Audit Record Deletions in Sensitive Tables

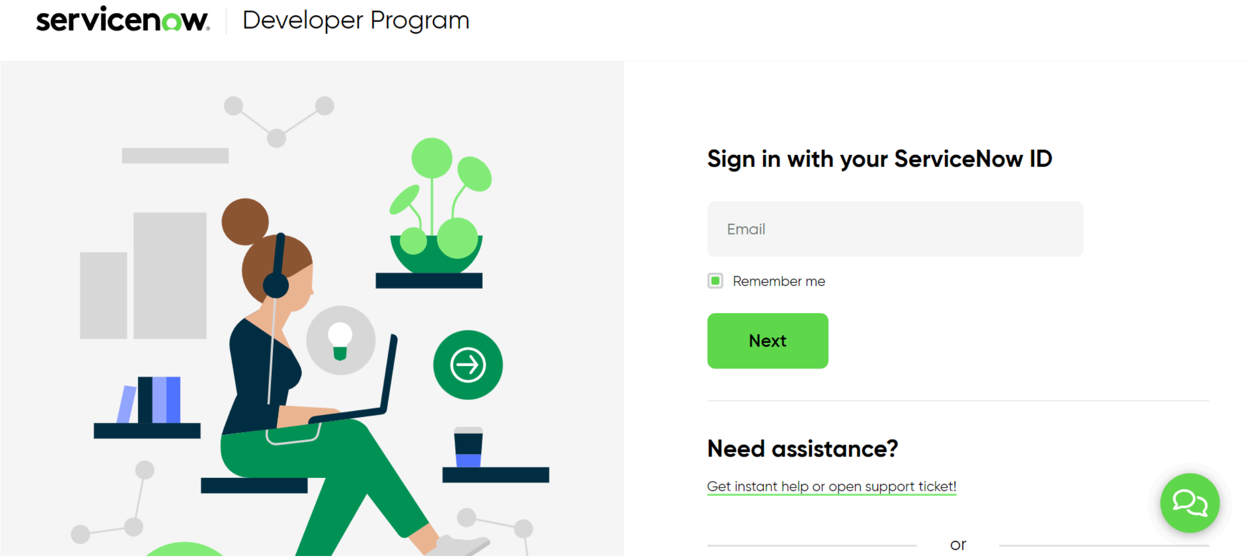
User Story: When records in sensitive tables (e.g., `sys_user`, `incident`, `cmdb_ci`) are deleted, automatically log the deletion details (who, when, what record) in a separate audit table. Additionally, notify the compliance team of any deletions for further review.

Objective:Automatically log details of record deletions in sensitive tables to maintain data integrity and ensure compliance. Notify the compliance team for timely review and action on deletion activities.

Skills: Business rule, Scripting, (GlideRecord), and notifications in ServiceNow.

Solution:

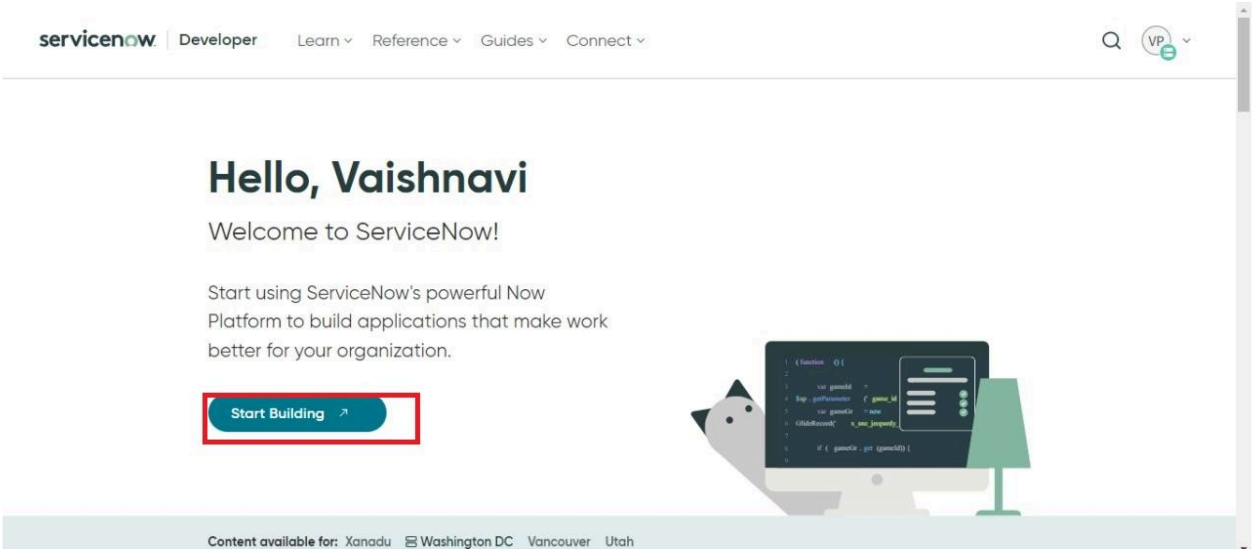
Step 1 : Sign into ServiceNow.


servicenow | Developer Program
Sign in with your ServiceNow ID
Email
Remember me
Next
Need assistance?
Get instant help or open support ticket!
or

Step 2 : Sign up for a developer account on the ServiceNow Developer site "https://developer.servicenow.com".

Step 3 : Once logged in, navigate to the "Personal Developer Instance" section.

Click on "Request Instance" to create a new ServiceNow instance.



Hello, Vaishnavi

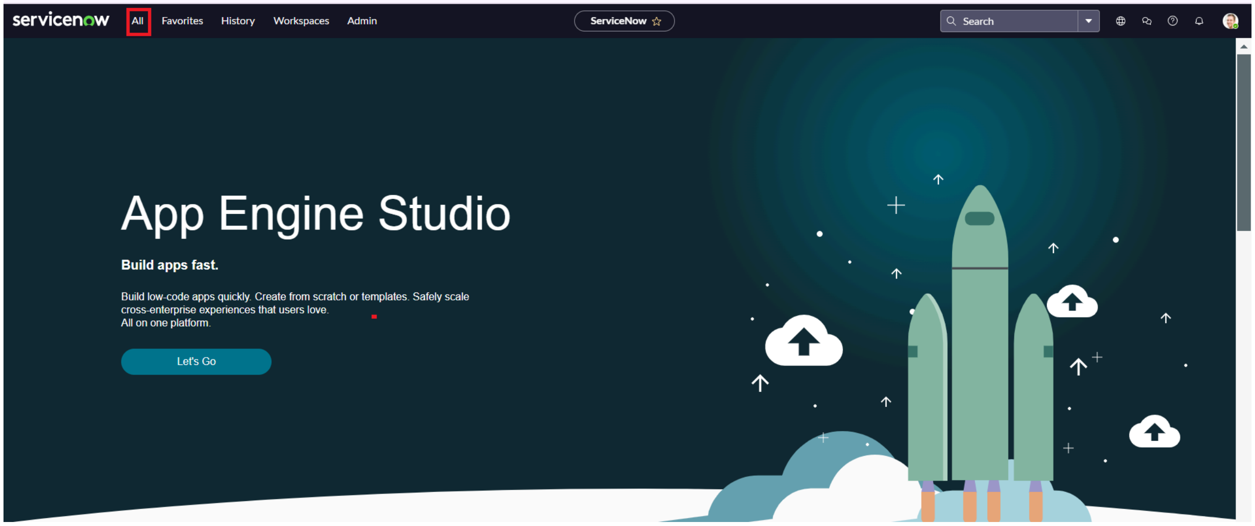
Welcome to ServiceNow!

Start using ServiceNow's powerful Now Platform to build applications that make work better for your organization.

Step 4 : Fill out the required information and submit the request.

Step 5 : You'll receive an email with the instance details once it's ready.

Step 6 : Log in to your ServiceNow instance using the provided credentials.
Now you will navigate to the ServiceNow.

