

# Guardium Integration Application for IBM Resilient.

## Table of Contents -

- [About this package](#)
- [Prerequisites](#)
- [Installation](#)
- [Configuration](#)
- [Resilient Configurations](#)
- [Rules](#)
- [Run Application](#)
- [Application Usage and Details](#)

## About this package

**This package provides the following features to the Resilient platform.**

1. Run Active Risk Spotter - Risky Users Scores.
2. Search for Entitlements to Sensitive Objects.
3. Search for User Outlier Details.
4. List Parameter Names By Report Name.
5. Search All Guardium Reports.
6. Block User from Data Source.
7. Generate Guardium Client Secret from Resilient.

## Use Cases

1. Enrich existing Resilient incidents with reporting data from Guardium Data Protection. These incidents do not have to be created by Guardium as there will be instances where Guardium data (for example, risky user names/IPs, risky database tables, sources of sensitive data, user anomalies) could be useful for an investigation, playbook and/or remediation.
2. Blocking a risky user or IP address in databases using Guardium Data Protection's blocking feature. A Resilient user needs to make sure to block the right user name or IP address and not the connection between an application and the database, which can stop the application from running.

## Prerequisites

- Resilient platform >= v34.0.5261
- Integrations Server running Resilient Circuits >= v35.0.203
- circuits>=3.2
- requests>=2.23.0
- resilient-lib>=35.0.203
- paramiko>=2.7.1
- six>=1.14.0
- paramiko\_expect>=0.2.8

## Installation

This package requires that it is installed on a RHEL or CentOS platform and uses the Resilient Circuits framework.

- Download the .tar.gz file from the App Exchange and extract it.
- Copy the `fn_guardium_integration-<version>.tar.gz` file to your Integration Server.
- To install the package, run: `pip install fn_guardium_integration-<version>.tar.gz`
- To import the function, example rules, message destinations, workflows, data tables and custom incident fields into your Resilient platform run: `resilient-circuits customize -y -l fn-guardium-integration`
- To uninstall a function from the Resilient platform, run the following: `pip uninstall fn_guardium_integration`

## Configuration

Run the following command to generate the `[fn_guardium_integration]` configuration section in the Resilient app.config file: `resilient-circuits config[-u/-c]`

The following Guardium Integration configuration data is added:

```
[fn_guardium_integration]
# Search results data table ID, should not be changed
search_table=guardium_search_report_data

# Search Sensitive objects table ID, should not be changed
sensitive_table=grd_sensitive_objects

# Search Outlier Details table ID, should not be changed
outlier_table=grd_outlier_details

# false - disable firewall authentication, true - enable firewall authentication
enable_firewall_auth=false

# Firewall Server IP Address
bso_ip=

# Firewall Auth User Name, should be given if `enable_firewall_auth=true`
bso_user=

# Firewall Auth Password, should be given if `enable_firewall_auth=true`
bso_password=

# Guardium http/https proxy server address, leave blank for no proxy
# Example https://proxy_server.com:8080
proxy=

# Guardium proxy used to generate client secret through ssh and cli user
#the command that should be executed and used as the proxy.
# example: /usr/bin/nc --proxy proxy.bar.com:8080 target_host target_port
proxy_command=

# Guardium Host IP/DNS
guardium_host=

# Guardium Restful service port.
port=8443
```

```

# Guardium User Name
guardium_user=

# Guardium password
guardium_password=

# SSL/TLS
guardium_cert=false

# Q-Radar Block group, The group which will be used to block the user access to database
q_radar_block_group=

# Q-Radar block group policy Name
block_policy_name=

# The following parameters 'cli_user' and 'cli_password' are used for the package selftest
function.
# These parameters should be defined only when the package selftest functionality is being
used.
cli_user=
cli_password=

```

Edit the [fn\_guardium\_integration] as follows:

