VECTRA XDR FOR SIR - USER GUIDE

Vectra XDR for SIR (2.0.0)

Table of Contents

1. Overview

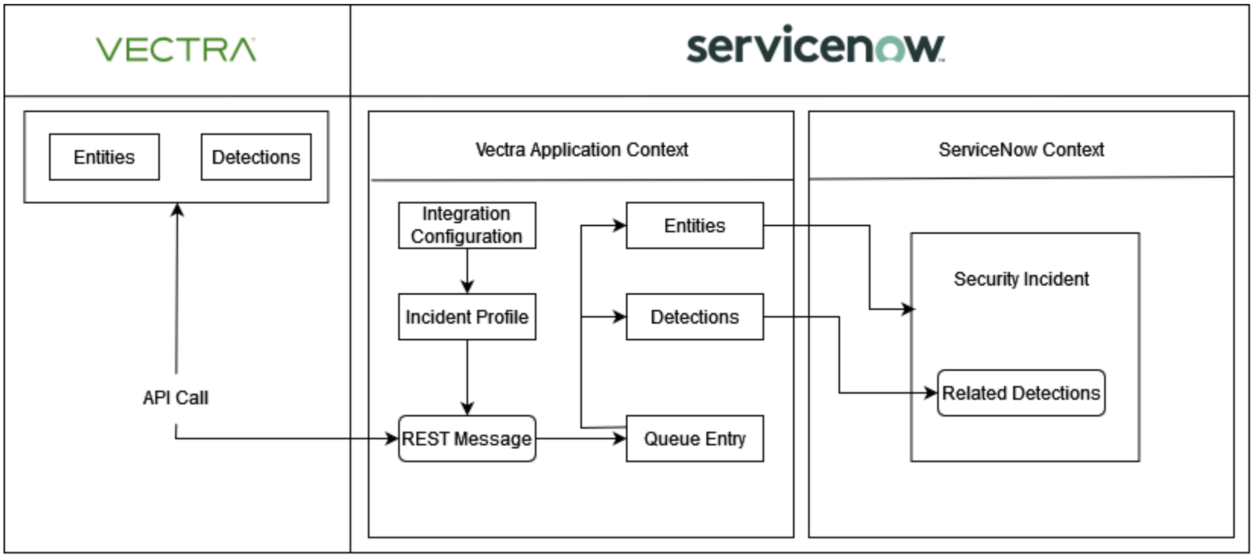
The Vectra threat detection & response platform captures packets and logs across your public cloud, SaaS, federated identity, and data center networks. It applies patented security-led AI to the surface, prioritizes threats, and integrates into your security stack for rapid response.

Vectra ServiceNow Application

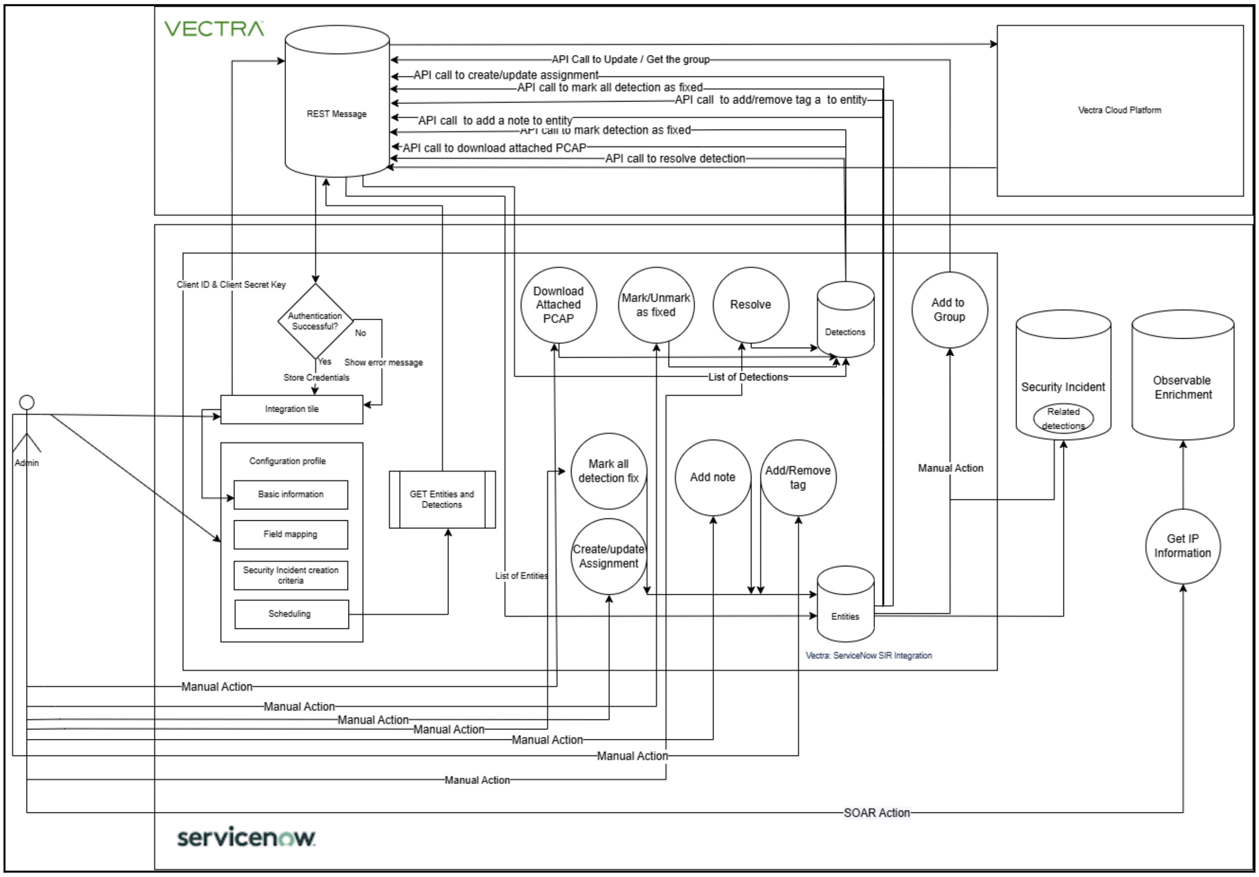
This application fetches Entities and Detections from the Vectra Detect based on the provided API filters and ingests data into the ServiceNow platform. It provides the capability of creating “Security Incidents” based on the defined condition/criteria. It also provides support to perform some manual actions on fetched entities and detections.

System Diagram

The diagram below depicts the high-level architecture of the integration.



Architectural Diagram



1.1. Application Features

The main features of the application are listed below.

- Ability to fetch Entities from the Vectra Detect based on the different types of API filters.
- Ability to fetch detections associated with the Entities.
- Ability to configure Security Incident creation criteria and create Security Incidents based on them.
- Ability to define CI Lookup Rules.
- Ability to assign Security Incidents to a specific user.
- Ability to map Entity fields with ServiceNow Security Incident fields.
- Ability to add/remove a tag to an Entity or detection in Vectra Detect.
- Ability to add a note to an entity or detection in Vectra Detect Platform.
- Ability to download a PCAP attached to a detection.
- Ability to mark/unmark the detection(s) as fixed from ServiceNow.
- Ability to mark all detections as fixed from an entity.
- Ability to add/update an assignment to an Entity on Vectra Detect.
- Ability to resolve the detection and entity.

- Ability to fetch the detections from the entity form view.
- Ability to get latest details of detection by performing Describe Detection action.
- Ability to assign the user to the entity on the Vectra platform from the Incident.
- Ability to assign a group to the entity by running the action “Add to Group”.

1.2. Compatibility Matrix

ServiceNow Version:

- Washington DC
- Xanadu
- Yokohama

Vectra Detect API Version:

- Entity data collection:
  - 3.4
- SOAR Actions: All APIs have current version 3.4 as on May 26.

2. Vectra XDR for SIR

2.1. Installation

This section describes how to download and install the Vectra XDR for SIR application from the ServiceNow app store.

2.1.1. Pre-Requisites

This section lists the prerequisites required to install the application.

- Vectra XDR ServiceNow SecOps

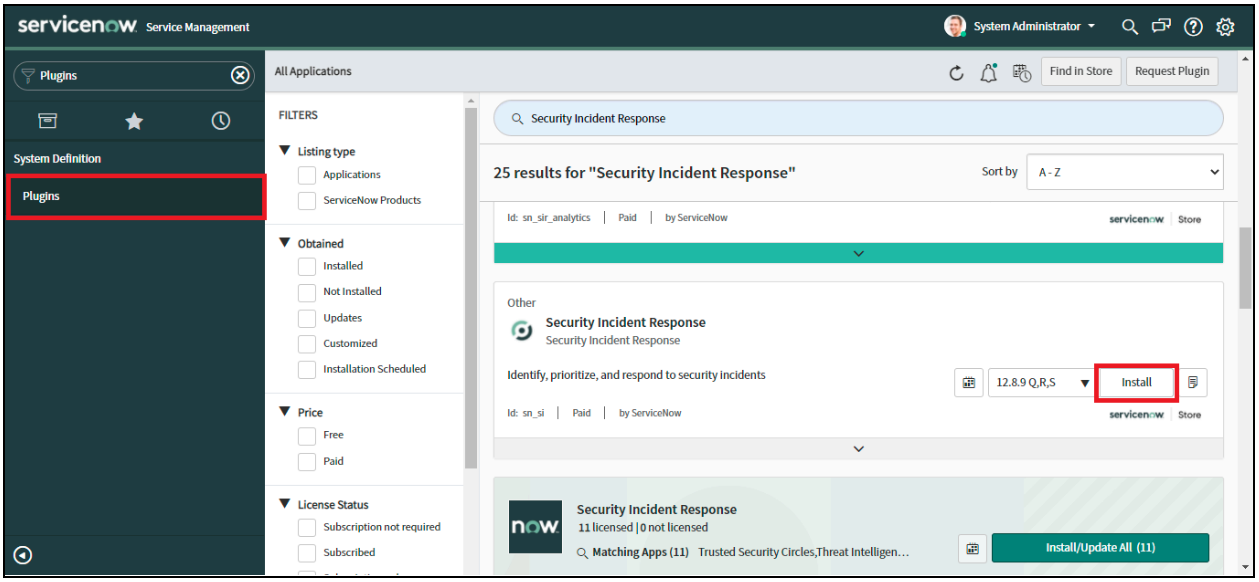
2.1.1.1. ServiceNow Plugins to be Installed

Below ServiceNow plugin must be Installed:

- Security Incident Response -version -

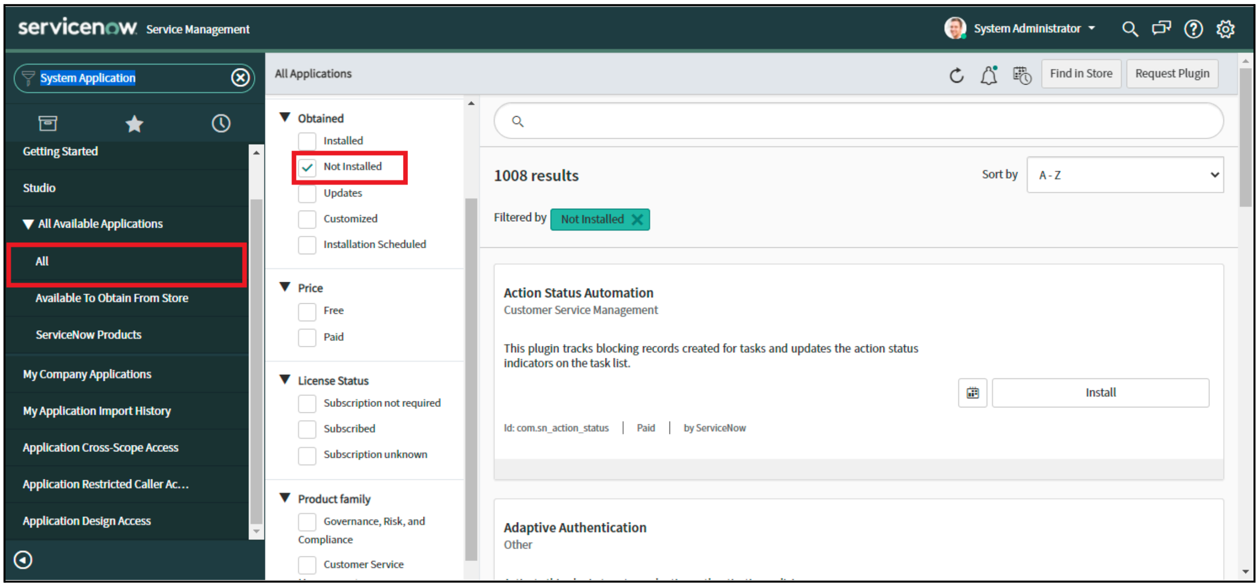
  To install this plugin:

  1. Log in to your instance with your user credentials.
  2. Verify you have the system administrator (admin) role.
  3. Navigate to System Definition > Plugins in your instance.
  4. Search and install the above plugins.


servicenow Service Management
System Administrator
Plugins
System Definition
Plugins
All Applications
Find in Store
Request Plugin
FILTERS
Listing type
Applications
ServiceNow Products
Obtained
Installed
Not Installed
Updates
Customized
Installation Scheduled
Price
Free
Paid
License Status
Subscription not required
Subscribed
Security Incident Response
25 results for "Security Incident Response"
Sort by
A - Z
Id: sn_sir_analytics | Paid | by ServiceNow
servicenow Store
Other
Security Incident Response
Security Incident Response
Identify, prioritize, and respond to security incidents
12.8.9 Q,R,S
Install
Id: sn_si | Paid | by ServiceNow
servicenow Store
now
Security Incident Response
11 licensed | 0 not licensed
Matching Apps (11) Trusted Security Circles,Threat Intelligen...
Install/Update All (11)

2.1.2. Application Download and installation

- Log in to the ServiceNow instance where you want to install the application.
- Navigate to System Applications > All Available Applications > All.

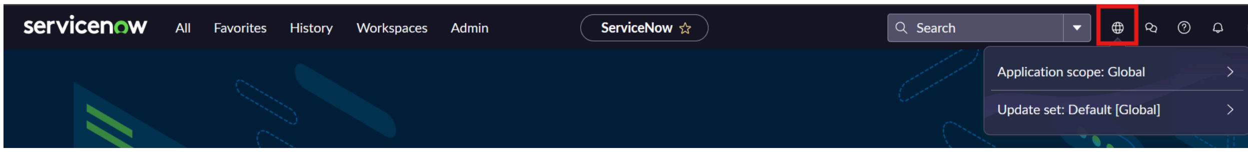

servicenow Service Management
System Administrator
System Application
Getting Started
Studio
All Available Applications
All
Available To Obtain From Store
ServiceNow Products
My Company Applications
My Application Import History
Application Cross-Scope Access
Application Restricted Caller Ac...
Application Design Access
All Applications
Find in Store
Request Plugin
Obtained
Installed
Not Installed
Updates
Customized
Installation Scheduled
Price
Free
Paid
License Status
Subscription not required
Subscribed
Subscription unknown
Product family
Governance, Risk, and Compliance
Customer Service
1008 results
Sort by
A - Z
Filtered by
Not Installed
Action Status Automation
Customer Service Management
This plugin tracks blocking records created for tasks and updates the action status indicators on the task list.
Install
Id: com.sn_action_status | Paid | by ServiceNow
Adaptive Authentication
Other

- Click on the “Not Installed tab”. A list of applications available for installation will be displayed.
- Locate the Vectra XDR for SIR app, select it, and click “Install”.
- The application will be installed on your instance.

