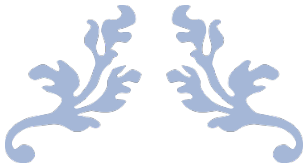
Change is good, capture it and control it wisely



AUDIT TRACKING 360

By The Snakul Group

FEBRUARY 1, 2019

THE SNAKUL GROUP LLC
10473 ATTLEBOROUGH DR, FRISCO TX 75035

360 Field History Tracking

(732) 925-3970 ANIL.KAMISETTY@THESNAKULGROUP.COM

Table of Contents

360 Field History Tracking

(732) 925-3970 ANIL.KAMISETTY@THESNAKULGROUP.COM

1. Revision History

Version Number	Change Description	Modified Date
1.0	Initial Draft	1st Feb 2019

360 Field History Tracking

(732) 925-3970 ANIL.KAMISETTY@THESNAKULGROUP.COM

2. Introduction

Every client will have their Unique needs. One Salesforce Org may be used by one Business Group where as other Org may be used by Multiple Business Groups. Traditionally not all fields will be shared by all Business Groups.

To cater for everyone's need, the Out of Box Field Tracking is not enough. It does not come to rescue when the need is to track Formula fields, Roll up fields, Cross Object fields or Insert / Delete / UnDelete Operations. Neither this helps when it is to track more than 20 fields. Some options are there to track, up to 60 fields but not further. Companies don't have an option if the need is to Audit every field on the object or to track User / Task / Event Objects. And the list goes on.

As name suggests, 360 Field History Tracking addresses all the above limitations. Infact, the package comes with many new innovative ideas for field tracking. By using this package, the client gets full control over the field history feature.

3. About US

The firm has individuals who have worked in the CRM Space for more than a decade and have seen clients from Financial, Property Casualty & Health Insurance domains. Based on the challenges faced by the clients, it was attempted to help them address all the limitations. Hence this package. If there are any recommendations / feedback, we welcome them, shoot them our way and we will have them considered for the upcoming releases.

4. Supported Features

4.1 Whom can be Audited

Traditionally when a track history is enabled for a field on any object, the field is edited for every record and for every User. It might not be required to track for every user, once they are matured. When a new User Join or a new branch is opened, it might be required to track "Just them". With the existing approach, it is not possible to track selective Users.

This package helps to track **USERS YOU NEED,** stop auditing every User every Record on the Object. Users can be selected in a variety of methods as outlined below. Administrator can choose any method or combination of methods for any objects, no strings attached. For the same object, administrator can choose more than one method if required, follow the execution sequence to see which User is audited on what definition.

1. All Users in the Organization
2. All Users with a Role

(732) 925-3970 ANIL.KAMISETTY@THESNAKULGROUP.COM

3. All Users with a Role, exclude one or more Users. This approach is same as option #6, just that User level definition is not required
4. All Users with a Profile
5. All Users with a Profile, exclude one or more Users. This approach is same as option #6, just that User level definition is not required
6. A Single User or a Set of Users

4.2 Execution Order

It is possible to define more than one method for a single object. When the Administrator defines multiples methods, the following execution order is followed per every User per object. Remember, for the below discussion, the audit definition records should be in Active State. If they are in inactive status, they are not considered.

1. If User level definition exists for the field history tracking, it overwrites any other definition for that User and for that Object
2. If Role level definition exists for the field history tracking and no User level for the field history tracking exists, the User will be audited based on the Role level definition
3. If Profile level definition exists for the field history tracking and no User / Role level for the field history tracking exists, the User will be audited based on the Profile level definition
4. If User / Role / Profile level definition does not exist and Object level definition exists for an Object, then the User is audited based on the Object level field history tracking definition

For any object, there can be many audit definition records. Following are the Maximum number of records. If duplicates are created, an error will be thrown. And not all types are mandatory for any object.

1. User Level: Equal to the Number of Users
2. Role Level: Equal to the Number of Roles
3. Profile Level: Equal to the Number of Profiles
4. Object Level: Maximum of One record per Object

4.3 What can be Audited

In the standard feature, Administrator can choose the audited fields from the list of available fields. Not all fields are available to choose at the first place though. A few implementations might choose a Field Set and it is Customer's responsibility to choose what field to audit. As and when any new fields are introduced, it is the Customer's responsibility to update the field set, if needed to audit the new field.