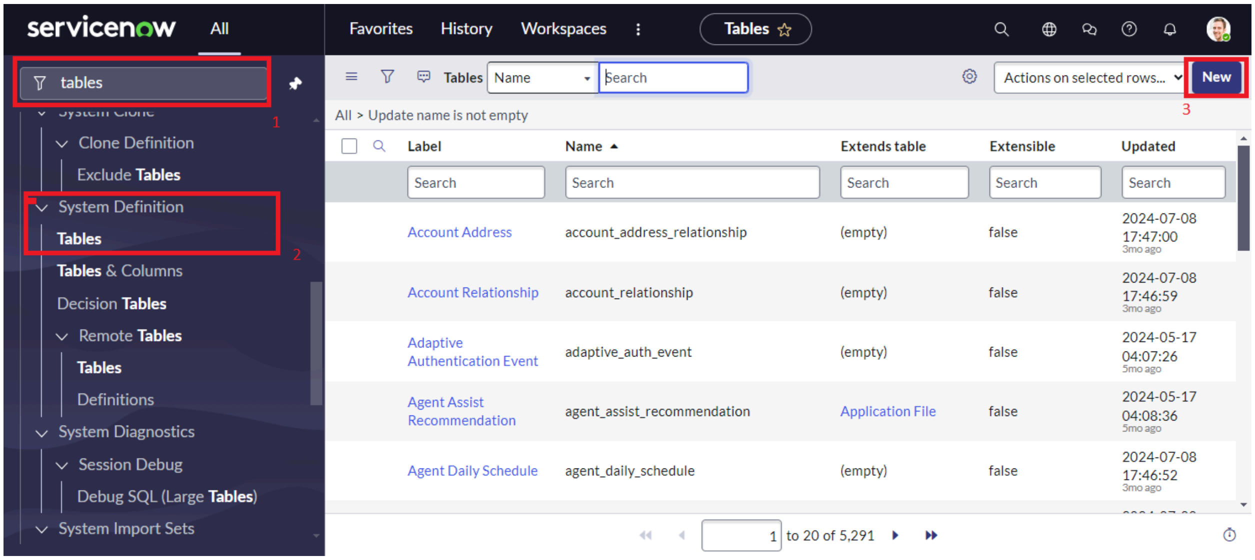


App Engine Studio

Build apps fast.

Build low-code apps quickly. Create from scratch or templates. Safely scale cross-enterprise experiences that users love.
All on one platform.

Step 7 : Open tables Under System Definition” >> Tables.Click on New.

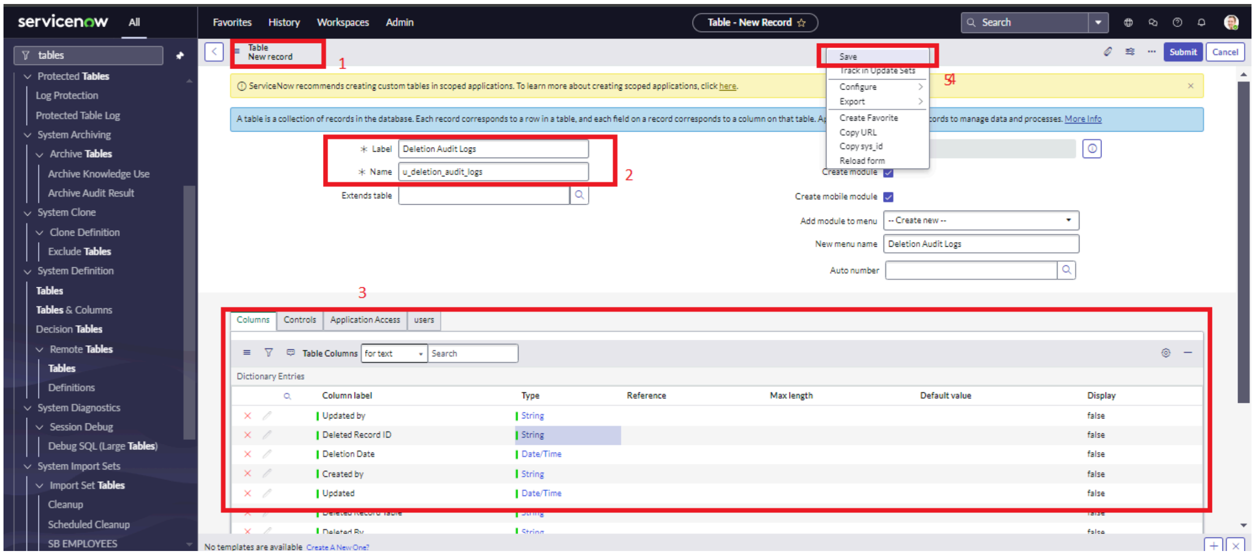


Label	Name ▲	Extends table	Extensible	Updated
Account Address	account_address_relationship	(empty)	false	2024-07-08 17:47:00 3mo ago
Account Relationship	account_relationship	(empty)	false	2024-07-08 17:46:59 3mo ago
Adaptive Authentication Event	adaptive_auth_event	(empty)	false	2024-05-17 04:07:26 5mo ago
Agent Assist Recommendation	agent_assist_recommendation	Application File	false	2024-05-17 04:08:36 5mo ago
Agent Daily Schedule	agent_daily_schedule	(empty)	false	2024-07-08 17:46:52 3mo ago

Step 8 : Fill the details as below

A) Label : deletion audit logs

B) Create fields deleted by,deletion date,deleted record date,deletion time.



ⓘ ServiceNow recommends creating custom tables in scoped applications. To learn more about creating scoped applications, click here.

A table is a collection of records in the database. Each record corresponds to a row in a table, and each field on a record corresponds to a column on that table. A… …cords to manage data and processes. More Info

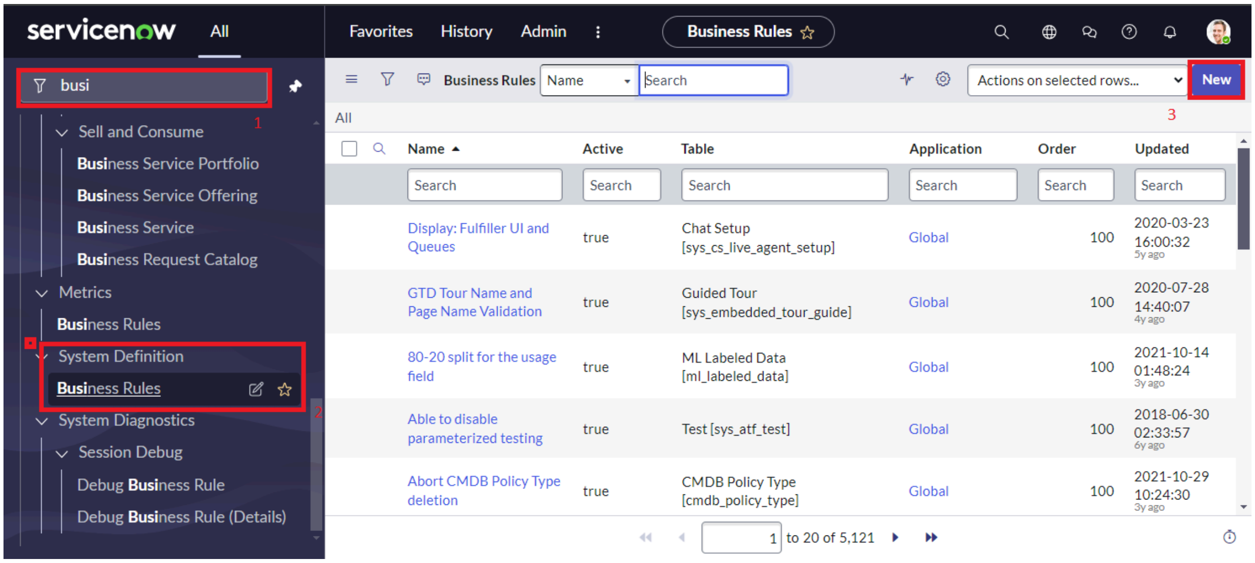
✱ Label	Deletion Audit Logs
✱ Name	u_deletion_audit_logs
Extends table	
Create module	☑
Create mobile module	☑
Add module to menu	-- Create new --
New menu name	Deletion Audit Logs
Auto number	

Dictionary Entries

Column label	Type	Reference	Max length	Default value	Display
Updated by	String				false
Deleted Record ID	String				false
Deletion Date	Date/Time				false
Created by	String				false
Updated	Date/Time				false
Deleted Record Table	String				false
Deleted By	String				false

No templates are available Create A New One?

