Lockbox - How To Guide

30 Steps View most recent version

Created by	Creation Date	Last Updated
DevGoats LLC	November 29, 2023	November 30, 2023

# Welcome

30 Steps

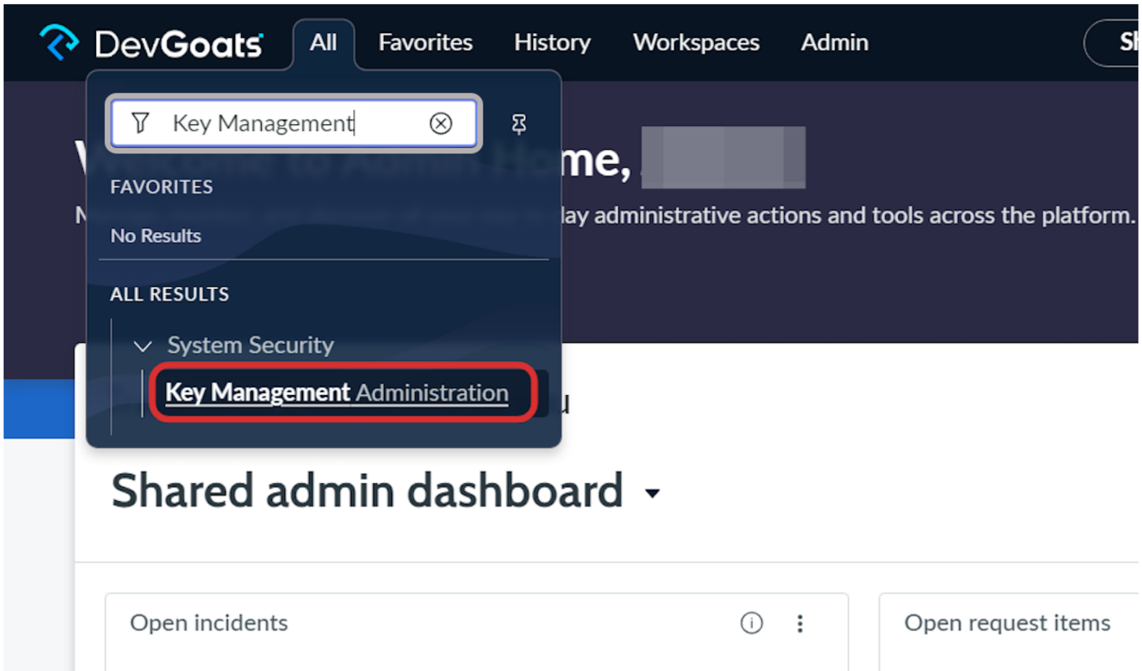
This document covers the installation guide of the application, including a default configuration of the "incident" table that allows you to enter secure data and set access to that data via the ITIL role policy. Granted, the ITIL role is just for demo purposes and in this case we are assuming itil users would be the ones that are allowed to see secure data. As always, consult with your internal security team on proper procedures for secure data access.

STEP 1

Let's Setup the Key Management Administration

To proceed, the "security_admin" role is required to access this page. Access into this module is required as we'll be creating a new key management crypto module along with access policies.

Navigate to the "ALL" menu filter navigator, and search "Key Management". Select "Key Management Administration".

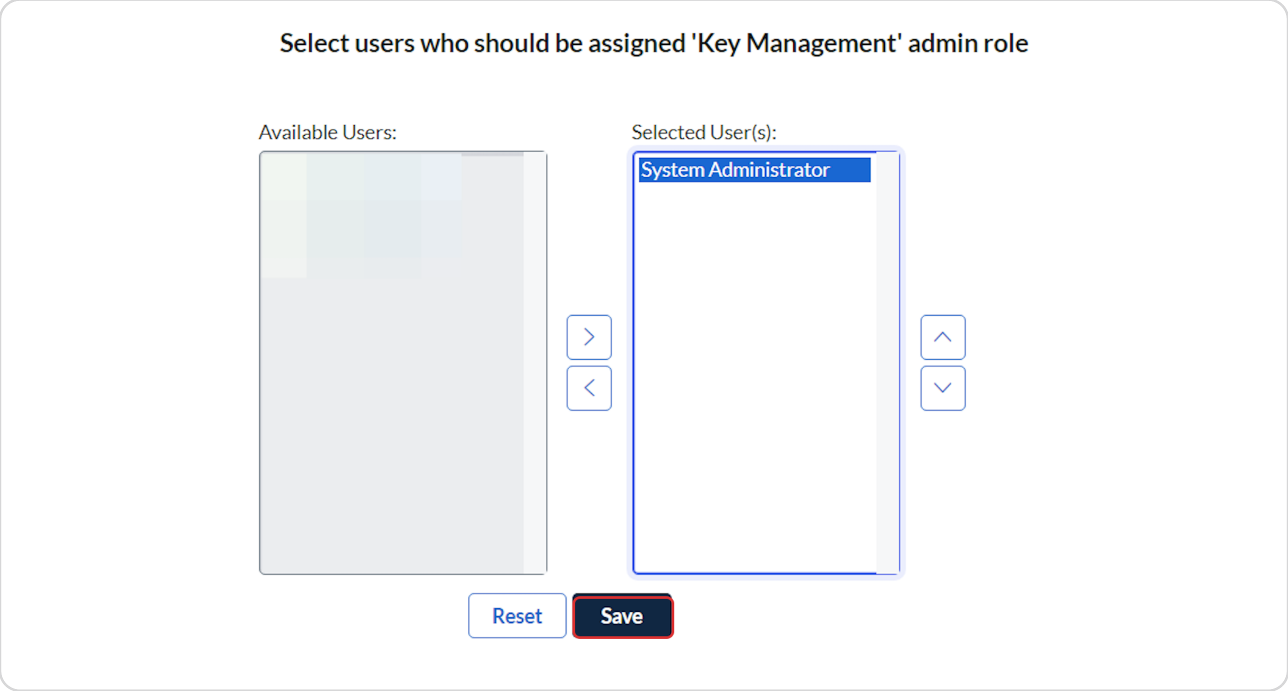


STEP 2

Select the user account that will configure the module and access policies.

In this demo, we're using the System Administrator account to grant access to the Key Management Framework.

Pick the account as shown and "Save" the record. After save, navigate back to your ServiceNow platform homepage.



Select users who should be assigned 'Key Management' admin role

Available Users:

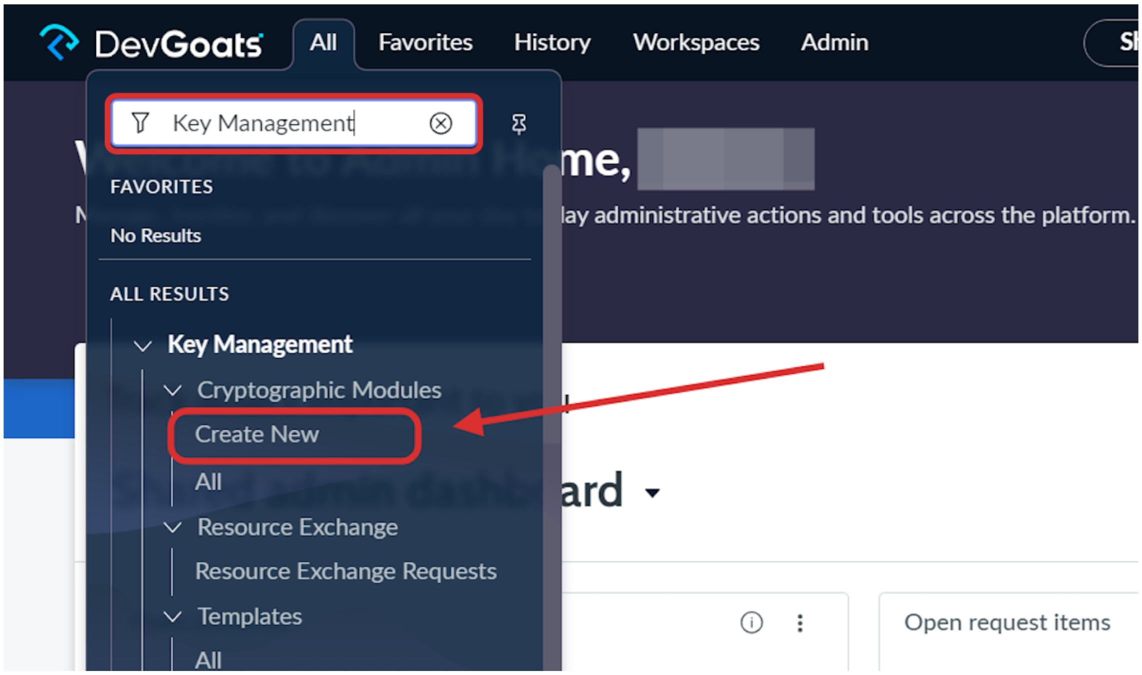
Selected User(s):

System Administrator

STEP 3

Let's setup the Crypto Module and Access Policies

Back on the ServiceNow platform home page, navigate to your filter navigator and type "Key Management". Click "Create New"



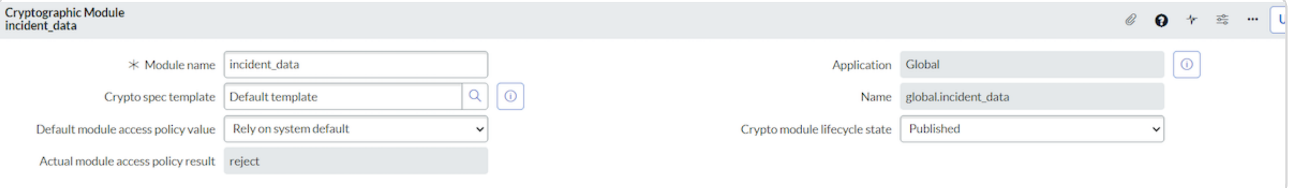
Key Management

STEP 4

Configure the record

Remember, we are starting with the incident table for this data. So, we're calling this module "incident_data". Note, the name has to be all one word and lowercase, you may use underscores.

