**Test case 141**

* The secure login must provide the user with the ability to enter both a username and a password.
* Username must default to the network username for the user that is logged into the PC.
  + If the username is longer than 8 characters, it must be truncated to include only the first 8 characters.
    - **Dev Note**: The character length must be changeable using a settings file or database entry.  There has been discussion regarding changing the length of the ORACLE username.
* The user must have the ability to:
  + Attempt login using the entered username and password;
  + Reset their password - navigating them to the existing VB password reset application.
* An invalid username and password combination must result in a message to the user indicating:
  + Invalid username/password. Please contact the Helpdesk x2740 if you have forgotten your username or password.
  + Upon closing the error message, the username and password fields must clear.
* The ORACLE database manages the username and password. This includes but is not limited to:
  + Requiring periodic password resets every 60 calendar days.
    - ORACLE passwords expire every 60 calendar days. When the user reaches 5 calendar days from expiration of the current ORACLE password, the user must receive a notification on the login screen for the new claim system indicating: "Your password will expire in <# of calendar days from expiration>. To avoid your account being locked, you need to change your password. Would you like to change your password now?"
      * User says "Yes" - user is navigated to the existing VB Password Reset application.
      * User says "No" - current username and password are validated against the database as per requirements.
      * This message must continue to appear each time the user attempts to login, as long as the password remains active and the user is at or within 5 calendar days of password expiration.
    - If the user does not change their password before the 60 days has elapsed, the account will be locked. If this occurs, the user must receive the following message when trying to log in: "Your account has been locked. Please contact the Helpdesk x2740 to unlock your account and obtain a password reset."
  + If the user attempts 6 successive, unsuccessful attempts to login with an invalid/incorrect password, their account will be locked.
    - If the user account is locked the user must receive the following message: "Your account has been locked. Please contact the Helpdesk x2740 to unlock your account and obtain a password reset."
* Upon Successful Login:
  + If the user only has access to one Shield Application, they must be navigated directly to the single Shield application.
  + If the user has access to more than one Shield Application, they must be navigated to the Initial Shield Launch page.

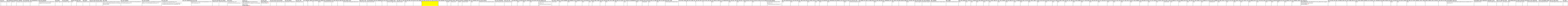
**Test case 143**

* The VB Password Reset Application is based on the same application used to change the password in the legacy policy system. The following differences must be accounted for in order to use with Shield.
  + There is no environment mapper with Shield.  Therefore, the VB Application must be capable of recognizing the environment of Shield the user is accessing so that the appropriate ORACLE environment password is changed.
    - i.e. If the user is using Shield UAT, the UAT.ORACLE password will be changed.  If the user is using Shield Production, the PROD.ORACLE password will be changed.
  + Upon successfully changing the password, the user must be navigated (or remain on) the login screen for Shield.

**Test case 148**

* The following rule applies to all screens except the Home screen:
  + If the user attempts to navigate to another screen within Policy Shield and there are unsaved changes made to any editable field, a warning message must be displayed:
    - There are un-saved changes to the policy. Do you wish to save your changes before navigating to another screen:
      * User Selects Yes - They remain on the current screen.
      * User Selects No - They will be navigated to the selected screen and changes made are not saved.
* The following rule applies regardless of which Policy Shield screen the user is on in the Primary Window.
  + If the user attempts to close the Primary Window/Tab of Policy Shield, they must always receive the following warning, regardless of whether or not changes were made to the screen they are currently on:
    - Please make sure you have saved any changes that you have made. Unsaved changes will be lost if you exit the Policy system. Are you sure you wish to exit the policy system?
      * User Selects OK - the warning message closes and the browser/tab is closed.
      * User Selects Cancel - the warning message closes and the user remains in the Policy system on the screen they were on at the time they chose to close the browser or tab.
* No messages will be displayed if the user attempts to close a Secondary Window/Tab.
  + **TESTING NOTE**: You will not be able to test this until we allow policies to be opened in Read Only mode (Project 2; Sprint 1).