Step 9 : Open business rules Under System Definition" >>Business Rules

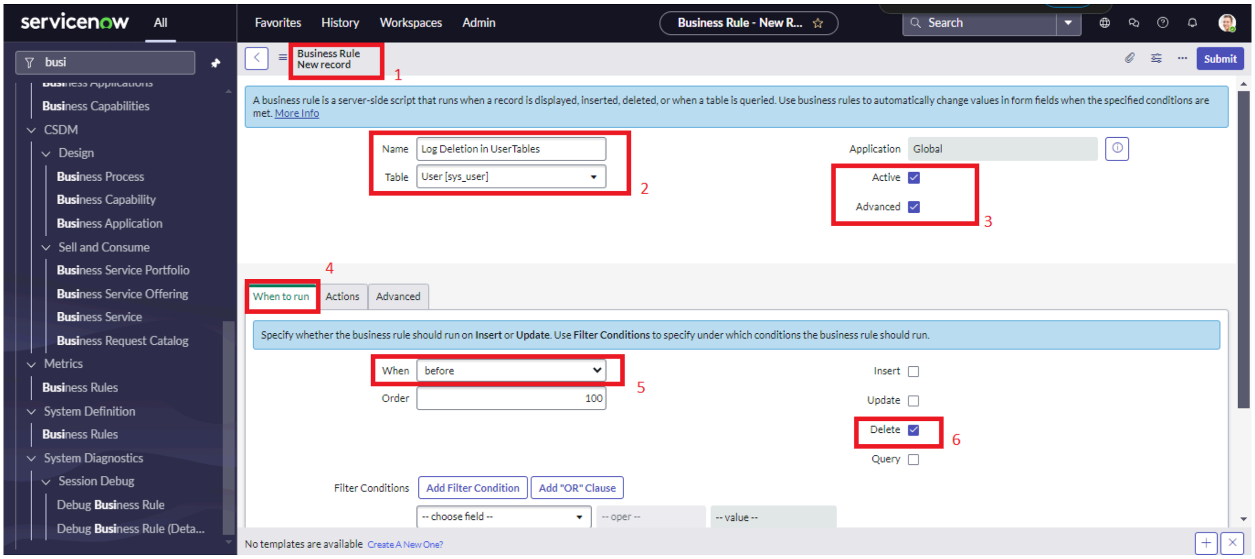


Name	Active	Table	Application	Order	Updated
Display: Fulfiller UI and Queues	true	Chat Setup [sys_cs_live_agent_setup]	Global	100	2020-03-23 16:00:32 5y ago
GTD Tour Name and Page Name Validation	true	Guided Tour [sys_embedded_tour_guide]	Global	100	2020-07-28 14:40:07 4y ago
80-20 split for the usage field	true	ML Labeled Data [ml_labeled_data]	Global	100	2021-10-14 01:48:24 3y ago
Able to disable parameterized testing	true	Test [sys_atf_test]	Global	100	2018-06-30 02:33:57 6y ago
Abort CMDB Policy Type deletion	true	CMDB Policy Type [cmdb_policy_type]	Global	100	2021-10-29 10:24:30 3y ago

1 to 20 of 5,121

Step 10 : Fill in the details as below.

1. Name : Log deletion in UserTables
2. Table : user[sys_user]
3. Check the active box
4. Under the when to run section select before and check delete box
5. Write business rule code in advanced section .Save and Submit.



A business rule is a server-side script that runs when a record is displayed, inserted, deleted, or when a table is queried. Use business rules to automatically change values in form fields when the specified conditions are met. More Info

Name: Log Deletion in UserTables
Table: User [sys_user]
Application: Global
Active ☑
Advanced ☑

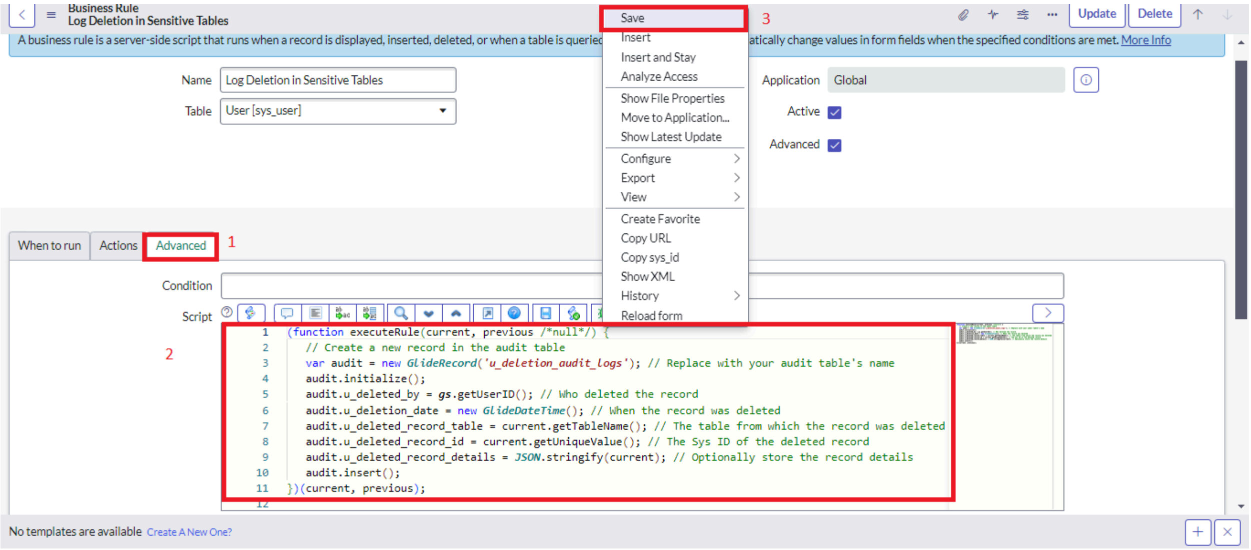
Specify whether the business rule should run on **Insert** or **Update**. Use **Filter Conditions** to specify under which conditions the business rule should run.

When: before
Order: 100
Insert □
Update □
Delete ☑
Query □
Filter Conditions

No templates are available

CODE:

```
(function executeRule(current, previous /*null*/) {
   // Create a new record in the audit table
   var audit = new GlideRecord('u_deletion_audit_logs'); // Replace with
your audit table's name
   audit.initialize();
   audit.u_deleted_by = gs.getUserID(); // Who deleted the record
   audit.u_deletion_date = new GlideDateTime(); // When the record was
deleted
   audit.u_deleted_record_table = current.getTableName(); // The table
from which the record was deleted
   audit.u_deleted_record_id = current.getUniqueValue(); // The Sys ID of
the deleted record
   audit.u_deleted_record_details = JSON.stringify(current); // Optionally
store the record details
   audit.insert();
})(current, previous);
```



A business rule is a server-side script that runs when a record is displayed, inserted, deleted, or when a table is queried ... atically change values in form fields when the specified conditions are met. More Info

Name: Log Deletion in Sensitive Tables

Table: User [sys_user]

Application: Global

Active ☑

Advanced ☑

Condition:

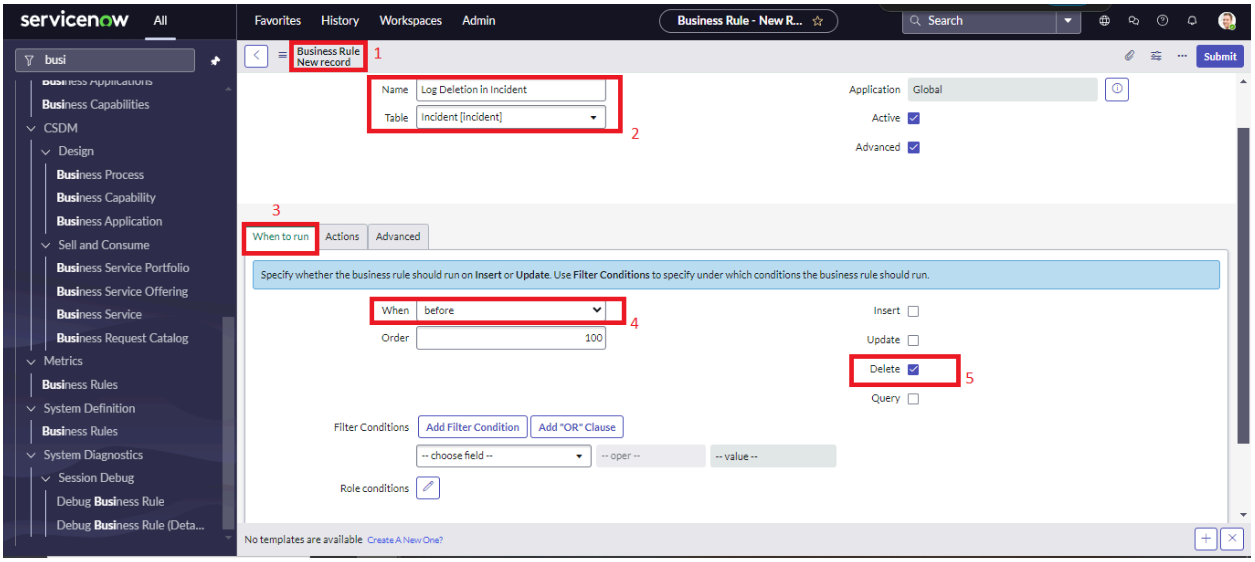
Script:

```
(function executeRule(current, previous /*null*/) {
   // Create a new record in the audit table
   var audit = new GlideRecord('u_deletion_audit_logs'); // Replace with your audit table's name
   audit.initialize();
   audit.u_deleted_by = gs.getUserID(); // Who deleted the record
   audit.u_deletion_date = new GlideDateTime(); // When the record was deleted
   audit.u_deleted_record_table = current.getTableName(); // The table from which the record was deleted
   audit.u_deleted_record_id = current.getUniqueValue(); // The Sys ID of the deleted record
   audit.u_deleted_record_details = JSON.stringify(current); // Optionally store the record details
   audit.insert();
})(current, previous);
```

No templates are available

Step 11 : Create a new business rule for the incident table.Fill in the details as below.