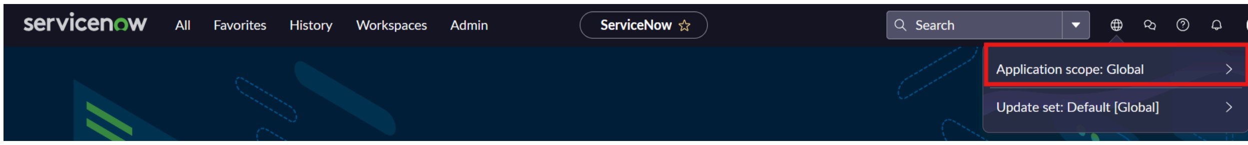
2.1.2.1. Configure Application scope

Follow the mentioned below steps to change the scope of the app.

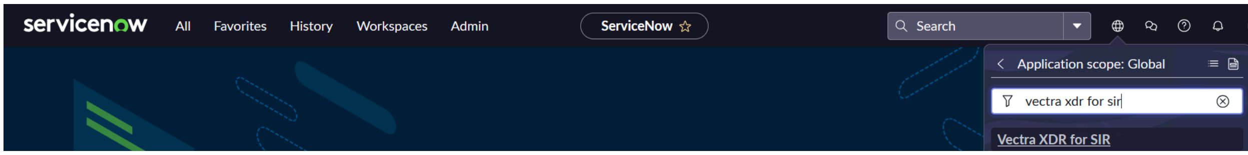
- Click on the “Application Scope” Icon



- Click on arrow



- Enter application name to search application scope.



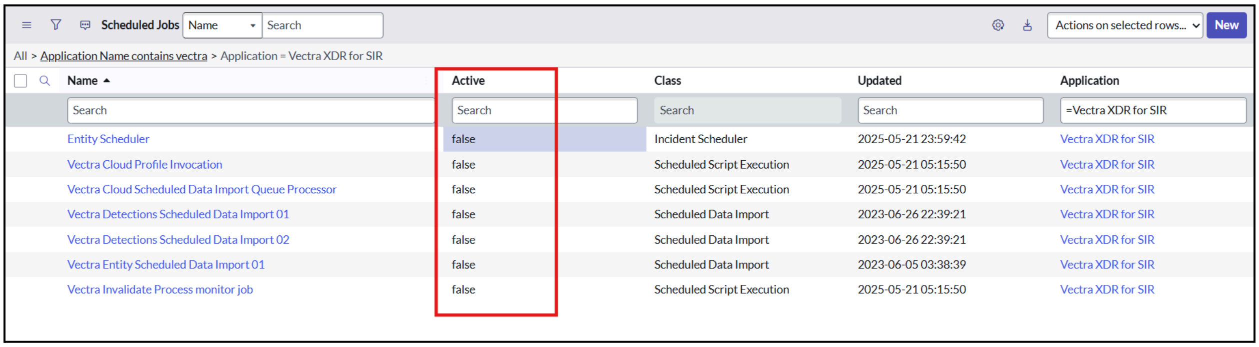
- From the Application Picker drop-down select “Vectra XDR for SIR” as the application scope.
- Note - Similarly, configure the application scope in other ServiceNow versions.

2.1.2.2. Scheduled Jobs Activation

Required roles: System administrator

A user needs to activate all the required scheduled jobs before continuing. Follow below steps to activate all the required scheduled jobs

- Navigate to All -> Vectra XDR for SIR -> Configuration -> Scheduled Jobs
- activate all the scheduled jobs listed here



All > Application Name contains vectra > Application = Vectra XDR for SIR

Name ▲	Active	Class	Updated	Application
Search	Search	Search	Search	=Vectra XDR for SIR
Entity Scheduler	false	Incident Scheduler	2025-05-21 23:59:42	Vectra XDR for SIR
Vectra Cloud Profile Invocation	false	Scheduled Script Execution	2025-05-21 05:15:50	Vectra XDR for SIR
Vectra Cloud Scheduled Data Import Queue Processor	false	Scheduled Script Execution	2025-05-21 05:15:50	Vectra XDR for SIR
Vectra Detections Scheduled Data Import 01	false	Scheduled Data Import	2023-06-26 22:39:21	Vectra XDR for SIR
Vectra Detections Scheduled Data Import 02	false	Scheduled Data Import	2023-06-26 22:39:21	Vectra XDR for SIR
Vectra Entity Scheduled Data Import 01	false	Scheduled Data Import	2023-06-05 03:38:39	Vectra XDR for SIR
Vectra Invalidate Process monitor job	false	Scheduled Script Execution	2025-05-21 05:15:50	Vectra XDR for SIR

2.1.3. Permissions and Roles

These ServiceNow roles and permissions are required to install the application:

Role	Contains role	Permissions
System administrator	NA	- Can Install the application - Can create Incident Profile - Can access Contact Support - Can access Log module - Can access Process monitor - Can run the SOAR actions
Vectra Admin (sn_si.admin+personalize_dictionary+view_changer)	- sn_si.analyst	- Can Install the application - Can create Incident Profile - Can access Contact Support - Can access Log module - Can access Process monitor - Can run the SOAR actions
Vectra Analyst (sn_si.analyst+Personalize_dictionary+view_changer)	- export_set_scheduler	- Accessing the Application. - Read access to the Incident Profile module. - Can run the SOAR actions. - Can access Support Contact . - Process Monitor (Read Only) - Read Access to the Detection and Entities tables (Only Deeplink navigation access) Deeplink) - Can access Support Contact
MSP Admin (sn_si.admin, personalize_dictionary, view_changer, x_cdsp_vectra_c_si.msp_admin)		Accessing tables - Scheduled Data Import Pool - Data Source Pool - Entites Staging - Detection Staging

2.1.4. Create Users : Non - MSP usecase

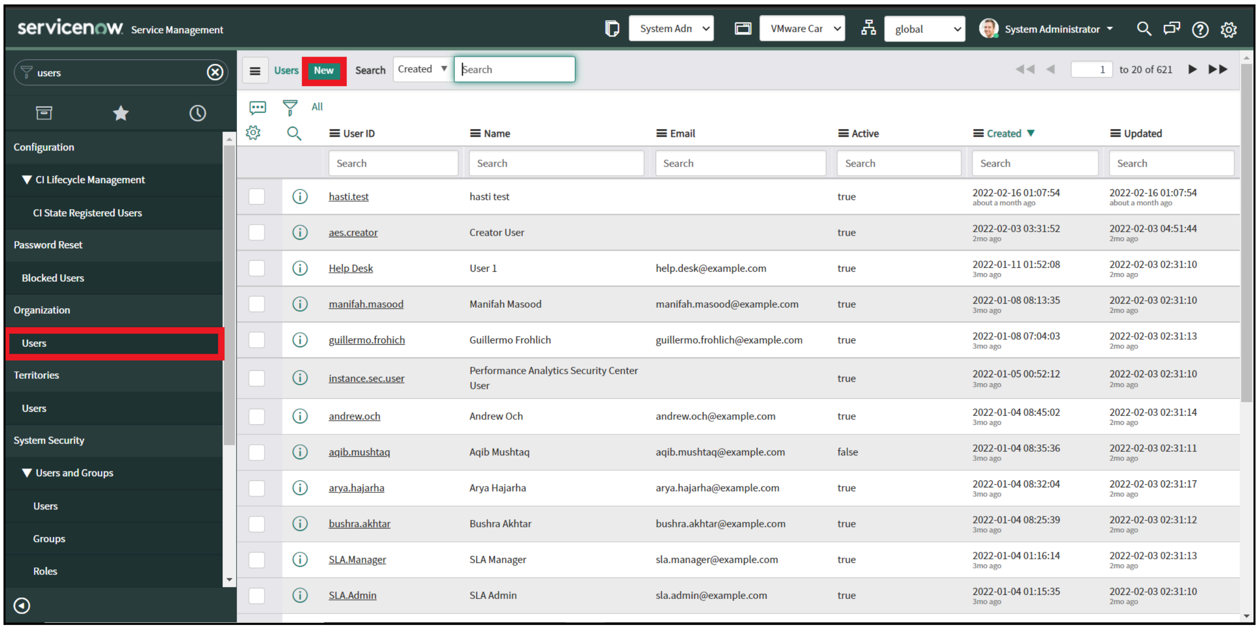
Role Required: System Administrator

The ServiceNow platform admin creates the various users for the Vectra SecOps applications for ServiceNow.

Username (for example)	Role to be assigned
Security Admin	sn_si.admin
Security Analyst	sn_si.analyst

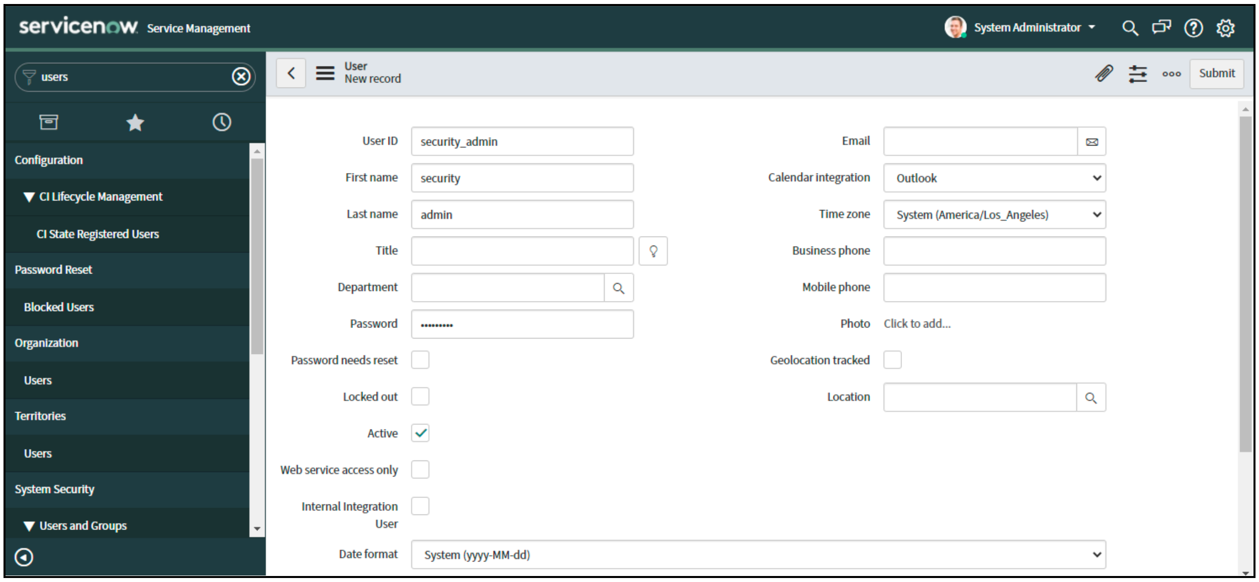
The example below shows how to create a Vectra user and assign a role to it.

1. **Create Security Admin User**
   - Navigate to Organization > Users.
   - Click the Users module.



	User ID	Name	Email	Active	Created	Updated
	Search	Search	Search	Search	Search	Search
ⓘ	hasti.test	hasti test		true	2022-02-16 01:07:54 about a month ago	2022-02-16 01:07:54 about a month ago
ⓘ	aes.creator	Creator User		true	2022-02-03 03:31:52 2mo ago	2022-02-03 04:51:44 2mo ago
ⓘ	Help Desk	User 1	help.desk@example.com	true	2022-01-11 01:52:08 3mo ago	2022-02-03 02:31:10 2mo ago
ⓘ	manifah.masood	Manifah Masood	manifah.masood@example.com	true	2022-01-08 08:13:35 3mo ago	2022-02-03 02:31:10 2mo ago
ⓘ	guillermo.frohich	Guillermo Frohlich	guillermo.frohlich@example.com	true	2022-01-08 07:04:03 3mo ago	2022-02-03 02:31:13 2mo ago
ⓘ	instance.sec.user	Performance Analytics Security Center User		true	2022-01-05 00:52:12 3mo ago	2022-02-03 02:31:10 2mo ago
ⓘ	andrew.och	Andrew Och	andrew.och@example.com	true	2022-01-04 08:45:02 3mo ago	2022-02-03 02:31:14 2mo ago
ⓘ	aqib.mushtaq	Aqib Mushtaq	aqib.mushtaq@example.com	false	2022-01-04 08:35:36 3mo ago	2022-02-03 02:31:11 2mo ago
ⓘ	arya.hajarha	Arya Hajarha	arya.hajarha@example.com	true	2022-01-04 08:32:04 3mo ago	2022-02-03 02:31:17 2mo ago
ⓘ	bushra.akhtar	Bushra Akhtar	bushra.akhtar@example.com	true	2022-01-04 08:25:39 3mo ago	2022-02-03 02:31:12 2mo ago
ⓘ	SLA.Manager	SLA Manager	sla.manager@example.com	true	2022-01-04 01:16:14 3mo ago	2022-02-03 02:31:13 2mo ago
ⓘ	SLA.Admin	SLA Admin	sla.admin@example.com	true	2022-01-04 01:15:35 3mo ago	2022-02-03 02:31:10 2mo ago

   - Above the User ID list, Click the “New” button. A new User form will be displayed.



