

Trusted Agentics

Hands-On Workshop

**Close the Trust Gap with the
Einstein Trust Layer and
Salesforce Trusted Services**



Attendee Guide

Disclaimer



The Salesforce products and features referenced in this workshop guide are subject to change at the discretion of Salesforce.com. Mention of specific products or features is intended for discussion purposes only and does not represent a guarantee of their availability. Please refer to Salesforce.com for the most current information on available products, editions, and functionality.

Table of Contents

Disclaimer-----	1
Table of Contents-----	2
Scenario-----	2
Exercise 1: Trust Layer Data Masking and Einstein Feedback-----	4
Exercise 2: Agent Permissions-----	7
Exercise 3: Shield Event Monitoring-----	12
Exercise 4: Shield Field Audit Trail-----	16
Exercise 5: Shield Platform Encryption-----	21
Exercise 6: Privacy Center-----	24
Want to learn more?-----	29
Get a Copy of This Guide:-----	29
Where Do We Go From Here?-----	29

Scenario

Your organization is looking at incorporating Agents and generative AI functions in order to improve customer service. Your Chief Information Security Officer (CISO) has asked you to ensure that you are using generative AI in a secure and compliant manner.

To innovate while enhancing trust you will leverage several important salesforce capabilities:

- Configure the Einstein Trust Layer for data masking and feedback
- Understand permissions needed for agent actions
- Create a data management policy for data minimization
- Configure a policy to reduce the risk of data exfiltration
- Enable encryption for sensitive fields
- Enable change history tracking on contact records

Get your workshop Salesforce org: <https://sfdc.co/getmyorg>

Your workshop facilitator will provide you with an Event Code for signup.

The form is titled "Event Code" and contains the following instructions: "Please enter the code provided by your presenter." Below this, there are six input fields arranged horizontally. Underneath the code inputs, there are three more input fields: "First Name" (placeholder: "Your first name"), "Last Name" (placeholder: "Your last name"), and "Email" (placeholder: "Your email address").

Exercise 1: Trust Layer Data Masking and Einstein Feedback

- **What to do:** Verify the configuration of the Einstein Trust Layer
 - **Value of it:** Understanding of how the Trust Layer is set up and the various configurations for Data Masking
 - **Tools used:** Einstein Trust Layer Setup
 - **Time to Complete:** 15 minutes
-
- Click the **Setup** icon  (it is in the upper right-corner of the browser window) and select **Setup**
 - In the Setup quick find box, type **Einstein Setup**, then select **Einstein Setup**
 - Switch “Turn on Einstein” from **Off** to **On**
 - Refresh your browser page
 - In the Setup quick find box, type **Agentforce**, and click **Agentforce Agents**.
 - Switch “Agentforce” to **On**
 - Switch “Enable the Agenforce (Default) Agent” to **On**
 - In the Setup quick find box, type **Trust Layer**, and click **Einstein Trust Layer**
 - If the “Large Language Model Data Masking” is **Off**, switch it to **On**

Agent Insights:



Why are we turning this on? Many customers want to protect sensitive types of data, such as Personally Identifiable Information (PII). In the current version of Agentforce Service Agent, data masking is disabled, and other options are available to protect sensitive data.

However, there is much more to know about the Einstein Trust Layer, when masking is used and when it's not.

- Scroll down to review the types of data that are selected for masking by default



Agent Insights:

Notice that the **Name** attribute is selected to be Masked. That means a person's first, middle, or last name, or a combination of these will be turned into a string like <PERSON_0> for a variable we use in a prompt, such as *User.FirstName*. That's an example of data masking happening before the prompt is sent through the LLM Gateway, which is part of the Einstein Trust Layer.

As it comes back through the Einstein Trust Layer it will return to its original format, as the CRM data point: *User.FirstName*. However, this is using Pattern Based masking, which isn't as accurate as Field Based masking, based on Compliance Categories and Data Sensitivity levels. Data Sensitivity Levels are metadata attributes applied to fields and can be configured to indicate the sensitivity of data. Compliance Categories are also metadata attributes applied to fields focused on a compliance act, regulation or definition. If you configured fields with these settings, they can also be masked when used in Prompts.

You will also see an option to mask Shield Platform Encrypted Fields. This will allow you to mask fields that have already been encrypted using Platform Encryption. This ensures that fields already considered sensitive will be masked if they are used in prompts.

It will be normal for customers to want to analyze what is happening with their prompts and the data going to and from the LLMs. This can be done with the data collected with Agent Analytics for topic usage, action usage, key metrics such as deflection, token count, and more. It can all be very useful for compliance purposes.

- In the Quick Find box, type **Einstein Setup**, and then select **Einstein Setup**
- Scroll down to **Collect and Store Einstein Generative AI Data**
- Click **Go to Einstein Data Collection**

Collect and Store Einstein Generative AI Data

Collect and store Einstein data in Data Cloud to enhance your generative AI applications. Use it for analytics, prompt adjustments, LLM training, and more.

[Go to Einstein Data Collection](#)

- Ensure that the following are set to **On**:
 - **Audit and Feedback**
 - **Agent Analytics**

By doing the above steps, you will eventually get two dashboards that are ready for you to review if you **navigate to Dashboards from the App Launcher**, then select **All Dashboards**. These dashboards will take some time to populate as the data comes from actively using the agent.

Look for the dashboards named:

Einstein Generative AI Audit & Feedback Data

Einstein Trust Layer

Once those dashboards are created and the underlying reports are populated, you can see the data that's in Data Cloud that you'll eventually have reports built from.