1. Name : Log deletion in Incident
2. Table : incident[incident]
3. Check the active box
4. Under the when to run section select before and check delete box
5. Write business rule code in advanced section .Save and Submit.



Business Rule
New record

Name: Log Deletion in Incident

Table: Incident [incident]

Application: Global

Active ☑

Advanced ☑

When to run | Actions | Advanced

Specify whether the business rule should run on **Insert** or **Update**. Use **Filter Conditions** to specify under which conditions the business rule should run.

When: before

Order: 100

Insert □

Update □

Delete ☑

Query □

Filter Conditions: Add Filter Condition | Add "OR" Clause

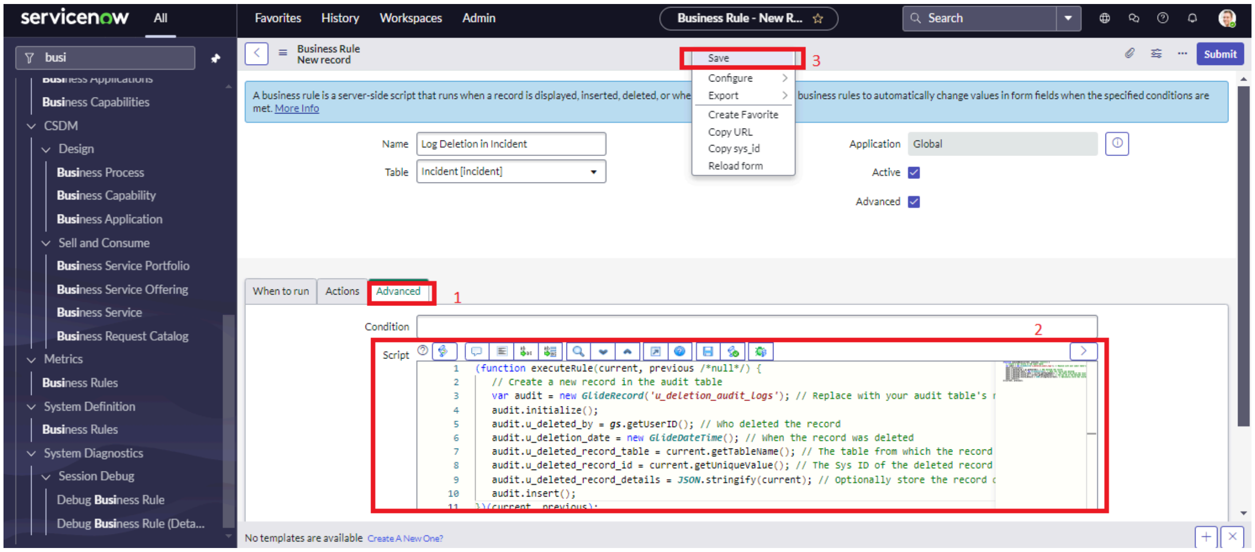
-- choose field -- | -- oper -- | -- value --

Role conditions

No templates are available Create A New One?

CODE:

```
(function executeRule(current, previous /*null*/) {
   // Create a new record in the audit table
   var audit = new GlideRecord('u_deletion_audit_logs'); // Replace with
your audit table's name
   audit.initialize();
   audit.u_deleted_by = gs.getUserID(); // Who deleted the record
   audit.u_deletion_date = new GlideDateTime(); // When the record was
deleted
   audit.u_deleted_record_table = current.getTableName(); // The table
from which the record was deleted
   audit.u_deleted_record_id = current.getUniqueValue(); // The Sys ID of
the deleted record
   audit.u_deleted_record_details = JSON.stringify(current); // Optionally
store the record details
   audit.insert();
})(current, previous);
```



A business rule is a server-side script that runs when a record is displayed, inserted, deleted, or whe... business rules to automatically change values in form fields when the specified conditions are met. More Info

Name: Log Deletion in Incident

Table: Incident [incident]

Application: Global

Active ☑

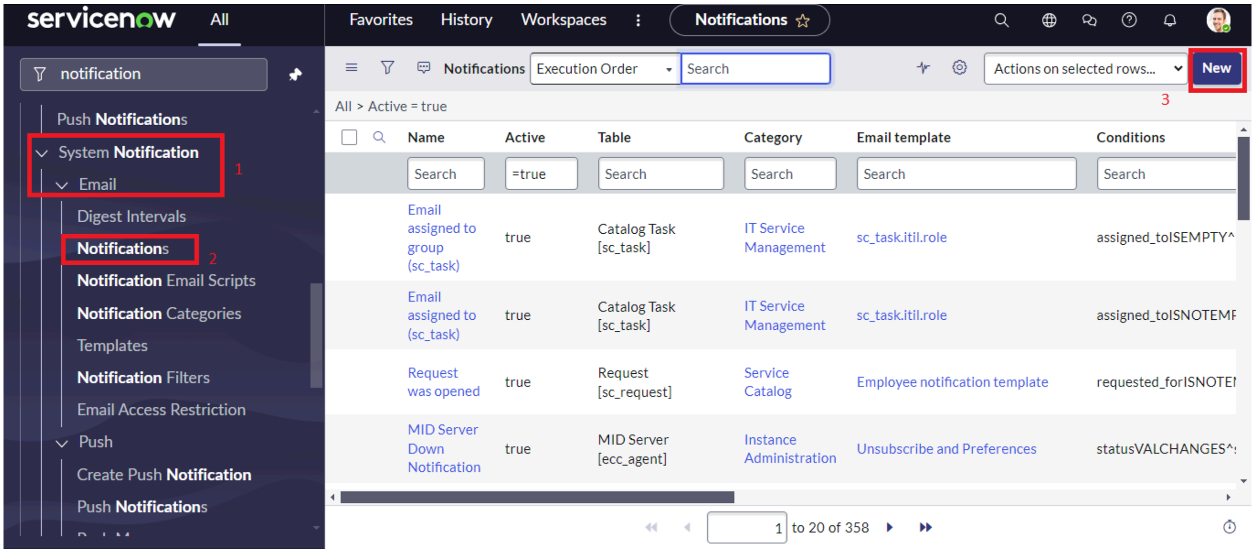
Advanced ☑

Condition:

Script:

```
(function executeRule(current, previous /*null*/) {
    // Create a new record in the audit table
    var audit = new GlideRecord('u_deletion_audit_logs'); // Replace with your audit table's r
    audit.initialize();
    audit.u_deleted_by = gs.getUserID(); // Who deleted the record
    audit.u_deletion_date = new GlideDateTime(); // When the record was deleted
    audit.u_deleted_record_table = current.getTableName(); // The table from which the record
    audit.u_deleted_record_id = current.getUniqueValue(); // The Sys ID of the deleted record
    audit.u_deleted_record_details = JSON.stringify(current); // Optionally store the record c
    audit.insert();
})(current, previous);
```