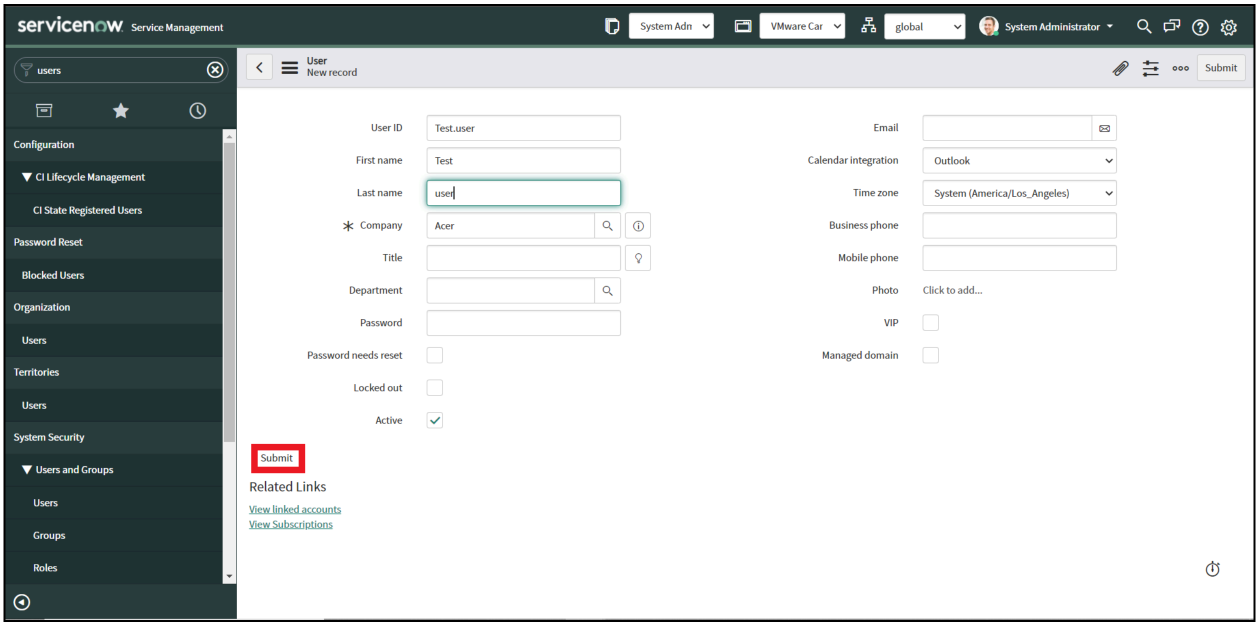
User ID	security_admin
First name	security
Last name	admin
Title	
Department	
Password	••••••••
Password needs reset	□
Locked out	□
Active	☑
Web service access only	□
Internal Integration User	□
Date format	System (yyyy-MM-dd)
Email	
Calendar integration	Outlook
Time zone	System (America/Los_Angeles)
Business phone	
Mobile phone	
Photo	Click to add...
Geolocation tracked	□
Location	

- Fill in the form.

Field	Description
User ID	Unique User ID for the role in your ServiceNow Platform instance. An example is security admin.
First Name	Person you are assigning
Last Name	Person you are assigning
Title	Job Title, for example, security user
Password	Unique password created for this role
Email	Unique email address

Note: Example values for the User ID title and email address are shown in the table below.

- Click “Submit.” Once submitted, you can assign the role.

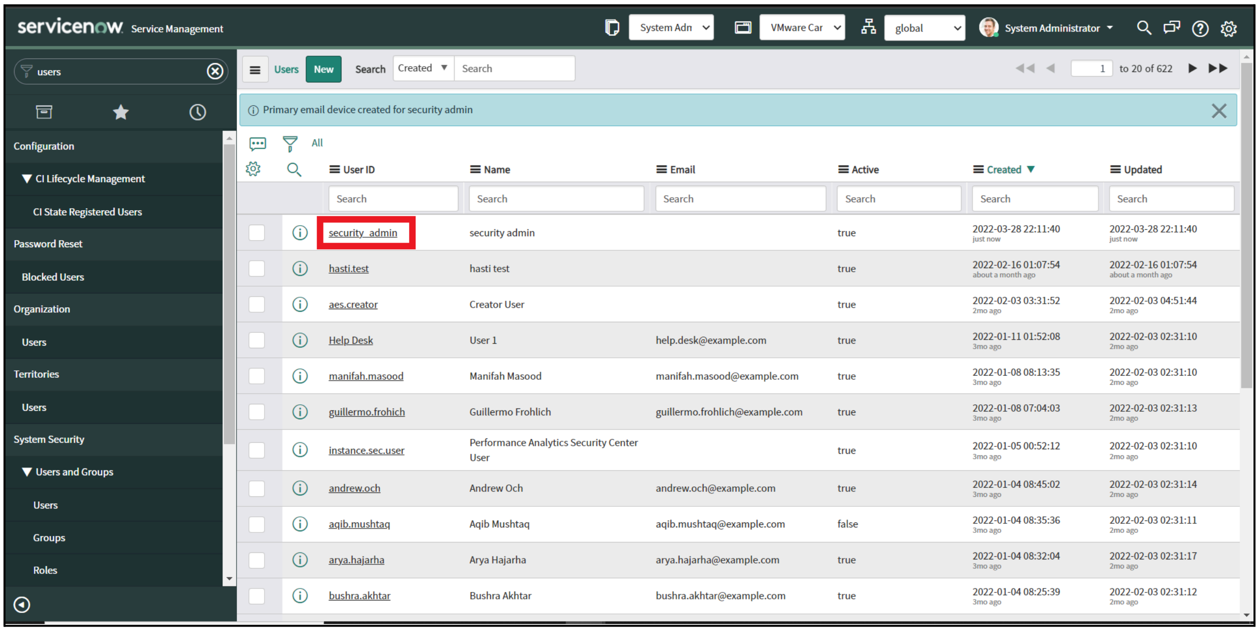


User ID: Test.user
First name: Test
Last name: user
Company: Acer
Title:
Department:
Password:
Password needs reset: □
Locked out: □
Active: ☑
Email:
Calendar integration: Outlook
Time zone: System (America/Los_Angeles)
Business phone:
Mobile phone:
Photo: Click to add...
VIP: □
Managed domain: □

Submit

Related Links
View linked accounts
View Subscriptions

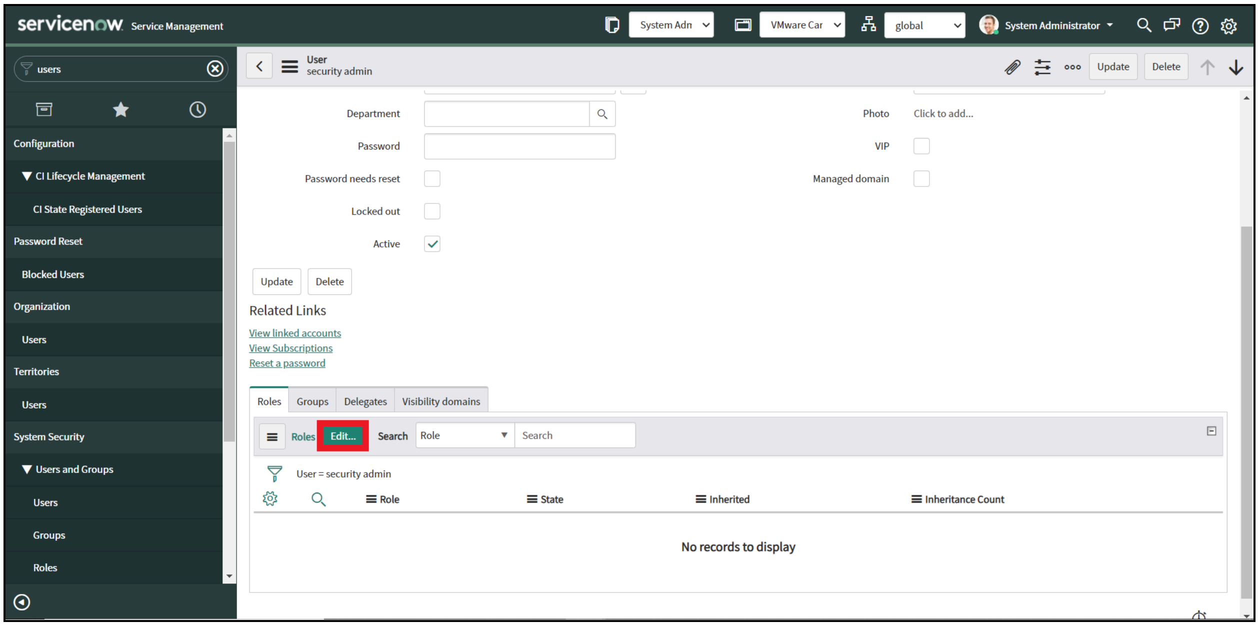
- Click the name of the new user you created.



Primary email device created for security admin

User ID	Name	Email	Active	Created	Updated
security_admin	security admin		true	2022-03-28 22:11:40 just now	2022-03-28 22:11:40 just now
hasti.test	hasti test		true	2022-02-16 01:07:54 about a month ago	2022-02-16 01:07:54 about a month ago
aes.creator	Creator User		true	2022-02-03 03:31:52 2mo ago	2022-02-03 04:51:44 2mo ago
Help Desk	User 1	help.desk@example.com	true	2022-01-11 01:52:08 3mo ago	2022-02-03 02:31:10 2mo ago
manifah.masood	Manifah Masood	manifah.masood@example.com	true	2022-01-08 08:13:35 3mo ago	2022-02-03 02:31:10 2mo ago
guillermo.frohich	Guillermo Frohlich	guillermo.frohlich@example.com	true	2022-01-08 07:04:03 3mo ago	2022-02-03 02:31:13 2mo ago
instance.sec.user	Performance Analytics Security Center User		true	2022-01-05 00:52:12 3mo ago	2022-02-03 02:31:10 2mo ago
andrew.och	Andrew Och	andrew.och@example.com	true	2022-01-04 08:45:02 3mo ago	2022-02-03 02:31:14 2mo ago
aqib.mushtaq	Aqib Mushtaq	aqib.mushtaq@example.com	false	2022-01-04 08:35:36 3mo ago	2022-02-03 02:31:11 2mo ago
arya.hajarha	Arya Hajarha	arya.hajarha@example.com	true	2022-01-04 08:32:04 3mo ago	2022-02-03 02:31:17 2mo ago
bushra.akhtar	Bushra Akhtar	bushra.akhtar@example.com	true	2022-01-04 08:25:39 3mo ago	2022-02-03 02:31:12 2mo ago

- Once the record is open, scroll down and go to the Roles section, and click “Edit”.



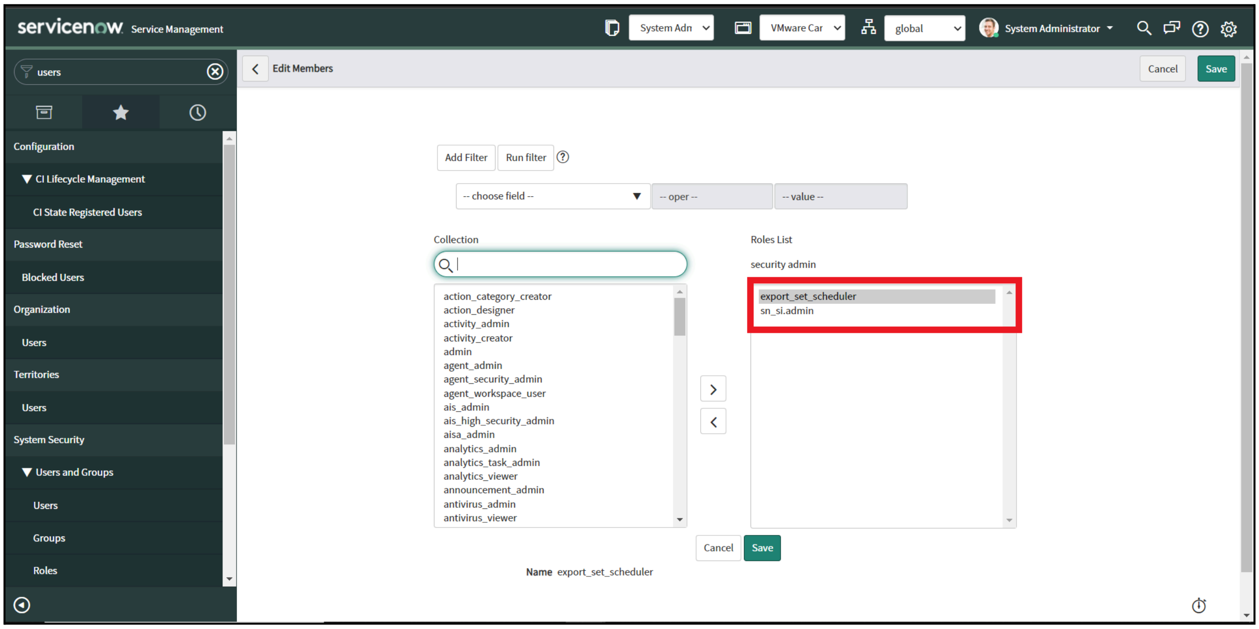
User
security admin

Department
Password
Password needs reset □
Locked out □
Active ☑
Photo Click to add...
VIP □
Managed domain □

User = security admin

No records to display

- When the Edit Members form displays, enter sn_si.admin in the Collection field.
- In the Collection column, select and move sn_si.admin to the Roles list.
- Click the Save button.
- Scroll down and open the role: “ sn_si. admin”
- Scroll down and click on the “Edit” button.
- Search the roles to be added.
- Select the roles and move it to “Contains Roles List” by either double-clicking on the role or clicking on the right arrow.



Collection

action_category_creator
action_designer
activity_admin
activity_creator
admin
agent_admin
agent_security_admin
agent_workspace_user
ais_admin
ais_high_security_admin
aisa_admin
analytics_admin
analytics_task_admin
analytics_viewer
announcement_admin
antivirus_admin
antivirus_viewer

Roles List

security admin

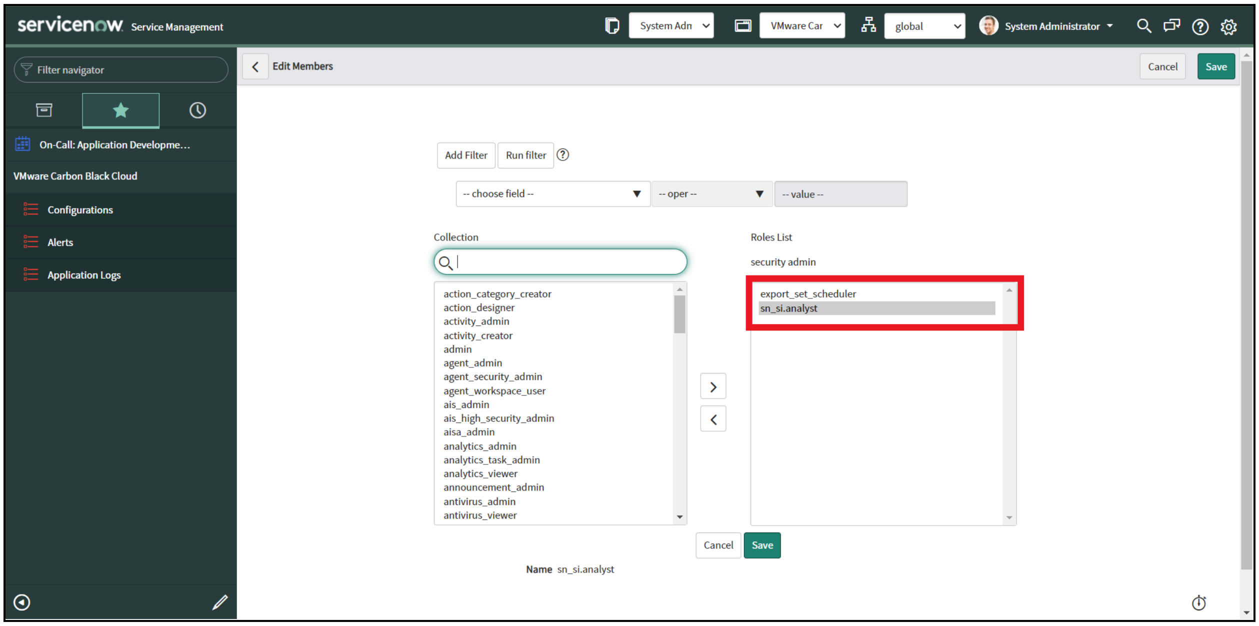
export_set_scheduler
sn_si.admin

Name export_set_scheduler

- When the Edit Members form displays, enter sn_si.admin and export_set_scheduler in the Collection field.
- In the Collection column, select and move sn_si.admin and export_set_scheduler to the Roles List.
- Click the Save button.