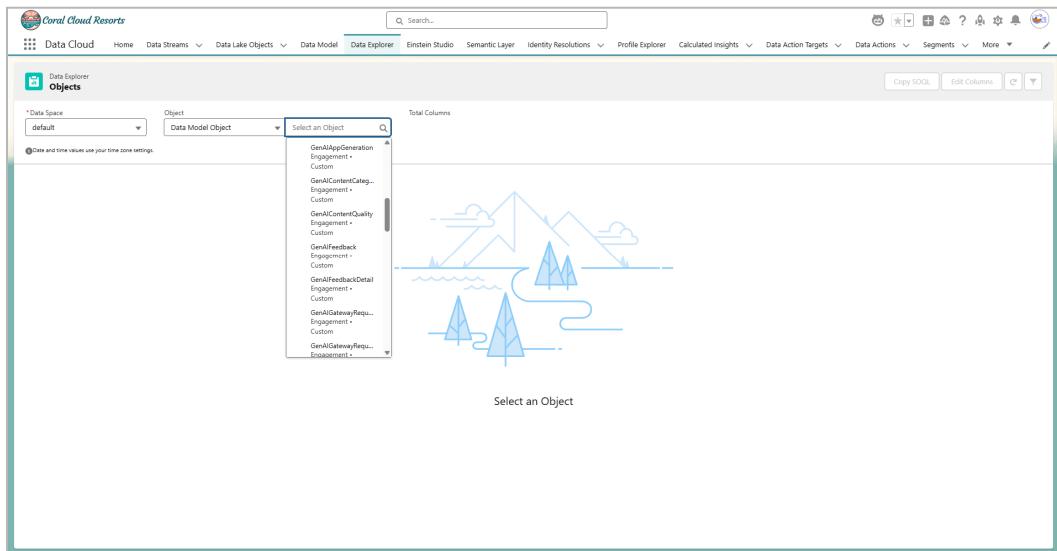
Follow these steps to see that data:

- Click the **App Launcher** and select **Data Cloud**
- Click the **Data Model** tab
- You now have a number of objects that start with **GenAI**

Note: If you don't see them, click the small refresh button on the right-hand side of the toolbar (not your browser's refresh button).

You can use Data Explorer to browse the Data Model objects that start with **GenAI**

- Click the **Data Explorer** tab
 - Select **default** for **Data Space**, for **Object** select **Data Model Object**
- Select any one of the objects that start with **GenAI** to view the columns in the object



Note: These are the objects that contain the data for the user feedback, audit data, and prompt usage that you just turned on. These objects will be populated with data after your agents and prompt templates have been used.

Exercise 2: Agent Permissions

- **What to do:** Verify that the Agent is returning the correct results and has proper permissions. You will identify the user that executes the Agent and verify it has the correct permissions.
- **Value of it:** Understanding what the Agent has permissions for will help with Least Privilege.
- **Tools used:** Who Sees What Explorer
- **Time to Complete:** 15 minutes

Agent Insights:



The Principle of Least Privilege (PoLP) is a core information security concept that dictates that a user, application, or system should only be granted the minimum level of access and permissions necessary to perform its required tasks, and nothing more.

In essence, it's about minimizing the "attack surface" and potential damage in case of a security breach. If an account or system is compromised, the impact is limited to only the resources it was explicitly authorized to access, preventing lateral movement and widespread compromise.

- In the Setup quick find box, type **Agent** and select **Agentforce Agents**
- Click the dropdown arrow on the **Coral Cloud Agent** and select **Open in Builder**

Agent Name	Type	Description	Created By	Active	Last Modified	Edit
> Coral Cloud Agent	Service Agent	This is the Coral Cloud Agent that helps customers ...	OrgFarm EPIC		Apr 11, 2025	Delete
> Einstein Copilot	Employee	An AI assistant for in-org business tasks.	OrgFarm EPIC	✓	Apr 10, 2025	Open in Builder

- If needed, click the 'Got It' button in the Conversation Preview

Got It

- Enter the following prompt to get us started:
I am sofiarodriguez@example.com and my membership number is 10008155
- After it responds, enter the next prompt:
Tell me about the Aqua Fitness in Paradise experience
- While the response does discuss the experience, it would be a better user experience for the user if the price was listed as well



Aqua Fitness in Paradise

Description: Immerse yourself in a unique fitness experience with Aqua Fitness in Paradise at Trial OrgFarm For U. Located in the refreshing resort pool, this invigorating session lasts 3 hours and caters to a medium fitness level. Join a group of up to 30 participants as you engage in a dynamic workout surrounded by the beauty of our tropical setting. Benefit from a full-body workout that is gentle on the joints while enjoying the serene atmosphere of our resort. Dive into wellness and fun with Aqua Fitness in Paradise!

Activity Level: Medium

Would you like to know more or perhaps book a session?



Lets make sure the coral cloud agent user has access to the proper field to get the price for the experience. We will use the “Who Sees What” explorer in the Security Center Extension to determine what permissions the **EinsteinServiceAgent User** has. We know this user is assigned the **Coral Cloud Service Agent Permissions** Permission Set, so we will search to make sure that the proper permissions have been assigned on the Experience object, which includes the Price field.

- Close out of Agentforce Builder by clicking the back arrow



- Click on **Coral Cloud Agent**
- On the bottom of this page the User assigned to this agent is displayed
The Coral Cloud Agent user's name is **EinsteinServiceAgent User**

The screenshot shows the 'AGENT DETAILS' section of the Coral Cloud Agent setup. It includes fields for API Name (Coral_Cloud_Agent), Type (Service Agent), and Active status (checked). Below this is a navigation bar with tabs: Details, Topics, System Messages, Language Settings, Connections, and Setup Checklist. The 'Details' tab is selected. The main content area displays various configuration settings:

- Name:** Coral Cloud Agent
- Created On:** February 26, 2025 at 12:36 PM
- API Name:** Coral_Cloud_Agent
- Created By:** Doug Cox
- Description:** This is the Coral Cloud Agent that helps customers learn more about Experiences as well as book sessions.
- Last Modified By:** Doug Cox
- Role:** The agent's job is to assist users in navigating and managing bookings for different experiences offered by Coral Cloud Resorts, ensuring a seamless customer service experience by providing accurate information and resolving issues promptly.
- Company:** Coral Cloud Resorts is a fictitious seaside resort that manages guests and their reservations. It offers a rich set of experiences.
- Agent User:** EinsteinServiceAgent User (coral_cloud_agent.ywswimhowssu.mg4jsirnkpvz.agrmn77)

A red arrow points from the text "Agent User" to the user entry in the list.

- Click the **App Launcher** icon and search for “**Security**”
- Open the **Security Center Extension** App and select **Who Sees What Explorer** (It might take minute to load since this is the first time it is starting up)
- Click “**Profiles and Permission Sets**”
- Search for “**Coral Cloud Service Agent Permissions**”

The screenshot shows the 'Select a Lens' interface with the 'Profiles & Permission Sets' tab selected. A search bar contains the text 'Coral Cloud S'. Below the search bar, there are two items listed under 'Coral Cloud Service Agent': 'Coral Cloud Service Agent' and 'Coral Cloud Service Agent Permissions'. A red arrow points from the text "Search a Profile" to the search bar.