1. *search\_table*: Field should not be altered.
2. *sensitive\_table*: Field should not be altered.
3. *outlier\_table*: Field should not be altered.
4. *enable\_firewall\_auth*: If Guardium is behind the firewall and needs firewall authentication to access the system, you must set this parameter. If set to **true**, to enable firewall authentication. Set to **false**, to disable firewall authentication.
5. *bsc\_ip*: if *enable\_firewall\_auth* is set to **true** then add the firewall IP Address.
6. *bsc\_user*: if *enable\_firewall\_auth* is set to **true** then update the firewall Authentication User.
7. *bsc\_password*: if *enable\_firewall\_auth* is set to **true** then update the firewall Authentication Password.
8. *proxy*: Guardium http/https proxy server address, leave blank for no proxy.
9. *proxy\_command*: The proxy command to generate the client secret if a proxy is being used. Can be left blank if no proxy .Ex: **/usr/bin/nc --proxy proxy.bar.com:8080 target\_host target\_port**
10. *guardium\_host*: Guardium host IP/DNS.
11. *port*: Guardium Restful service port. Default is 8443.
12. *guardium\_user*: Guardium username, which is used to generate an access token from Guardium.
13. *guardium\_password*: Guardium password used to generate an access token from Guardium.
14. *guardium\_cert*: Guardium certificate. Use a TSL/SSL certificate path if required.
15. *q\_radar\_block\_group*: Guardium group used for blocking a user from Data Source.
16. *block\_policy\_name*: Guardium policy used for blocking a user from Data Source. This policy should be installed in the Guardium system.
17. *cli\_user*: Parameter used for the selftest function package only; parameter should be defined only when the package selftest functionality is used.

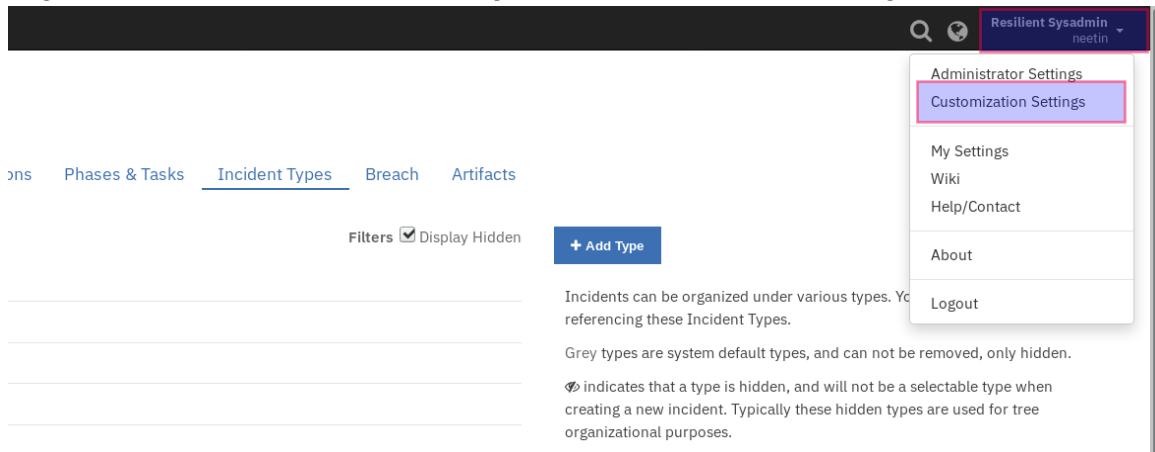
18. *cli\_password*: Parameter used for the selftest function package only; parameter should be defined only when the package selftest functionality is used.

## Resilient Configurations

### Add Results table

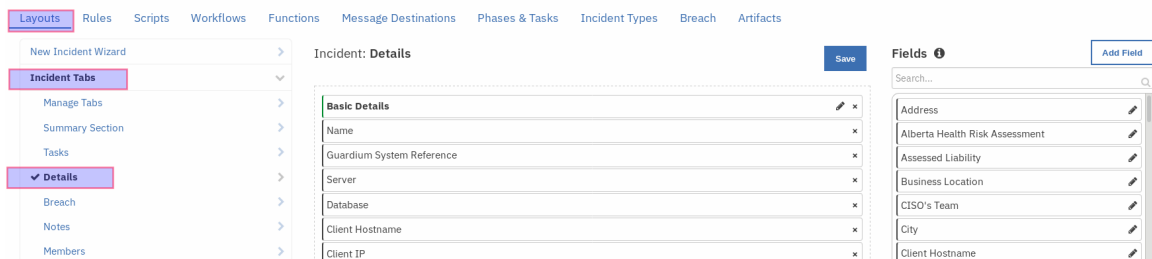
To add data tables to incident tabs, use the following steps.

