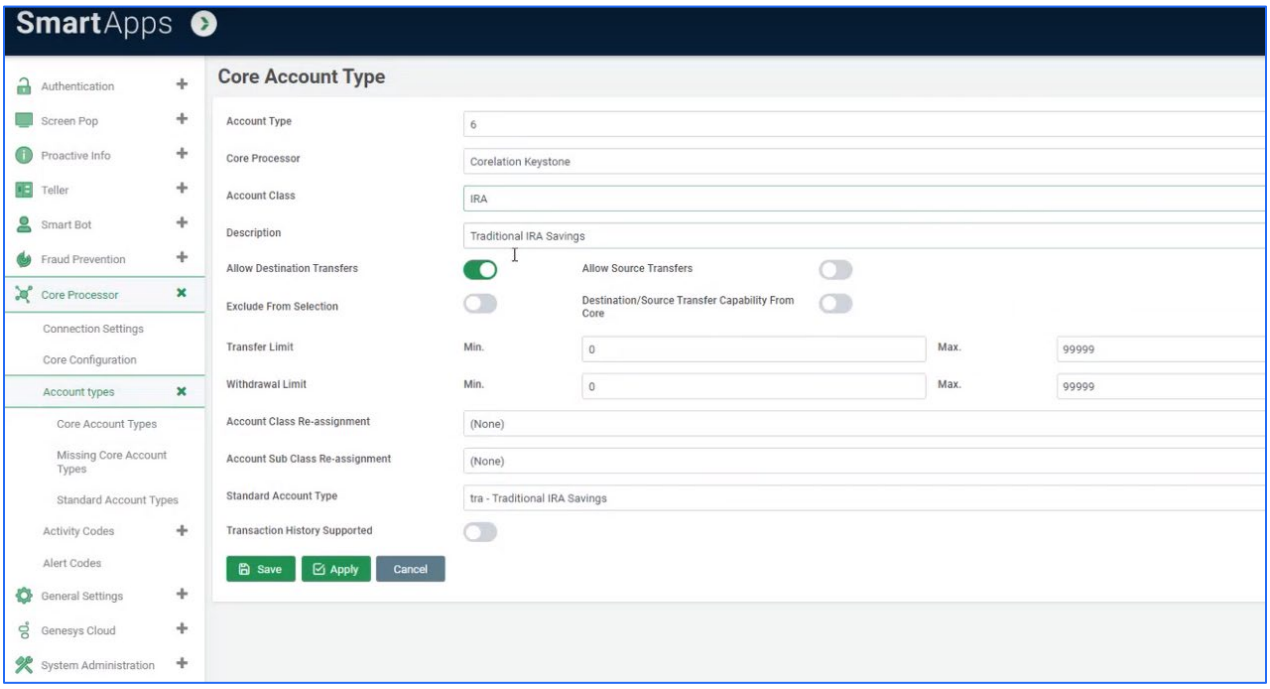


Table:

| Product | Received from Core as: | Reclassified as and other notes |
|---|---|---|
| Checking | Checking | N/A |
| Savings | Savings | N/A |
| IRAs | Savings | N/A |
| Certificate | Certificate | N/A |
| Loan – Open end | Loan | Loan – Open end; Must be assigned a subclass of open-end |
| Loan – Closed end | Loan | Loan – Closed end; Must be assigned a subclass of closed-end |
| Loans – Open End External | Loan | Loan – Open end; Must be assigned a subclass of open-end and the External indicator should be turned on |
| Loans – Closed End External | Loan | Loan – Closed end; Must be assigned a subclass of closed-end and the External indicator should be turned on |
| Mortgage – Internal | Loan | N/A |
| Mortgage – External | Mortgage | External indicator should be turned on |
| Credit Card- Internal | Loan | N/A |
| Credit Card - External | Credit Card | External indicator should be turned on |

## 10.2.6. Notes on products

### 10.2.6.1. Check Stop Payments

There are two configuration parameters that can be used to control the information that is posted to the core when a check stop payment request is processed. The following parameters control information that is posted on the stop payment fee information:

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 804 | Keystone Stop Payment Fee Verbiage | This field will contain the verbiage that will be posted to the core when a stop payment fee is charged against the share. This setting will work with parameter 805 – Keystone Stop Payment Fee Include Check Number(s) to determine if the check or checks will be appended to the end of the verbiage. |
| 805 | Keystone Stop Payment Fee Include Check Number (s) | This field will indicate if the check or check range will be appended to the end of the Keystone Stop Payment Fee verbiage listed in parameter 804. |
| 548 | Keystone Post Stop Check Fee to core | This field will indicate if the IVR should post the stop check fee to the core processor. T/F |

### 10.2.7. Joint Account Determination

**Support for Joint Account Holders:** Keystone supports joint account holders, and Smart Apps can determine and manage their access levels.

**Assignment Levels:** Joint members can be assigned at different levels:

- Member/Account Level
- Share Level
- Loan Level

**Access Implications:**

- Joint members assigned at the member/account level are assumed to have access to all shares and loans under the membership.
- Joint members assigned at the share or loan levels are specific to the share or loan they are assigned to within the system.

**Determining Joint Members:**

- Joint members are determined by examining the `SH_PERSON_LINK/LN_PERSON_LINK` records associated with the account.
- These records are tied to a person for assignment purposes.

**Default Behavior in Smart Apps:** Unless configured otherwise, Smart Apps will consider all `SH_PERSON_LINK/LN_PERSON_LINK` record associations when determining joint accounts.

**Configuration for Joint Processing:**

- To restrict or configure specific `SH_PERSON_LINK/LN_PERSON_LINK` records for joint processing, two site parameters are provided.
- These parameters allow a site to specify joint categories to be considered, and any categories not included will be excluded.

**Parameters for Configuration:**

- The field in the `SH_PERSON_LINK/LN_PERSON_LINK` record used for this analysis is `CATEGORY.`
- The site parameters for configuration are used for both agent viewpoint and authentication viewpoint, which may be different.
- Parameters for agent viewpoint: [Parameter Name for Agent Viewpoint]

- Parameters for authentication viewpoint: [Parameter Name for Authentication Viewpoint]

Keystone allows the assignment of joint members at different levels, and Smart Apps determine joint accounts based on the associations in **`SH_PERSON_LINK/LN_PERSON_LINK`** records. Configuration parameters enable the restriction and specification of joint categories for processing in both agent and authentication viewpoints. The **`CATEGORY`** field in these records is crucial for this analysis.

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 579 | Keystone – Joint Name Types for Smart Screen Pop Display<br><br>(Agent viewpoint) | This field will contain a list of name types that should be retrieved when building the joint accountholder lists to be displayed within Smart Screen Pop. This will be a delimited list using \| as the delimiter. If this field is blank, only primary, and joint (name types 0 and 1) will be retrieved.<br>Example: 0\|3 |
| 578 | Keystone – Joint Name Types<br><br>(Authentication viewpoint) | This field will contain a list of name types that should be retrieved when building the joint accountholder lists. This will be a delimited list using \| as the delimiter. If this field is blank, only primary, and joint (name types 0 and 1) will be retrieved.<br>Example: 0\|3 |

### 10.2.8. Joint consideration during authentication

When determining joints for authentication, the site should only add joint categories that they wish to allow for authentication purposes. Assuming the authentication system is set up to authenticate joint accounts, the authentication questions in level 2 must ask questions that enable the system to identify a joint account. Data elements that can be used to identify someone are SSN (Social Security Number), Date of birth, driver's license, etc. When questions are asked, the responses for these questions are compared against all people on the account

and when a unique person is found, the authentication is completed, and the joint person is identified.

#### 10.2.8.1. Joint consideration for agent review

When determining joints for agent review, the site should only add joint categories that they wish to allow for viewing purposes for agents. This setting can be different than the joints used for authentication as there may be joint accounts that the agent may need to see that should not necessarily be able to authenticate. The joint members will be displayed on the agent screens.