- In the “**Search Objects & Fields**” box, type “**Experience**”

The screenshot shows the 'Coral Cloud Service Agent Permissions' page. At the top, there are tabs for 'Objects & Fields' (selected) and 'Permissions'. Below the tabs, there is a search bar containing the word 'Experience'. A red circle with the number '1' is positioned above the search bar. The main content area shows a table with one row, indicated by a red arrow pointing to the table border.

- Expand the **Experience** object and scroll down to the **Price** field. You will see that the Effective Access is “No Access”

FIELD ↑	API NAME	SENSITIVITY LEVEL	DATA TYPE	EFFECTIVE ACCESS	FIELD READ	FIELD EDIT
Price	Price__c		Currency(4, 2)	No Access	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Rating	Rating__c		Formula (Number)	No Access	<input type="checkbox"/>	<input type="checkbox"/>
Reviews Summary	Reviews_Summary__c		Long Text Area(32768)	No Access	<input type="checkbox"/>	<input type="checkbox"/>
Sum of Guest Reviews	Sum_of_Guest_Revie...		Roll-Up Summary (SUM (No Access	<input type="checkbox"/>	<input type="checkbox"/>
Total Guest Reviews	Total_Guest_Reviews...		Roll-Up Summary (COUNT	No Access	<input type="checkbox"/>	<input type="checkbox"/>

- Click on the “No Access” link on the Price field. This screen will provide more information on the Reason for Access and the Field Details
- Click the “Coral Cloud Service Agent Permissions (Perm Set)” link. This will open up the permission set so that you can edit the permissions

The screenshot shows the 'Reasons For Access' and 'Field Details' sections for the Price field. The 'Reasons For Access' section lists various permissions and their status. The 'Field Details' section shows the current field settings.

Object Create	Object View All
• No Access	• Coral Cloud Service Agent Permissions (Perm Set)
Object Read	Object Modify All
• Coral Cloud Service Agent Permissions (Perm Set)	• No Access
Object Edit	Field Read
• No Access	• No Access
Object Delete	Field Edit
• No Access	• No Access

Buttons at the bottom: Previous Field, Next Field

- In the Apps section, click **Object Settings**
- In the Find Settings... box, search for **Experience**
- Select **Experiences** from the list

[Experiences](#) Experience__c

- Click **Edit**
- Scroll down to the Field Permissions and select the **Read Access check box** for the Price field:

The screenshot shows the 'Field Permissions' section for the Price field. The 'Read Access' checkbox is selected (indicated by a blue border).

- Click **Save**

- Now, let's go back and test the agent again. In the Setup quick find box, type **Agent** and select **Agentforce Agents**
- Click the dropdown arrow on the **Coral Cloud Agent** and select **Open in Builder**

Agent Name	Type	Description	Created By	Active	Last Modified	Edit	Delete	Open in Builder
> Coral Cloud Agent	Service Agent	This is the Coral Cloud Agent that helps customers ...	OrgFarm EPIC		Apr 11, 2025			
> Einstein Copilot	Employee	An AI assistant for in-org business tasks.	OrgFarm EPIC	✓	Apr 10, 2025			Open in Builder

- Select the refresh icon at the top of the Conversation Preview



- Enter the following prompt to get us started:
I am sofiarodriguez@example.com and my membership number is 10008155
- After it responds, enter the next prompt:
Tell me about the Aqua Fitness in Paradise experience
- Now you will see the price in the response

Exercise 3: Shield Event Monitoring

Salesforce Shield **Transaction Security** is a feature that provides advanced security and risk monitoring capabilities for critical business processes and data within the Salesforce platform. It is one of the advanced features found in the Shield Event Monitoring solution. It helps organizations detect and prevent potential threats, fraud, and policy violations by analyzing and evaluating user actions and transactions in real-time.

Transaction Security allows administrators to define transaction policies that specify the criteria for identifying potentially risky or anomalous activities. These policies can be based on various factors, such as user profiles, IP addresses, geographic locations, time of day, or specific data patterns.

When a user performs an action that violates a defined policy, Transaction Security can take appropriate actions, such as blocking the transaction, requiring additional verification steps, or generating alerts and notifications to administrators or security teams.

By continuously monitoring and evaluating transactions, Transaction Security helps organizations maintain the integrity of their Salesforce data and processes. It provides a detailed audit trail of user activities, enabling organizations to investigate and respond to potential security incidents effectively.

Objective:

- Set up a policy to prohibit downloads of sensitive data from Data Cloud

Estimated Time: 7 minutes

Instructions:

- See How Users can Download Sensitive Data
 - Use the App Launcher to navigate to Reports
 - Click the **New Report** button
 - Select the **Accounts & Contacts** Category
 - Select the **Contacts & Accounts** Report Type
 - Click **Start Report**

Create Report

Category	Select a Report Type	Details
Recently Used		
All		
Data Cloud		
Accounts & Contacts	<input type="text" value="contac"/> Showing results for contac	Contacts & Accounts Standard Report Type Start Report
Opportunities	Report Type Name	Category
Forecasts	Contacts & Accounts	Standard
Customer Support Reports	Accounts with Contact Roles	Standard
Leads	Contacts with Assets	Standard
Campaigns	Contact History	Standard
Activities		
Contracts and Orders		
Price Books, Products and Assets		
Administrative Reports		
File and Content Reports		
Quotes		
Individuals		
Other Reports		

- Click the **Filters** tab and change the **Created Date** filter to a date in 2024 and click **Apply**
- Enable **Update Preview Automatically** to view your changes
- Click **Save & Run**, accept the defaults and click **Save**

Note that this report includes almost 1000 rows of sensitive data like names, street addresses, phone numbers, and email addresses, which are considered personally identifiable information (PII) and protected by data privacy laws, including GDPR and CCPA.