2. Create Analyst User

- All of the steps for creating admin users are applicable for analyst users also, but you must add roles specific to analyst i.e. sn_si.analyst +personalize_dictionary(Check the permissions and roles section).



Collection

action_category_creator
action_designer
activity_admin
activity_creator
admin
agent_admin
agent_security_admin
agent_workspace_user
ais_admin
ais_high_security_admin
aisa_admin
analytics_admin
analytics_task_admin
analytics_viewer
announcement_admin
antivirus_admin
antivirus_viewer

Roles List

security admin

export_set_scheduler
sn_si.analyst

Name sn_si.analyst

2.1.5. Create Users : MSP usecase

Role Required: System Administrator

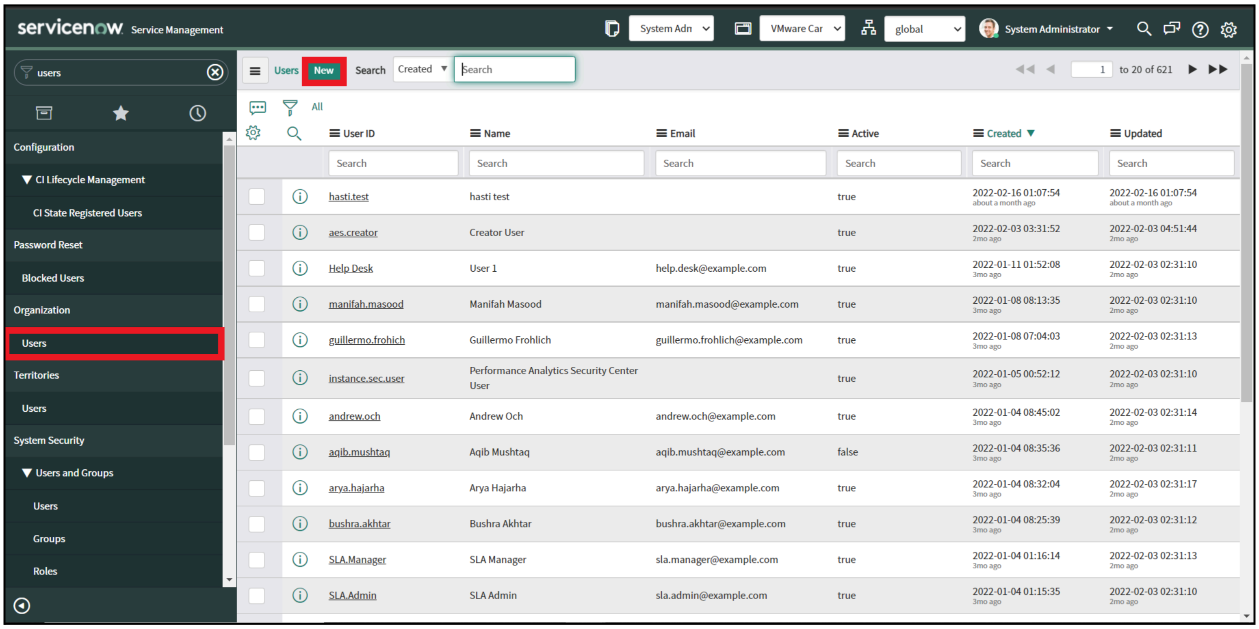
The ServiceNow platform admin creates the various users for the Vectra SecOps applications for ServiceNow.

Username (for example)	Role to be assigned
Security Admin	sn_si.admin
Security Analyst	sn_si.analyst
MSP Admin	x_cdsp_vectra_c_si.msp_admin

The example below shows how to create a Vectra user and assign a role to it.

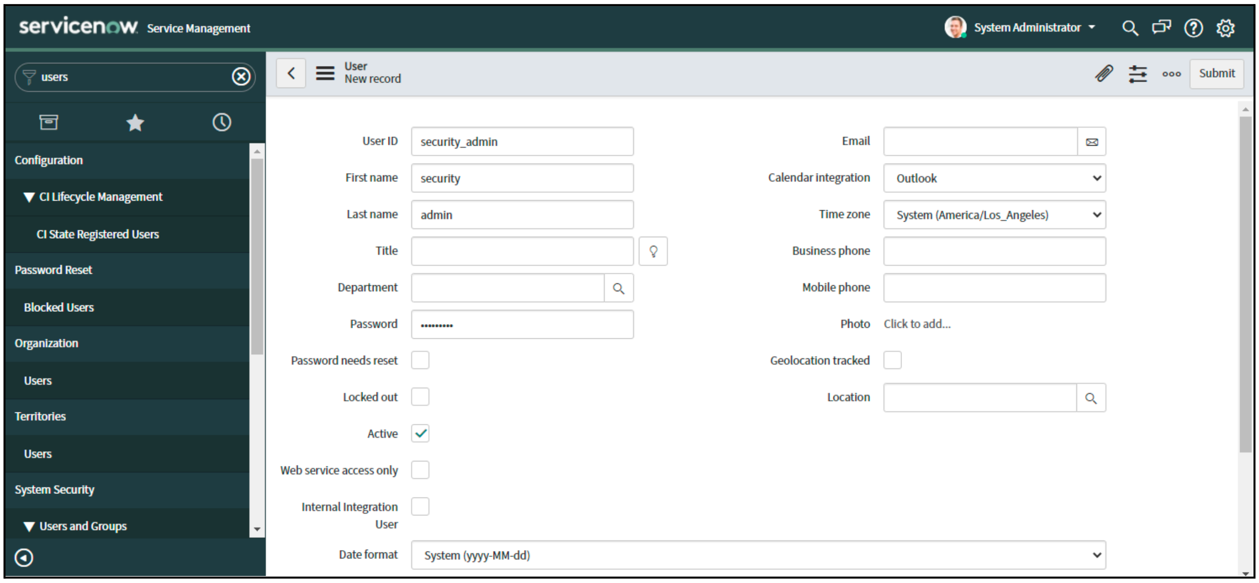
3. Create Security Admin User

- Navigate to Organization > Users.
- Click the Users module.



User ID	Name	Email	Active	Created	Updated
hasti.test	hasti test		true	2022-02-16 01:07:54 about a month ago	2022-02-16 01:07:54 about a month ago
aes.creator	Creator User		true	2022-02-03 03:31:52 2mo ago	2022-02-03 04:51:44 2mo ago
Help Desk	User 1	help.desk@example.com	true	2022-01-11 01:52:08 3mo ago	2022-02-03 02:31:10 2mo ago
manifah.masood	Manifah Masood	manifah.masood@example.com	true	2022-01-08 08:13:35 3mo ago	2022-02-03 02:31:10 2mo ago
guillermo.frohich	Guillermo Frohlich	guillermo.frohlich@example.com	true	2022-01-08 07:04:03 3mo ago	2022-02-03 02:31:13 2mo ago
instance.sec.user	Performance Analytics Security Center User		true	2022-01-05 00:52:12 3mo ago	2022-02-03 02:31:10 2mo ago
andrew.och	Andrew Och	andrew.och@example.com	true	2022-01-04 08:45:02 3mo ago	2022-02-03 02:31:14 2mo ago
aqib.mushtaq	Aqib Mushtaq	aqib.mushtaq@example.com	false	2022-01-04 08:35:36 3mo ago	2022-02-03 02:31:11 2mo ago
arya.hajarha	Arya Hajarha	arya.hajarha@example.com	true	2022-01-04 08:32:04 3mo ago	2022-02-03 02:31:17 2mo ago
bushra.akhtar	Bushra Akhtar	bushra.akhtar@example.com	true	2022-01-04 08:25:39 3mo ago	2022-02-03 02:31:12 2mo ago
SLA.Manager	SLA Manager	sla.manager@example.com	true	2022-01-04 01:16:14 3mo ago	2022-02-03 02:31:13 2mo ago
SLA.Admin	SLA Admin	sla.admin@example.com	true	2022-01-04 01:15:35 3mo ago	2022-02-03 02:31:10 2mo ago

- Above the User ID list, Click the “New” button. A new User form will be displayed.



User
New record

User ID	security_admin	Email	
First name	security	Calendar integration	Outlook
Last name	admin	Time zone	System (America/Los_Angeles)
Title		Business phone	
Department		Mobile phone	
Password	••••••••	Photo	Click to add...
Password needs reset	□	Geolocation tracked	□
Locked out	□	Location	
Active	☑		
Web service access only	□		
Internal Integration User	□		
Date format	System (yyyy-MM-dd)		

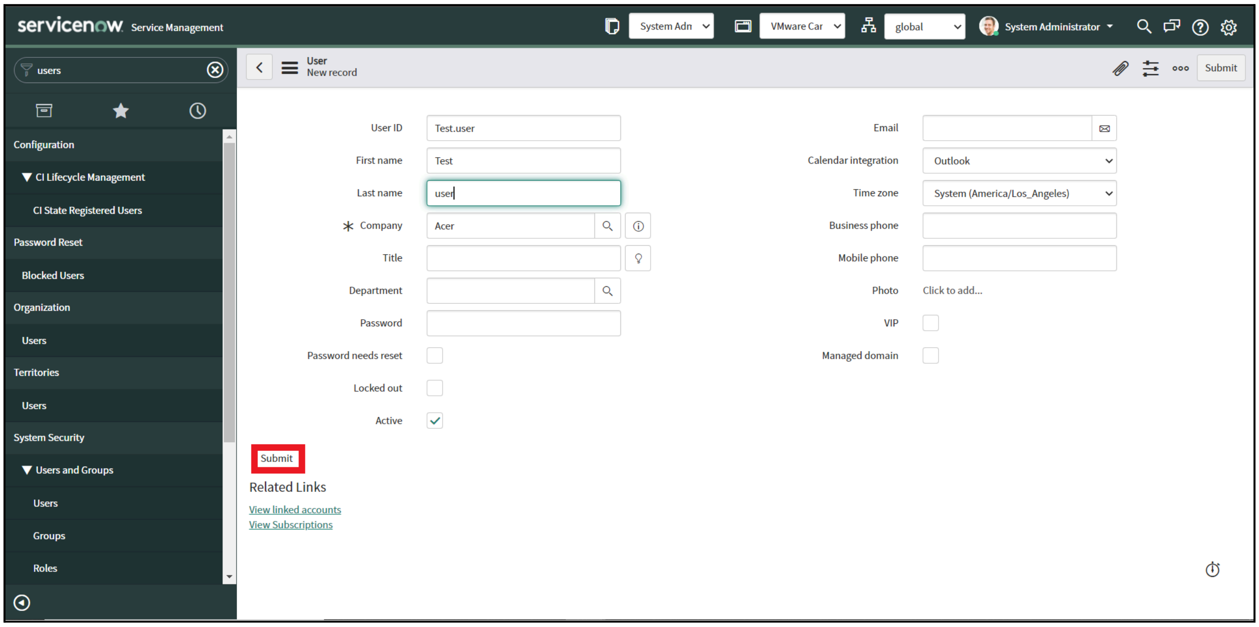
- Fill in the form.

Fiel d	Description

User ID	Unique User ID for the role in your ServiceNow Platform instance. An example is security admin.
First Name	Person you are assigning
Last Name	Person you are assigning
Title	Job Title, for example, security user
Password	Unique password created for this role
Email	Unique email address

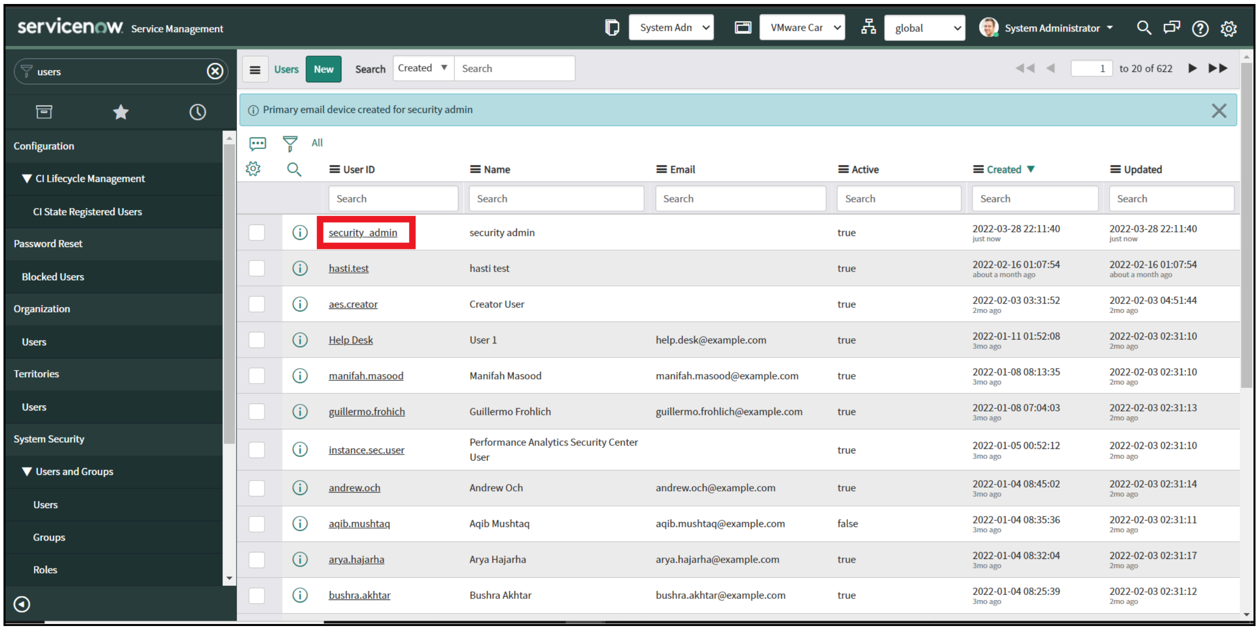
Note: Example values for the User ID title and email address are shown in the table below.

- Click “Submit.” Once submitted, you can assign the role.