Configure the other fields as shown.

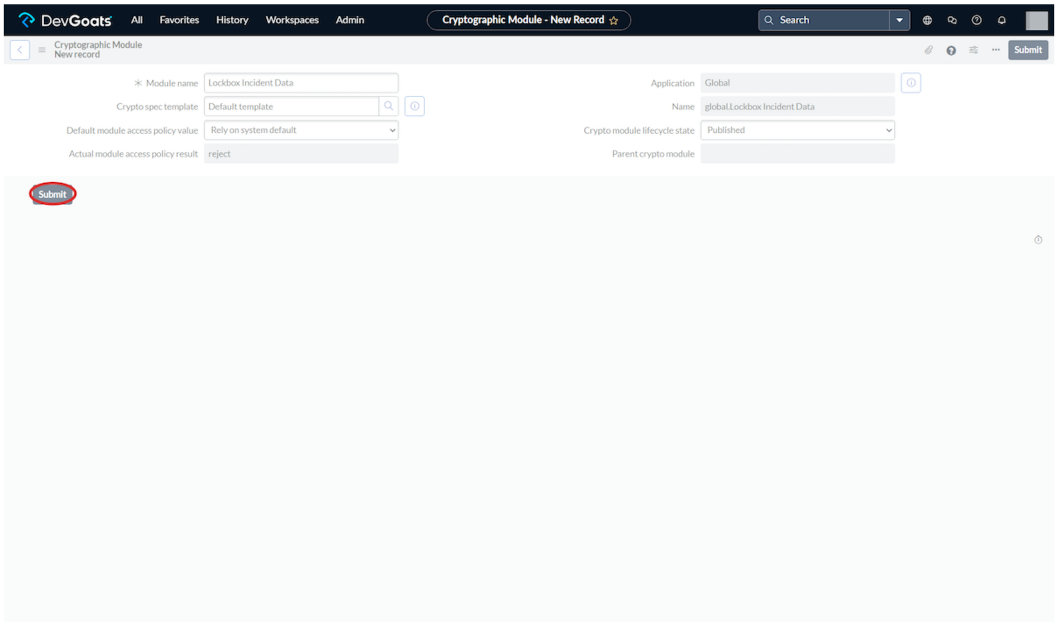


Cryptographic Module
incident_data

* Module name	incident_data	Application	Global
Crypto spec template	Default template	Name	global.incident_data
Default module access policy value	Rely on system default	Crypto module lifecycle state	Published
Actual module access policy result	reject		

STEP 5

Submit the record



Module name: Lockbox Incident Data

Crypto spec template: Default template

Default module access policy value: Rely on system default

Actual module access policy result: reject

Application: Global

Name: global.Lockbox Incident Data

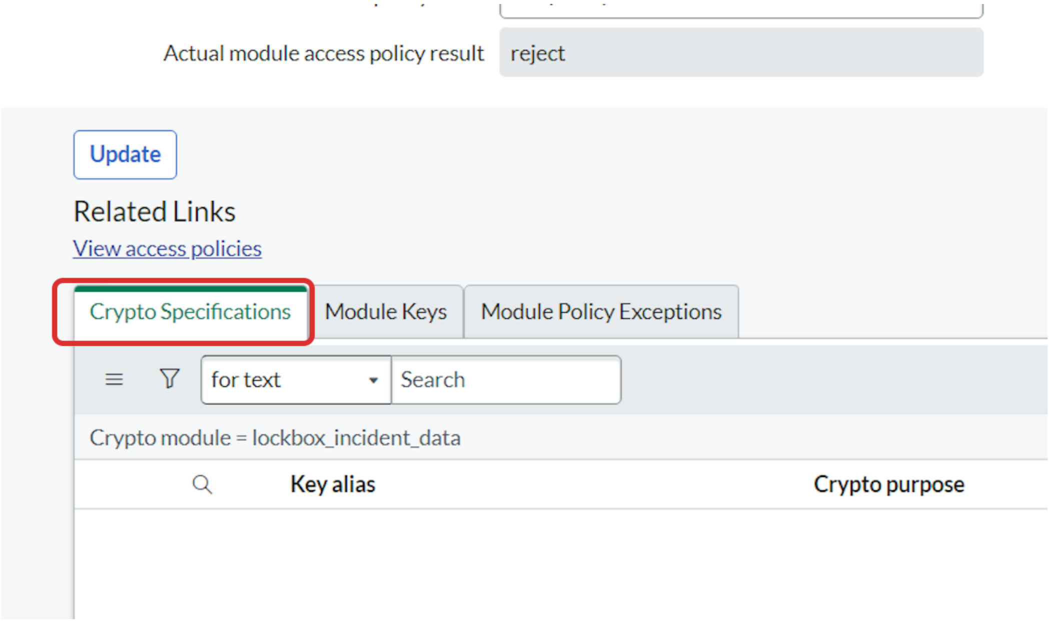
Crypto module lifecycle state: Published

Parent crypto module:

STEP 6

Setup the Crypto Specifications

Click the "New" button. Confirm you are on the "Crypto Specifications" tab.



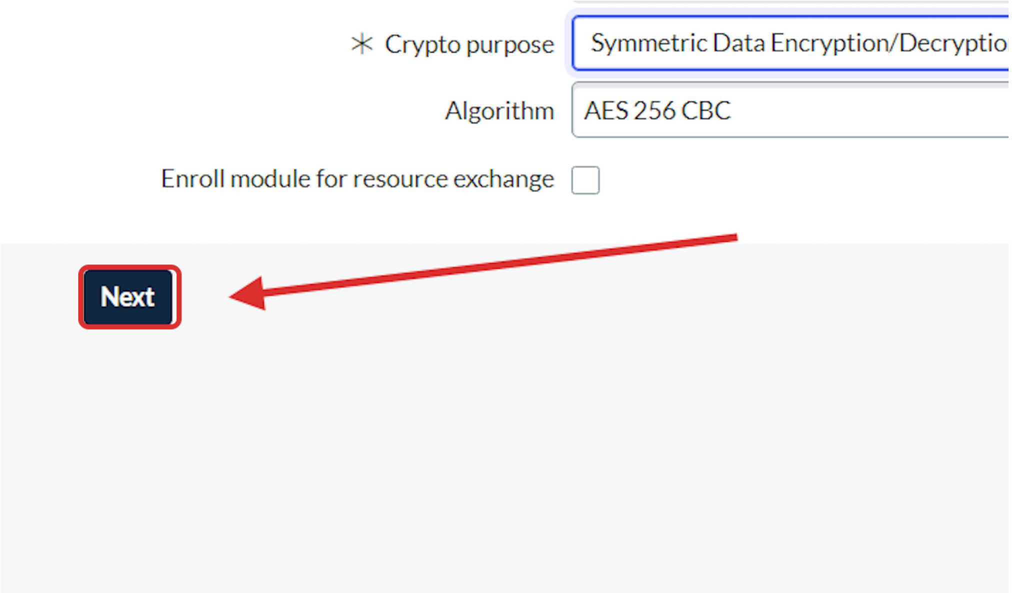
Actual module access policy result: reject

Crypto module = lockbox_incident_data

STEP 7

For each section, we'll enter the details as shown in the screenshots.

After setting the follow values as shown, click next.



✳ Crypto purpose: Symmetric Data Encryption/Decryptio

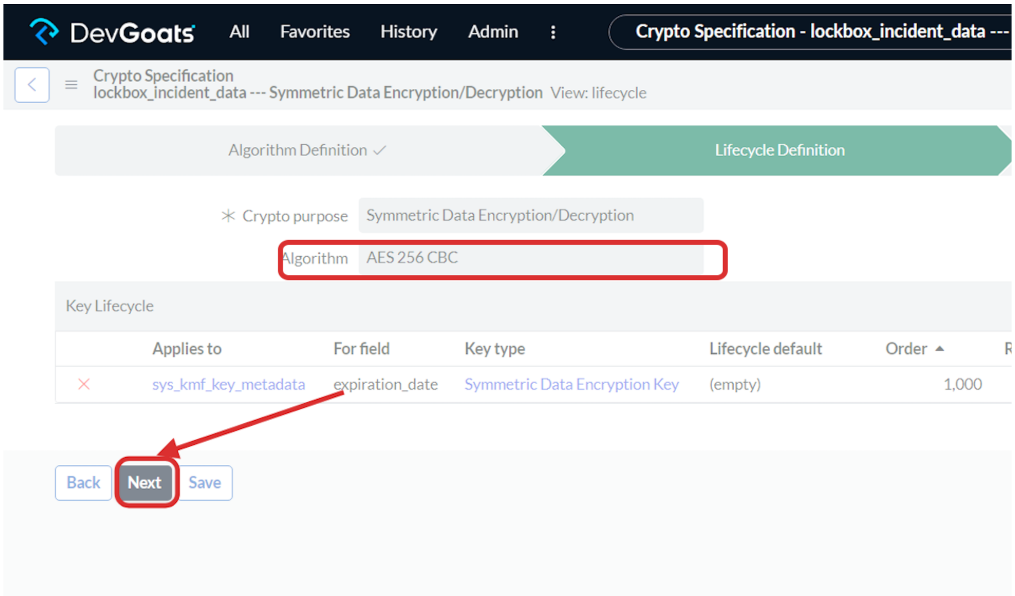
Algorithm: AES 256 CBC

Enroll module for resource exchange ☐

STEP 8

Configure Step 2

Choose the AES 256 CDC Algorithm. After confirming, choose "Next"