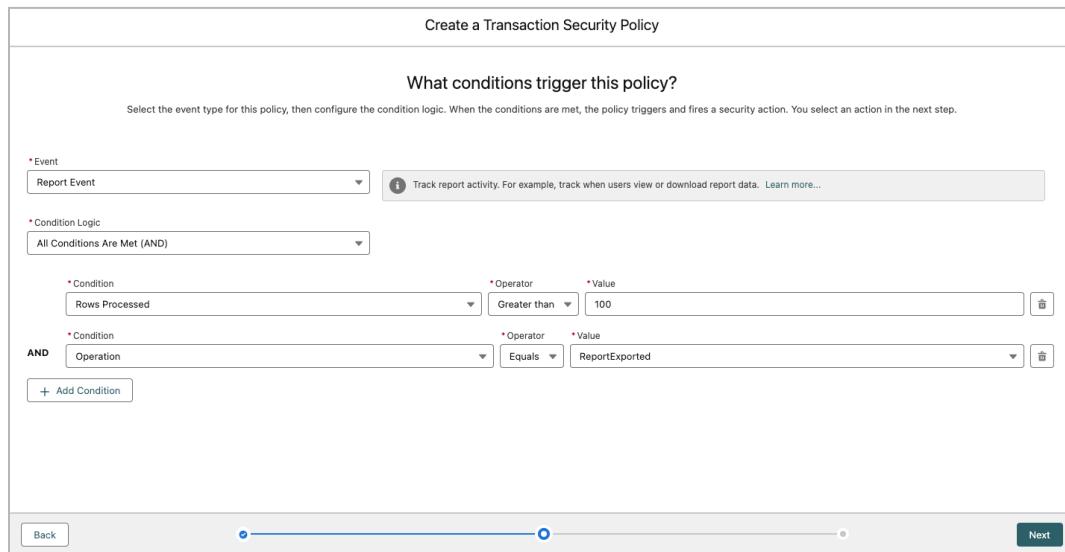
Report: Contacts & Accounts
New Contacts & Accounts Report

Total Records 992

	Salutation	First Name	Last Name	Title	Account Name	Mailing Street	Mailing City	Mailing State/Province	Mailing Zip/Postal Code	Mailing
1	-	Frayda	Dowsing	-	Dowsing Household - 11607054	94046 Grasskamp Junction	Honolulu	Hawaii	96815	United :
2	-	Nedi	Heinsius	-	Heinsius Household - 13487288	75563 Farwell Drive	Peoria	Arizona	85383	United :
3	-	Cornelius	Reape	-	Reape Household - 10274612	77205 Vahlen Court	San Francisco	California	94121	United :
4	-	Iormina	McGinn	-	McGinn Household - 10648549	8 Meadow Vale Center	Louisville	Kentucky	40233	United :
5	-	Barry	Osmant	-	Osmant Household - 10368216	4 Wayridge Crossing	Des Moines	Iowa	50936	United :
6	-	Savina	Solon	-	Solon Household - 10724157	3475 Morning Point	Bridgeport	Connecticut	06606	United :
7	-	Briano	Marnes	-	Marnes Household - 12903684	64266 Everett Park	Waterbury	Connecticut	06705	United :
8	-	Shirlee	Millichap	-	Millichap Household - 11536822	237 Cordelia Drive	Washington	District of Columbia	20370	United :
9	-	Gay	Ragge	-	Ragge Household - 11435758	8 Talisman Plaza	Jacksonville	Florida	32230	United :
10	-	Fabiano	Tall	-	Tall Household - 12470393	3260 Pawling Hill	El Paso	Texas	88579	United :

- In the top-right corner, select the down arrow next to **Edit** and select **Export**
- Select **Details Only** and click **Export**
- Click **Cancel**. You've validated a user could export the report data by getting to the Save dialog
- Create a **Transaction Security Policy** to Block Downloads of Sensitive Data

- Use the App Launcher to Navigate to the Shield app. Enter **Shield** in the search box
- Select the **Event Monitoring** tab
- Click **Transaction Security Policies** in the left navigation pane
- Click the **Enable** button
- Click the **New** button
- Click **Condition Builder** and click **Next**
- On the Create a Transaction Security Policy page, set the following values:
 - Event: **Report Event**
 - Condition Logic: **All Conditions Are Met (AND)**
 - Condition: **Rows Processed**
 - Operator: **Greater than**
 - Value: **100**
 - Click **+Add Condition** 
 - Condition: **Operation**
 - Operator: **Equals**
 - Value: **ReportExported**



The screenshot shows the 'Create a Transaction Security Policy' page. At the top, it says 'What conditions trigger this policy?'. Below that, a note reads: 'Select the event type for this policy, then configure the condition logic. When the conditions are met, the policy triggers and fires a security action. You select an action in the next step.' The configuration area has the following fields:

- Event:** Report Event (dropdown menu with a tooltip: 'Track report activity. For example, track when users view or download report data. Learn more...')
- Condition Logic:** All Conditions Are Met (AND) (dropdown menu)
- Condition:** Rows Processed (dropdown menu)
 - Operator:** Greater than (dropdown menu)
 - Value:** 100 (input field)
- AND** (operator between the first and second conditions)
- Condition:** Operation (dropdown menu)
 - Operator:** Equals (dropdown menu)
 - Value:** ReportExported (input field)
- + Add Condition** (button)

At the bottom, there are 'Back' and 'Next' buttons.

- Click **Next**
- Set the following values:
 - Action: **Block**
 - Custom Block Message: **Download of more than 100 rows not allowed** (feel free to customize this message text)
 - In-App notification: **Checked**
 - Recipient: **OrgFarm EPIC (your User)**
 - Name: **Block large report downloads**
 - Status: click to **Enabled**

Create a Transaction Security Policy

What actions do you want to take when the policy is triggered?
Choose an action and who gets notified when the policy is triggered. To start enforcing the policy right away, enable the policy.

* Action: Block

* Block Message: Custom Block Message
Default Block Message
Custom Block Message (selected)

* Block Message Text: Download of more than 100 rows not allowed

* Notification: In-App notification (selected)
Email notification

* Recipient: OrgFarm EPIC

* Name: Block Large Report Downloads

Description:

Status: Enabled (checked)

Back Finish

- Click **Finish**
- Return to the **Contacts & Accounts report**
- Attempt the download again: click the down arrow next to **Edit** and select **Export**
- You should see a message that the download of large amounts of data is not allowed and the action has been blocked



Transaction Security blocks and/or alerts on risky actions in real-time!

Exercise 4: Shield Field Audit Trail

Salesforce Shield Field Audit Trail is a compliance and governance tool that allows organizations to track the state and value of their data over time. It provides a comprehensive, long-term forensic trail of field-level changes, enabling businesses to satisfy strict regulatory requirements and internal auditing standards.