User ID	Test.user	Email	
First name	Test	Calendar integration	Outlook
Last name	user	Time zone	System (America/Los_Angeles)
* Company	Acer	Business phone	
Title		Mobile phone	
Department		Photo	Click to add...
Password		VIP	□
Password needs reset	□	Managed domain	□
Locked out	□		
Active	☑		

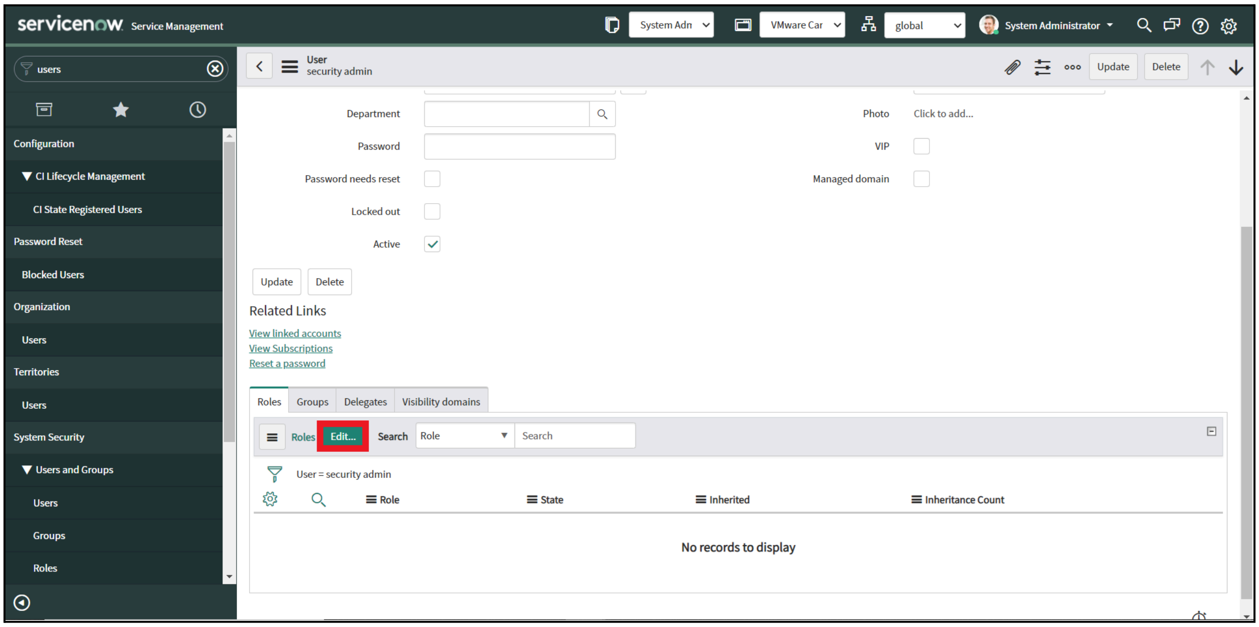
- Click the name of the new user you created.



Primary email device created for security admin

User ID	Name	Email	Active	Created	Updated
security_admin	security admin		true	2022-03-28 22:11:40 just now	2022-03-28 22:11:40 just now
hasti.test	hasti test		true	2022-02-16 01:07:54 about a month ago	2022-02-16 01:07:54 about a month ago
aes.creator	Creator User		true	2022-02-03 03:31:52 2mo ago	2022-02-03 04:51:44 2mo ago
Help Desk	User 1	help.desk@example.com	true	2022-01-11 01:52:08 3mo ago	2022-02-03 02:31:10 2mo ago
manifah.masood	Manifah Masood	manifah.masood@example.com	true	2022-01-08 08:13:35 3mo ago	2022-02-03 02:31:10 2mo ago
guillermo.frohich	Guillermo Frohlich	guillermo.frohlich@example.com	true	2022-01-08 07:04:03 3mo ago	2022-02-03 02:31:13 2mo ago
instance.sec.user	Performance Analytics Security Center User		true	2022-01-05 00:52:12 3mo ago	2022-02-03 02:31:10 2mo ago
andrew.och	Andrew Och	andrew.och@example.com	true	2022-01-04 08:45:02 3mo ago	2022-02-03 02:31:14 2mo ago
aqib.mushtaq	Aqib Mushtaq	aqib.mushtaq@example.com	false	2022-01-04 08:35:36 3mo ago	2022-02-03 02:31:11 2mo ago
arya.hajarha	Arya Hajarha	arya.hajarha@example.com	true	2022-01-04 08:32:04 3mo ago	2022-02-03 02:31:17 2mo ago
bushra.akhtar	Bushra Akhtar	bushra.akhtar@example.com	true	2022-01-04 08:25:39 3mo ago	2022-02-03 02:31:12 2mo ago

- Once the record is open, scroll down and go to the Roles section, and click “Edit”.



User
security admin

Department		Photo	Click to add...
Password		VIP	□
Password needs reset	□	Managed domain	□
Locked out	□		
Active	☑		

Related Links

View linked accounts
View Subscriptions
Reset a password

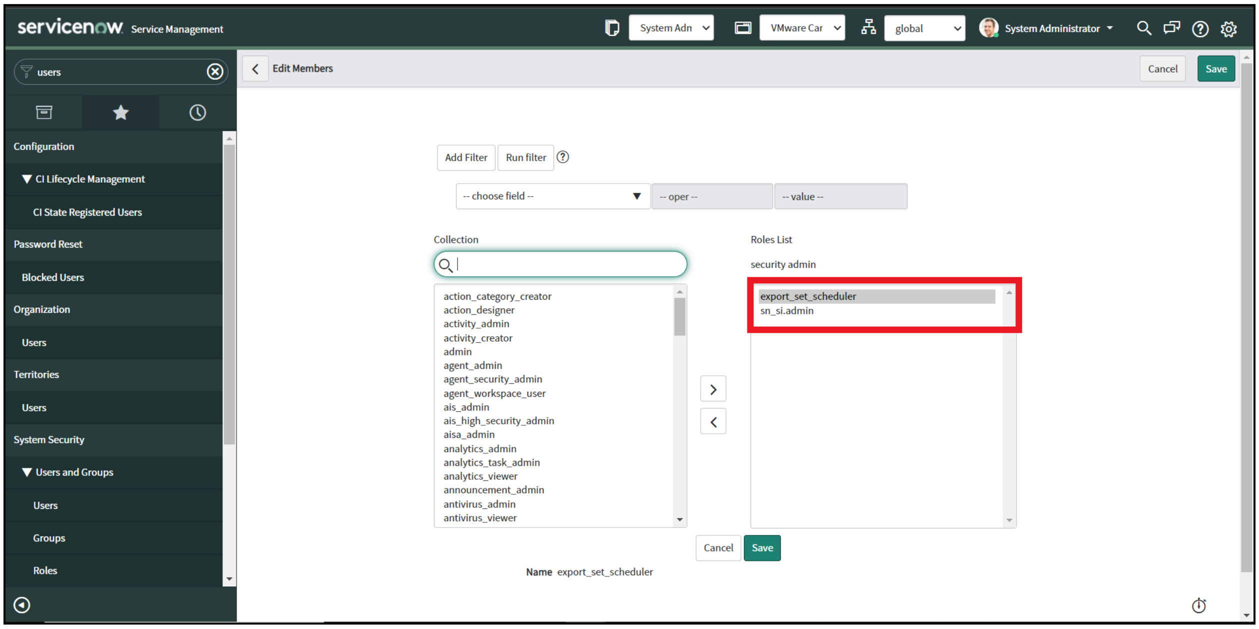
User = security admin

Role	State	Inherited	Inheritance Count

No records to display

- When the Edit Members form displays, enter sn_si.admin in the Collection field.
- In the Collection column, select and move sn_si.admin to the Roles list.
- Click the Save button.
- Scroll down and open the role: “ sn_si. admin”
- Scroll down and click on the “Edit” button.
- Search the roles to be added.

- Select the roles and move it to “Contains Roles List” by either double-clicking on the role or clicking on the right arrow.



Collection

action_category_creator
action_designer
activity_admin
activity_creator
admin
agent_admin
agent_security_admin
agent_workspace_user
ais_admin
ais_high_security_admin
aisa_admin
analytics_admin
analytics_task_admin
analytics_viewer
announcement_admin
antivirus_admin
antivirus_viewer

Roles List

security admin

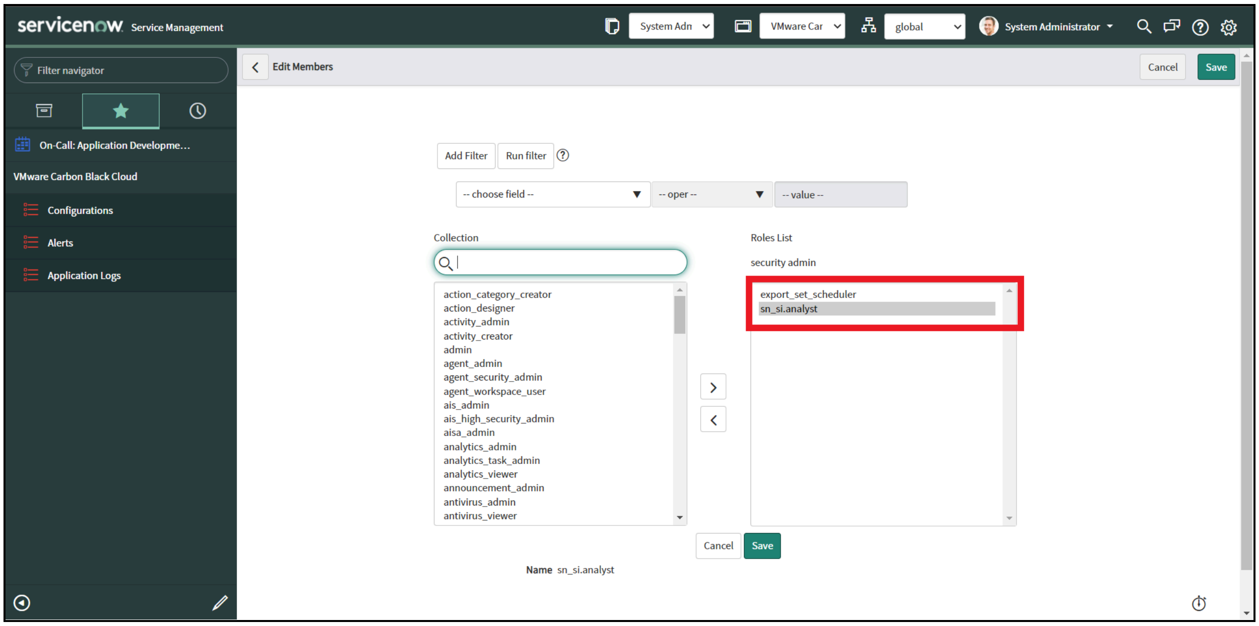
export_set_scheduler
sn_si.admin

Name export_set_scheduler

- When the Edit Members form displays, enter sn_si.admin and export_set_scheduler in the Collection field.
- In the Collection column, select and move sn_si.admin and export_set_scheduler to the Roles List.
- Click the Save button.

4. Create Analyst User

All of the steps for creating admin users are applicable for analyst users also, but you must add roles specific to analyst i.e. sn_si.analyst +personalize_dictionary(Check the permissions and roles section).



Collection

action_category_creator
action_designer
activity_admin
activity_creator
admin
agent_admin
agent_security_admin
agent_workspace_user
ais_admin
ais_high_security_admin
aisa_admin
analytics_admin
analytics_task_admin
analytics_viewer
announcement_admin
antivirus_admin
antivirus_viewer

Roles List

security admin

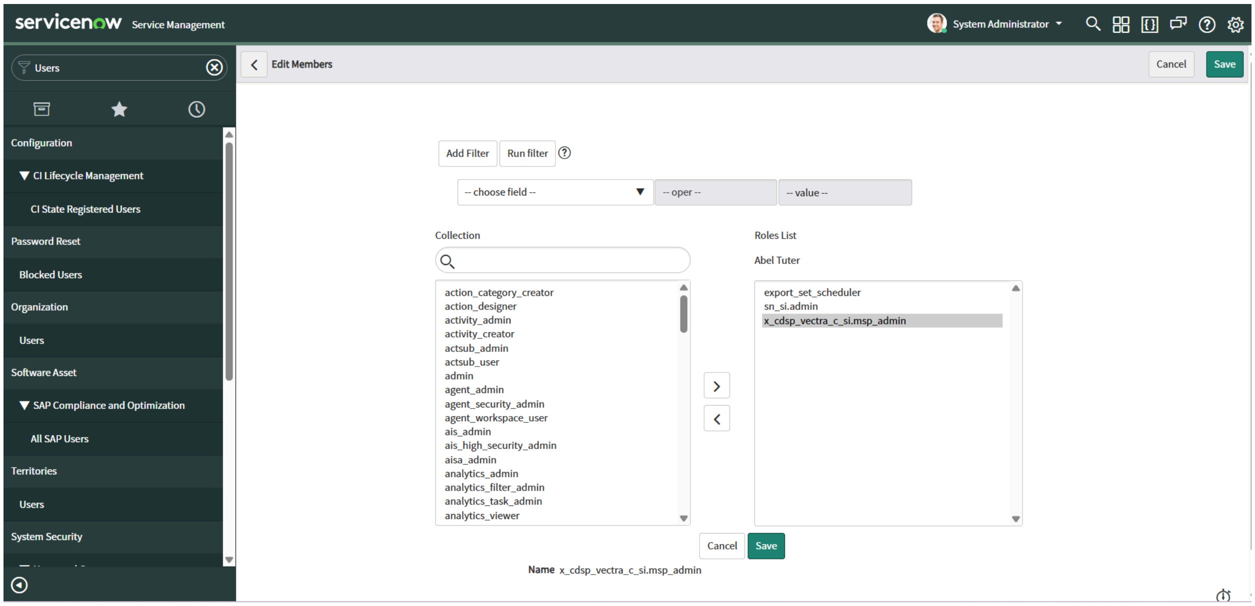
export_set_scheduler
sn_si.analyst

Cancel Save

Name sn_si.analyst

5. **Create MSP Admin**

All of the steps for creating admin users are applicable for MSP Admin also, but you must add roles specific to MSP Admin i.e. x_cdsp_vectra_c_si.msp_admin (Check the permissions and roles section).



Collection

action_category_creator
action_designer
activity_admin
activity_creator
actsub_admin
actsub_user
admin
agent_admin
agent_security_admin
agent_workspace_user
ais_admin
ais_high_security_admin
aisa_admin
analytics_admin
analytics_filter_admin
analytics_task_admin
analytics_viewer

Roles List

Abel Tuter

export_set_scheduler
sn_si.admin
x_cdsp_vectra_c_si.msp_admin

Cancel Save

Name x_cdsp_vectra_c_si.msp_admin

2.2. Configuration

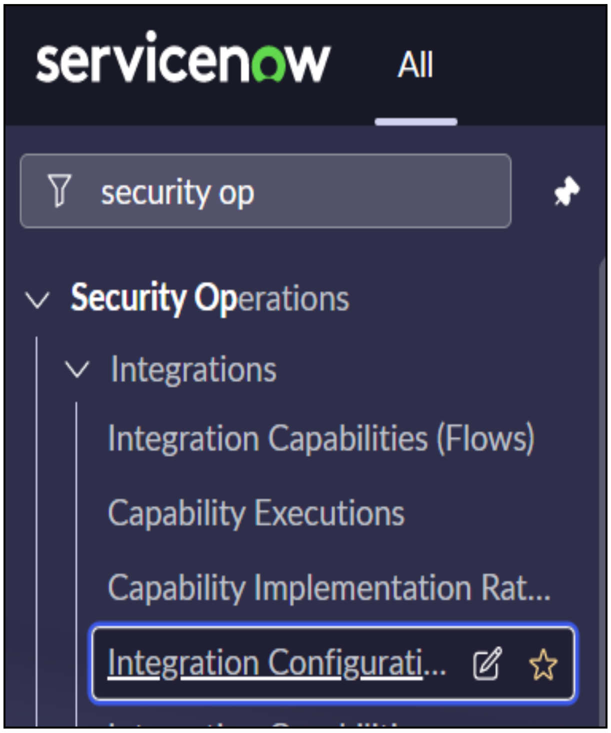
This section describes how to configure ServiceNow and Vectra Detect to use the application.