(732) 925-3970 ANIL.KAMISETTY@THESNAKULGROUP.COM

The Package offer a wide variety of Options to choose what to Audit. Administrator can choose any method or methods, for any audit definition. During Audit definition creation time, statistics are shown helping the administrator understand the number of fields with the respective type.

1. Field Set Wise: When this option is chosen, the fields selected in the field set are audited. If a new field is introduced, it is Customer's responsibility to choose the field. No limit on number of fields to choose.
2. DML wise: There are four operations available (Insert, Update, Delete, UnDelete). One or more options can be chosen and accordingly those operations are audited. Can choose all operations too
3. Object Wise: If this option is chosen, all fields are audited, no exceptions. If a new field is introduced, the new field is audited automatically
4. Field Wise: On any Object, there can be three different set of fields (Standard, Custom and System). System fields are those fields which User don't have access to modify (CreatedByID, CreatedDate, ModifiedBYId, Id etc.). By choosing any option, the respective fields are audited. If the Custom option is chosen, the new fields are audited automatically
5. Data type: Salesforce supports a wide variety of data types (Text, Boolean, Picklist, Date, Number etc.). If the auditing is enabled for any data type, new fields when created, will be auditable automatically without Customer's intervention
6. Record Type: Master record type is the default record type for any object. If additional record types are introduced, administrator can choose the record types to be audited. When the record types are chosen, then this option will be applied in addition to the DML & data type selection
7. Record Wise: Administrator can give the responsibility for record selection to the end User. When this option is chosen, this will be applied in addition to the Record Type / Data type / DML wise selection

4.4 Unique Features

Following are some of the Unique features which the Package Offers. None of these features are available in other packages or salesforce offering.

Change Data Capture: This feature enables to capture the Record Change Details (in JSON format). One common place for storing the event, for all objects. No need to build different Integrations for "multiple objects", one is enough for all objects. Thus removing the need to have additional expenditure to extend the CDC (more than 5 objects) or pumping more number of record changes.

Mutually exclusive definition: In the normal course, every User will be audited for the chosen fields. No exceptions can be defined. The package offers ability to define mutually exclusive field definition from User to User, User to Role, User to Profile, Role to Profile or All Object definition vs any other definition. For example, a User can be audited for Account Object for 75 fields where as another user can be audited

(732) 925-3970 ANIL.KAMISETTY@THESNAKULGROUP.COM

for 65 fields on the Account Object. There does not need to have any overlap between 65 and 75 fields though.

Unlimited number of fields: Traditionally the number of fields tracked are limited per object level (20 fields). Sometimes, the limit can be increase to 60. With this package, there are no limits on the number of fields to audit.

Extensibility: The field history feature can be extended to an object on the Org (Standard and Custom) within minutes. All it needs is an Audit definition record and two lines of Code, no custom development is required. Code can blend into the Customer Code.

All DML Operations: Other field tracking products does track the field history for Update Operations only. This package provides field wise history for all DML operations, including Create, Delete and UnDelete operations.

Data Types: The package supports all data types, including **Formula fields, Roll up Summary fields, Cross Object Formula** etc. All Lookup fields are tracked, showing the record names not just the record Id value. No longer required to write custom logic for tracking the lookup fields or formula / rollup fields. When the source record in the Lookup field gets modified, it can be noticed at the Child Record. As an example, Account is a lookup field on the Contact Record. If the Account ➔ Name gets modified, the change in the Account Name will be recorded as the change on the related Contact Records.

Inline Search: Field History can be displayed in the Detail page. Supports User to search for the history based on every column displayed. By doing so, the results are shown based on the User selection, thus avoiding search on every page (no need to use Next/Previous links)

Intuitive Reporting Interface: It is proven that the Field history grows very fast. Salesforce has limitations when the number of records exceed 10K, none of the Custom list views work. The package offers a User-Friendly Interface to browse through the Field History. If the number of records is in millions for say few objects, it should not take more than few seconds to see a records field history.