**Test case 135**

* When the user saves or suspends a policy, a record is created/updated in the Policy Shield system (*PCOMMON*).
* The following defines the record that is created when the user first creates a policy as a Suspended New Business Policy, Suspended Renewal Policy, New Business Policy (Inforce), and Renewal Policy (Inforce):
  +   
    - This information may also be viewed in the "PCOMMON - Create" tab of the following spreadsheet: \\legend\filedept$\itech\projects\12038\_Main Project - Policy Shield\2\_RA\Exhibits.xlsx
    - **NOTE**: A14\_NEXT\_PACTDATE and A13\_NEXT\_PACTIVITY are fields used for legacy features/processes that may not have a workflow in Policy Shield.
    - D14\_STATUS indicates that for New Business and Renewal Policies, the code is "I".  "I" stands for an Inforce policy.  Policies must only be inforce once completed.  A completed policy includes units and coverages/forms.  Since Units and Coverages/Forms will not be completed in Sprint 1, it will not be possible to create an "Inforce" policy.  As stated in requirement 133, Sprint 1 testing focuses on save time validations with a pop up for successful validations.  The user will only be able to create policies in a Suspended state after Sprint 1.
  + The following new fields require database fields be created:
    - Alternate Policy #
    - SIC Code
    - NAICS Code
      * G70\_NAIC\_CODE currently exists in PCOMMON. Development needs to determine if this is appropriate or if a new field must be created.
    - Product
    - Subprogram
    - MEP %
    - Fac MEP %

**Test case 155**

* When the user selects "New Business" from the Create function, they must be navigated to the Policy Detail Screen in a New Business Policy Creation scenario.

**Test case 156**

* When the user selects "Renewal" from the Create function, they must be navigated to the Expiring Policy-Edition selection screen to begin the process of creating the Renewal edition of an existing policy.

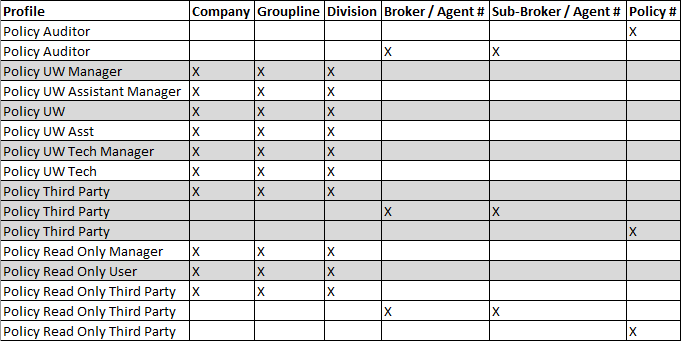
**Test case 167**

* Status must display the current status of the policy.
  + Suspended New Business - New Business Policies whose initial booking is incomplete or has been suspended instead of saved to inforce.
  + Suspended Renewal - Renewal Policies that have been suspended and not yet saved to inforce.
  + Inforce
    - Policies whose initial booking is completed and saved; and
    - The expiration date is later than the current date.
  + Cancelled Prorata - Policy is currently cancelled prorata.
  + Cancelled Short - Policy is currently cancelled short.
  + Cancelled Flat - Policy is currently cancelled flat.
  + Expired
    - Policy is not suspended or cancelled; and
    - The current date is on or after the expiration date; and
    - There are no later editions of the same policy # with an effective date on or after the expiration date of the policy-edition that is being displayed.
  + Renewed
    - Policy is not suspended or cancelled; and
    - The current date is on or after the expiration date; and
    - There are later editions of the same policy # with an effective date on or after the expiration date of the policy-edition that is being displayed.

**Test case 168**

* **PROJECT 1 (ALL SPRINTS)**
  + Because Project 1 will not build functionality to browse or edit existing policies, the Transaction Type must not be editable and default as follows:
    - For policies with a status of Suspended New Business, display "Suspended New Business" if the user has the appropriate security privileges.  If the user does not have the appropriate security privileges, Transaction Type will be blank.
    - For policies with a status of Suspended Renewal, display "Suspended Renewal" if the user has the appropriate security privileges.  If the user does not have the appropriate security privileges, Transaction Type will be blank.
    - For all other statuses, the field must be blank.
* **ALL PROJECTS AND SPRINTS**
  + Transaction Type is a required field to open a policy.  If the user attempts to open a policy without a transaction type, the system must display the following error: "Please select a transaction type to open and perform on this policy."  The user will remain on the Policy at a Glance screen.
    - Note: Since Sprint 1 will default to blank when the policy is not suspended, the user will be unable to open inforce, expired, cancelled, and renewed policies.
* FUTURE PROJECT SPRINTS
  + The Transaction Type field will allow the user to define what transaction they wish to perform to the policy-edition.  This includes opening policies in Read Only mode.
  + The items available for selection will vary based on current status of the policy and the users security privileges.
  + Available options and when they are available will be defined in the sprints in which they are built.