2.2.1. Integration Configuration

Required roles: Application admin(sn_si.admin) Or System administrator.

The user needs to configure the tile to establish the authentication and communication between ServiceNow and Vectra Detect.

- Users should be able to see the ServiceNow Security Incident Response Integration with Vectra XDR tile by navigating to All -> Security Operations -> Integrations -> Integration Configurations


servicenow
All
security op
Security Operations
Integrations
Integration Capabilities (Flows)
Capability Executions
Capability Implementation Rat...
Integration Configurati...

Open the Vectra Cloud for Security Incident Response tile and add details in the below-listed fields and submit.

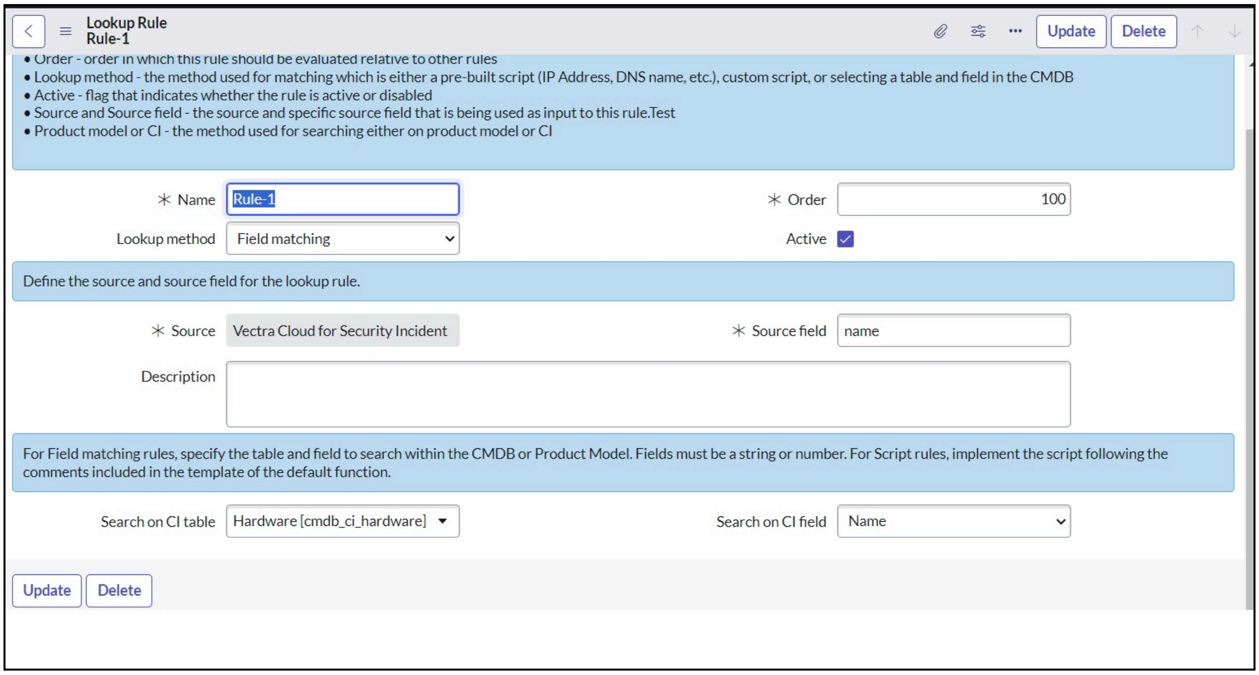
- Name: String field where the user will enter the name of the integration configuration.
- Vectra Detect URL: URL type field where the user will enter Vectra Detect instance URL in “https://<vectra-instance-url>” format.
- Client Id: Password type field where the user will enter the Client ID of the authorization credentials.
- Client Secret Key: Password type field where the user will enter a Client secret key.

2.2.2. CI Lookup Rule

Vectra application allows to create multiple rules and based on the “Order”, it does the lookup into the CMDB tables.It will attach the CI records in Security tables, based on the lookup configured in the CI Lookup rules.

Note: The table selected in the CI Lookup rule does not have configuration item then Security incident will not have association with CI and remain blank.

- Login to the ServiceNow instance.
- Search for the “CI Lookup” under Vectra application.
- Click on New Button.
- Provide the Name,Source field and select value in destination fields “Search on CI table” and “Search on CI field”.
- Click on the Submit button.



- Order - order in which this rule should be evaluated relative to other rules
- Lookup method - the method used for matching which is either a pre-built script (IP Address, DNS name, etc.), custom script, or selecting a table and field in the CMDB
- Active - flag that indicates whether the rule is active or disabled
- Source and Source field - the source and specific source field that is being used as input to this rule.Test
- Product model or CI - the method used for searching either on product model or CI

✱ Name	Rule-1	✱ Order	100
Lookup method	Field matching	Active	☑

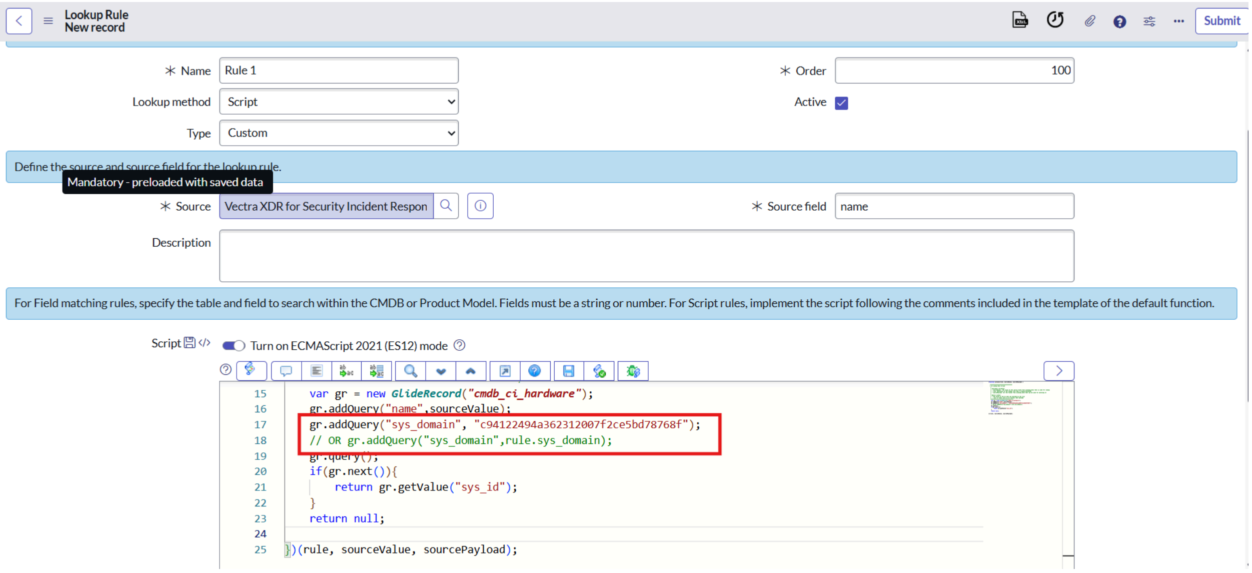
Define the source and source field for the lookup rule.

✱ Source	Vectra Cloud for Security Incident	✱ Source field	name
Description			

For Field matching rules, specify the table and field to search within the CMDB or Product Model. Fields must be a string or number. For Script rules, implement the script following the comments included in the template of the default function.

Search on CI table	Hardware [cmdb_ci_hardware]	Search on CI field	Name

- When using the lookup method as “script” make sure to include domain query in the script, to avoid mapping incorrect CI items during data ingestion.



∗ Name: Rule 1

∗ Order: 100

Lookup method: Script

Active: ☑

Type: Custom

Define the source and source field for the lookup rule.

Mandatory - preloaded with saved data

∗ Source: Vectra XDR for Security Incident Respon

∗ Source field: name

Description:

For Field matching rules, specify the table and field to search within the CMDB or Product Model. Fields must be a string or number. For Script rules, implement the script following the comments included in the template of the default function.

Script — Turn on ECMAScript 2021 (ES12) mode

```
    var gr = new GlideRecord("cmdb_ci_hardware");
    gr.addQuery("name",sourceValue);
    gr.addQuery("sys_domain", "c94122494a362312007f2ce5bd78768f");
    // OR gr.addQuery("sys_domain",rule.sys_domain);
    gr.query();
    if(gr.next()){
        return gr.getValue("sys_id");
    }
    return null;

})(rule, sourceValue, sourcePayload);
```

- Now Run the scheduler and once job is completed Security Incident has a record linked in the field “Configuration Item” field.

2.2.3. Incident Profiles

This section describes options for bringing Vectra entities and detections into ServiceNow and creating Incidents based on Incident creation criteria. Set conditions to specify when the Vectra entity should generate ServiceNow Security Incidents in an automated way.

Role Required: Vectra admin/System admin

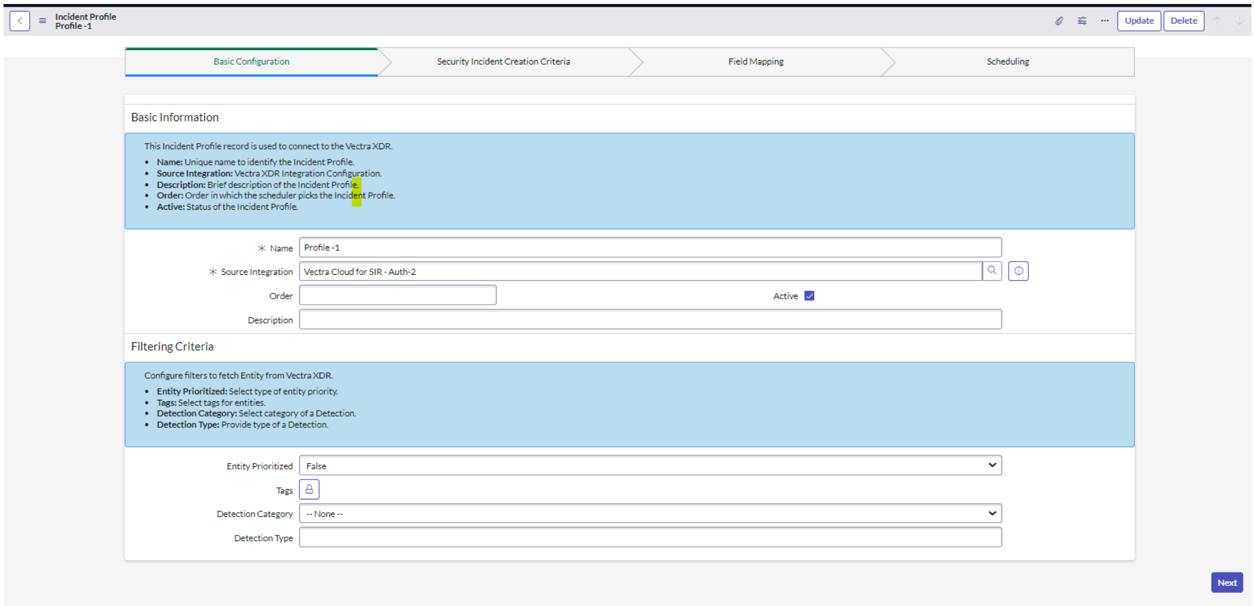
- As ServiceNow Vectra App Admin, I should be able to configure the profile to control the Vectra Detect data flow. I should be able to control what entity and detection data to fetch from the Vectra Detect and convert it to Security Incidents in ServiceNow.

2.2.3.1. Basic Configuration

Role Required: Vectra admin

Procedure:

- Login to the ServiceNow instance.
- Navigate to Vectra application > Incident Profile.
- Enter Profile Name and select “Source Integration”.
- Provide the order in which the scheduler picks the Incident Profile.
- Provide the details in Filter Criteria.



Basic Information

This Incident Profile record is used to connect to the Vectra XDR.

- **Name:** Unique name to identify the Incident Profile.
- **Source Integration:** Vectra XDR Integration Configuration.
- **Description:** Brief description of the Incident Profile.
- **Order:** Order in which the scheduler picks the Incident Profile.
- **Active:** Status of the Incident Profile.

* Name	Profile -1
* Source Integration	Vectra Cloud for SIR - Auth-2
Order	
Active	☑
Description	

Filtering Criteria

Configure filters to fetch Entity from Vectra XDR.

- **Entity Prioritized:** Select type of entity priority.
- **Tags:** Select tags for entities.
- **Detection Category:** Select category of a Detection.
- **Detection Type:** Provide type of a Detection.

Entity Prioritized	False
Tags	
Detection Category	-- None --
Detection Type	

- “Entity Prioritized” is default set to “All” so select the value accordingly.
- Provide a Tag to filter data tag-wise.(Tag populates in the list after one successful job run)
- Select “Detection Category” and/or “Detection Type” to filter the data and based on this, it populates the data of Detection.
- Now click on the Next button to move to the Security Incident Creation Criteria tab.

2.2.3.2. Security Incident Creation

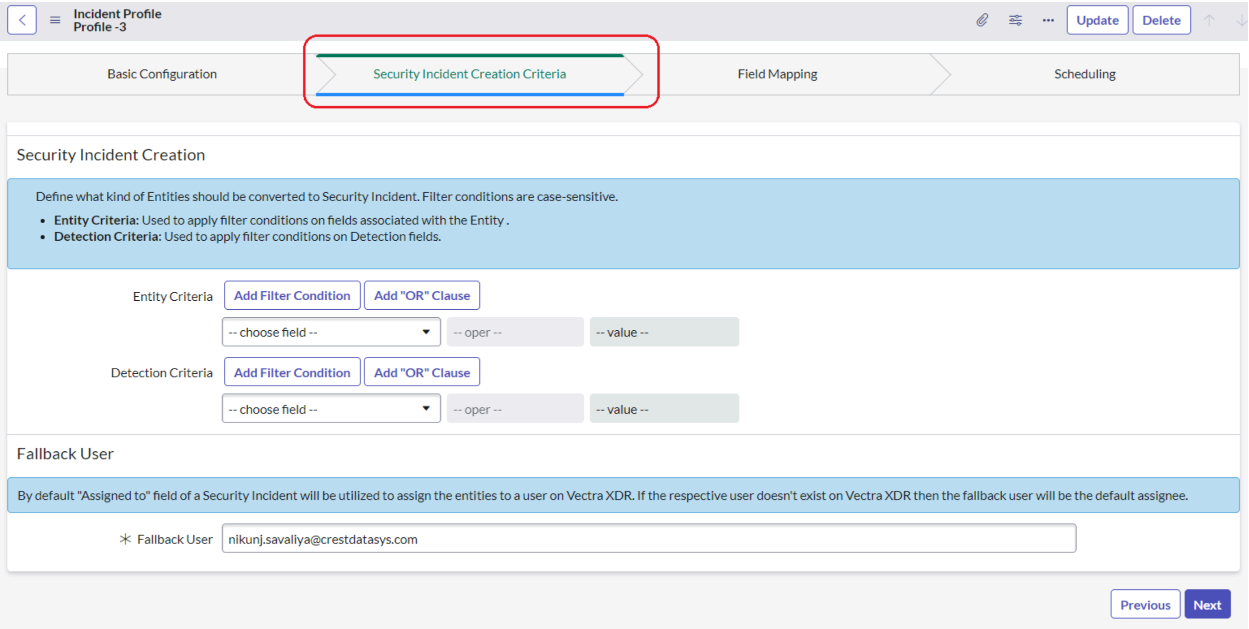
Role Required: Vectra admin

Procedure:

- Login to the ServiceNow instance.
- Navigate to Vectra application > Incident Profile.
- Complete the Basic Configuration.
- Click on Next to move to “Security Incident Creation”.