1. Log in to the Resilient platform and navigate to the Customization Settings tab.



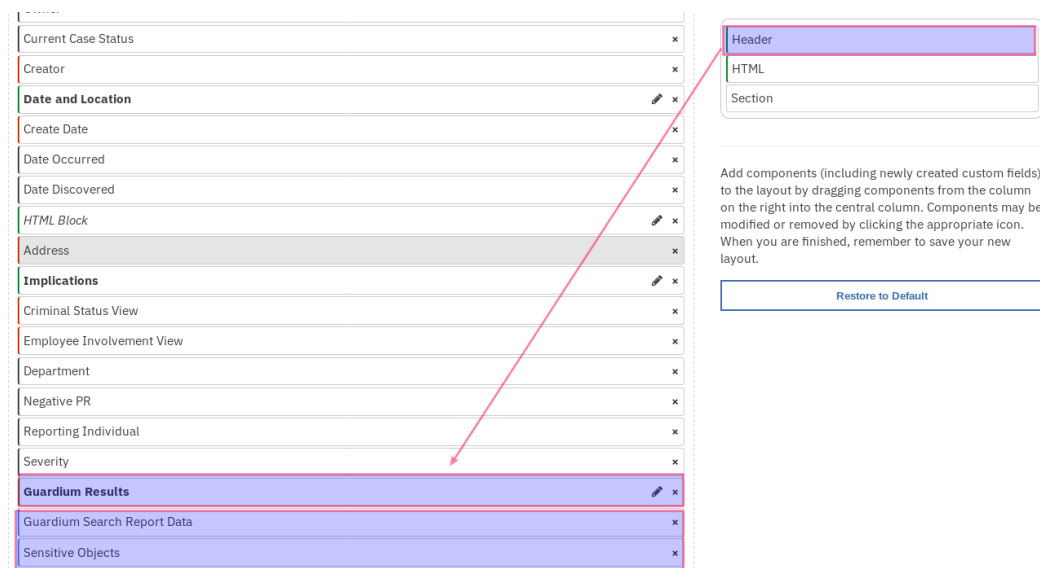
2. Navigate to Layout settings and click on Incident Tabs then select the Details Incident Tab.

Customization Settings



3. Add a Header block and name it **Guardium Results**.

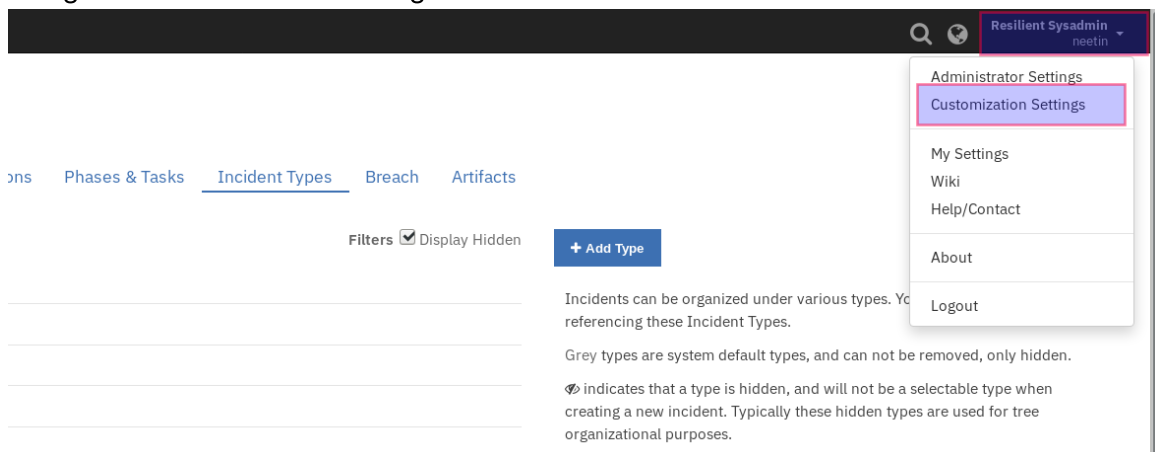
4. Drag and drop the data tables, **Guardium Search Report Data**, **Outlier Details**, and **Sensitive Objects**. and When done, save the tab.



## Add Customized Incident Fields

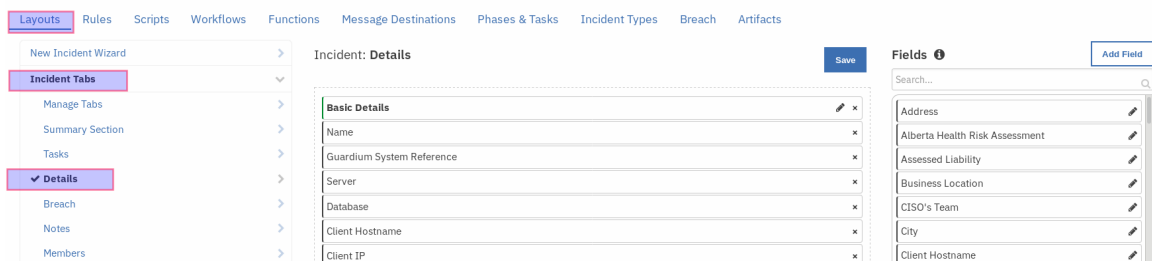
To add custom incident fields to incident tabs, use the following steps.