Crypto Specification
lockbox_incident_data --- Symmetric Data Encryption/Decryption View: lifecycle

✳ Crypto purpose: Symmetric Data Encryption/Decryption

Algorithm: AES 256 CBC

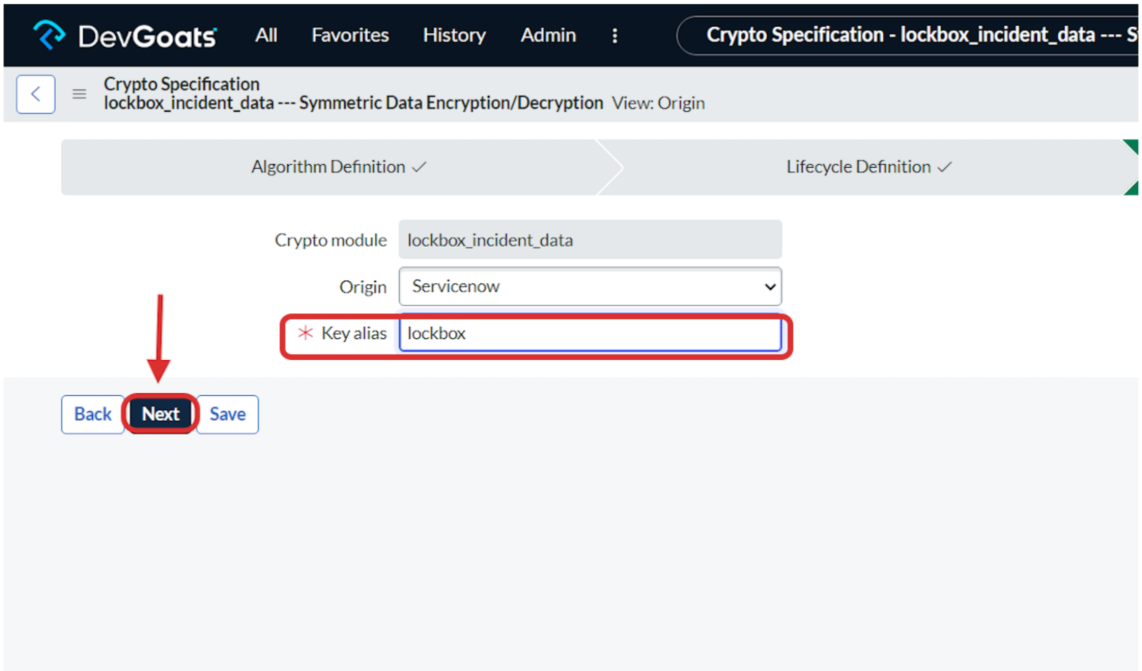
Key Lifecycle

	Applies to	For field	Key type	Lifecycle default	Order ▲	R
✕	sys_kmf_key_metadata	expiration_date	Symmetric Data Encryption Key	(empty)	1,000	

STEP 9

Configure Step 3

For the "Key Alias", choose a name to identify the source. We choose lockbox so we know the app is using that module to encrypt our secure entries. After the name is set, choose "Next".



Crypto Specification
lockbox_incident_data --- Symmetric Data Encryption/Decryption View: Origin

Crypto module: lockbox_incident_data

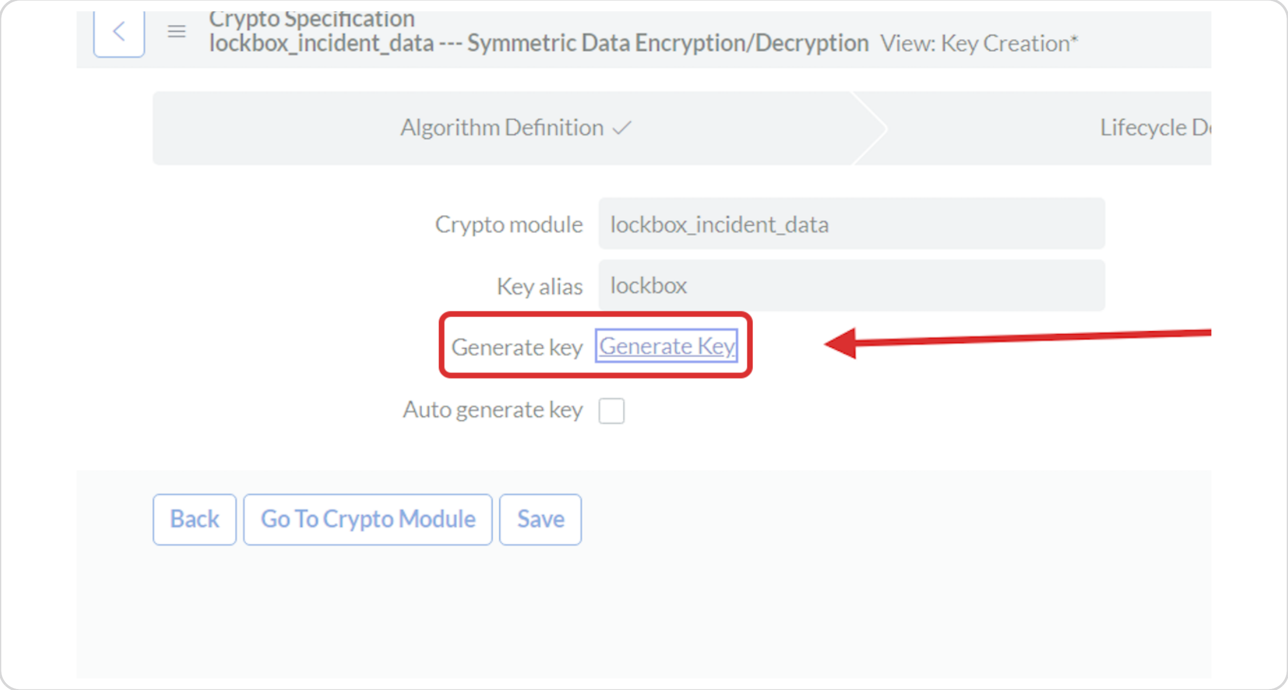
Origin: Servicenow

* Key alias: lockbox

STEP 10

Configure Step 4

Click on Generate Key and Save. Once you generate a key, this setup action is now complete. Continue back to the home page for the access policy configuration.



Crypto Specification
lockbox_incident_data --- Symmetric Data Encryption/Decryption View: Key Creation*

Crypto module: lockbox_incident_data

Key alias: lockbox

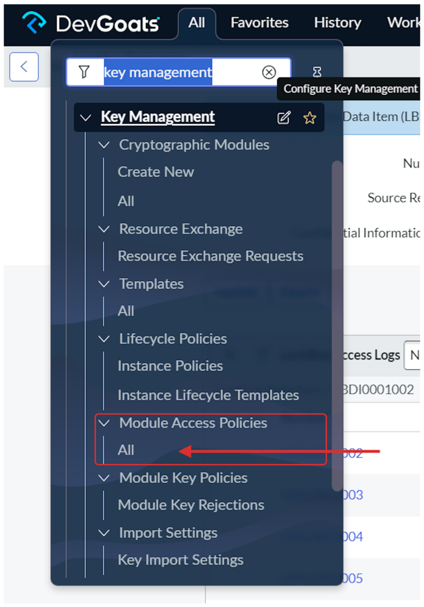
Generate key: Generate Key

Auto generate key □

STEP 11

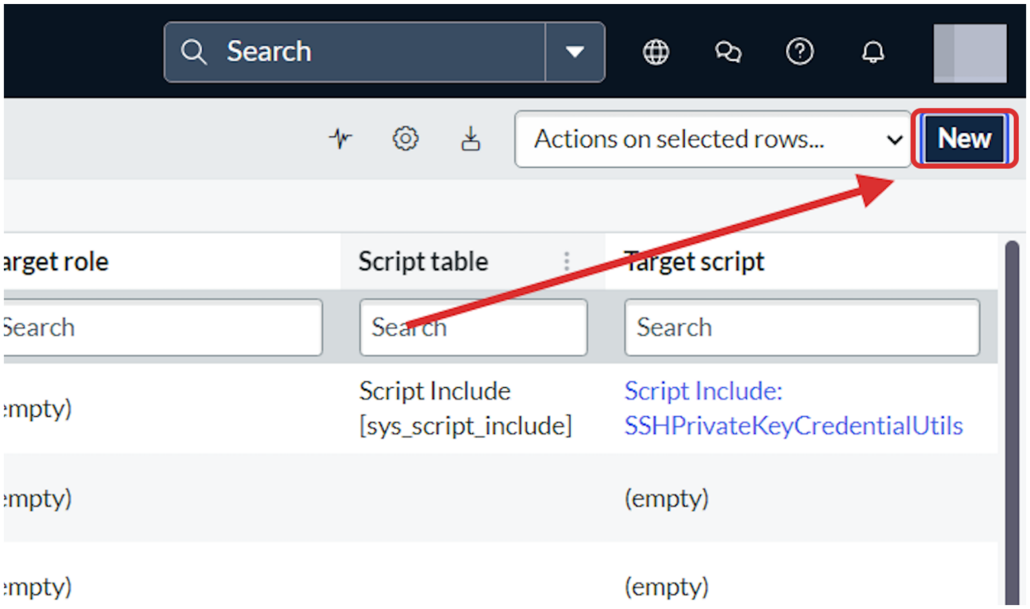
On the home page, in the filter navigator. Type "Key Management". You will see a list of options.