#### 10.2.8.2. Primary Only

A site may choose to only allow the primary member to authenticate. If this is the case, the only person that will be used for consideration is the primary person on the account. It should be noted that a joint member who attempts to authenticate in this environment will not be able to authenticate even if they answer all authentication correctly for their demographics.

#### 10.2.8.3. Determining access for joint members

There are two ways to handle access to shares and loans with Smart Apps. A site may configure to allow all joint members to have access to all shares and loans regardless of their association with the share or loan. In other words, all joint members will have access to all shares and loans with no regard to the **`SH_PERSON_LINK/LN_PERSON_LINK`** record associations or where the association occurs.

However, a site may want to strictly follow the **`SH_PERSON_LINK/LN_PERSON_LINK`** record associations configured within the core to determine the access a member will receive after authentication. In this situation, the member will only receive access to the shares and loans they are explicitly associated with within the core. It should be noted that the primary member will always have access to all shares and loans on the account.

To configure the system to process in one of the two methods described, the following site parameter should be configured:

| Site Parameter | Site Parameter Name | Description |
|---|---|---|
| 995 | Keystone/Keystone Joint Member Accounts Restricted | This field will indicate the method used by the system to handle share/loan access based on the primary versus joint indication.<br>Value T/F (Default = F)<br>True = Joint members will only have access to Shares/Loans where they are listed on the name record<br>False = Joint members have access to ALL Shares/Loans, External Loans, Mortgages, and Credit Cards on the account |

### 10.2.9. Share/Suffix/Account Access Configuration and Explanation

To be completed

### 10.2.10. Account Centric versus person/member centric

Need to be typed out

**Identifying the member/account using social security numbers** :

Smart Apps allow a member to select any account associated with their social security number. If a site chooses to allow a member to identify themselves using a social security number in the level 1 authentication questions, the system can determine if multiple logins may exist with the social security number. The members will be provided with a list of logins where they can choose which login to use for the session.

This smart apps will attempt to find logins will attempt to find the login associated with the person that has a matching or that matches the Social Security number period for account centric logins, the system will find all logins associated with accounts that have a primary person that matches the Social Security number.

### 10.2.11. Loan/Mortgage Payoff Availability

Keystone supports the ability to retrieve a loan or mortgage payoff. Support for future payoffs is not currently supported by Keystone.

### 10.2.12. Fund Transfers/Payments/Withdrawal Capabilities

Keystone supports a full set of capabilities for processing fund transfers and payments. The following features are supported within Keystone:

| Feature | Description/Note |
|---|---|
| Transfer funds within your own account | |
| Transfer funds to another member of the credit union | Controlled using the access preferences entries on the core |
| Transfer funds from another member of the credit union | Controlled using the access preferences entries on the core |
| Loan Payments | Supported for all internal loans and external loans if supported by the site. The ability to determine if a specific loan type can support payments is indicated within the Core Account Type screen. |
| Mortgage Payments | Supported for all internal mortgages and external mortgages if supported by the site. The ability to determine if a specific mortgage type can support payments is indicated within the Core Account Type screen. |
| Credit Card Payments | Supported for all internal credit cards and external credit cards if supported by the site. The ability to determine if a specific credit card type can support payments is indicated within the Core Account Type screen. |
| Scheduled Payments | Supported for all loan, mortgage, or credit card payments that an on-demand payment is supported |
| Scheduled Transfers | Supported for all shares as configured by the site |

Shared loan access records

### 10.2.13. System Restriction Overrides

There are no system restriction overrides that can be established for Keystone.

# 11. Site Parameters

## 11.1. Symitar

| ID | Site Parameter Name | Existing Description | Updated Description |
|---|---|---|---|
| 263 | Dormant account threshold | This field will indicate the inactivity period allowed before an account is considered dormant. This field is expressed in days. | This site parameter indicates inactivity period allowed before an account is considered Dormant. This parameter is expressed in Days and has a value of 365. |
| 729 | Symitar – Invalid attempts before freezing | Indicates the number of times a caller can enter valid account number with other invalid authentication information before the system freezes the account. This parameter should be synced with the INV ATTEMPTS BEFORE FROZEN within the SymConnect parameters. Symitar will only freeze accounts that use PINs in the authentication process. This parameter enables the SmartApps applications to freeze the account if authentication information other than PIN is entered incorrectly.<br>0 = Do not freeze<br>1 – 999 Number of attempts allowed | This site parameter indicates |
| 599 | Symitar Bankruptcy Statement Codes | This field will contain a delimited list of statement codes that will be used to | This site parameter indicates |