1. Navigate to Customization Settings tab.

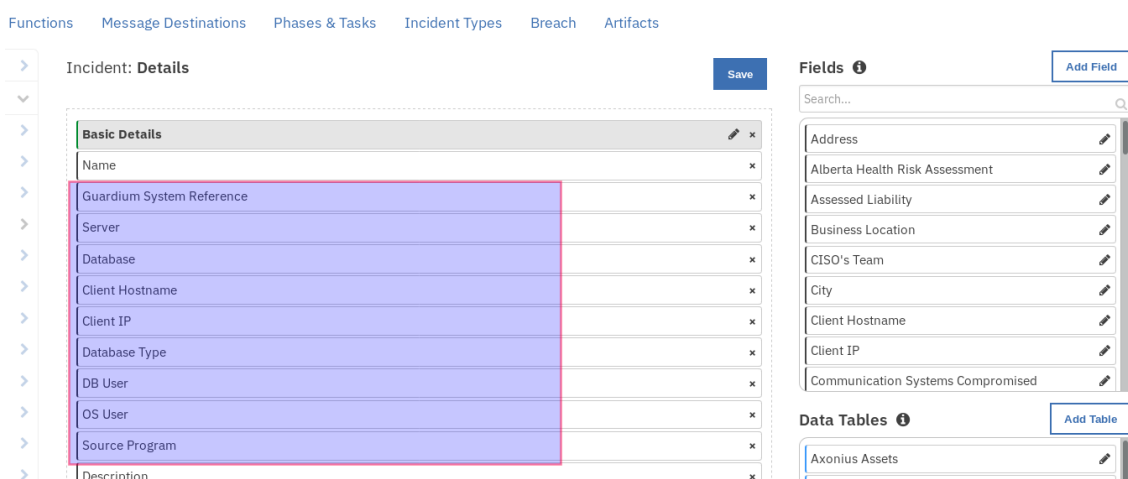


2. Navigate to Layout settings and click on Incident Tabs then select the Details Incident Tab.

Customization Settings



3. Drag and drop the following fields to the selected tab, [server, database\_type, os\_user, client\_hostname, client\_ip, database, source\_program, db\_user, confidence\_score, rare\_or\_new\_behavior, diverse\_behavior, unusual\_working\_hours, high\_volume\_outlier, vulnerable\_obj\_outlier, error\_outlier, ongoing\_outlier, privileged\_user]. When done, save the tab.



## Rules

Rules configurations are listed below, please verify Resilient rules section after package customization.

Rule Name	Object Type	Workflow Triggered	Activity Fields	Condition
Guardium: 1. Run Active Risk Spotter - Risky Users Scores	Incident	Example: Guardium Search Report	Enter Period From, Enter Period To, fetch size	None
Guardium: 2. Search for Entitlements to Sensitive Objects	Incident	Example: Guardium Search Report	Enter Period From, Enter Period To	Incident Type != Guardium Outliers
Guardium: 3. Search for User Outlier Details	Incident	Example: Guardium Search Outlier Details	Enter Period From, Enter Period To	Incident Type != Guardium Policy violations
Guardium: 4A. List Parameter Names By Report Name	Incident	Example: Guardium List Parameter Names by Report Name	Select Report	None
Guardium: 4B. Search All Guardium Reports	Incident	Example: Guardium Search Report	Select Report, Enter Period From, Enter Period To, fetch size, Show Aliases, Remote Data Source, Parameter label, Parameter value, Sort Column, Sort Type	None
Guardium: 5. Block User from Data Source	Incident	Example: Guardium Block User Access to DB	DB User Name	None
Guardium: Generate Client Secret	Incident	Example: Generate Guardium Client Secret	Guardium Cli User, Guardium Cli Password	None

## Run Application

- Start Resilient Circuits by executing the following command. `resilient-circuits run`

## Application Usage and Details

Guardium: Generate Client Secret:

Function Guardium Generate Client Secret

The function should only be executed after a fresh installation of the Guardium integration or after upgrading the Guardium system. The function generates the Guardium client secret and client ID. The function also detects the Guardium system unit type (standalone or central manager type) and updates the search function remote datasource option as per the available Guardium hosts. The system details acquired by the function are used to generate a Guardium access token. This is used in successive API calls from the Resilient integration. The Resilient field, **guardium\_system\_reference**, is used to store the client secret data.

Function Workflow:

Example: Generate Guardium Client Secret

This workflow can be invoked from any Resilient incident action menu.