Entity Criteria:

- Entity Criteria has an Entities field to choose from.
- Select the fields to create single or multiple conditions; based on the condition, it will create Security incidents from entities.
- Select “AND” or “OR” to add multiple conditions.
- Between Entity and Detection criteria there is an OR condition, so if either of the conditions gets matched, the application will create the Security incident.



Security Incident Creation

Define what kind of Entities should be converted to Security Incident. Filter conditions are case-sensitive.

- **Entity Criteria:** Used to apply filter conditions on fields associated with the Entity .
- **Detection Criteria:** Used to apply filter conditions on Detection fields.

Entity Criteria

Detection Criteria

Fallback User

By default "Assigned to" field of a Security Incident will be utilized to assign the entities to a user on Vectra XDR. If the respective user doesn't exist on Vectra XDR then the fallback user will be the default assignee.

✳ Fallback User: nikunj.savaliya@crestdatasys.com

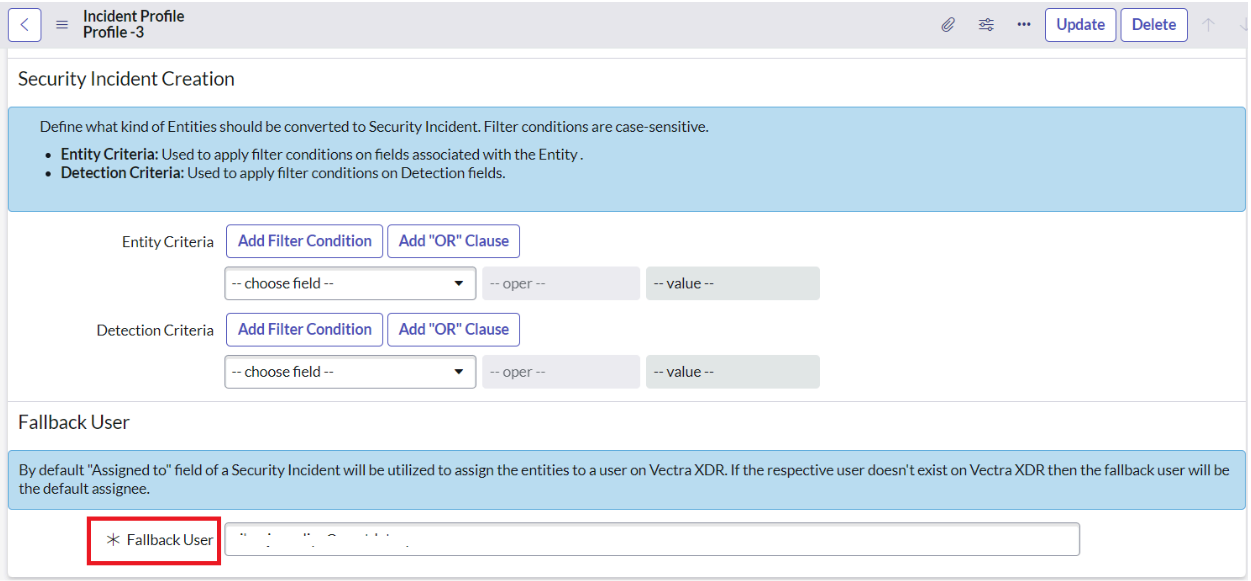
- e.g. if there are no entities matching the condition provided here, it will look for the detection condition, if the detection condition gets matched application will create the incident based on the detection condition.

Detection Criteria:

- Detection Criteria has a “Detections” field to choose from.
- Select the fields to create single or multiple conditions and security incidents should be created based on that.
- Select “AND” or “OR” to add multiple conditions.
- Note: Between Entity Criteria and Detection there is OR condition so if any of the conditions matches application will create incidents.

Fallback User:

- Specify the user to assign the entity to that user on Vectra Respond UX, if “Assigned to” users of Security Incident are not present on Vectra Detect.
- Click on the “Next” button to save the changes and move to the next tab.
- If the provided “Fallback User” does not exist on Vectra Respond UX then “Fallback User provided does not exist on Vectra Detect” an error message will be displayed.
- When assigning the user from the Security Incident and the selected user is not present on Vectra then in this case, it will check for the user provided in the Fallback user and will assign that user on the Vectra entity.



Security Incident Creation

Define what kind of Entities should be converted to Security Incident. Filter conditions are case-sensitive.

- **Entity Criteria:** Used to apply filter conditions on fields associated with the Entity .
- **Detection Criteria:** Used to apply filter conditions on Detection fields.

Fallback User

By default "Assigned to" field of a Security Incident will be utilized to assign the entities to a user on Vectra XDR. If the respective user doesn't exist on Vectra XDR then the fallback user will be the default assignee.

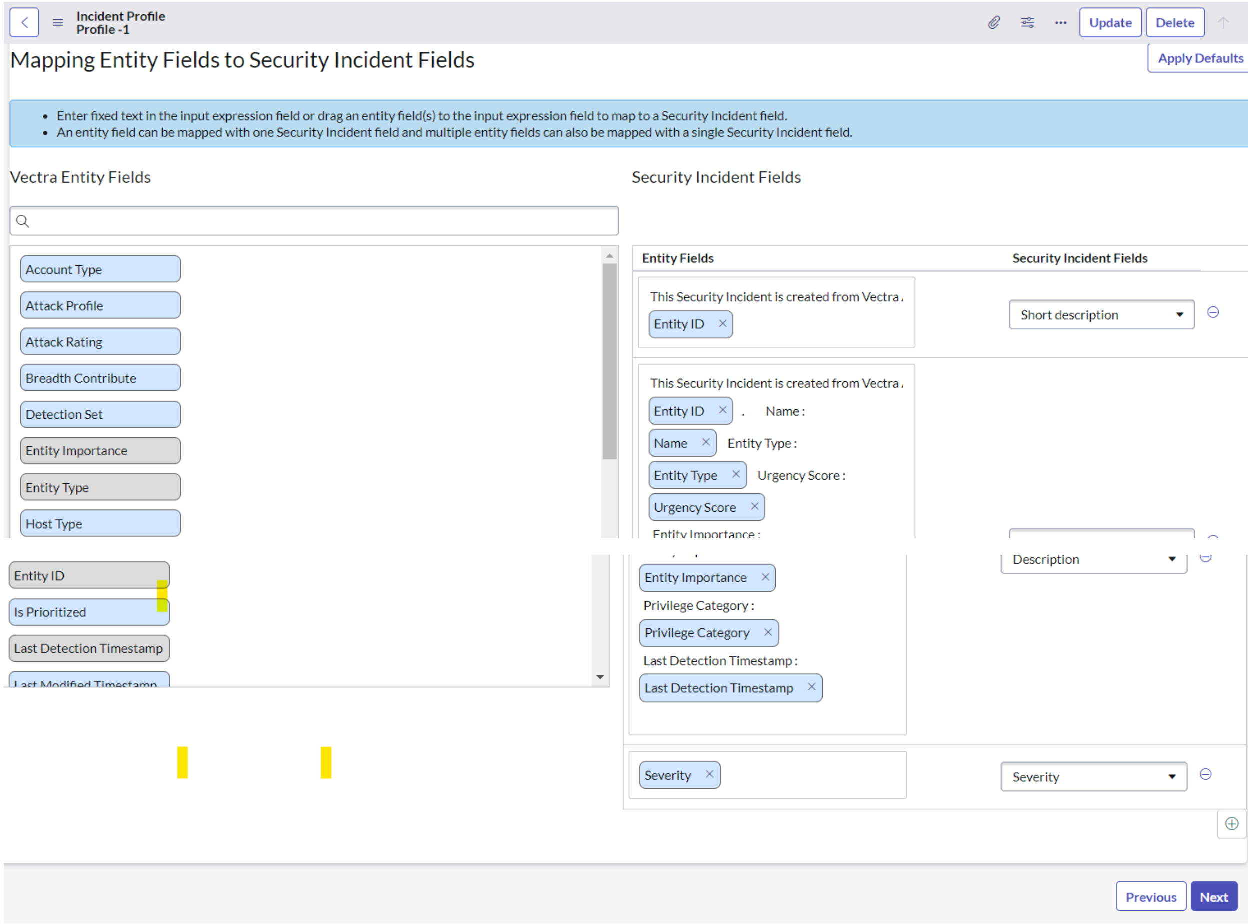
2.2.3.3. Field Mapping

This section shows how to map Vectra Entity fields with ServiceNow SecOps Security Incident fields.

Role Required: Vectra admin

Procedure:

- Login to the ServiceNow instance.
- Navigate to Vectra application > Incident Profile.
- Complete the Basic Configuration, and Security Incident Creation Criteria.
- Click on Next to move to the “Mapping” tab.
- In the “Field mapping” tab, there are two sections. On the left side, there are fields for “Entities” and on the right side, there are fields for “Security Incidents”.
- Provide which fields of Entities get mapped with which fields of Security Incidents.
- You can also provide Input expression value by entering the value in the text field.
- Create multiple field mappings and can also drag and drop entities fields to map with Security Incident fields.
- Add a custom value (Input Expression) to the entity field after dropping it to the right side in the UI apart from the reference fields of the Security Incident table.
- To add “Add More” pairs of Input Expressions to map more fields and to remove a pair of Input Expressions click on the remove icon to remove the mapping.
- You can add/remove Security Incident fields by clicking on the remove (minus)/add (plus) buttons.
- Different Security Incident fields can be selected from the dropdown list as needed.



Mapping Entity Fields to Security Incident Fields

- Enter fixed text in the input expression field or drag an entity field(s) to the input expression field to map to a Security Incident field.
- An entity field can be mapped with one Security Incident field and multiple entity fields can also be mapped with a single Security Incident field.

Vectra Entity Fields: Account Type, Attack Profile, Attack Rating, Breadth Contribute, Detection Set, Entity Importance, Entity Type, Host Type, Entity ID, Is Prioritized, Last Detection Timestamp, Last Modified Timestamp

Security Incident Fields

Entity Fields	Security Incident Fields
This Security Incident is created from Vectra. Entity ID	Short description
This Security Incident is created from Vectra. Entity ID . Name : Name Entity Type : Entity Type Urgency Score : Urgency Score Entity Importance : Entity Importance Privilege Category : Privilege Category Last Detection Timestamp : Last Detection Timestamp	Description
Severity	Severity

- To map default fields click on the “Apply Defaults” button on the right side of the “Mapping Entity Fields to Security Incident Fields” heading in the “Field Mapping” tab. When it is clicked the default field mapping will be applied.
- Now click on the Next button to move to the Scheduling section.
- Note: Single field of Vectra can be mapped against single field of ServiceNow fields. One field cannot be mapped twice with the ServiceNow field.

2.2.3.4. Scheduling

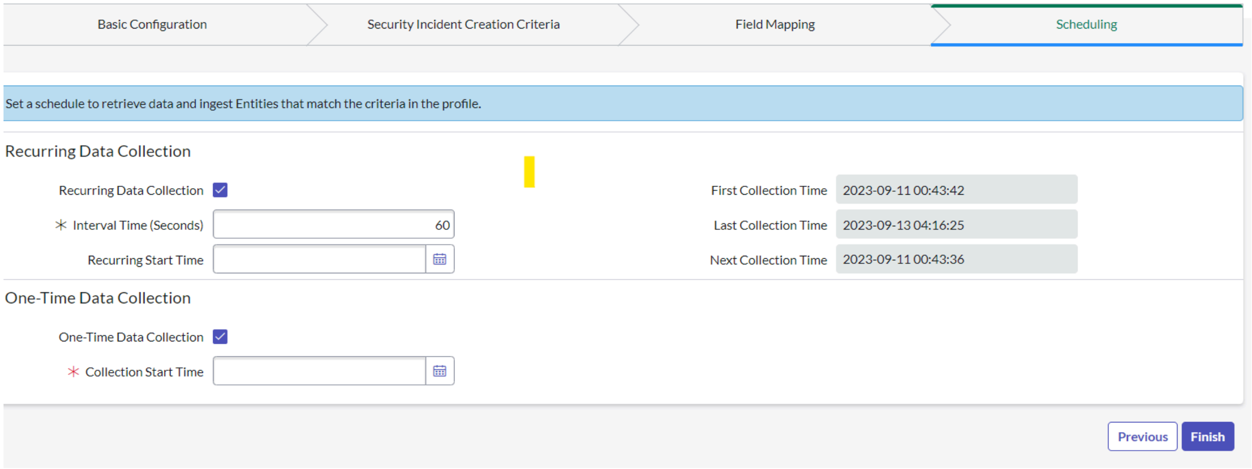
Use this page to control when or how often data is collected from Vectra Detect. There are two settings that can be configured: Recurring Data Collection and One-Time Data Collection.

Role Required: Vectra admin

Procedure:

- Login to the ServiceNow instance.
- Navigate to Vectra application > Incident Profile.

- Complete the Basic Configuration, Security Incident Creation Criteria, and Mapping.
- Click on Next to move to the “Scheduling” tab.
- Check the Recurring data collection checkbox.
- Enter time Interval in seconds. The default Interval time is 60 Seconds.
- Provide the Collection Start time as per the need from the calendar. The Collection Start date can be a future date only.
- If the future date is provided then ingestion will start at that provided future time.
- Optionally, to configure data ingestion for a bounded window of time in the past, check the One Time Collection Checkbox.
- Provide a One-time data collection Start time in “Collection Start Time”.
- Once the One-time data collection is completed the Recurring ingestion will start based on the date provided.
- Now Click on the “Finish button”. After clicking Finish, a pop-up window warns that the profile is inactive and suggests activating the profile.
- Next you are navigated to the Incident Profile page and you can see the profile you created in the list.
- You can create multiple profiles with the same and different sources. With the same source only one profile can be activated at a time.
- If you try an active profile that has an associated source already linked in another active profile then it shows the information message that the profile with the same source is already active.
- Inactive profile can make active by selecting the checkbox of Active from the Basic Configuration tab while editing/updating the profile.