| | | | |
|---|---|---|---|
| | | suppress any share or loan with this code. | |
| 794 | Symitar Employee Account Types | This field will contain a delimited list of Employee Account Types that can be used to determine the members that are employees.<br>Example:<br>49\|33\|67 | This site parameter indicates |
| 910 | Symitar Business Account Determination | This field will indicate how the system determines a business account from a personal account within a Symitar system. Valid options are:<br>N = Name Format<br>A = Account Type | This site parameter indicates |
| 911 | Symitar Business Account Types | This field will contain a delimited list of Member Account types that can be used to determine the members that are business accounts.<br>Examples:<br>01\|45\|23 | This site parameter indicates |
| 405 | External Credit Card Type Determination | This field will specify the method that will be used to determine the type of credit card for external cards. Valid Values are:<br>1=Record Type/Card Code<br>2=Card Pattern (BIN) | This site parameter indicates |
| 326 | Speak Loan Type instead of sub | This parameter will indicate whether the loan code description should be spoken | This site parameter indicates |

| | | | |
|---|---|---|---|
| | classification if available | when identifying accounts to IVR callers.<br><br>Symitar Only | |
| 539 | Symitar Loan Draft Types | This field will identify all loan types that have draft capability.<br>The format is: xx\|xx\|xx\|xx | This site parameter indicates |
| 208 | Collect payer type on mortgage payment | This option will indicate if the system should request that the person making the mortgage payment indicate if they are the borrower or co-borrower.<br>NOTE: This function is only available for the Symitar core processor | This site parameter indicates |
| 547 | Symitar Nickname Field | This field will identify the field name to be used where retrieving the nickname information from Symitar | This site parameter indicates |
| 556 | Symitar Payroll Deposit Options | This field will indicate the method used in retrieving payroll deposits. Valid options are:<br>P = Use Transaction source of P<br>A = Use transaction source of E (ACH)<br>B = Use both transaction source P and E | This site parameter indicates |
| 597 | Symitar - Repgen to be used in Balance on a specific Day | This field will indicate the name of the RepGen that will be used in the routines that calculate balance on a specific date. | This site parameter indicates |

| | | | |
|---|---|---|---|
| 804 | Symitar Stop Payment Fee Verbiage | This field will contain the verbiage that will be posted to the core when a stop payment fee is charged against the share. This setting will work in conjunction with parameter 805 – Symitar Stop Payment Fee Include Check Number(s) to determine if the check or checks will be appended to the end of the verbiage. | This site parameter indicates |
| 805 | Symitar Stop Payment Fee Include Check Number (s) | This field will indicate if the check or check range will be appended to the end of the Symitar Stop Payment Fee verbiage listed in parameter 804. | This site parameter indicates |
| 548 | Symitar Post Stop Check Fee to core | This field will indicate if the IVR should post the stop check fee to the core processor.<br>T/F | This site parameter indicates |
| 557 | Symitar Check Processor Code for withdrawals | This field will indicate how the checks are processed when performing withdrawals and loan advances. Valid values are :<br>S = server or Symitar (Default)<br>C = client system<br>T = third party | This site parameter indicates |
| 596 | Symitar – Check Request Reference Data | This field will specify the verbiage that will be inserted in the check reference field when a check withdrawal is | This site parameter indicates |