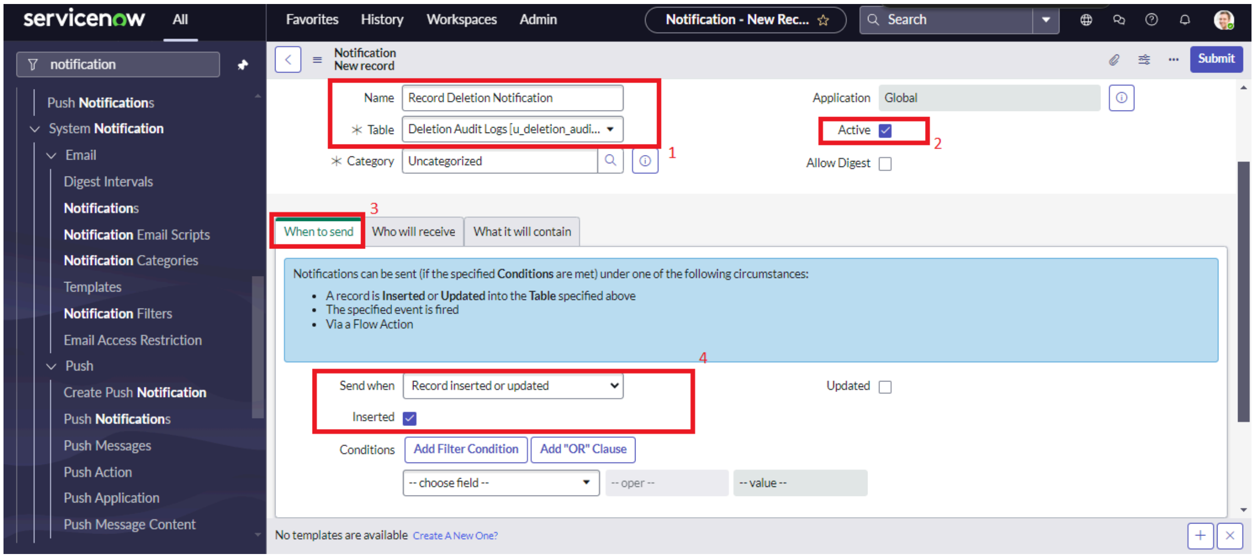
Step 12 : Open notifications Under System Definition" >>Email>>Notifications.Click on new.



Name	Active	Table	Category	Email template	Conditions
Search	=true	Search	Search	Search	Search
Email assigned to group (sc_task)	true	Catalog Task [sc_task]	IT Service Management	sc_task.itil.role	assigned_toISEMPTY^
Email assigned to (sc_task)	true	Catalog Task [sc_task]	IT Service Management	sc_task.itil.role	assigned_toISNOTEMF
Request was opened	true	Request [sc_request]	Service Catalog	Employee notification template	requested_forISNOTEI
MID Server Down Notification	true	MID Server [ecc_agent]	Instance Administration	Unsubscribe and Preferences	statusVALCHANGES^

Step 13: Fill in the details in the

1. Name : Record deletion notification
2. Table : deletion audit logs table
3. when to send' : record is inserted or updated
4. 'who will receive' : select a user and
5. 'what will it contain' : include the message



Notification
New record

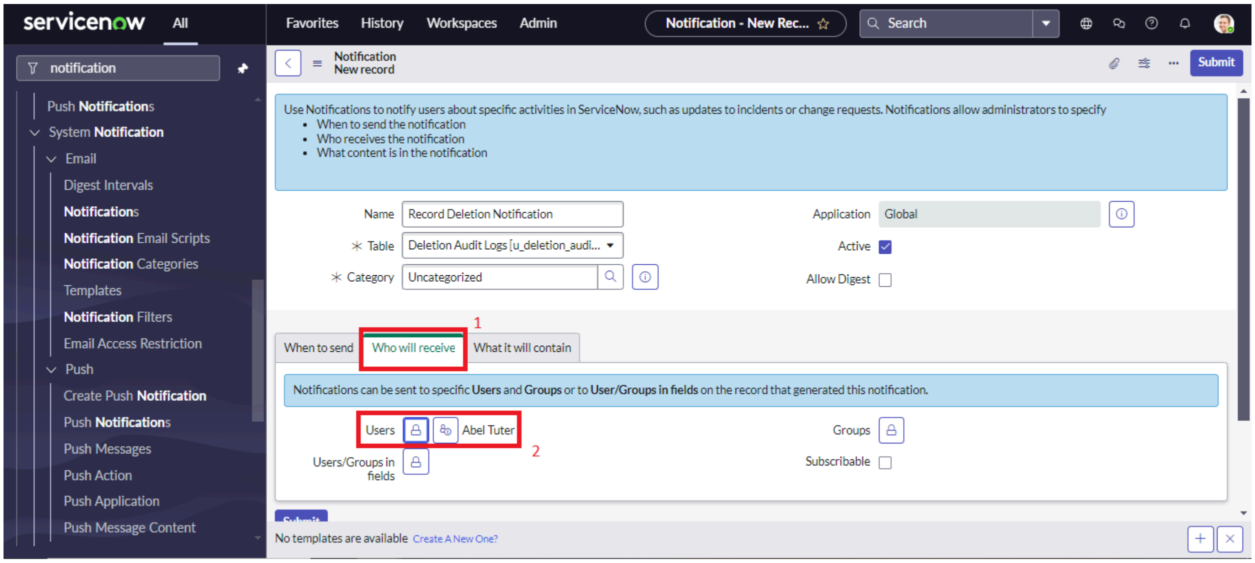
Name	Record Deletion Notification	Application	Global
* Table	Deletion Audit Logs [u_deletion_audi...	Active	☑
* Category	Uncategorized	Allow Digest	□

Notifications can be sent (if the specified **Conditions** are met) under one of the following circumstances:

- A record is **Inserted** or **Updated** into the **Table** specified above
- The specified event is fired
- Via a Flow Action

Send when	Record inserted or updated	Updated	□
Inserted	☑		
Conditions	-- choose field --	-- oper --	-- value --

No templates are available Create A New One?



Notification
New record

Use Notifications to notify users about specific activities in ServiceNow, such as updates to incidents or change requests. Notifications allow administrators to specify

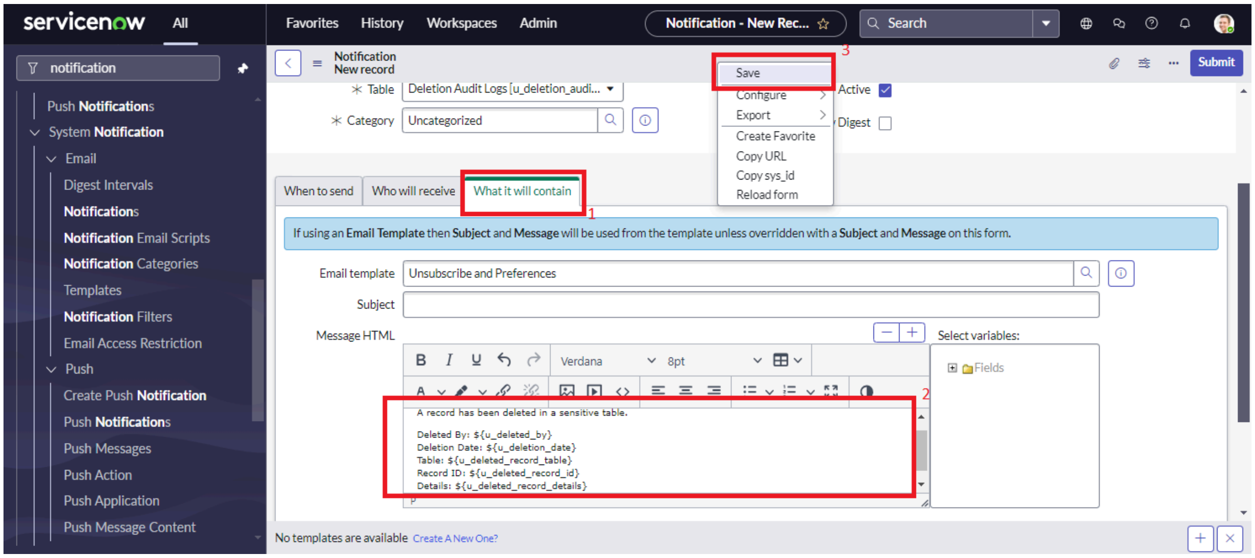
- When to send the notification
- Who receives the notification
- What content is in the notification

Name	Record Deletion Notification	Application	Global
* Table	Deletion Audit Logs [u_deletion_audi...	Active	☑
* Category	Uncategorized	Allow Digest	□

Notifications can be sent to specific **Users** and **Groups** or to **User/Groups in fields** on the record that generated this notification.

Users	Abel Tuter	Groups	
Users/Groups in fields		Subscribable	□

No templates are available Create A New One?



* Table: Deletion Audit Logs [u_deletion_audi...

* Category: Uncategorized

Active ☑

Digest □

If using an Email Template then Subject and Message will be used from the template unless overridden with a Subject and Message on this form.

Email template: Unsubscribe and Preferences

Subject:

Message HTML:

```
A record has been deleted in a sensitive table.

Deleted By: ${u_deleted_by}
Deletion Date: ${u_deletion_date}
Table: ${u_deleted_record_table}
Record ID: ${u_deleted_record_id}
Details: ${u_deleted_record_details}
```

No templates are available Create A New One?