With Field Audit Trail, administrators can define data retention policies and specify which fields should be tracked for audit purposes across standard and custom objects. This includes the ability to monitor up to 60 fields per object—triple the capacity of standard field history tracking—extending the reach of compliance monitoring to a wider range of business-critical data.

Field Audit Trail provides a verifiable "proof of state" for any record at any point in time. It integrates seamlessly with Salesforce's metadata API, allowing developers and admins to manage retention policies programmatically or through tooling.

Objectives:

- Enable Field Audit Trail
- Track changes on the Contact object's First Name, Last Name and Email fields
- Add the field history component to the Contact Record Page
- Create a report showing all Contact record changes

Estimated Time: 10 minutes

Instructions:

In our use case we have determined that our organization needs to track changes to the contact records in our Salesforce org. Changes to the First Name, Last Name and Email fields of contact records need to be tracked, including when the change was made, who made the change and what the prior value was before the change.

First we'll enable **History Tracking** (Field Audit Trail) in **Setup**, then you add a component to the Contact record Page Layout. Then, you'll edit a contact record to ensure Field Audit Trail is functioning as expected. Finally, you'll create a report to view all contact Field Audit Trail tracked changes.

Start by enabling History Tracking on the Contact object and desired fields.

- Click the **Setup** icon  (it is in the upper right-corner of the browser window) and select **Setup**
- Click the **Object Manager** tab
- Enter **Contact** in the Quick Find
- Click **Contact** in the results to open the Contact object
- Click **Fields & Relationships** in the **Details** panel

- Click Set History Tracking on the top right of the page

Fields & Relationships
37+ Items, Sorted by Field Label

Quick Find New Deleted Fields Field Dependencies Set History Tracking

- Click Enable Contact History to enable it
- Click Email and Name ensuring you have a check in each box
- Click Save

You'll now add the History component to the Page Layout

- Click Page Layouts in the Details panel
- Click the Contact Layout
- On the Contact Layout page scroll down in the list and click Related Lists
- Click and Drag Contact History to the top of the Related Lists section, above Bookings

Save Quick Save Preview As... Cancel Undo Redo Layout Properties

Quick Actions Mobile & Lightning Actions Expanded Lookups Related Lists Report Charts Components

Quick Find		Related List Name *									
		Activity History Campaign History Credits Groups Messaging Users Privacy Holds Work Orders									
		Approval History Cases Data Integration . Guest Reviews Notes & Attachme Service Contracts		Assets Contact History Entitlements HTML Email Statu Open Activities Social Personas		Bookings Content Deliverie Files Messaging Sessi Opportunities Social Posts					

Save Quick Save Preview As... Cancel Undo Redo Layout Properties

Quick Actions Mobile & Lightning Actions Expanded Lookups Related Lists Report Charts Components

Related Lists

Contact History This list is not customizable

Bookings New Change Owner

- Click Save
- Click Yes if prompted to Overwrite Users' Related List Customizations

You'll now verify Field Audit Trail is working correctly

- Click the App Launcher and select Sales
- In the Search bar, type "Sofia" and click the contact record for Sofia Rodriguez

Coral Cloud Resorts

Sales Home Analytics Opportunities

Search: All sofia

Sofia Rodriguez Contact • Rodriguez Household - 12877917 Email: Warm Welcome to Trial OrgFarm For U, Sofia... Task

Do more with Search! Get the right answers by searching... "[user name] leads"

- Click the Related tab

- Notice the **Contact History (0)** list is displayed, this will display the tracked changes
- Click the **Edit** button on the top of the record
- Change Sofia's email address to whatever you'd like
- Change Sofia's name, for example Sophia
- Click **Save**
- The page will update and the **Contact History** list will show your changes including Date, Field Changed, User Name, and the Original and New Values

Contact
Sofia Rodriguez

Details **Related** Activity

We found no potential duplicates of this Contact.

Contact History (3)
3 items • Sorted by Date • Updated 5 minutes ago

Date	Field	User	Original Value	New Value
1 12/16/2025, 1:42 PM	First Name	OrgFarm EPIC	Sophia	Sofia
2 12/16/2025, 1:22 PM	First Name	OrgFarm EPIC	Sofia	Sofia
3 12/16/2025, 1:21 PM	Email	OrgFarm EPIC	sofiarodriguez@example.com	sofiarodriguez@example.com

[View All](#)

Now you'll create a Contact History Report to easily view changes

- Click the **Reports** tab
- Click **New Report**

Search recent reports...

New Report

New Folder

- Click **Accounts & Contacts** in the Category list
- Click **Contact History** in the report type list

Create Report

Category	Select a Report Type	Category
Recently Used	<input type="text" value="Search Report Types..."/>	Standard
All		Standard
Data Cloud		Standard
Accounts & Contacts	Accounts	Standard
	Accounts & Accounts	Standard
	Accounts with Partners	Standard
	Account with Account Teams	Standard
	Accounts with Contact Roles	Standard
	Accounts with Assets	Standard
	Contacts with Assets	Standard
	Account History	Standard
	Contact History	Standard

- Click **Start Report**
- In the report editor enter **Contact ID** in the **Columns** search box

REPORT

New Contact History Report Contact History

Previewing a limited number of records. Run the report to			
	Contact Owner	Edited By	Field / Event
1	Astro Admin	Astro Admin	First Name
2	Astro Admin	Astro Admin	Last Name
3	Astro Admin	Astro Admin	Email
4	Astro Admin	Astro Admin	Email
5	Astro Admin	Astro Admin	Last Name
6	Astro Admin	Astro Admin	Mobile
7	Astro Admin	Astro Admin	First Name
	Astro Admin	Astro Admin	Email

Fields

Outline Filters 1

Groups

GROUP ROWS

Add group... Contact History

Columns

Contact ID Contact History

CONTACT FIELDS

Contact ID

Field / Event Contact ID

- Click the down arrow on **Contact ID**
- Select **Group Rows by This Field**

Update Preview Automatically		
First Name	Last Name	Contact ID
Benjamin		
Benjamin		
Benjamin		
Allyson		
Sophia		

A context menu is open over the third row of the table, specifically over the "Last Name" column cell containing "Benjamin". The menu items are:

- ↑ Sort Ascending
- ↓ Sort Descending
- Group Rows by This Field** (This option is highlighted with a blue box and has a blue arrow pointing to it from above.)
- Group Columns by This Field
- Show Unique Count
- ← Move Left
- Move Right

- Click **Save & Run**
- Accept defaults and click **Save**

Exercise 5: Shield Platform Encryption

Salesforce Shield Platform Encryption is a data protection tool that allows organizations to encrypt sensitive data at rest within their Salesforce org and Data Cloud. It provides an additional layer of security by rendering data unintelligible to anyone or any system that does not have the appropriate decryption keys.