**Test case 332**

* The table below defines the different attributes that must be used to grant access based on specific policy attributes for various system roles:
  +   
    - **Grant Access to Policies Assigned to Select Attributes -**These columns identify attributes the system must be able to specify. An individual user may have one or more security attributes defined, which will identify the attributes a policy must have in order for the user to be able to create or open that policy.
      * **Company**- Indicates that the system may grant access to policies based on the Insurance Company assigned to the policy-edition.
      * **Groupline -**Indicates that the system may grant access to policies based on the Groupline assigned to the policy-edition.
      * **Division**- Indicates that the system may grant access to policies based on the Division assigned to the policy-edition.
      * **Broker / Agent #** - Indicates that the system may grant access to policies based on the Broker / Agent # assigned to the policy-edition.
      * **Sub-Broker / Sub-Agent #**- Indicates that the system may grant access to policies based on the Sub-Broker / Sub-Agent # assigned to the policy-edition.
      * **Policy #** - Indicates that the system may grant access to policies based on the policy #. Edition # is not considered.
    - For each row in the table above, if an "X" appears in more than one column in that row, the two attributes are inclusive of one another (i.e. if Company, Groupline, and Division have an "X", that means the system must define the access granted based on all three attributes together).
    - A single user may have more than one attribute rule (i.e. they may be granted access to specific Company, Groupline and Division combinations, but then also granted access to a specific Broker / Agent #).  When more than one attribute rule applies, the rules are exclusive of one another.
    - The security framework/setup must be capable of allowing security to be set up for "All Companies", "All Grouplines", "All Divisions" or "All Sub-Broker / Sub-Agent #s" to make the setup easier in situations where specificity is not required.

**Test case 31**

* **All Create/Suspend Scenarios**
  + The alternate policy # must allow the user to enter up to 30 alphanumeric and special characters.
  + Screen Level Validation
    - The combination of Alternate Policy # and Edition # can not exist on another policy in the system.  If this rule is not met, the following error must be displayed: "The Alternate Policy # and Edition # you have indicated already exists in Policy Shield." The system must not save/suspend.

**Test case 32**

* Brokerages and Agencies are defined by a 5 digit Broker / Agent # and a Brokerage / Agency name.  The #'s and names already exist within the policy system databases.
* Broker / Agent # - The user must be able to enter a 5 digit Broker / Agent # and the system must display the Brokerage / Agency name for the entered number in the Brokerage / Agency field.
  + Broker / Agent # must be restricted to those Broker / Agent #s the user has access to based their security profile. This restriction will be controlled by the Broker / Agent # Detail Level Access Security (DLAS) setup for the user.
    - If the user is not restricted by Broker / Agent #, they will have access to all Broker / Agent #s.
* **Brokerage / Agency** - The user must be able to search for Brokerage / Agency names.  This may be accomplished by a progressive starts with/contains search that displays matching values within the list or using a special search control designed for searching and selecting a valid Brokerage / Agency name.
  + Once the user selects a Brokerage / Agency name, the Broker / Agent # field must display the associated Broker / Agent # for the selected Brokerage / Agency name.
  + Brokerage / Agency must be restricted to those Brokerage / Agencies the user has access to based on their security profile. The restriction will be controlled by the Broker / Agent # DLAS setup for the user.
* Both the Broker / Agent # and Brokerage / Agency must be displayed on the Policy Detail screen when assigned to the policy.
* Real-Time, Screen Level Validation
  + If the Broker / Agent # entered is not found in the system, the following error must be displayed: "The Broker / Agent # you have entered is invalid."
  + If the Brokerage / Agency typed in the field does not match an existing Brokerage / Agency name, the Broker / Agent # field will not populate and the following error will be displayed: "The Broker / Agent # you have entered is invalid."
  + If the Broker / Agent # exists but the user does not have access to create policies for the Broker / Agent # based on their DLAS setup, the following error will be displayed: "You do not have security rights to create policies for this Broker / Agent #."
  + These validations must occur when the user clicks out of the respective fields as well as when the user attempts to save or suspend the policy.  If occurring when the user attempts to save or suspend, the system must terminate the Save or Suspend process.
* Save and Suspend Validation
  + Broker / Agent # must be active for the type of policy (New Business or Renewal) as of effective date of the policy.
    - Policy Effective Date >= Active Broker / Agent Status Date for New Business or Renewal
    - If the Broker / Agent # is not active as of the effective date of the policy, the following error must be displayed: "Broker / Agent # <Broker / Agent #> is inactive." System must not save / suspend.
  + Broker / Agent # must be authorized to write business for the Company, Rating State, Groupline and Reinsurance Code assigned to the policy as of the effective date of the policy.
    - Broker / Agent Licensing records exist in the Policy System database, which define the Companies, States, Grouplines and Reinsurance Codes a broker/agent is allowed to write with the Insured.  Each record can have an Effective Date and Expiration Date.
      * Policy Effective Date >= Effective Date of License Record
      * Policy Effective Date < Expiration Date of License Record
        + If the agent licensing record for the Company, Rating State, Groupline and Reinsurance Code is blank, then it is not expired.
    - If not authorized, the following error must be displayed: "Broker / Agent # <Broker / Agent #> is not authorized for the Company, Rating State, Groupline, and Reinsurance Code selected."  System must not save / suspend.
  + Broker / Agent # is required.
    - If incomplete, the following error must be displayed: "Broker / Agent # is required." The system must not save/suspend.
* The Broker / Agent # and Brokerage / Agency labels must have a red asterisk to denote a required field.
* *Select distinct ac.a04\_anum, na.b27\_name1, ac.d14\_status as New\_Business\_Status, ac.d15\_status\_fdate as New\_Business\_Status\_date, ac.d14\_agt\_ren\_status as Renewal\_Status,*