| | | | |
|---|---|---|---|
| | | processed. 40 Character maximum. | |
| 753 | Symitar – Joint Name Types for Smart Screen Pop Display<br><br>(Agent viewpoint) | This field will contain a list of name types that should be retrieved when building the joint accountholder lists to be displayed within Smart Screen Pop. This will be a delimited list using \| as the delimiter. If this field is blank, only primary, and joint (name types 0 and 1) will be retrieved.<br>Example:<br>0\|3 | This site parameter indicates |
| 797 | Symitar – Joint Name Types<br><br>(Authentication viewpoint) | This field will contain a list of name types that should be retrieved when building the joint accountholder lists. This will be a delimited list using \| as the delimiter. If this field is blank, only primary, and joint (name types 0 and 1) will be retrieved.<br>Example:<br>0\|3 | This site parameter indicates |
| 995 | Symitar/Keystone Joint Member Accounts Restricted | This field will indicate the method used by the system to handle share/loan access based on the primary versus joint indication.<br>Value T/F (Default = F)<br>True = Joint members will only have access to Shares/Loans where they are listed on the name record | This site parameter indicates |

| | | | |
|---|---|---|---|
| | | False = Joint members have access to ALL Shares/Loans, External Loans, Mortgages, and Credit Cards on the account | |
| 319 | Allow IVR Interaction Mode | This field will indicate if the IVR Interaction Mode feature will be available to callers. IVR Interaction Mode allows callers to select Menu Mode or Expert Mode navigation settings. Menu Mode will present instructional navigation menus to callers. Expert Mode will allow callers to enter or select pre-defined service codes for specific IVR features and functions.<br>T/F | This site parameter indicates |
| 320 | Enable New User Interaction Mode Setup | This parameter will indicate if a first time IVR user should be prompted to setup their Interaction Mode.<br>T/F | This site parameter indicates |
| 324 | Use language from core if available | This field will indicate if the IVR should look at the core for the preferred language for the caller. If a preferred language is found, the caller will not be prompted for language.<br>T/F | This site parameter indicates |
| 522 | Symitar Debit Card Types | This field contains a delimited list of account types associated with debit cards. The format is: xx\|xx\|xx\|xx | This site parameter indicates |

| | | | |
|---|---|---|---|
| 540 | Symitar ATM Card Types | This field contains a delimited list of card types associated with ATM cards.<br>The format is: xx\|xx\|xx\|xx | This site parameter indicates |
| 629 | Symitar Credit Card Types | This field contains a delimited list of account types associated with credit cards.<br>The format is: xx\|xx\|xx\|xx | This site parameter indicates |
| 713 | Symitar – Card Block code | Block code to be used in card block features. If this field is blank, the block code will not be updated. | This site parameter indicates |
| 714 | Symitar – Card Reissue code | Reissue code to be used in card block features. If this field is blank, the reissue code will not be updated. Valid values 0 – 4. | This site parameter indicates |
| 715 | Symitar – Card Block Status Reason Code | Card block status reason to be used in card block features. If this field is blank, the status reason code will not be updated. Valid values 0 – 199. | This site parameter indicates |
| 380 | Cross Account conflict handling | This parameter will specify the method used to handle accounts that have transfer specific preference records for accounts and (or) shares but also have an indication that any account can be used for a destination transfer. Valid values are:<br>1 = Ignore ability to transfer to any account | This site parameter indicates |

| | | | |
|---|---|---|---|
| | | 2 = Ignore account specific transfer preferences<br>3 = Handle both situations with a menu selection | |
| 128 | Allow Cross Account funds transfers | This option will indicate if cross account transfers will be allowed.<br>T/F | This site parameter indicates |
| 237 | Allow Scheduled Transfers | This option will indicate if the system allows the caller to process a scheduled transfer if the core supports this capability.<br>T/F | This site parameter indicates |
| 238 | Allow Scheduled Payments | This option will indicate if the system allows the caller to process a scheduled payment if the core supports this capability.<br>T/F | This site parameter indicates |
| 329 | Allow Member to Member Account transfers for Checking to Loan Transfers | This parameter will indicate if the system should offer a member-to-member account transfer on the Checking to Loan Transfer feature.<br>T/F | This site parameter indicates |
| 330 | Allow Member to Member Account transfers for Savings to Loan Transfers | This parameter will indicate if the system should offer a member-to-member account transfer on the Savings to Loan Transfer feature.<br>T/F | This site parameter indicates |
| 331 | Allow Member to Member Account transfers for Loan to Checking Transfers | This parameter will indicate if the system should offer a member-to-member account | This site parameter indicates |