Choose "All" under the Module Access Policies



STEP 12

Click on New

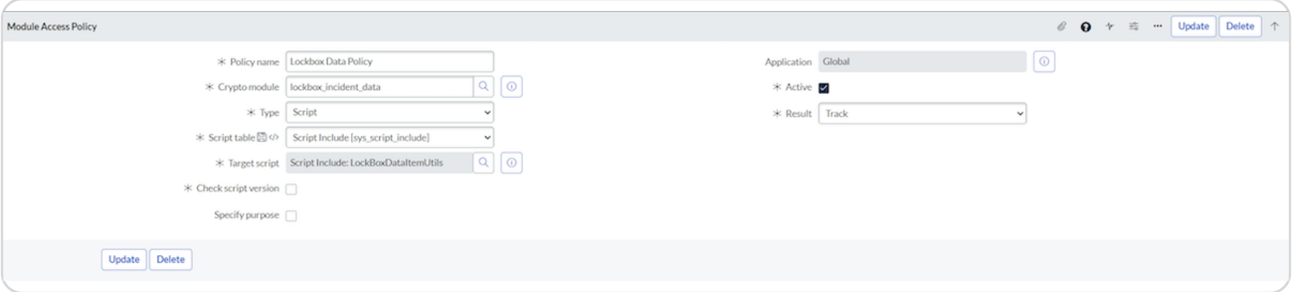


arget role	Script table	Target script
Search	Search	Search
:mpty)	Script Include [sys_script_include]	Script Include: SSHPrivateKeyCredentialUtils
:mpty)		(empty)
:mpty)		(empty)

STEP 13

Configure the Access Policy

Configure your access policy as shown.



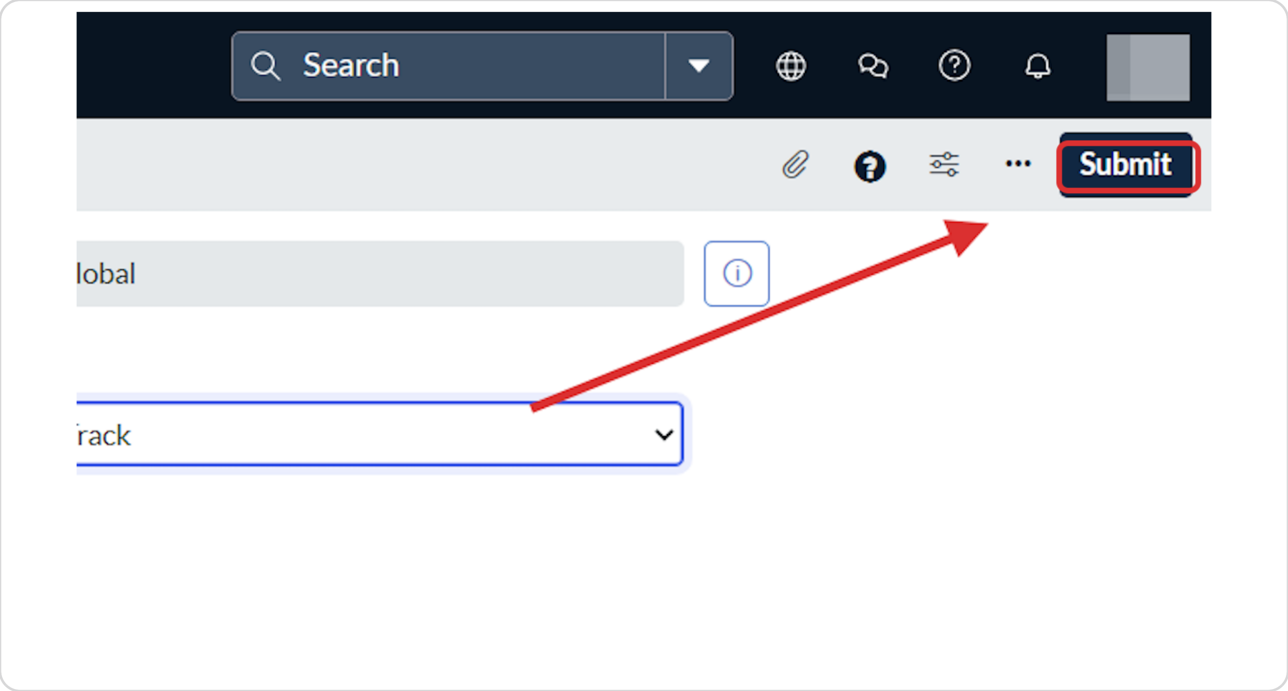
Module Access Policy

* Policy name	Lockbox Data Policy	Application	Global
* Crypto module	lockbox_incident_data	* Active	☑
* Type	Script	* Result	Track
* Script table	Script Include [sys_script_include]		
* Target script	Script Include: LockBoxDataItemUtils		
* Check script version	□		
Specify purpose	□		

STEP 14

Confirm Configuration

Once you have confirmed configuration, save the record.

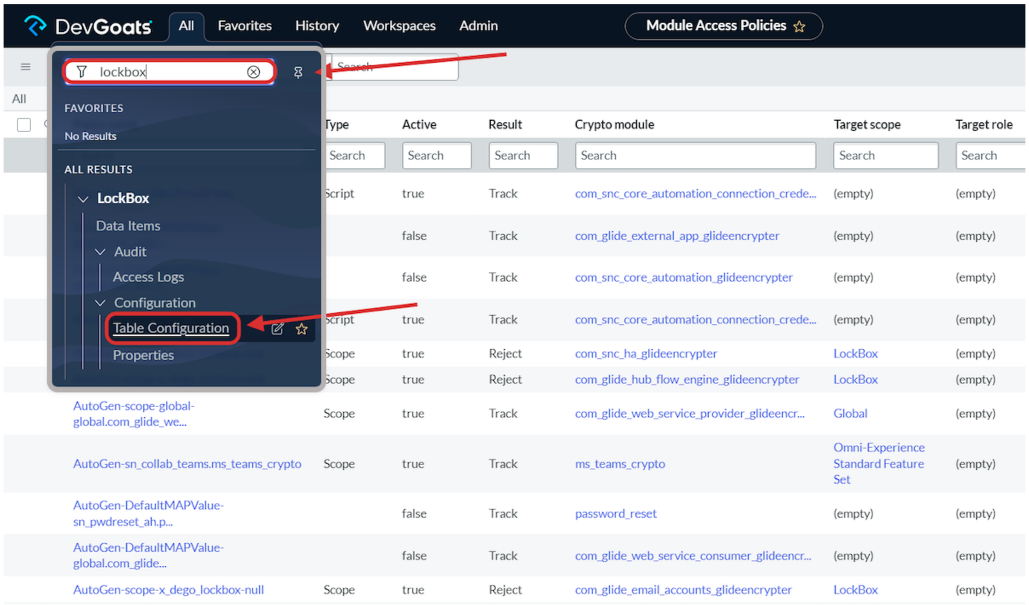


NOTE! We are configuring the "incident" table for this product setup/demo. You may create a entry for any table as you desire by repeating the below steps.

STEP 15

Setup the Table Configuration within the LockBox Application.

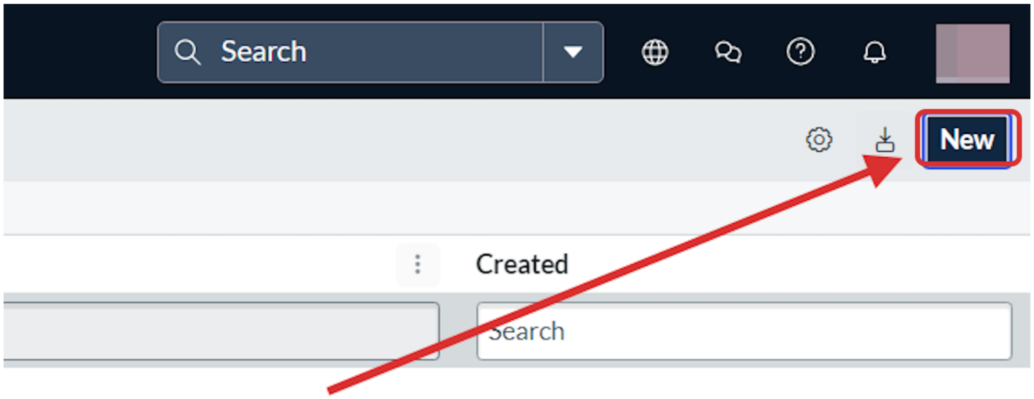
This will enable the the UI Action (button) to be displayed on the incident table. Type LockBox in the filter navigator then select "Table Configuration".