Data Archiving Tool: If the field history data grows fast, package provide an option to archive the data automatically or to delete data. And the retention period can vary for every field definition history record. Archived data can be re-imported back for compliance requirements if required.

Supports All Objects: Not all objects are supported by the Field history offerings. Salesforce Offering does not audit all objects. The package audits all triggerable objects, including **Task / Event / User** Objects. Child objects like **Opportunity Team Member** is also audited.

Managed Package Understanding: Salesforce hides the Managed Package Code. By auditing the entire object, it would help us understand what fields and what objects are touched / modified by the managed package and this provide good insight into the workings of the Managed Package.

Snapshot: The package helps to generate the Snapshot of the record as of “a date in the past” for all the Audited fields. This helps the end Users tremendously to know and see the values of different fields at a point in time.

360 Field History Tracking

(732) 925-3970 ANIL.KAMISETTY@THESNAKULGROUP.COM

Global Picture: A Record will be created and then modified multiple times. On a Click of a button, end User would be able to get the complete picture of record's history (what field got modified at what time and who did the change)

Development Tool: By enabling this feature, the developers are greatly benefited. This provides good insight into the field history (unlimited number of fields) and managed package workings, thus reducing the troubleshooting time. By looking at multiple updates in the same Unit of work, the developer can work on reducing the # of simultaneous DML operations / reduce CPU Time. Thus, helping to optimizing the Custom business logic.

Data Migration: Like other offerings, existing Field history data (if any) can be migrated.

Frequently Asked Questions

1. How to enable Change Data Capture on the Org ?
    a. On the Audit Setting Custom Object, please enable the Capture Image Flag. When enabled, the Record change (all fields) is capture in the following fields
        i. Before Image
        ii. Before Image2
        iii. Before Image3
        iv. Before Image4
        v. After Image
        vi. After Image2
        vii. AfterImage3
        viii. After Image4

    There might have been Audit definition for the object, saying capture for "selective fields". The Record Change history for these fields is captured in the following fields

        ix. Audit Snapshot
        x. Audit Snapshot2
2. What needs to be done after Installation?
    a. Update the Remote site Settings for the right Domain / Org
    b. Create Audit definitions records for all objects
    c. Insert the two line of code with the right Triggering Events (in Trigger logic or Trigger Handler logic)
3. Can the package support all objects on the Org?
    a. Yes, it supports every triggerable object
4. Is it easy to extend the functionality to another object?
    a. Yes, it is very easy to extend the functionality. All it needs is a new audit definition record on the Audit Setup object and two lines of code in the related Trigger or Trigger Handler. Ensure that the triggering events are captured
5. What are the triggering events for capturing the Field History?

(732) 925-3970 ANIL.KAMISETTY@THESNAKULGROUP.COM

   a. It is very important to use the correct triggering events and they are After Insert, After Update, Before Delete, After Undelete
6. Can the Field be tracked without the knowledge of the User?
   a. Yes, it is possible. But every user in the Org needs to have access to the related trigger and trigger handler. There are two permission sets which come in the package, assign the User permission set to every User to get Read access on the Audit Setup definition Object
7. Does every User need to have access to the package?
   a. Yes, it is required to have every User access on the package level, when the Audit is enabled. The first step is to check if the User has any audit definition created in the Audit Setup object, hence it is bare minimum need
8. Can we audit different set of fields for different Users on the same Object?
   a. Yes, it is very much possible to define different set of fields for different Users. In fact, it can be mutually exclusive set of fields also. This package provides a means to audit a single user vs a set of users or profile or roles.
9. I do have an audit definition for a User and Profile. Can I have definition for All Users on the same object?
   a. Yes, we can have User / Profile level definition in addition to All Users definition. All User definition covers Users who does not have User level definition and does not belong to the Profile (which has the audit definition available)
10. Can the End User choose which record to have the Audit enabled?
    a. Yes, the End User can choose what record to audit. Administrator would have specified already which fields to audit for the User, but User can choose if he wants to audit a record or not. Administrator has the option to disable the feature or control which User has access to it.
11. Does the Audited Data reside outside of the Org?
    a. No, Data resides within the Org. Nothing goes outside the Org