Workflows / Example: Generate Guardium Client Secret

Name \*

Example: Generate Guardium Client Secret

API Name \*

example\_generate\_guardium\_client\_secret

Description

A Workflow to generate guardium client secret, finds guardium unit type(i.e standalone, central manager), creates outliers & violation incidents types, updates guardium data source hosts IP/DNS to 'Remote Data Source' rule action field

Object Type \*

Incident

Creator

Resilient Sysadmin

Last Modified

06/15/2020 17:33

Last Modified By

Resilient Sysadmin

Associated Rules

Guardium: Generate Client Secret

START

Function Guardium Generate Client...

END

A Workflow to generate guardium client secret, finds guardium unit type(i.e standalone, central manager), creates outliers & violation incidents types, updates guardium data source hosts IP/DNS to 'Remote Data Source' rule action field.

Timeline

Artifacts

Email

Filter: Active

Selected

Add Task

Flags

Actions

Actions

Guardium: Block User

Guardium: Generate Client Secret

Guardium: List Parameter Names By Report Name

Guardium: Run Active Risk Spotter - Risky Users Scores

Guardium: search for sensitive object

Guardium: Search Reports

Action Status

Workflow Status

Close Incident

Delete Incident

information or personal data

2020-06-18

7/16

# Guardium: Generate Client Secret



Guardium Cli User \*

Guardium Cli Password \*

Cancel

Execute

Enter the Guardium cli user name and password and press Execute to invoke the workflow. Navigate to the Notes section of the incident and wait for the message: *Guardium client secret generation completed*.

**Note:** After generating the client secret, if the Resilient rules condition section has in-consistencies as shown below in red, customize the package once again to resolve the issue.

-	Guardium: 1. Run Active Risk Spotter - Risky Users Scores	Menu Item	Incident			
-	Guardium: 2. Search for Entitlements to Sensitive Objects	Menu Item	Incident	Incident Type		
-	Guardium: 3. Search for User Outlier Details	Menu Item	Incident	Incident Type		
-	Guardium: 4A. List Parameter Names By Report Name	Menu Item	Incident			
-	Guardium: 4B. Search All Guardium Reports	Menu Item	Incident			
-	Guardium: 5. Block User from Data Source	Menu Item	Incident			
-	Guardium: Generate Client Secret	Menu Item	Incident			

## 1. Guardium: Run Active Risk Spotter - Risky Users Scores:

### Function Guardium Search Report

This function is used to run the **active risk spotter - risky users scores** report. Risk scores are 0-10 with 10 being the most risky. Learn more here:

[https://www.ibm.com/support/knowledgecenter/SSMPHH\\_11.1.0/com.ibm.guardium.doc/protect/risk\\_spotter\\_results.html](https://www.ibm.com/support/knowledgecenter/SSMPHH_11.1.0/com.ibm.guardium.doc/protect/risk_spotter_results.html)

### Function Workflow:

#### Example: Guardium Run Active Risk Spotter:

This workflow can be invoked from any Resilient incident action menu.

**Enter Period From** - Report start Date & Time. **Enter Period To** - Report end Date & Time. **fetch size** - Maximum number of records to be fetched.

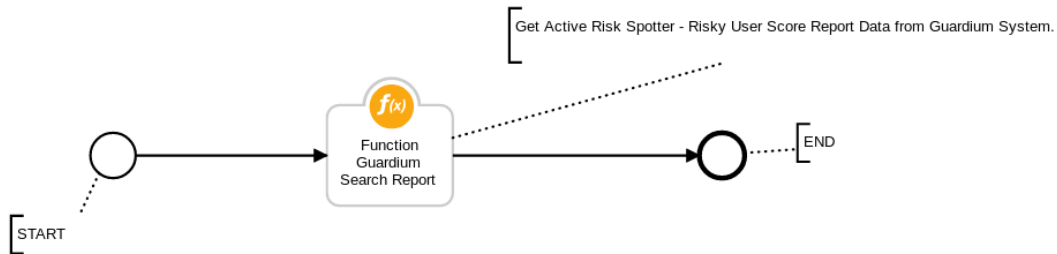


Name \*

API Name \*

Description

Object Type \*



## Guardium: Run Active Risk Spotter - Risky Users Scores ✕

Enter Period From \*

Enter Period To \*

Remote Data Source \*

fetch size \*

Cancel

Execute

### Guardium Search Report Results

Guardium Search Report Data

Report Name	Generated Date	Column Data
Active Risk Spotter - Risky Users Scores	04/09/2020 17:57:22	<b>DB User:</b> SIGRID <b>Server IP:</b> 9.42.29.160 <b>Total Risk Score:</b> 5.72 <b>Activity Date:</b> 2020-03-26 00:00:00 <b>Threat analytics Score:</b> 0 <b>Violations Score:</b> 0.56 <b>Vulnerability Score:</b> 0 <b>Sensitive Objects Score:</b> 0 <b>Select Queries Score:</b> 0 <b>DDL Queries Score:</b> 0 <b>DML Queries Score:</b> 0 <b>Administrative Queries Score:</b> 0 <b>High Volume Activity Score:</b> 0 <b>Off Work Activity Score:</b> 1 <b>Group State Description:</b> Top Riskys Only