With Shield Platform Encryption, administrators can define encryption policies and specify which fields, files, and attachments should be encrypted in their Salesforce org. This includes standard and custom fields, Communities, and other Salesforce features.

The encryption process is seamless and transparent to users, as Salesforce automatically encrypts and decrypts data as it moves in and out of the platform. Encrypted data remains protected even in backups, exports, and other data operations.

Platform Encryption uses industry-standard AES-256 bit encryption and supports various key management options, including tenant secrets, customer-supplied keys, and key management services like AWS KMS or Azure Key Vault.

Objectives:

- Generate a Tenant Secret
- Enable Encryption Key Management for Data Cloud
- Enable Encryption for Files and Attachments
- Enable Encryption for Sensitive Fields

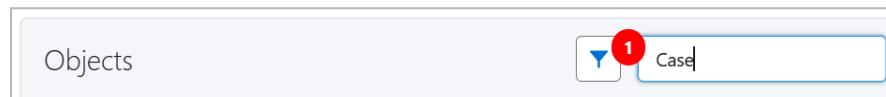
Estimated Time: 10 minutes

Instructions:

In our use case we have determined that our users are inputting sensitive data in a few fields that are associated with cases. In order to protect that sensitive data we are going to encrypt those fields using Platform Encryption.

First we are going to use the **Platform Encryption Analyzer** as part of the **Shield Extension** to verify that we will have no issues with field level encryption for the fields we intend to encrypt.

- Click the **App Launcher** in the upper right hand corner and search for “**Shield Extension**”
- Click on the **Platform Encryption Analyzer**
- After the **Platform Encryption Analyzer** opens, **refresh** your web browser.
- Search for “**Case**” in the **Objects** filter



- Select the **Case** object
- In the **Case Fields** list, select **Description** and **Subject**
- In the **Objects** filter select **Case Comment**
- In the **Case Comment Fields** list select **Body** and **Rich-Text Body**
- Click the **Analyze** button in the upper right corner

You will now see the Analysis job progress. It will take a few minutes for it to complete.

- When analysis is complete
Click **Exit Job Progress**
- The 4 fields we have selected are clear for encryption. You can see the results by selecting the **Case** and **Case Comment** objects and verifying the green checkbox in the results column.

Now we are going to enable Platform Encryption and encrypt those fields as well as encrypt our Data Cloud instance.

- Use the App Launcher to navigate to the **Shield app**
- Select the **Platform Encryption** tab
- Select **Key Management** in the left navigation bar
- Click **Generate Tenant Secret** 

Key Management Table							Key Management Help ?
Encrypts data using the probabilistic encryption scheme, including data in fields, files and attachments, and files other than search index files.							
Fields and Files (Probabilistic)		Search Index	Event Bus				
Actions	Version	Tenant Secret Type	Status	Key Material Source	Key Derivation	Created By	Last Modified By
Export	1	Fields and Files (Probabilistic)	Active	HSM	✓	Admin User, 2/14/2024, 10:11 AM	Admin User, 2/14/2024, 10:11 AM

- In the Setup Quick Find box, Search for “**Encryption**”
- Click **Encryption Settings**
- In the **Encryption Policy** section turn on following settings:
 - Manage Data Cloud Keys
 - Encrypt Files and Attachments
- Scroll down to “**Advanced Encryption Settings**” and turn on the following settings
 - **Restrict Access to Encryption Policy Settings**
 - Encrypt Standard Fields → Click **Select Fields** 
 - On the next screen - Click **Edit** 
 - Scroll down to **Case** and select the “**Subject**” and “**Description**” fields
 - On **Case Comment** select the **Body** and **Rich-Text Body** fields
 - You should have the following fields checked:

Case
<input checked="" type="checkbox"/> Subject
<input checked="" type="checkbox"/> Description
Case Comment
<input checked="" type="checkbox"/> Body
<input checked="" type="checkbox"/> Rich-Text Body

- Click **Save** 
- Go back to the **Key Management** settings
- You will now see two sections for Key Management, one for Salesforce Platform and one for Data Cloud



- Select the **Data Cloud Tab**
- Salesforce generates a root key for you. This triggers the encryption of all previously ingested data in Data Cloud.



Congratulations! You have now encrypted sensitive data in both the Salesforce Core Platform and Data Cloud

Exercise 6: Privacy Center

Salesforce Privacy Center is a centralized hub that helps organizations manage and maintain compliance with various data privacy regulations, such as the General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA). It provides a single point of control for managing data privacy requests, consent tracking, and preference management within the Salesforce ecosystem. This also ensures that data being used for Agentforce is up to date to ensure agent accuracy.

With Privacy Center, organizations can streamline the process of handling data subject requests, such as requests for access, deletion, or rectification of personal data. Users can submit requests through a self-service portal, and administrators can manage and track the fulfillment of these requests from within Privacy Center.

Privacy Center also enables organizations to capture and manage individual consent preferences, ensuring that personal data is processed and used in accordance with the consent provided by individuals. This includes tracking consent for marketing communications, data sharing, and other relevant activities.