| | | | |
|---|---|---|---|
| | | transfer on the Loan to Checking Transfer feature.<br>T/F | |
| 332 | Allow Member to Member Account transfers for Loan to Savings Transfers | This parameter will indicate if the system should offer a member-to-member account transfer on the Loan to Savings Transfer feature.<br>T/F | This site parameter indicates |
| 333 | Allow Member to Member Account transfers for Checking to Savings Transfers | This parameter will indicate if the system should offer a member-to-member account transfer on the Checking to Savings Transfer feature.<br>T/F | This site parameter indicates |
| 334 | Allow Member to Member Account transfers for Savings to Checking Transfers | This parameter will indicate if the system should offer a member-to-member account transfer on the Savings to Checking Transfer feature.<br>T/F | This site parameter indicates |
| 335 | Allow Member to Member Account transfers for Loan to Deposit Transfers | This parameter will indicate if the system should offer a member-to-member account transfer on the Loan to Deposit Transfer feature.<br>T/F | This site parameter indicates |
| 336 | Allow Member to Member Account transfers for Deposit to Loan Transfers | This parameter will indicate if the system should offer a member-to-member account transfer on the Deposit to Loan Transfer feature.<br>T/F | This site parameter indicates |
| 337 | Allow Member to Member Account | This parameter will indicate if the system should offer a member-to-member account | This site parameter indicates |

| | | | |
|---|---|---|---|
| | transfers for Deposit-to-Deposit Transfers | transfer on the Deposit-to-Deposit Transfer feature.<br>T/F | |
| 463 | Allow Member to Member transfers for Savings to Savings Transfers | This parameter will indicate if the system should offer a member- to-member transfer on the Savings to Savings Transfer feature.<br>T/F | This site parameter indicates |
| 464 | Allow Member to Member transfers for Checking-to-Checking Transfers | This parameter will indicate if the system should offer a member-to-member transfer on the Checking- to-Checking Transfer feature.<br>T/F | This site parameter indicates |
| 475 | Suppress fund transfers from another account | This option will indicate that fund transfers from another member's account will be suppressed even if the transfer preferences support this function. | This site parameter indicates |
| 912 | Symitar Service Codes | This field will contain delimited lists of Service Codes and capabilities.<br>Examples:<br>21\|T\|F\|F*42\|F\|T\|T<br>In this example, 21 is the service code, the next value represents Transfer In capability, the next field represents Transfer Out capability, and the next field represents Withdrawal capability. A second delimiter (*) is used to define the next service code. | This site parameter indicates |

## 11.2. Keystone

| ID | Site Parameter Name | Existing Description | Updated Description |
|---|---|---|---|
| 263 | Dormant account threshold | This field will indicate the time period of inactivity allowed before an account is considered dormant. The field is expressed in days. | This site parameter indicates inactivity period allowed before an account is considered Dormant. This parameter is expressed in Days and has a value of 365. |
| 513 | Keystone - Set Lock Flag to Disable Logins | Keystone has the capability to automatically disable further login attempts when a failed login attempts threshold is met. When this site parameter is set to true, Smart Suit applications will assume that the login disable failed threshold setting is turned off and will manually set the locked flag on a login record when the failed attempts threshold set in Site Parameter 514 is reached. | This site parameter gives keystone the capability to automatically block additional login attempts once the threshold for failed login attempts is reached.. SmartApps assumes that login disable threshold for failed login attempts is inactive when the site parameter is set to True. Manual action is required to set the lock when the number of failed attempts specified in Site Parameter 514 is reached. |
| 514 | Keystone - Invalid Attempts Before disabling Logins | Indicates the number of times a caller can enter valid Login ID with other invalid authentication information before the system locks the login/disables the login. Keystone out of the box only has the capability of locking out members if PIN Authentication is used. This parameter is used for 2 purposes- locking out a login record when authentication info other than PIN is used as well as in conjunction with Site Parameter 513 to manually set the lock flag if the Credit Union prefers to use the lock flag.<br><br>0 = Do not lock/disable<br>1-999 = Number of attempts allowed | This site parameter indicates the maximum count of attempts allowed using a valid Login ID but with incorrect authentication information, before the system enforces a lock. This parameter performs two functions, 1. It allows the automatic locking of a login record when information other than PIN is used, because Keystone supports locking only when PIN is used for authentication.<br>2. Manually set the lock in coordination with Site Parameter 513.<br>0: Do not lock.<br>Number between 1 and 999: the number of allowed login attempts. |
| ~~548~~ | ~~Keystone Post Stop Check Fee to core~~ | ~~This field will indicate if the IVR should post the stop check fee to the core processor.~~<br>~~T/F~~ | ~~This site parameter indicates whether the IVR should post the stop check fee to the core processor.~~<br>~~**True** implies posting the stop check fee to the core processor.~~<br>~~**False** implies not to post the stop check fee to the core processor.~~ |
| 578 | Keystone - Joint Account Types (Authentication Viewpoint) | This field will contain a list of all Joint Account Types that should be included for access when determining the accounts that should be accessed within the system. This field is a | This site parameters contains the list of Joint Account Types that must be considered when the system determines the accounts accessed for authentication. This parameter |