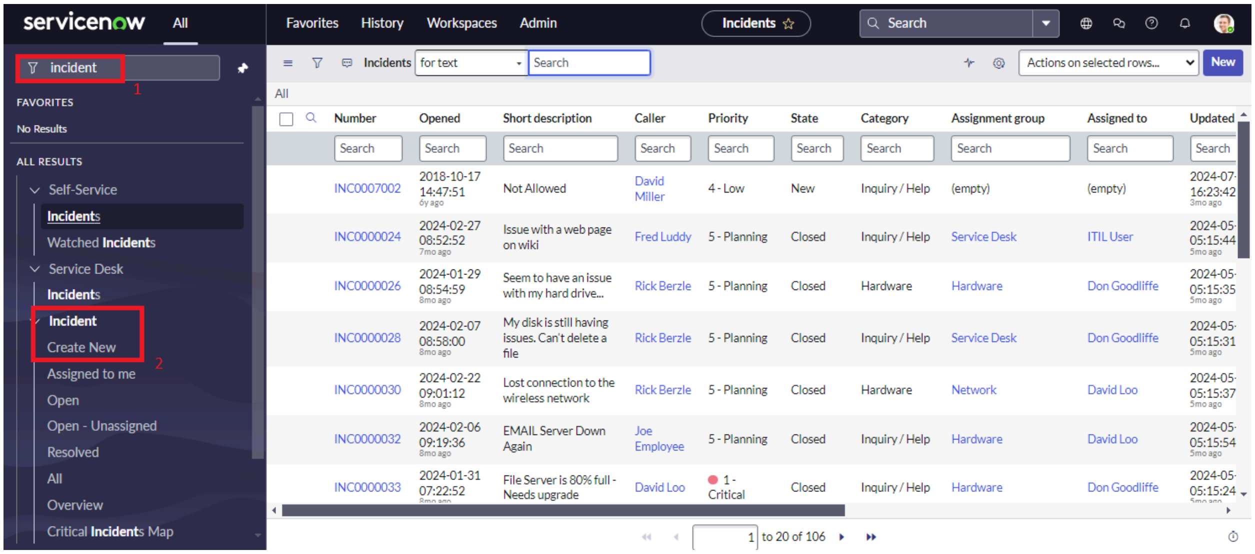
HTML Message:

A record has been deleted in a sensitive table.

Deleted By: ${u_deleted_by}
Deletion Date: ${u_deletion_date}
Table: ${u_deleted_record_table}
Record ID: ${u_deleted_record_id}
Details: ${u_deleted_record_details}

Result：

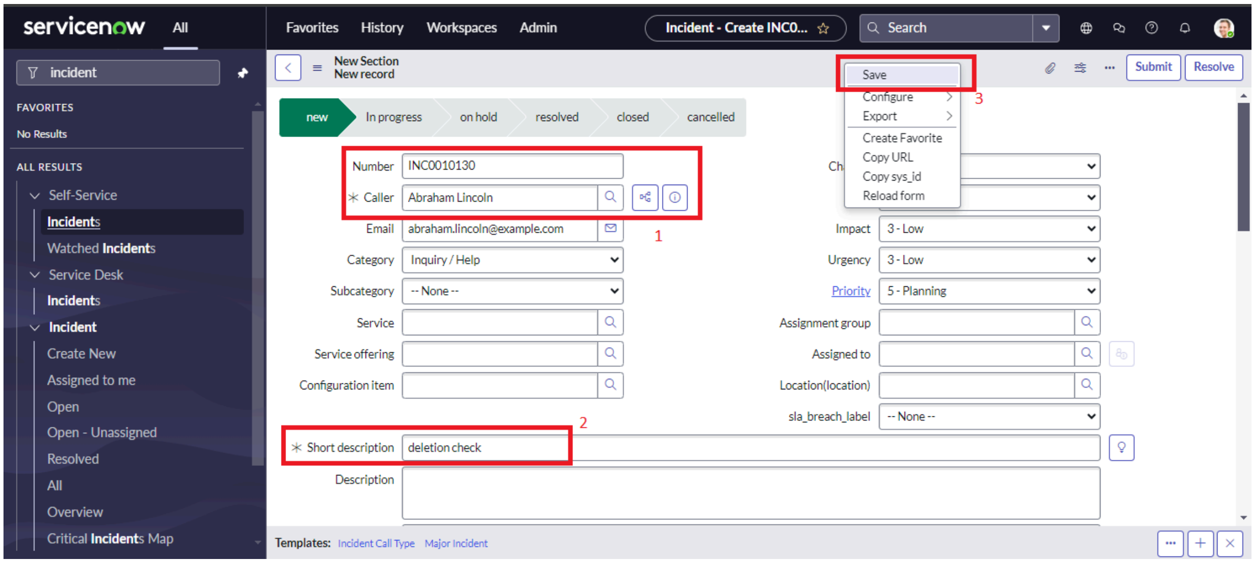
Step 1: Open incident >> all . Click on New.



Number	Opened	Short description	Caller	Priority	State	Category	Assignment group	Assigned to	Updated
INC0007002	2018-10-17 14:47:51 6y ago	Not Allowed	David Miller	4 - Low	New	Inquiry / Help	(empty)	(empty)	2024-07- 16:23:42 3mo ago
INC0000024	2024-02-27 08:52:52 7mo ago	Issue with a web page on wiki	Fred Luddy	5 - Planning	Closed	Inquiry / Help	Service Desk	ITIL User	2024-05- 05:15:44 5mo ago
INC0000026	2024-01-29 08:54:59 8mo ago	Seem to have an issue with my hard drive...	Rick Berzle	5 - Planning	Closed	Hardware	Hardware	Don Goodliffe	2024-05- 05:15:35 5mo ago
INC0000028	2024-02-07 08:58:00 8mo ago	My disk is still having issues. Can't delete a file	Rick Berzle	5 - Planning	Closed	Inquiry / Help	Service Desk	Don Goodliffe	2024-05- 05:15:31 5mo ago
INC0000030	2024-02-22 09:01:12 8mo ago	Lost connection to the wireless network	Rick Berzle	5 - Planning	Closed	Hardware	Network	David Loo	2024-05- 05:15:37 5mo ago
INC0000032	2024-02-06 09:19:36 8mo ago	EMAIL Server Down Again	Joe Employee	5 - Planning	Closed	Inquiry / Help	Hardware	David Loo	2024-05- 05:15:54 5mo ago
INC0000033	2024-01-31 07:22:52	File Server is 80% full - Needs upgrade	David Loo	● 1 - Critical	Closed	Inquiry / Help	Hardware	Don Goodliffe	2024-05- 05:15:24

1 to 20 of 106

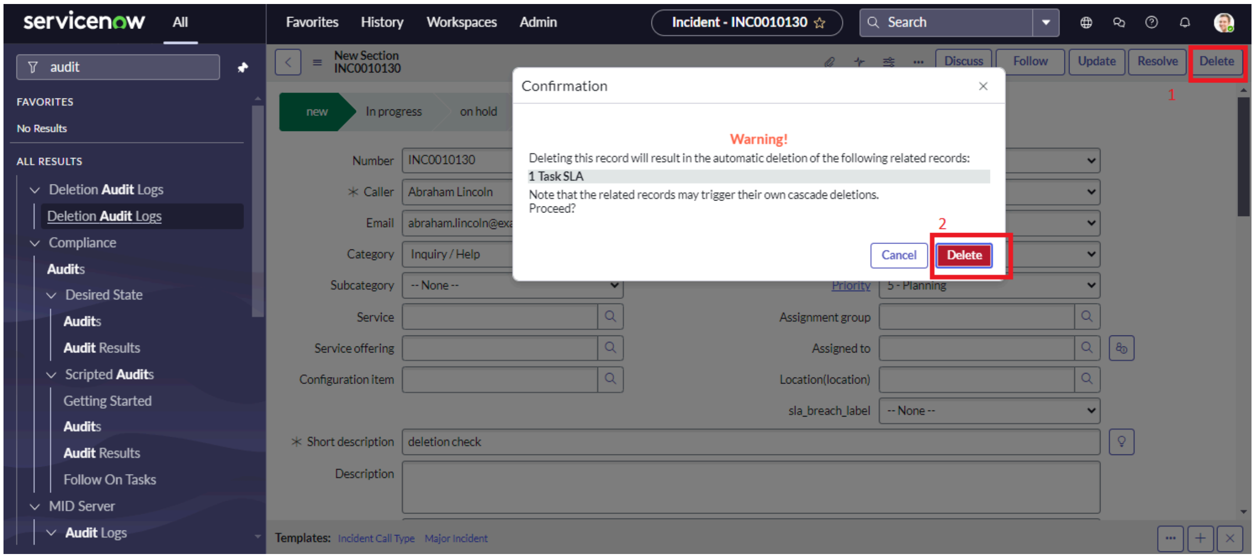
Step 2: Fill in the required details and save the incident.