The returned results are used to refresh the data table, **Guardium Search Report Data**.

Guardium: 2. Search for Entitlements to Sensitive Objects:

### Function Guardium Search Sensitive Object

2020-06-18

9/16

This function retrieves the sensitive objects. The returned report contains user entitlements to sensitive objects, which is useful for breach investigation and remediation. Guardium search results from Access category are filtered by incident field values from **DB User & Client IP** and Guardium **Sensitive objects** group elements.

**Function Workflow:**

**Example: Guardium Search Sensitive Objects**

This workflow can be invoked from any Resilient incident action menu except for incidents of type **Guardium Outliers**. **Enter Period From** - Report start Date & Time. **Enter Period To** - Report end Date & Time.

Name \*

Example: Guardium Search Sensitive Objects

API Name \* ⓘ

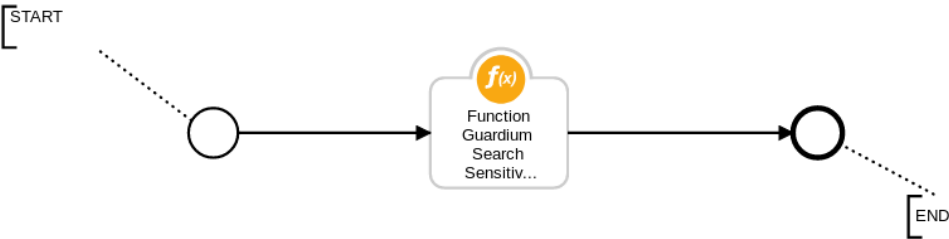
example\_guardium\_search\_sensitive\_objects

Description

A Workflow to search for sensitive objects.

Object Type \*

Incident



## Guardium: search for sensitive object

×

Enter Period From \* ⓘ

07/01/2019 00:00:00 +05:30

📅

Enter Period To \* ⓘ

05/19/2020 00:44:29 +05:30

📅

Cancel

Execute

## Sensitive Objects

Sensitive Objects				
		Search...		
		Print Export		
Date generated	Event category	Event property	Highest count (property)	
06/09/2020 01:55:10	Who	DB User:1 OS User:1 Client Host name:1 Client IP:1	DB2_KVER:48 ROOT:48 9.32.164.142:48 9.32.164.142:48	...
06/09/2020 01:55:10	Where	Guardium Appliance:1 Server:1 Database:1 DB Type:1 Source Program:1	gpart1-col14.guard.swg.usma.ibm.com:48 9.32.164.142:48 DB2INST1:48 DB2:48 DB2JCC_APPLICATION:48	...
06/09/2020 01:55:10	When	Date:1	2020-04-23:48	...
06/09/2020 01:55:10	What	Object:0 Verb:4	select:47 delete:27 update:20 INSERT:1	...
06/09/2020 01:55:10	Exception	Error:0 Violation:0 Severity:0	—	...

Displaying 1 - 5 of 5

The returned results are used to refresh the data table, [Sensitive Objects](#).

### Guardium: 3. Search for User Outlier Details:

#### Function Guardium Search Outlier Details

This function retrieves the outlier details. This report allows a user to enrich a Resilient incident with user outlier data (for instance: SQL errors, password errors, excessive download size). Guardium Search results from Outlier category are filtered by incident field values from [Database](#), [Server](#), [DB User](#), and [Date Discovered](#).

#### Function Workflow:

#### Example: Guardium Search Outlier Details

This workflow can be invoked from any Resilient incident action menu except for incidents of type [Guardium Policy Violations](#).

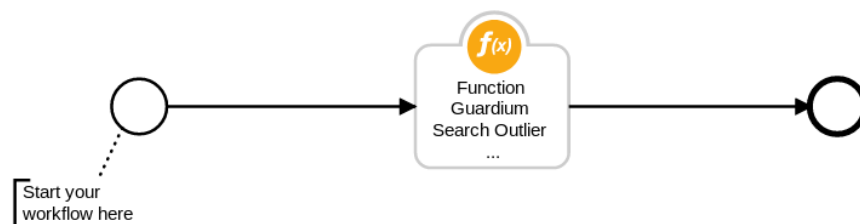
[Enter Period From](#) - Report start Date & Time. [Enter Period To](#) - Report end Date & Time.