| | | | |
|---|---|---|---|
| | | delimited list. EXAMPLE JT\|TR\|BE. delimiter. If this field is blank, only primary, and joint (name types 0 and 1) will be retrieved.<br>Example:<br>0\|3 | uses delimited format with \| as the connector. If the parameter is empty only primary and joint account names get returned (name types 0 and 1). Example 0\|3. |
| 579 | Keystone - Joint Account Types For Smart Screen Pop Display (Agent Viewpoint) | This field will contain a list of all Joint Account Types that should be included for access when building the joint account holder lists to be displayed within Smart Screen Pop. This will be a delimited list using \| as the delimiter. EXAMPLE: JT\|TR\|BE<br><br>JOINT ACCOUNT TYPE CODES:<br><br>(AD) Administrator<br>(AS) Authorized Signer<br>(AU) Authorized user<br>(BC) Contingent Beneficiary<br>(BE) Beneficiary<br>(BO) Beneficial Owner<br>(CB) Co-borrower<br>(CO) Collateral owner<br>(CS) Cosigner<br>(CU) Custodian<br>(CV) Conservator<br>(EX) Executor<br>(GD) Guardian<br>(GU) Guarantor<br>(IB) Irrevocable trust beneficiary<br>(JT) Joint owner<br>(OT) Other related party<br>(PA) Power of attorney<br>(RB) Revocable trust beneficiary<br>(RC) Contingent revocable trust beneficiary<br>(RP) Representative payee<br>(SA) Statement addressee<br>(SC) Successor Custodian<br>(ST) Successor trustee<br>(TR) Trustee<br>(VF) VA fiduciary | This site parameter indicates a list of Joint Account Types considered when creating the joint account holder list which gets displayed in the Screen Pop. This parameter uses delimited format with \| as the connector. Example JT\|TR\|BE<br><br>JOINT ACCOUNT TYPE CODES:<br><br>(AD) Administrator<br>(AS) Authorized Signer<br>(AU) Authorized user<br>(BC) Contingent Beneficiary<br>(BE) Beneficiary<br>(BO) Beneficial Owner<br>(CB) Co-borrower<br>(CO) Collateral owner<br>(CS) Cosigner<br>(CU) Custodian<br>(CV) Conservator<br>(EX) Executor<br>(GD) Guardian<br>(GU) Guarantor<br>(IB) Irrevocable trust beneficiary<br>(JT) Joint owner<br>(OT) Other related party<br>(PA) Power of attorney<br>(RB) Revocable trust beneficiary<br>(RC) Contingent revocable trust beneficiary<br>(RP) Representative payee<br>(SA) Statement addressee<br>(SC) Successor Custodian<br>(ST) Successor trustee<br>(TR) Trustee<br>(VF) VA fiduciary |
| 580 | Keystone - Login Channel Serial for SmartApps Authentication | This field will indicate the Login Channel Serial (Login Grouping) used by Smart Apps in the Keystone Core. | This site parameter indicates the Login Channel Serial (Login Grouping) employed by SmartApps in the Keystone core. |
| ~~804~~ | ~~Keystone Stop Payment Fee Verbiage~~ | ~~This field will contain the verbiage that will be posted to the core when a stop payment fee is charged against the share. This setting will work with parameter 805 – Keystone Stop~~ | ~~This site parameter indicates the message posted to the core when a stop payment fee is applied to a Share account. It works with Site Parameter 805 to determine whether~~ |