	Type	Active	Result	Crypto module	Target scope	Target role
	Search	Search	Search	Search	Search	Search
	Script	true	Track	com_snc_core_automation_connection_crede...	(empty)	(empty)
		false	Track	com_glide_external_app_glideencrypter	(empty)	(empty)
		false	Track	com_snc_core_automation_glideencrypter	(empty)	(empty)
	Script	true	Track	com_snc_core_automation_connection_crede...	(empty)	(empty)
	Scope	true	Reject	com_snc_ha_glideencrypter	LockBox	(empty)
	Scope	true	Reject	com_glide_hub_flow_engine_glideencrypter	LockBox	(empty)
AutoGen-scope-global-global.com_glide_we...	Scope	true	Track	com_glide_web_service_provider_glideencr...	Global	(empty)
AutoGen-sn_collab_teams.ms_teams_crypto	Scope	true	Track	ms_teams_crypto	Omni-Experience Standard Feature Set	(empty)
AutoGen-DefaultMAPValue-sn_pwdreset_ah.p...		false	Track	password_reset	(empty)	(empty)
AutoGen-DefaultMAPValue-global.com_glide...		false	Track	com_glide_web_service_consumer_glideencr...	(empty)	(empty)
AutoGen-scope-x_dego_lockbox-null	Scope	true	Reject	com_glide_email_accounts_glideencrypter	LockBox	(empty)

STEP 16

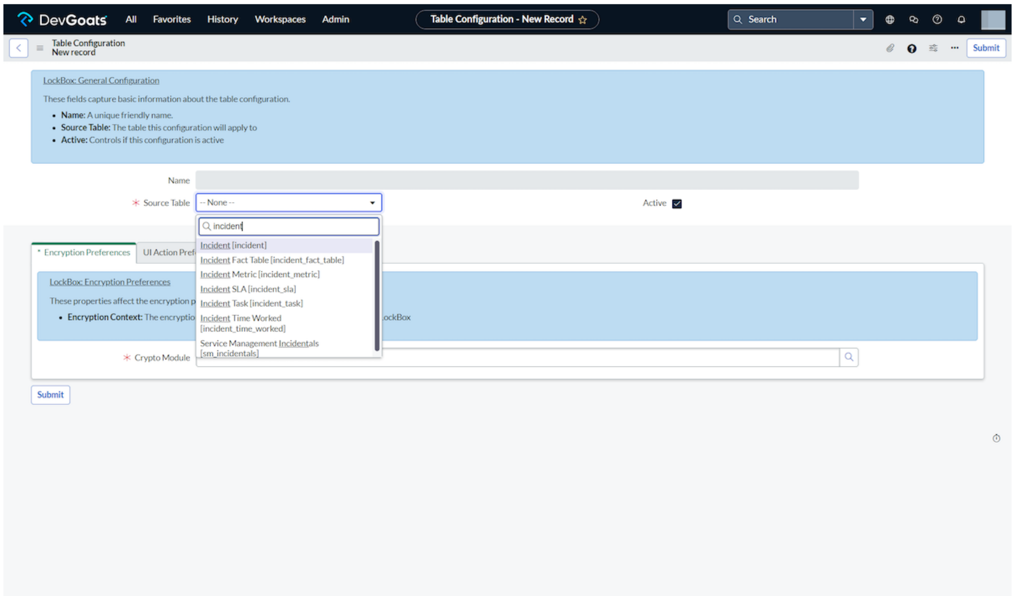
Click on New



STEP 17

Configure Form

Select "incident" as the source table. Confirm the record is "active" (box is checked).



LockBox: General Configuration

These fields capture basic information about the table configuration.

- **Name:** A unique friendly name.
- **Source Table:** The table this configuration will apply to
- **Active:** Controls if this configuration is active

Name			
* Source Table	-- None --	Active	☑

incident

- Incident [incident]
- Incident Fact Table [incident_fact_table]
- Incident Metric [incident_metric]
- Incident SLA [incident_sla]
- Incident Task [incident_task]
- Incident Time Worked [incident_time_worked]
- Service Management Incidentals [sm_incidentals]

LockBox: Encryption Preferences

These properties affect the encryption p

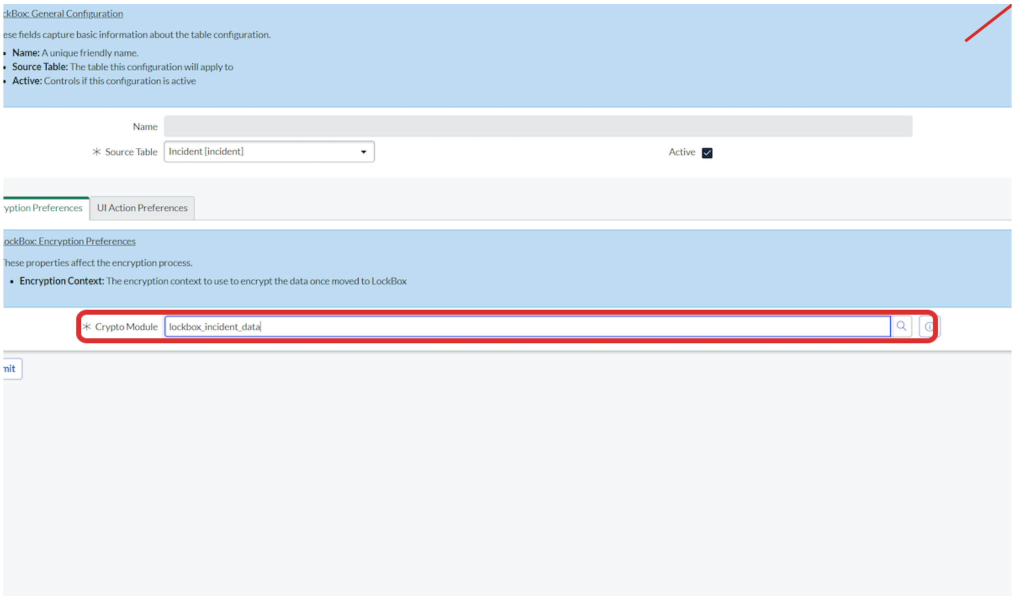
- **Encryption Context:** The encryptio ockBox

* Crypto Module

STEP 18

Select the Crypto Module to be associated with the table configuration.

This is important, you must select the same module you created in steps 3 - 5.



kBox: General Configuration

ese fields capture basic information about the table configuration.

- **Name:** A unique friendly name.
- **Source Table:** The table this configuration will apply to
- **Active:** Controls if this configuration is active

Name			
* Source Table	Incident [incident]	Active	☑

ockBox: Encryption Preferences

hese properties affect the encryption process.

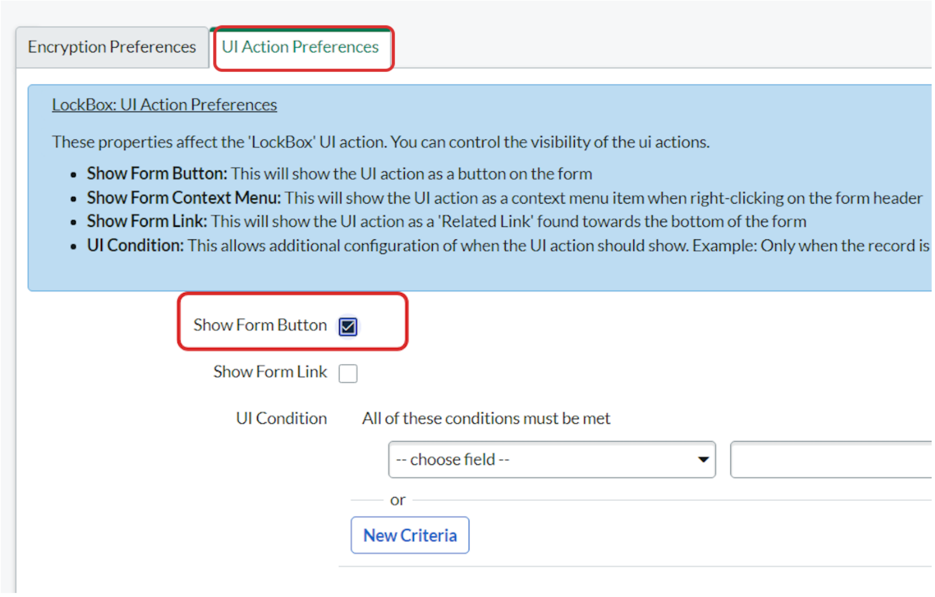
- **Encryption Context:** The encryption context to use to encrypt the data once moved to LockBox

* Crypto Module: lockbox_incident_data

STEP 19

Click on UI Action Preferences Section

Check "Show Form Button". Submit the Record.



LockBox: UI Action Preferences

These properties affect the 'LockBox' UI action. You can control the visibility of the ui actions.