Number	INC0010130		
* Caller	Abraham Lincoln		
Email	abraham.lincoln@example.com	Impact	3 - Low
Category	Inquiry / Help	Urgency	3 - Low
Subcategory	-- None --	Priority	5 - Planning
Service		Assignment group	
Service offering		Assigned to	
Configuration item		Location(location)	
		sla_breach_label	-- None --
* Short description	deletion check		
Description			

Templates: Incident Call Type Major Incident

Step 3: Now delete the record which is created.



Number	INC0010130
Caller	Abraham Lincoln
Email	abraham.lincoln@exa
Category	Inquiry / Help
Subcategory	-- None --
Priority	5 - Planning
sla_breach_label	-- None --
Short description	deletion check

Confirmation

Warning!

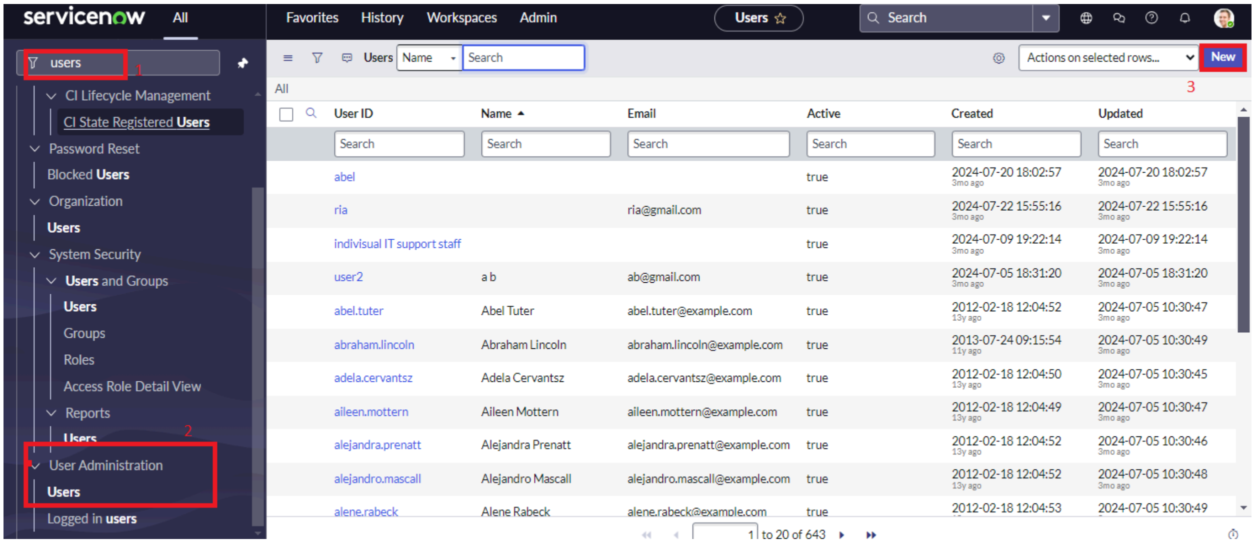
Deleting this record will result in the automatic deletion of the following related records:

1 Task SLA

Note that the related records may trigger their own cascade deletions.
Proceed?

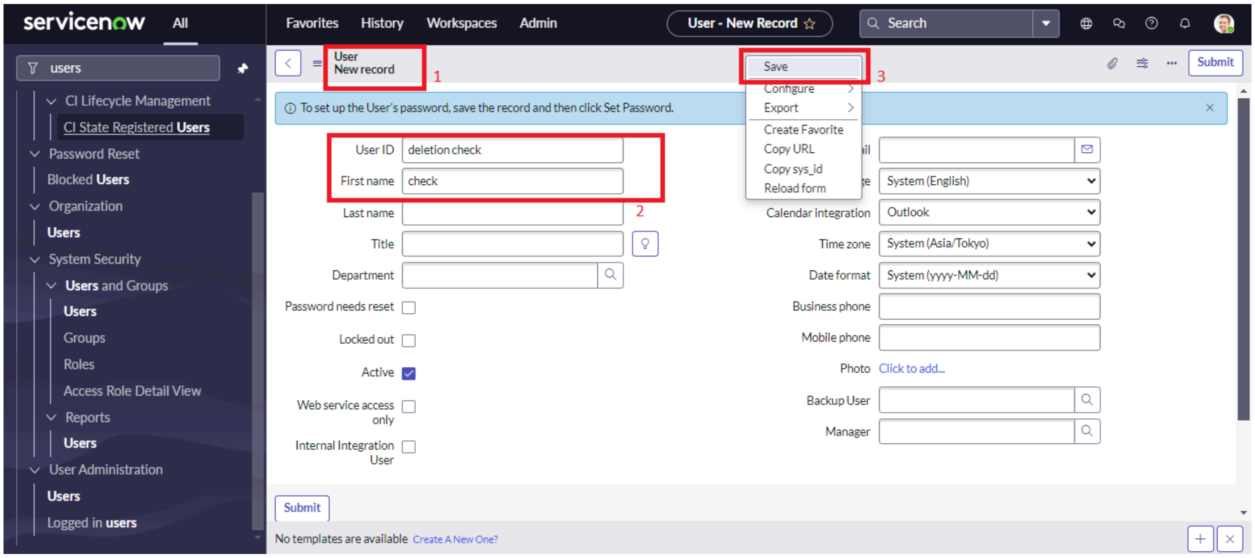
Cancel Delete

Step 4 : Open User Administration >> User. Click on New. Fill in the details and save the form.



User ID	Name	Email	Active	Created	Updated
abel			true	2024-07-20 18:02:57 3mo ago	2024-07-20 18:02:57 3mo ago
ria		ria@gmail.com	true	2024-07-22 15:55:16 3mo ago	2024-07-22 15:55:16 3mo ago
indivisual IT support staff			true	2024-07-09 19:22:14 3mo ago	2024-07-09 19:22:14 3mo ago
user2	a b	ab@gmail.com	true	2024-07-05 18:31:20 3mo ago	2024-07-05 18:31:20 3mo ago
abel.tuter	Abel Tuter	abel.tuter@example.com	true	2012-02-18 12:04:52 13y ago	2024-07-05 10:30:47 3mo ago
abraham.lincoln	Abraham Lincoln	abraham.lincoln@example.com	true	2013-07-24 09:15:54 11y ago	2024-07-05 10:30:49 3mo ago
adela.cervantsz	Adela Cervantsz	adela.cervantsz@example.com	true	2012-02-18 12:04:50 13y ago	2024-07-05 10:30:45 3mo ago
aileen.mottern	Aileen Mottern	aileen.mottern@example.com	true	2012-02-18 12:04:49 13y ago	2024-07-05 10:30:47 3mo ago
alejandra.prenatt	Alejandra Prenatt	alejandra.prenatt@example.com	true	2012-02-18 12:04:52 13y ago	2024-07-05 10:30:46 3mo ago
alejandro.mascall	Alejandro Mascall	alejandro.mascall@example.com	true	2012-02-18 12:04:52 13y ago	2024-07-05 10:30:48 3mo ago
alene.rabeck	Alene Rabeck	alene.rabeck@example.com	true	2012-02-18 12:04:53	2024-07-05 10:30:49