*ac.d15\_agt\_ren\_fdate as Renewal\_Status\_Date,al.b31\_state, al.a01\_company, ls.a01\_company\_desc, al.a36\_groupline, ls.a36\_groupline\_desc, al.g78\_program\_code, rc.g78\_description as Reinsurance\_Code,*

*al.a08\_fdate as License\_Effective,*

*Case*

*When al.a09\_xdate is null then sysdate + 1*

*Else al.a09\_xdate*

*End as License\_Expiration*

*from acommon ac left join name\_address na*

*on ac.e04\_anamnum = na.e04\_orignum*

*join alicense al*

*on ac.a04\_anum = al.a04\_anum*

*JOIN*

*(Select distinct a01\_company\_code, a01\_company\_desc, a36\_groupline\_code, a36\_groupline\_desc*

*from LA01\_SBL\_COV*

*where e62\_asl\_code != '000') ls*

*ON (al.A01\_COMPANY = LS.A01\_COMPANY\_CODE*

*AND al.A36\_GROUPLINE = LS.A36\_GROUPLINE\_CODE)*

*join lg78\_program\_code rc*

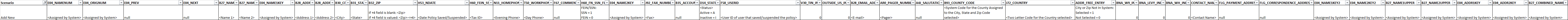
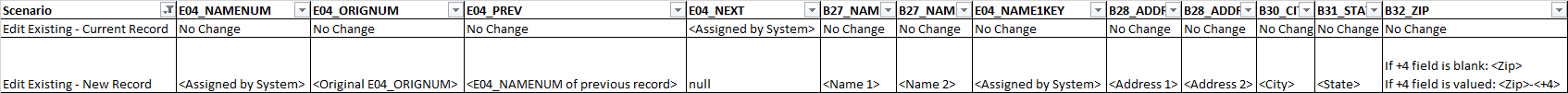
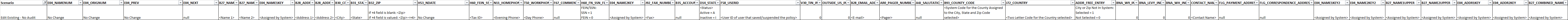
*on al.g78\_program\_code = rc.g78\_program\_code*

*where na.e04\_next is null*

*and ac.j03\_sub\_anum is null*

*order by ac.a04\_anum, al.a01\_company, al.a36\_groupline;*

**Test case 131**

* Upon Saving Primary Insured Details, database records must be created or updated depending on the action completed by the user:
  + Add a New Primary Insured:
    - Insert a new record in NAME\_ADDRESS:
      * 
    - Insert a new record in NAME\_XREF:
      * http://tfs2017:8080/tfs/Core/4b8a92c1-c32e-47ff-84f1-bb686b176e78/_apis/wit/attachments?FileNameGuid=c5d13e25-dd68-4aff-9c28-2a1853c4813b&FileName=temp1504124832967.png
  + Editing an Existing Primary Insured:
    - The Parties system allows for an audit trail.  A new record must be created to maintain the audit trail whenever any of the following field values are changed:
      * Name 1
      * Name 2
      * Zip Code (+4)
      * City or Zip Not In System
      * Address Type
      * City / Province / Postal Code
    - When a field that requires an audit record be created, the current active record must be updated and a new record with the changed information must inserted into NAME\_ADDRESS:
      * 
    - If no fields requiring an audit record have been changed, the current active record must be updated with the latest information for the changed fields.  A new record will not be created.
      * 
  + New database fields will need to be created on NAME\_ADDRESS for the following fields:
    - Address Type
    - City / Province / Postal Code

The images in this requirement can also be viewed in the NAME\_XREF and NAME\_ADDRESS tabs of the Exhibits file in the project folder.