- **Show Form Button:** This will show the UI action as a button on the form
- **Show Form Context Menu:** This will show the UI action as a context menu item when right-clicking on the form header
- **Show Form Link:** This will show the UI action as a 'Related Link' found towards the bottom of the form
- **UI Condition:** This allows additional configuration of when the UI action should show. Example: Only when the record is

Show Form Button ☑

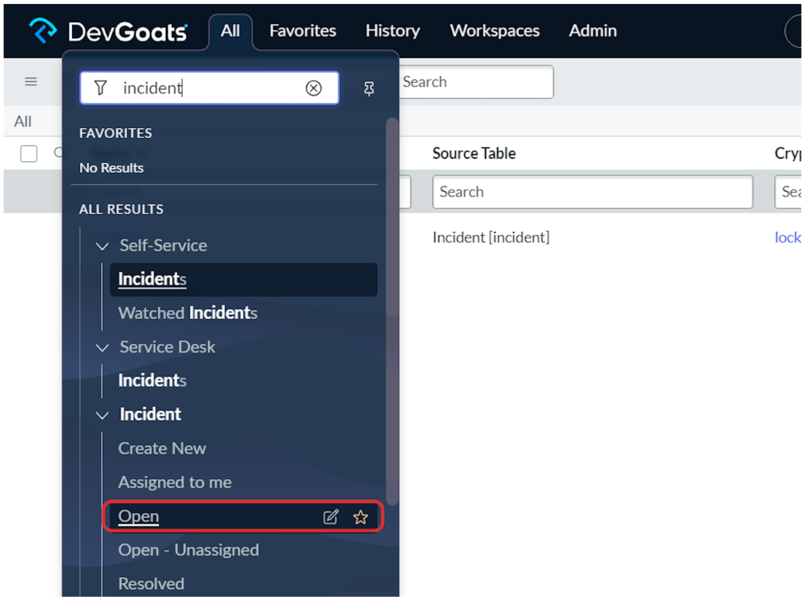
Show Form Link □

UI Condition All of these conditions must be met

STEP 20

Let's test our configuration

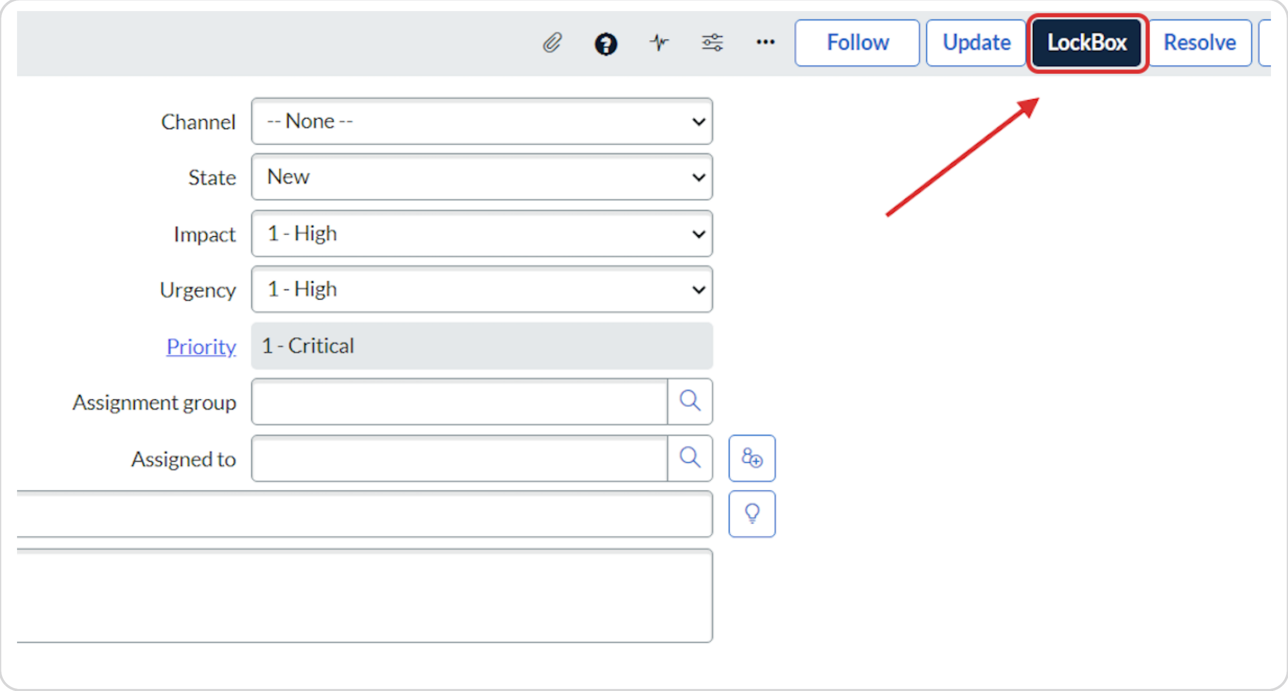
In your filter navigator. Navigate to the incident list.



STEP 21

Find a "active" or (open) incident.

Once you have opened an incident, you will notice the new button named "LockBox".

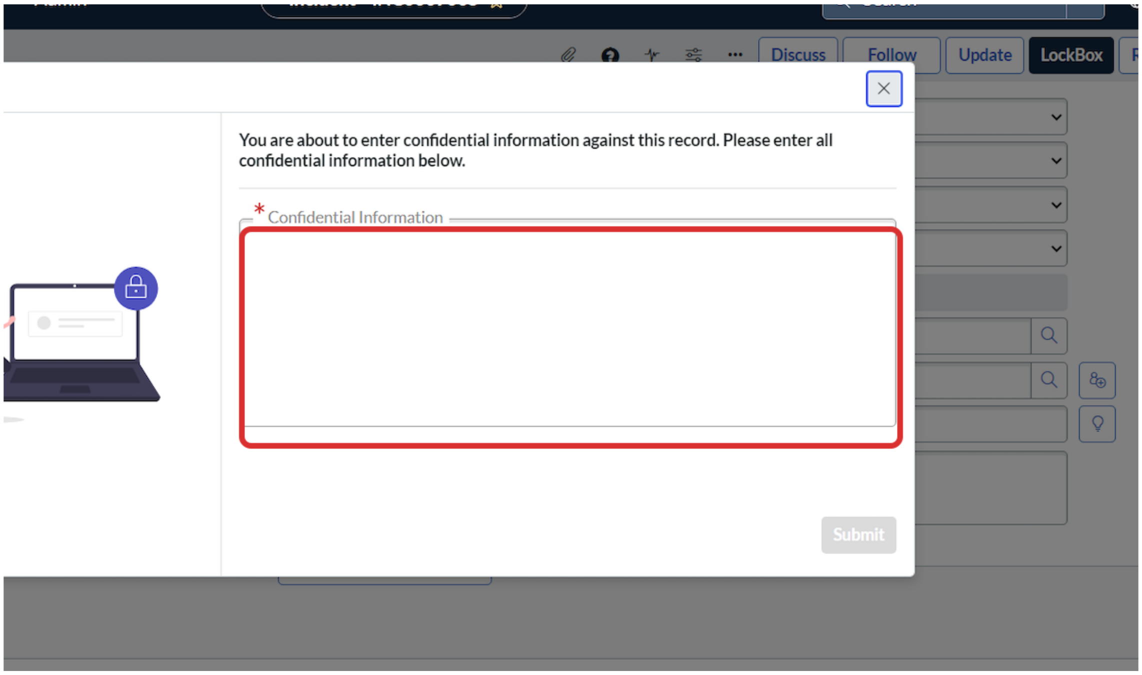


Channel	-- None --
State	New
Impact	1 - High
Urgency	1 - High
Priority	1 - Critical
Assignment group	
Assigned to	

STEP 22

Click on the LockBox Button

Once you have the modal open, you may type your sensitive information that will be stored securely within a encrypted record.



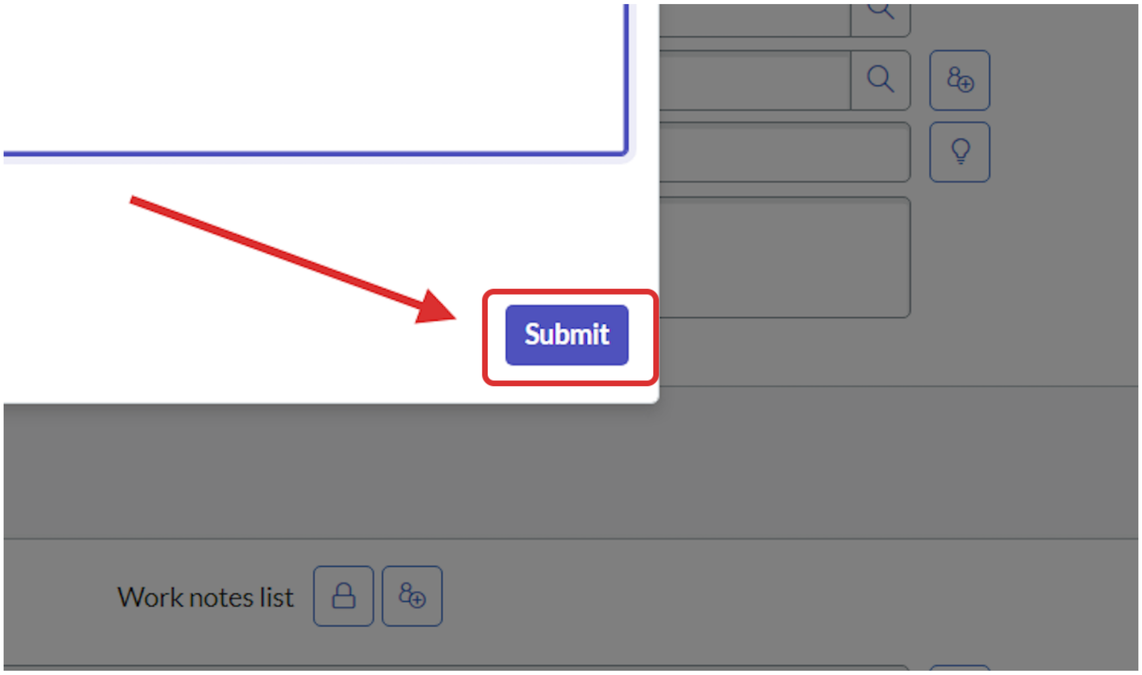
You are about to enter confidential information against this record. Please enter all confidential information below.