1 to 20 of 643

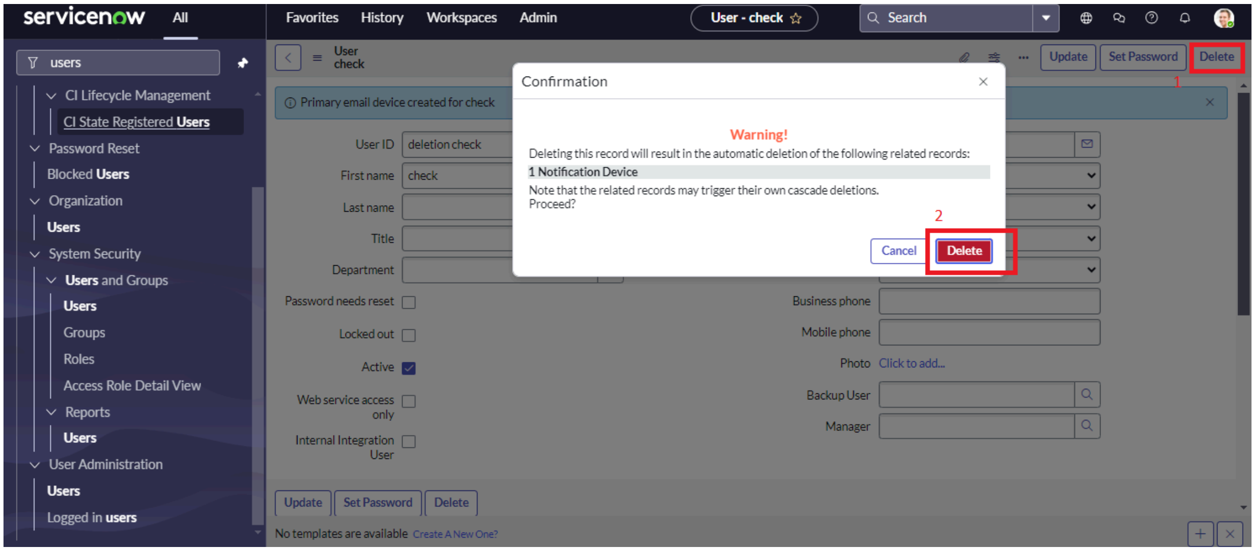


User
New record

To set up the User's password, save the record and then click Set Password.

User ID	deletion check	Email	
First name	check	Language	System (English)
Last name		Calendar integration	Outlook
Title		Time zone	System (Asia/Tokyo)
Department		Date format	System (yyyy-MM-dd)
Password needs reset	□	Business phone	
Locked out	□	Mobile phone	
Active	☑	Photo	Click to add...
Web service access only	□	Backup User	
Internal Integration User	□	Manager	

Step 5 : Now delete the user record which was created.



User
check

Primary email device created for check

User ID deletion check

First name check

Active ☑

Confirmation

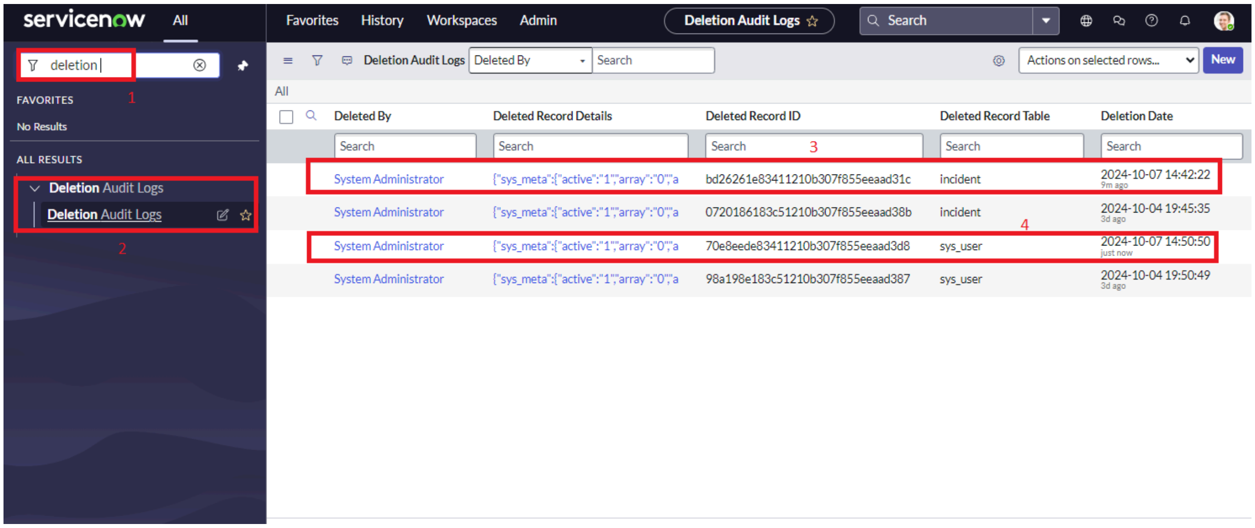
Warning!

Deleting this record will result in the automatic deletion of the following related records:

1 Notification Device

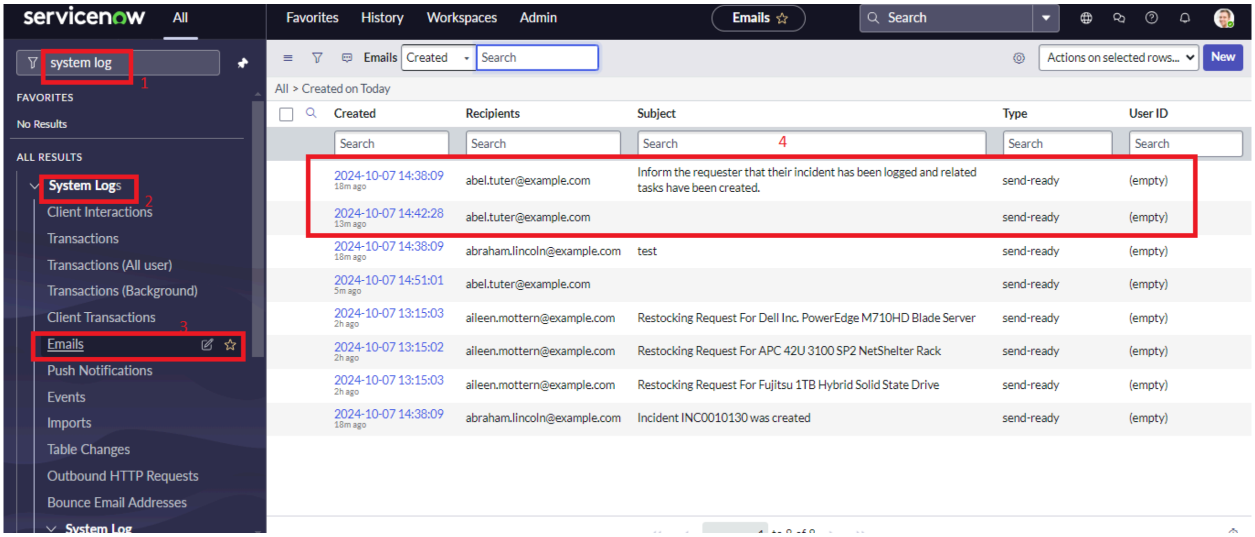
Note that the related records may trigger their own cascade deletions.
Proceed?

Step 6: Open Deletion Audit logs tables ,we can see the incident and user records which were deleted .



Deleted By	Deleted Record Details	Deleted Record ID	Deleted Record Table	Deletion Date
Search	Search	Search	Search	Search
System Administrator	{"sys_meta":{"active":"1","array":"0","a	bd26261e83411210b307f855eeaad31c	incident	2024-10-07 14:42:22 9m ago
System Administrator	{"sys_meta":{"active":"1","array":"0","a	0720186183c51210b307f855eeaad38b	incident	2024-10-04 19:45:35 3d ago
System Administrator	{"sys_meta":{"active":"1","array":"0","a	70e8eede83411210b307f855eeaad3d8	sys_user	2024-10-07 14:50:50 just now
System Administrator	{"sys_meta":{"active":"1","array":"0","a	98a198e183c51210b307f855eeaad387	sys_user	2024-10-04 19:50:49 3d ago

Step 7 : Open System logs >> email. You can see the email notification sent.



Created	Recipients	Subject	Type	User ID
Search	Search	Search	Search	Search
2024-10-07 14:38:09 18m ago	abel.tuter@example.com	Inform the requester that their incident has been logged and related tasks have been created.	send-ready	(empty)
2024-10-07 14:42:28 13m ago	abel.tuter@example.com		send-ready	(empty)
2024-10-07 14:38:09 18m ago	abraham.lincoln@example.com	test	send-ready	(empty)
2024-10-07 14:51:01 5m ago	abel.tuter@example.com		send-ready	(empty)
2024-10-07 13:15:03 2h ago	aileen.mottern@example.com	Restocking Request For Dell Inc. PowerEdge M710HD Blade Server	send-ready	(empty)
2024-10-07 13:15:02 2h ago	aileen.mottern@example.com	Restocking Request For APC 42U 3100 SP2 NetShelter Rack	send-ready	(empty)
2024-10-07 13:15:03 2h ago	aileen.mottern@example.com	Restocking Request For Fujitsu 1TB Hybrid Solid State Drive	send-ready	(empty)
2024-10-07 14:38:09 18m ago	abraham.lincoln@example.com	Incident INC0010130 was created	send-ready	(empty)