| | | | |
|---|---|---|---|
| | | ~~Payment Fee Include Check Number(s) to determine if the check or checks will be appended to the end of the verbiage.~~ | ~~the check or checks should be added to the end of the message.~~ |
| ~~805~~ | ~~Keystone Stop Payment Fee Include Check Number (s)~~ | ~~This field will indicate if the check or check range will be appended to the end of the Keystone Stop Payment Fee verbiage listed in parameter 804.~~ | ~~This site parameter indicates whether to append the check or check range to the end of the Keystone Stop Payment Fee Verbiage specified in Site Parameter 804.~~ |
| 898 | Keystone – Login ID Contents description | This parameter will allow you to specific the contents of the login-id on a Keystone system which will be spoken if multiple accounts are found under the same login-id.<br>1 = Tax ID<br>2 = Phone Number<br>3 = Selection From site parm 601<br>4 = Account<br>5 = SSN | This site parameter indicates the specific contents to be spoken for the Login ID when multiple accounts are associated with the same Login ID. |
| 960 | Keystone – Login Channel for Home Banking | This parameter will indicate the login channel that will be used if the member is enrolled in Home Banking. | This site parameter indicates the login channel mode used by members enrolled in Home Banking. |
| 961 | Keystone – Login Channel mode for Home Banking | This parameter will indicate the login mode for the Home Banking channel. Valid values are:<br>A = Account Centric<br>P = Person Centric | This site parameter indicates the login channel mode for the Home Banking channel. The valid options are:<br>A: Account Centric and,<br>P: stands for Person Centric |
| 962 | Keystone – Login Channel for Mobile Banking | This parameter will indicate the login channel that will be used if the member is enrolled in Mobile Banking. | This site parameter indicates the login channel mode used by members enrolled in Mobile Banking. |
| 963 | Keystone – Login Channel mode for Mobile Banking | This parameter will indicate the login mode for the Mobile Banking channel. Valid values are:<br>A= Account centric<br>P= Person centric | This site parameter indicates the login channel mode for the Mobile Banking channel. The valid options are:<br>A: Account Centric and,<br>P: Person Centric |
| 964 | Keystone - Card Mass Reissue Note Type | This Parameter will contain a note type serial for a note that would be added to the card record to indicate a mass reissue of the cards. | This site parameter stores a note type serial for a note denoting a mass reissue of cards. |
| 995 | Keystone Joint Member Accounts Restricted | This field will indicate the method used by the system to handle share/loan access based on the primary versus joint indication.<br>Value T/F (Default = F)<br>True = Joint members will only have access to Shares/Loans where they are listed on the name record<br>False = Joint members have access to ALL Shares/Loans, External Loans, Mortgages, and Credit Cards on the account | This site parameters indicate the system's approach to manage Share and Loan access through primary and joint designations. The default value is False.<br>True: Joint members get access to Shares and Loans if they listed on the same record.<br>False: Joint members get access to all Shares, Loans, External Loans, Mortgages and Credit Cards associated with the account. |

| | | | |
|---|---|---|---|
| 1026 | Keystone Return Primary Account For Person | Determines what to return when multiple accounts are found for the identified individual. True: return the first account where the identified person is Primary. False – return a list of all accounts where the identified person is Primary or Joint. | This site parameter indicates the multiple accounts for a member. The default value is false.<br>True: Returns the first account where the member is Primary.<br>False: Returns all accounts where the member is either Primary or Joint. |