* Confidential Information

STEP 23

Message Input

Type a message you would like secured. Choose Submit when done.

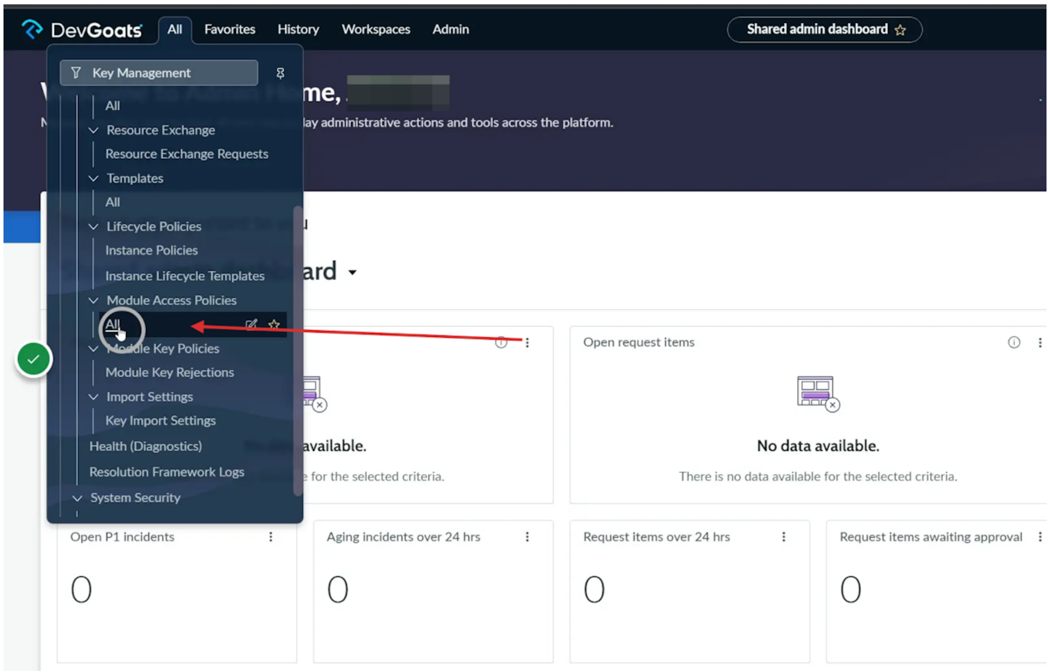


NOTE: You cannot view the saved data until we configure the next steps to setup a new access policy that will grant users with the ITIL role to view the secure data. Note, for this demo we are choosing the ITIL role. Confirm with your System Administration or Security team to see which role needs access to view the secure data.

STEP 24

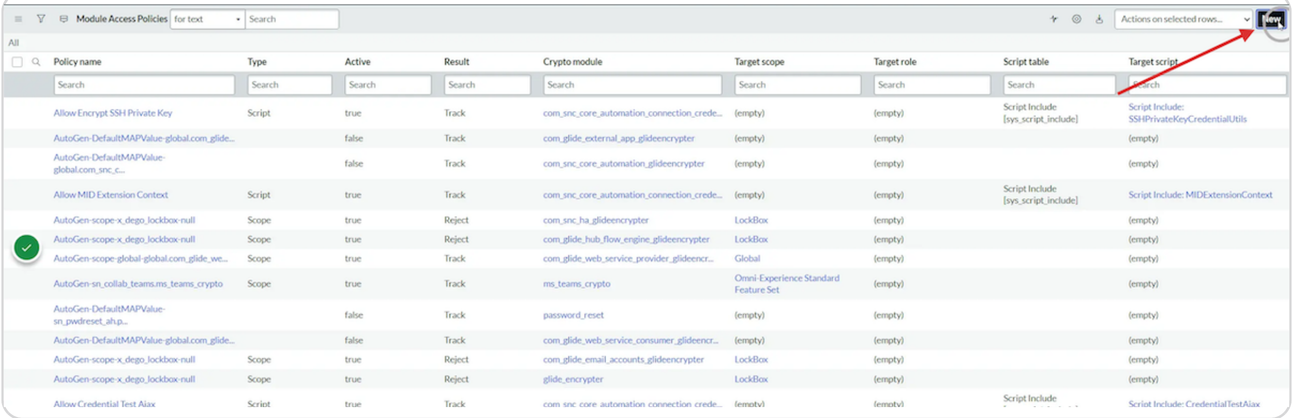
Create new ITIL Access Policy

Search "Key Management" in your filter navigator. Find the "All" menu option under the Module Access Policies



STEP 25

Click Create New

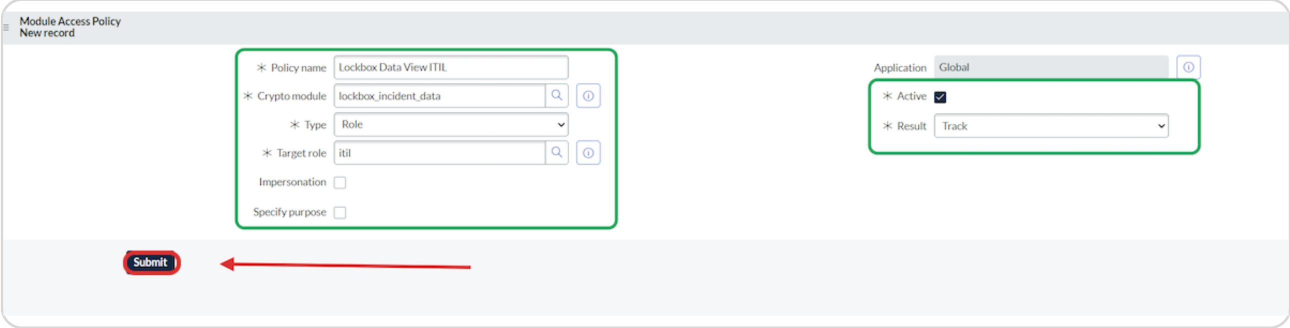


Policy name	Type	Active	Result	Crypto module	Target scope	Target role	Script table	Target script
Allow Encrypt SSH Private Key	Script	true	Track	com_snc_core_automation_connection_crede...	(empty)	(empty)	Script Include [sys_script_include]	Script Include: SSHPrivateKeyCredentialUtils
AutoGen-DefaultMAPValue-global.com_glide...		false	Track	com_glide_external_app_glideencrypter	(empty)	(empty)		(empty)
AutoGen-DefaultMAPValue-global.com_snc_c...		false	Track	com_snc_core_automation_glideencrypter	(empty)	(empty)		(empty)
Allow MID Extension Context	Script	true	Track	com_snc_core_automation_connection_crede...	(empty)	(empty)	Script Include [sys_script_include]	Script Include: MIDExtensionContext
AutoGen-scope-x_dego_lockbox-null	Scope	true	Reject	com_snc_ha_glideencrypter	LockBox	(empty)		(empty)
AutoGen-scope-x_dego_lockbox-null	Scope	true	Reject	com_glide_hub_flow_engine_glideencrypter	LockBox	(empty)		(empty)
AutoGen-scope-global-global.com_glide_we...	Scope	true	Track	com_glide_web_service_provider_glideencr...	Global	(empty)		(empty)
AutoGen-sn_collab_teams.ms_teams_crypto	Scope	true	Track	ms_teams_crypto	Omni-Experience Standard Feature Set	(empty)		(empty)
AutoGen-DefaultMAPValue-sn_pwdreset_ah.p...		false	Track	password_reset	(empty)	(empty)		(empty)
AutoGen-DefaultMAPValue-global.com_glide...		false	Track	com_glide_web_service_consumer_glideencr...	(empty)	(empty)		(empty)
AutoGen-scope-x_dego_lockbox-null	Scope	true	Reject	com_glide_email_accounts_glideencrypter	LockBox	(empty)		(empty)
AutoGen-scope-x_dego_lockbox-null	Scope	true	Reject	glide_encrypter	LockBox	(empty)		(empty)
Allow Credential Test Ajax	Script	true	Track	com_snc_core_automation_connection_crede...	(empty)	(empty)	Script Include	Script Include: CredentialTestAjax

STEP 26

Configure Record as shown

This example we are setting the ITIL role to be able to access the secure entries under our 'lockbox_incident_data' module. Once you have configured the record as shown below, submit the record.



Module Access Policy
New record

* Policy name: Lockbox Data View ITIL
* Crypto module: lockbox_incident_data
* Type: Role
* Target role: itil
Impersonation: □
Specify purpose: □

Application: Global
* Active: ☑
* Result: Track

NOTE: Since you have modified access policies you must logout of ServiceNow and log back in for the access to take effect.