Name \*

API Name \*

Description

Object Type \*



## Guardium: search for outlier details

Enter Period From \*

Enter Period To \*

Cancel

Execute

Outlier Details

Search...													<a href="#">Print</a>	<a href="#">Export</a>
Date Generated	Description	Confidence Score	High volume Outlier	Vulnerable obj. Outlier	Rare or New Behavior	Diverse Behavior	Error Outlier	Server	Database	DB User	Un W H			
05/18/2020 19:14:48	Excessive activity related to DB User on members; Select Command (238:4.02)	100	true	false	false	false	false	9.32.16 4.78	9.32.164. 78:5.7.22	BARR Y	w			
05/18/2020 19:14:48	Excessive activity related to DB User on categoryNames; Select Command (91:2.32)	100	true	false	false	false	false	9.32.16 4.78	9.32.164. 78:5.7.22	BARR Y	w			
05/18/2020 19:14:48	Excessive activity related to DB User on members; Select Command (137:2.43)	100	true	false	false	false	false	9.32.16 4.78	9.32.164. 78:5.7.22	BARR Y	w			
05/18/2020 19:14:48	Excessive activity related to DB User on status; Select Command (145:2.65)	100	true	false	false	false	false	9.32.16 4.78	9.32.164. 78:5.7.22	BARR Y	w			
05/18/2020 19:14:48	Excessive activity related to DB User on department; Select Command (104:2.21)	100	true	false	false	false	false	9.32.16 4.78	9.32.164. 78:5.7.22	BARR Y	w			

The returned results are used to refresh the data table, **Outlier details**.

Guardium: 4A. List Parameter Names By Report Name :

## Function Guardium List Parameter Names by Report Name

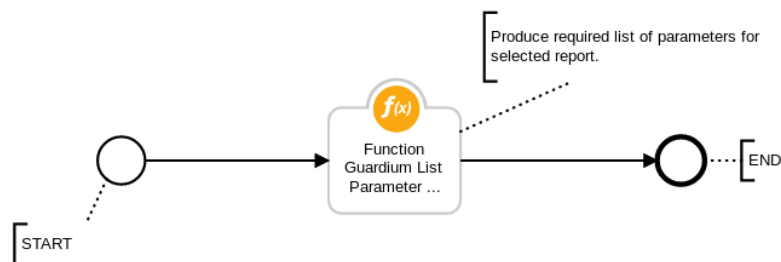
This function is used to get the additional parameters required to run Guardium reports. The function is used prior to executing a Guardium report to get a list of the required parameters for the execution.

### Function Workflow:

#### Example: Guardium List Parameter Names by Report Name

This workflow can be invoked from any incident action menu. Select any report from the drop-down menu to retrieve the required list of Guardium parameters.

Name *	Example: Guardium List Parameter Names by Report Name
API Name * ⓘ	example_guardium_list_parameter_names_by_report_name
Description	A Workflow to get required list of parameters for the selected guardium report & update function result to incident notes.
Object Type *	Incident



## Guardium: List Parameter Names By Report Name

Select Report \*

Command Details

Cancel

Execute

Resilient Sysadmin added a note to the Incident 04/05/2020 15:58

Report Name: Sensitive Objects Usage

Report ID: 108

Parameter Names: SHOW\_ALIASES, QUERY\_TO\_DATE, QUERY\_FROM\_DATE, REMOTE\_SOURCE

A note is added to the incident with information on selected report parameters.

## Guardium: 4B. Search All Guardium Reports :

### Function Guardium Search Report

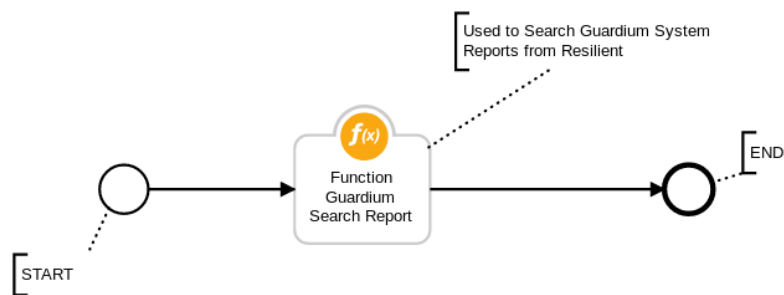
This function is used to search Guardium reports. The function has access to all default Guardium reports. This option is for a user who is familiar with Guardium. It allows the user to choose from any of Guardium's 600+ out of the box reports which can be used for enrichment of Resilient data. This option is under the pre-canned options as it requires knowledge of Guardium to choose the most useful reports.