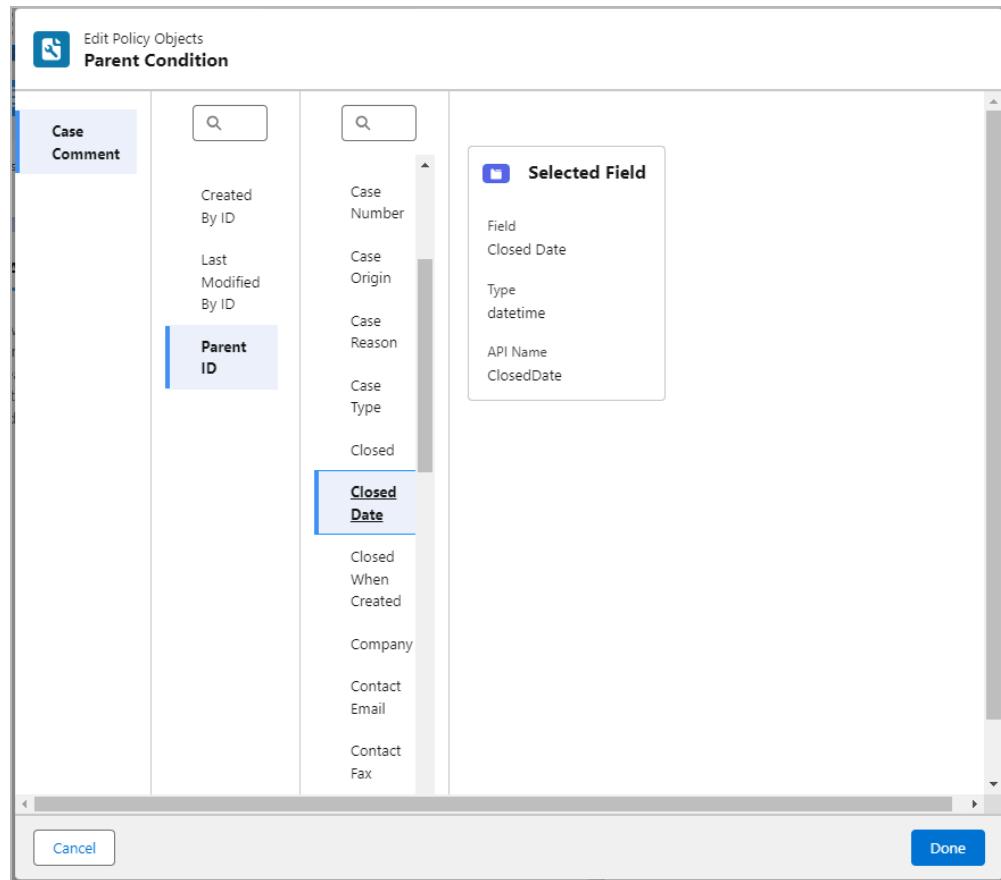
Additionally, Privacy Center complements other Salesforce features, such as Salesforce Shield and Data Detect, to provide a comprehensive data governance and compliance solution. It supports audit trails, encryption, and data masking, further enhancing data privacy and security within the Salesforce platform.

- **What to do:** You will create a case Data Management policy to delete old cases in order to ensure accuracy of data used in Generative AI workloads
- **Value of it:** Understand how to configure data management policies
- **Tools used:** Privacy Center
- **Time to Complete:** 15 minutes

Instructions:

- Create a Data Management Policy to delete any Case Comment records associated with cases that have been closed for more than three years
 - Use the **App Launcher** to navigate to the **Privacy Center** app
 - Click the link **Go to Data Management Policies**
 - Click **New**
 - Select **Data Management Policy** and click **Next**
 - For **Data Management Policy Name**, enter “Cases - delete comments 3 years after closed”
 - Click **Save**
 - Under **Active Objects**, click **Add Object**
 - In the Quick Find box under **Available Objects**, type “Case”, and then select the **Case Comment** Object

- Click **Next**
- On the **Apply data filters** page, click the **Add Parent Condition** button
- Click **Parent ID**, then click **Closed Date**, and click **Done**



- On the **Apply data filters** page, set the **Operator** to "is beyond the last"
- Set **Number of Days Relative to Policy Execution Date** to "3"
- Set **Criteria** to "Years"

Apply data filters
Create a data filter to capture the data you want. Use conditions to indicate which object fields are processed when the policy is run.

Filter conditions

Apply Policy
When All Conditions are Met

Object Field (Parent Condition) * Operator * Number of Years Relative to Policy Execution Date
Apply when:
ParentId.ClosedDate is beyond ... 3 Criteria Years

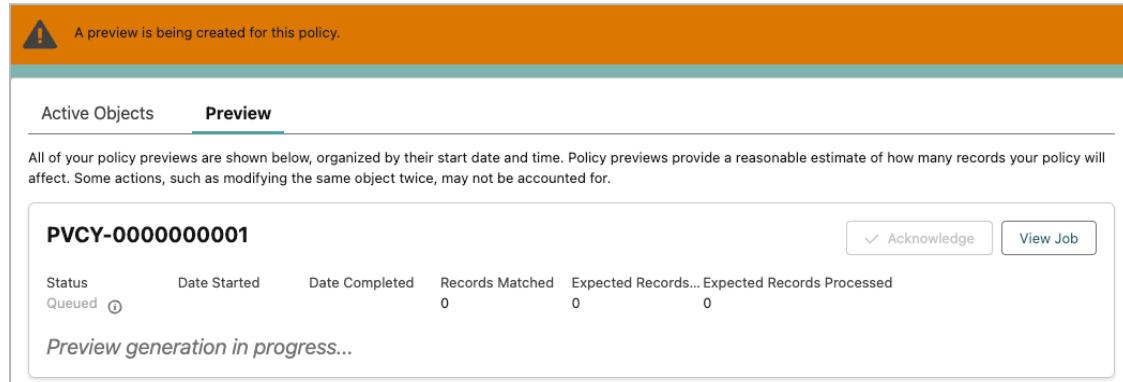
+ Add Condition Add Parent Condition Q Add Cross-Object Query

Summary (Note: This content is for informational purposes and isn't a valid SOQL query.)
ParentId.ClosedDate < LAST_N_YEARS:3

Back Next

- Click **Next**
- On the **Add data transformation rules** page, scroll to the bottom, and next to **Action on Files and Attachments**, choose **Delete All**
- Click **Next**
- Click **Done**
- Delete any Case records that have been closed for more than three years
 - Click **Add Object**
 - In the **Available Objects** Quick Find box, type “Case” and select the **Case** Object
 - Click **Next**
 - Click **+ Add Condition**
 - For **Object Field**, select the **Closed Date (DATETIME)** field
 - For **Operator**, select “is beyond the last”
 - For **Number of Days**, enter “3”
 - Set **Criteria** to “Years”
 - Click **Next**
 - Click **Next**
 - Click **Done**

- Click 
- Click  on the top right of the page
- Click  Generation may take a minute
- Click the **Preview** tab