STEP 27

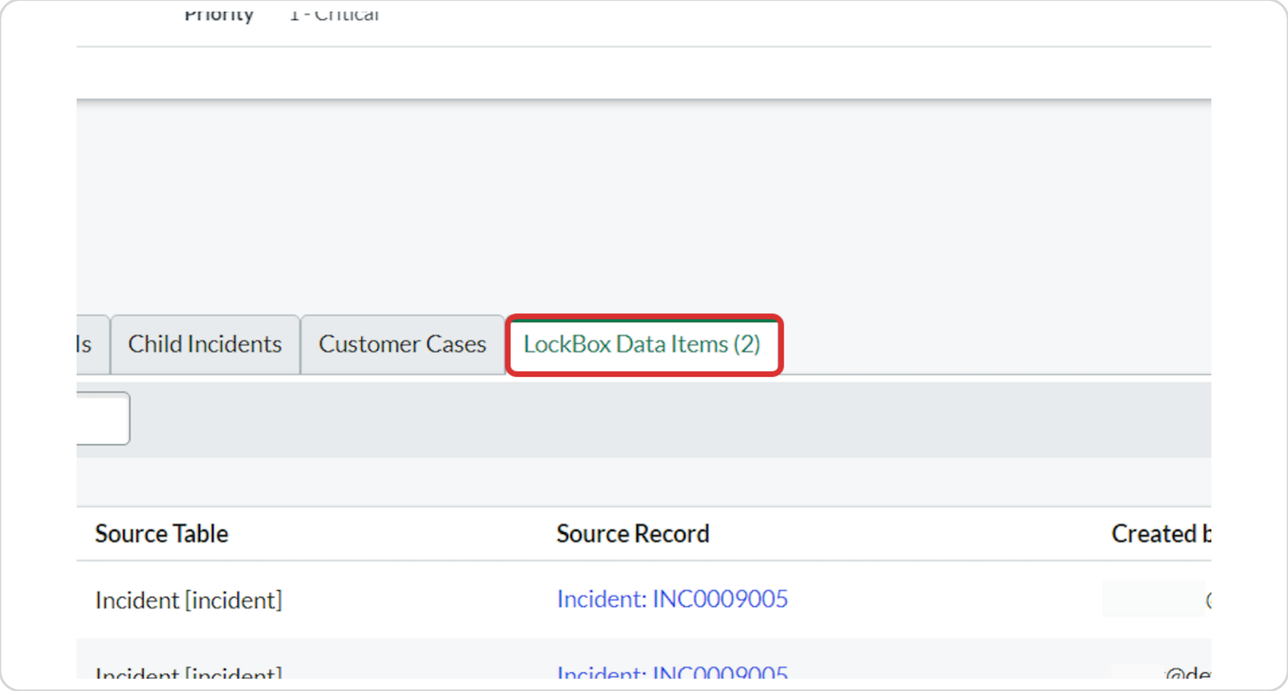
Let's revisit our previous incident.

Once you have logged out of ServiceNow, and reauthenicated back in. You may navigate back to the previous incident where we stored our new secure message.

STEP 28

Viewing the saved data

On the incident record you previously added a new entry to. Confirm you have a tab/list of "LockBox Data Items" on the bottom of the record as shown.



Source Table	Source Record	Created b
Incident [incident]	Incident: INC0009005	(
Incident [incident]	Incident: INC0009005	@de

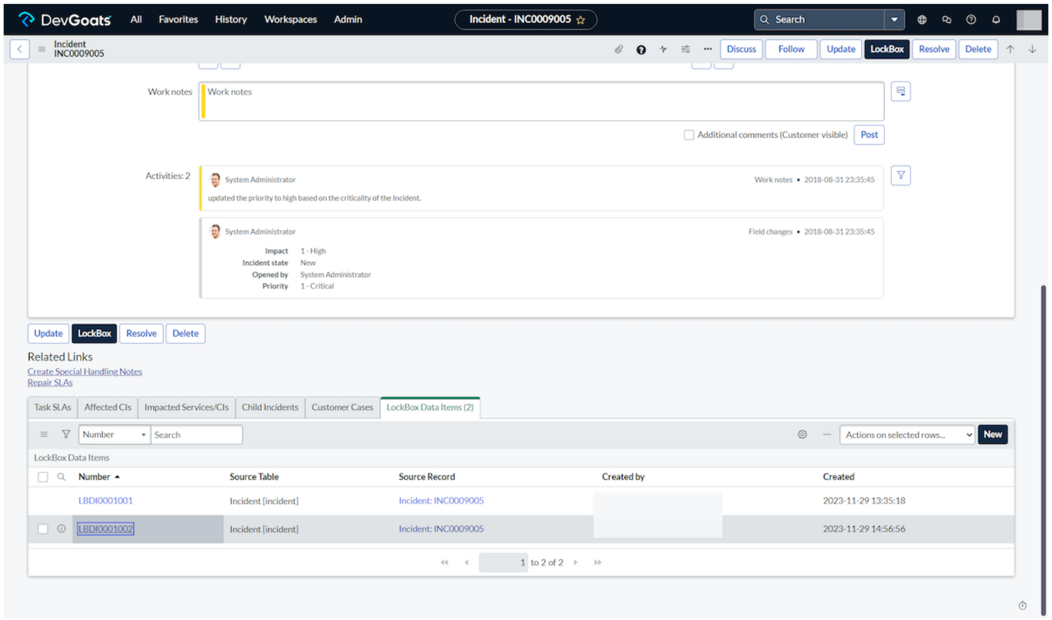
If the related list does not show the Lockbox Data Items as shown above, please follow the configuration steps as found here: https://docs.servicenow.com/bundle/vancouver-platform-user-interface/page/use/using-forms/task/t_SelectRelatedRecords.html

The list name will be "LockBox Data Items".

STEP 29

Find the most recent entry to view the record/data that you have saved.

Note: Access to view this record will be dependent on the module access policies. By default, no one has access to the record. We fixed that by configuring the ITIL Access Policy above. You must repeat this process or any custom role or access policy you would like to grant.



Work notes: Work notes

□ Additional comments (Customer visible)

Activities: 2

System Administrator — Work notes • 2018-08-31 23:35:45

updated the priority to high based on the criticality of the Incident.

System Administrator — Field changes • 2018-08-31 23:35:45

Impact: 1 - High
Incident state: New
Opened by: System Administrator
Priority: 1 - Critical

Related Links
Create Special Handling Notes
Repair SLAs

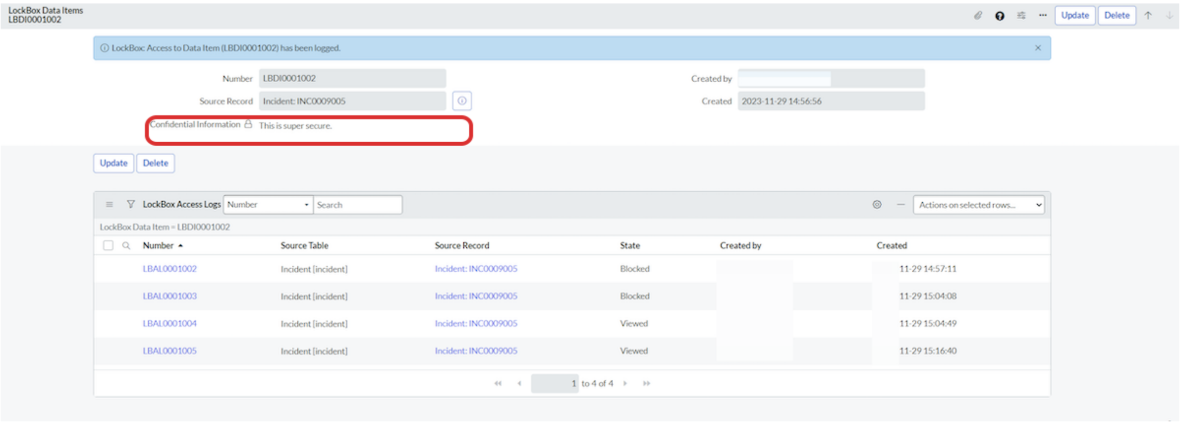
LockBox Data Items

Number ▲	Source Table	Source Record	Created by	Created
LBDI0001001	Incident [incident]	Incident: INC0009005	[redacted]	2023-11-29 13:35:18
LBDI0001002	Incident [incident]	Incident: INC0009005	[redacted]	2023-11-29 14:56:56

STEP 30

Open the Secure Entry

You can see the secure data is now available as the user viewing the record as the ITIL role as required by the previous access policy that we setup.



ⓘ LockBox Access to Data Item (LBDI0001002) has been logged.

Number: LBDI0001002
Source Record: Incident: INC0009005
Confidential Information 🔒 This is super secure.
Created by: [redacted]
Created: 2023-11-29 14:56:56

LockBox Data Item = LBDI0001002

Number ▲	Source Table	Source Record	State	Created by	Created
LBAL0001002	Incident [incident]	Incident: INC0009005	Blocked	[redacted]	11-29 14:57:11
LBAL0001003	Incident [incident]	Incident: INC0009005	Blocked	[redacted]	11-29 15:04:08
LBAL0001004	Incident [incident]	Incident: INC0009005	Viewed	[redacted]	11-29 15:04:49
LBAL0001005	Incident [incident]	Incident: INC0009005	Viewed	[redacted]	11-29 15:16:40

Note: The access logs will help show who has viewed that record. The data is hidden in the demo for privacy reasons.