### Function Workflow:

#### Example: Guardium Search Report

This workflow can be invoked from any incident action menu.

Name *	<input type="text" value="Example: Guardium Search Report"/>
API Name * ⓘ	<input type="text" value="example_guardium_search_report"/>
Description	<input type="text" value="Workflow to search guardium reports."/>
Object Type *	<input type="text" value="Incident"/>



# Guardium: Search Reports



Select Report \*

Enter Period From \*

Enter Period To \*

Show Aliases \*

Remote Data Source \*

Parameter label

Parameter value

fetch size \*

Sort Column

Sort Type

Cancel

Execute

Guardium Search Report Data

Search...



Print

Export

Report Name	Generated Date	Column Data	
Detailed Enterprise S-TAP View	05/19/2020 00:25:52	<b>Software Tap Host:</b> 9.32.164.142 <b>Tap Version:</b> STAP-11.2.0.0_r108380_v11_2_1-20200323_1927 <b>DB Server Type:</b> oracle <b>Status:</b> Active <b>Timestamp:</b> 2020-05-18 14:45:13 <b>Primary Host Name:</b> 9.70.145.96 <b>Ktap Installed:</b> Yes <b>TEE Installed:</b> No <b>MSS Shm:</b> No <b>DB2 Shm:</b> No <b>Local TCP:</b> Yes <b>Pipes:</b> No <b>Encrypted?:</b> Unencrypted <b>Datasource Name:</b> adir-vm02.guard.swg.usma.ibm.com <b>DB Install Dir:</b> /home/oracle12	...
Detailed Enterprise S-TAP View	05/19/2020 00:25:52	<b>Software Tap Host:</b> 9.42.29.244 <b>Tap Version:</b> STAP-11.0.0.0_r106287_trunk_1-20190324_1932 <b>DB Server Type:</b> oracle <b>Status:</b> Inactive <b>Timestamp:</b> 2020-04-06 10:30:00 <b>Primary Host Name:</b> 9.70.157.72 <b>Ktap Installed:</b> No <b>TEE Installed:</b> No <b>MSS Shm:</b> No <b>DB2 Shm:</b> No <b>Local TCP:</b> Yes <b>Pipes:</b> No <b>Encrypted?:</b> Unencrypted	...

The returned results are used to refresh the data table **Guardium Search Report Data**.

## Guardium: 5. Block User from Data Source:

### Function Guardium block user

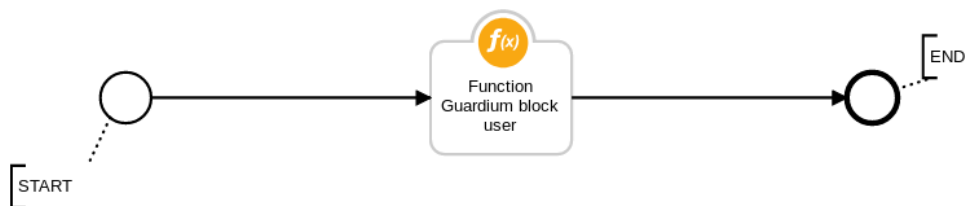
This function can be used to block user access to the Database.

## Function Workflow:

### Example: Guardium Block User Access to DB

This workflow can be invoked from any incident actions menu.

Name *	Example: Guardium Block User Access to DB
API Name * ⓘ	example_guardium_block_user_access_to_db
Description	A workflow to block user access to guardium Database
Object Type *	Incident



## Guardium: Block User

DB User Name \*

User Name 101

Cancel

Execute

Tasks Details Breach Notes Members News Feed Attachments Stats Timeline Artifacts Email

Sans Serif Normal B I U G H A W

Post

Cancel

Search...



☒ Show Task Notes ☐ Oldest Notes First

Created By: 0 selected Date Created: All

Resilient Sysadmin added a note to the Incident 05/19/2020 00:13

Successfully blocked user: User Name 101. adir-vm02.guard.swg.usma.ibm.com ID=20000 Policy Violation\_DDL\_AdminCommands-high has been reinstalled successfully gpart1-col14.guard.swg.usma.ibm.com ID=20000 Policy Violation\_DDL\_AdminCommands-high has been reinstalled successfully



A note is added to the incident with result of workflow.

:copyright:IBM Corp. 2010, 2020. All Rights Reserved.