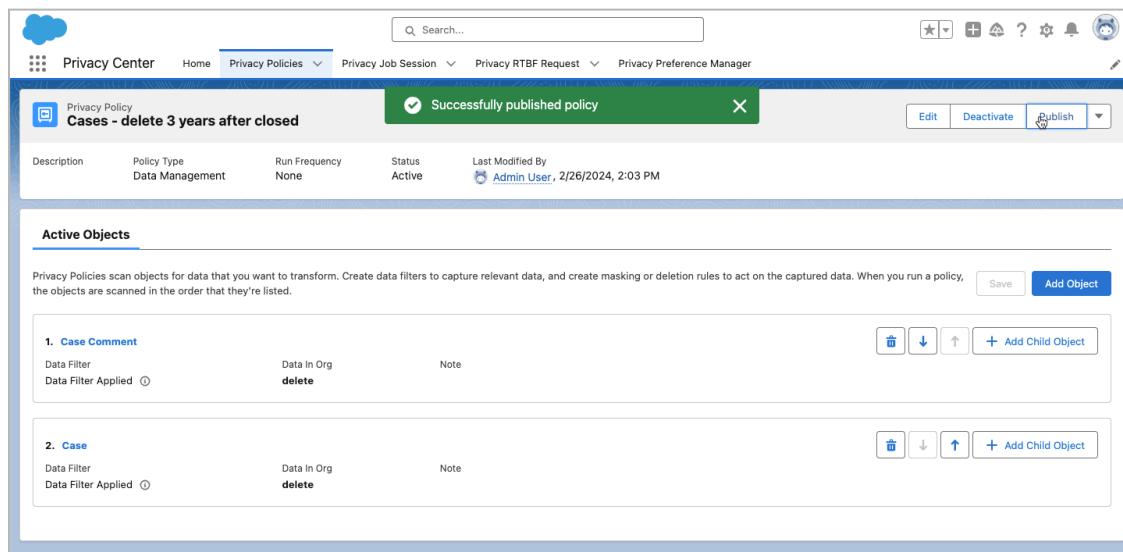


A preview is being created for this policy.

PVCY-00000000001

Status: Queued Date Started: Date Completed: Records Matched: 0 Expected Records...: 0 Expected Records Processed: 0

Preview generation in progress...



Successfully published policy

Cases - delete 3 years after closed

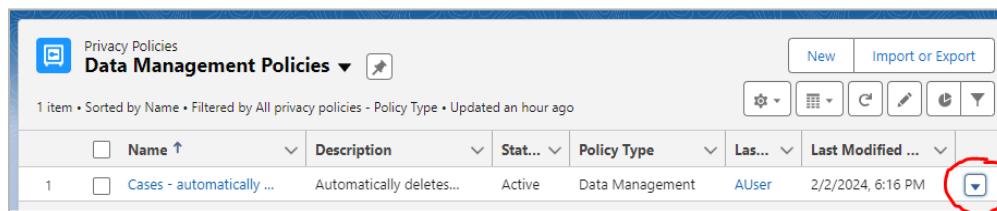
Description: Policy Type: Data Management Run Frequency: None Status: Active Last Modified By: Admin User, 2/26/2024, 2:03 PM

Active Objects

Privacy Policies scan objects for data that you want to transform. Create data filters to capture relevant data, and create masking or deletion rules to act on the captured data. When you run a policy, the objects are scanned in the order that they're listed.

Object Type	Data Filter	Data In Org	Note	Action Buttons
1. Case Comment	Data Filter Data Filter Applied: 	delete		    
2. Case	Data Filter Data Filter Applied: 	delete		    

- Schedule your policy to run on a regular basis
 - Click the **Privacy Policies** tab
 - Click the down-arrow (right-hand side) next to your newly saved policy and select **Edit**



Data Management Policies

1 item • Sorted by Name • Filtered by All privacy policies - Policy Type • Updated an hour ago

Name	Description	Status	Policy Type	Last Modified	Action
Cases - automatically ...	Automatically deletes...	Active	Data Management	AUser 2/2/2024, 6:16 PM	

- Under **Run Frequency**, set the Interval to **Run Weekly**
- Set the start date and time to this Friday at 7 pm

- Tick the checkboxes at the bottom of the page to delete records from the related history object, delete records from Field Audit Trail, and permanently delete records rather than move them to the recycle bin.

Run Frequency

Start date and time

Interval: Run Weekly Date: Jun 7, 2024 Time: 7:00 PM

Action on Associated Records

Indicate whether to delete associated records captured by the policy.

Delete records from related history object
 Delete records from Field Audit Trail
 Permanently delete records

- Click Save



Note: Privacy Center includes the ability address Data Subject Requests as well as data minimization.

Want to learn more?

As the capabilities of Einstein and Salesforce Trusted Services continue to expand, Salesforce is providing a growing set of enablement offerings to help customers maximize the value of the platform. A wide range of resources are now available to learn more about getting started with AI and closing the trust gap.

Trailhead

There are many courses on **Trailhead** to help you get up to speed. Check out some Trailmixes at <http://sfdc.co/tai-thsec>.

Community Groups

You are not alone. People all over the world are learning about AI and Security. Salesforce has a forum for those people (and you) to discuss and learn.

- Join the Einstein Group: <http://sfdc.co/tai-einsteingroup>
- Join the Salesforce Shield and Security Center Group: <http://sfdc.co/tai-shieldgroup>

Documentation

- Add Intelligence To Your Apps: <http://sfdc.co/tai-intelligent>
- Einstein Generative AI: <http://sfdc.co/tai-genai>
- Sales Cloud Einstein: <http://sfdc.co/tai-sales>
- Shield Learning Map: <https://shieldlearningmap.com/>
- Security Center: <http://sfdc.co/tai-securitycenter>
- Privacy Center: <http://sfdc.co/tai-privacycenter>
- Salesforce Backup: <http://sfdc.co/tai-backup>

Certification Support

- Salesforce Certified AI Associate credential: <http://sfdc.co/tai-aiassociate>
- Salesforce Certified AI Specialist credential: <http://sfdc.co/tai-aispecialist>

Get a Copy of This Guide:

- Download a copy of this guide from: <http://sfdc.co/tai-guide>
- Get a copy of the workshop presentation: <http://sfdc.co/tai-preso>

Where Do We Go From Here?

Reach out to your Account Executive today to schedule a customized session with our Security Architects. Together, we'll explore how you can close the trust gap at your own company with the Einstein Trust Layer and Salesforce Trusted Services.