Set a schedule to retrieve data and ingest Entities that match the criteria in the profile.

Recurring Data Collection

Recurring Data Collection	☑	First Collection Time	2023-09-11 00:43:42
* Interval Time (Seconds)	60	Last Collection Time	2023-09-13 04:16:25
Recurring Start Time		Next Collection Time	2023-09-11 00:43:36

One-Time Data Collection

One-Time Data Collection	☑
* Collection Start Time	

Notes:

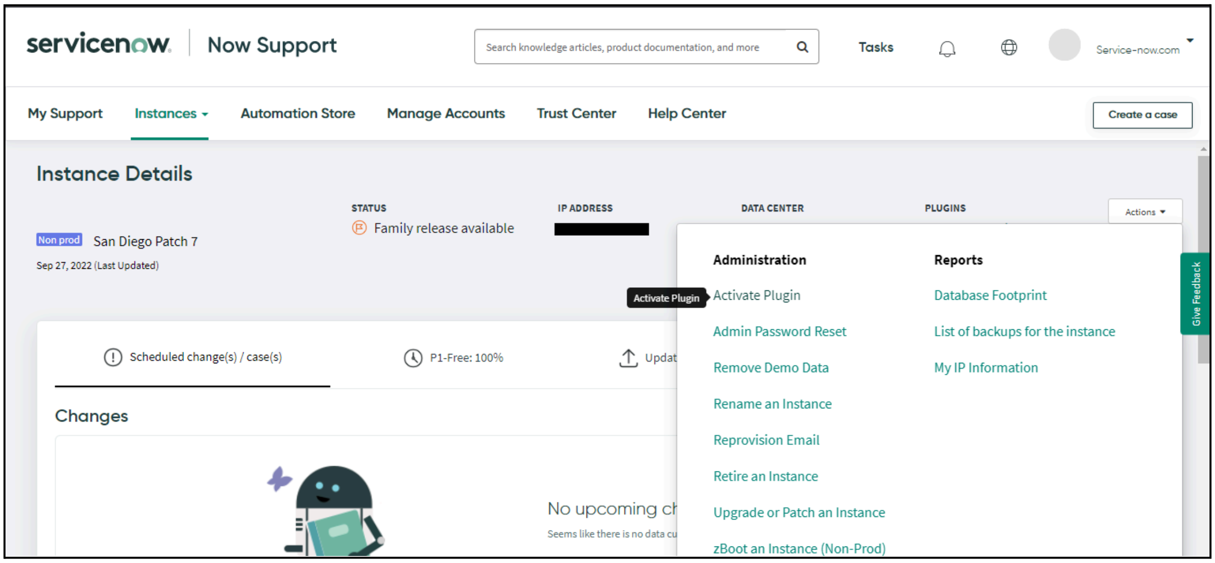
- For different URLs and ID users can create multiple profiles to fetch the data and if the URL and ID are the same even can create multiple profiles but at a time only one profile can be Active.
- If a user deletes the tile/source which is configured in the profile then that source will get deleted from the profile also and it will not run the scheduler.

2.3. Use Cases

2.3.1.1. MSP Support

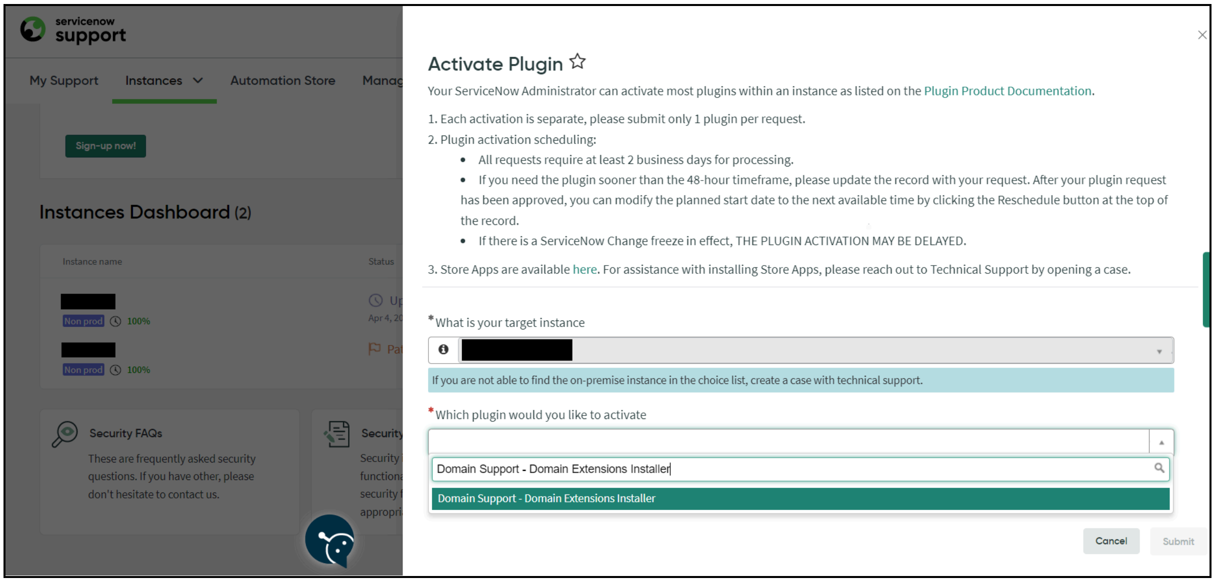
To use the MSP support user must activate the “Domain Separation” Plugin, to activate the plugin follow below steps:

a. Sign in to your Instance email account from https://support.servicenow.com/
b. From My Instance, under Instance Action, select Activate Plugin



c. Search for the plugin “Domain Support - Domain Extensions Installer” and click Activate > Activate plugin

d. Once you click Activate plugin, a request is sent for plugin activation. Once the Plugin is activated, you will receive a notification mail indicating so.



[redacted]

Activate Plugin ☆

Your ServiceNow Administrator can activate most plugins within an instance as listed on the Plugin Product Documentation.

1. Each activation is separate, please submit only 1 plugin per request.
2. Plugin activation scheduling:
   - All requests require at least 2 business days for processing.
   - If you need the plugin sooner than the 48-hour timeframe, please update the record with your request. After your plugin request has been approved, you can modify the planned start date to the next available time by clicking the Reschedule button at the top of the record.
   - If there is a ServiceNow Change freeze in effect, THE PLUGIN ACTIVATION MAY BE DELAYED.
3. Store Apps are available here. For assistance with installing Store Apps, please reach out to Technical Support by opening a case.

*What is your target instance

[redacted]

If you are not able to find the on-premise instance in the choice list, create a case with technical support.

*Which plugin would you like to activate

Domain Support - Domain Extensions Installer

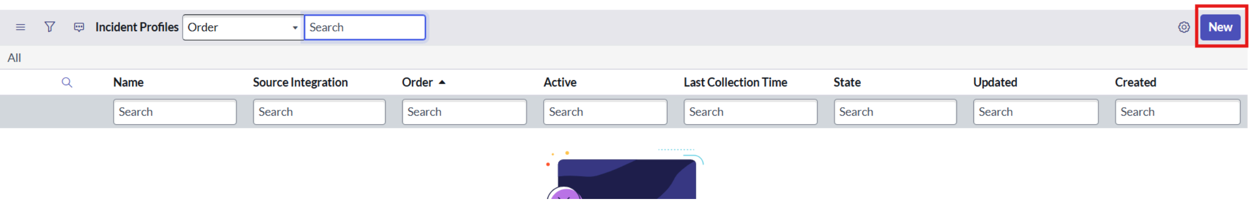
Domain Support - Domain Extensions Installer

Cancel Submit

e. Once the plugin is activated on the instance, you can install the application.

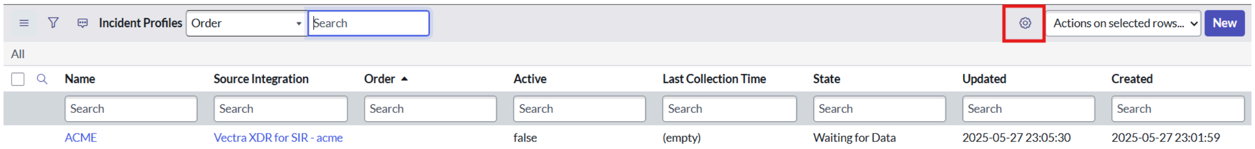
After the plugin is activated user may see the following changes in that instance:

- If any configuration is configured by the user with any domain, then we can see that those configurations will be made in the same domain of the user.
- create a new incident profile click the button on the top right corner.



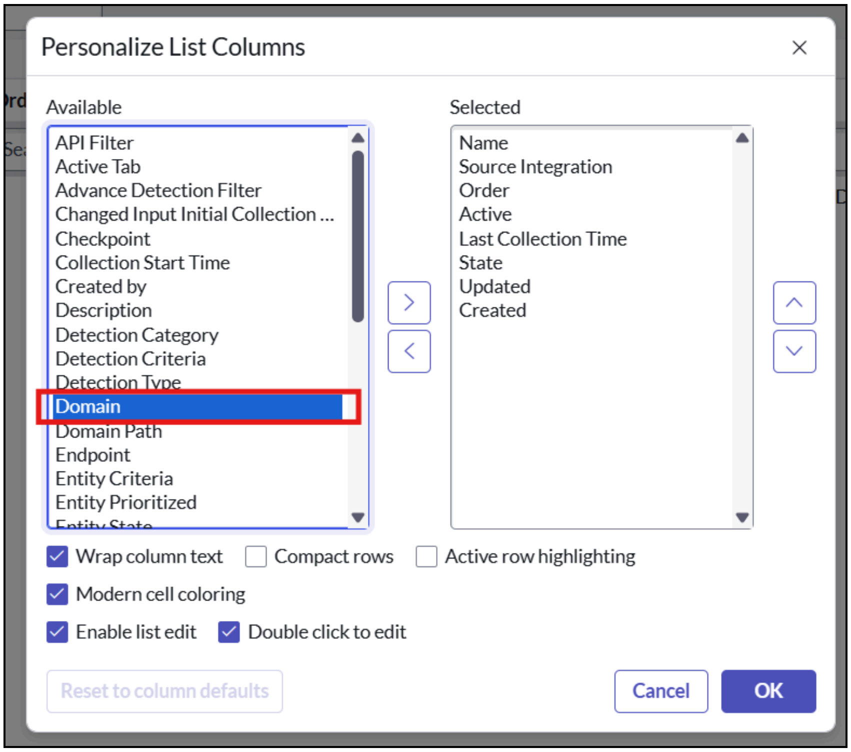
Name	Source Integration	Order ▲	Active	Last Collection Time	State	Updated	Created
Search	Search	Search	Search	Search	Search	Search	Search

- Once the profile is created users may change the layout using the gear icon on the top right corner to see the domain column.



Name	Source Integration	Order ▲	Active	Last Collection Time	State	Updated	Created
Search	Search	Search	Search	Search	Search	Search	Search
ACME	Vectra XDR for SIR - acme		false	(empty)	Waiting for Data	2025-05-27 23:05:30	2025-05-27 23:01:59

- In the “Personalize List Column” select “domain” and shift it to “Selected” list



Personalize List Columns

Available

- API Filter
- Active Tab
- Advance Detection Filter
- Changed Input Initial Collection ...
- Checkpoint
- Collection Start Time
- Created by
- Description
- Detection Category
- Detection Criteria
- Detection Type
- Domain
- Domain Path
- Endpoint
- Entity Criteria
- Entity Prioritized
- Entity State

Selected

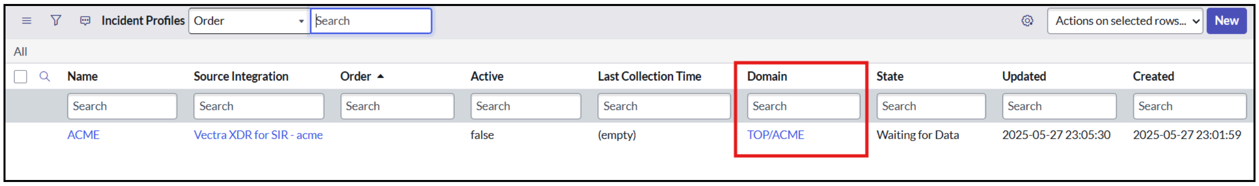
- Name
- Source Integration
- Order
- Active
- Last Collection Time
- State
- Updated
- Created

☑ Wrap column text □ Compact rows □ Active row highlighting

☑ Modern cell coloring

☑ Enable list edit ☑ Double click to edit

- Now we can see the domain of the configured profile.



Name	Source Integration	Order	Active	Last Collection Time	Domain	State	Updated	Created
ACME	Vectra XDR for SIR - acme		false	(empty)	TOP/ACME	Waiting for Data	2025-05-27 23:05:30	2025-05-27 23:01:59

- Now if any entity, detection, security incident is pulled/created by this profile then those will be populated in the same domain.

Note : Domain Separation is never activated on production instances containing customer data. Instead, it is enabled on a new instance, and customer data is migrated directly into the appropriate domains. This is because, prior to Domain Separation being activated, all data resides in the global domain. Once Domain Separation is enabled, any data remaining in the global domain becomes visible across all domains, potentially exposing sensitive information.

2.3.2. Entity and Detection Ingestion

- Ingest entities and Detections from Vectra Detect to populate the entities in the Entities table and Detection into the Detections table in ServiceNow.
- Once you configure the Profile and active data collection the application starts fetching the entities and detections from Vectra Detect and populates them in the entities and detection table in ServiceNow.

Role Required: Vectra admin

Procedure:

a. Login to the ServiceNow instance.
b. Navigate to Vectra SIR > Select Incident Profile
c. Provide the Security Incident creation criteria
d. Navigate to the Entities table.
e. Open any record to view the details
f. See associated detection in the related list.
g. Now navigate to the Detection table
h. Both the tables are now populated with data.
i. Open any record to view the details
j. See the associated entity in the related list

2.3.2.1. Detection:

- Users should not be able to create detection records manually from ServiceNow.
- Open any detection record to view, all fields will be read-only except the “Tags” field.
- Users can add/remove a tag, all tags will be updated in the ServiceNow platform as well as in the Vectra Detect.
- Users can mark detection as fixed, for that click on the “Mark as Fixed” button then detection will get inactive on the Vectra Detect. If Detection is already fixed then the message “Detection is already fixed on Vectra Detect” will be displayed on top of the form view.
- To download the PCAP file, click on the "Download PCAP” button the PCAP file will be downloaded from Vectra Detect and get attached to the detection record.
- When the Vectra admin/user posts any note/s from ServiceNow then that note should also be synced to Vectra Detect.

2.3.2.2. Entity:

- All the fetched entities will be listed under the Entity table.
- Open a record to view, all fields will be read-only except the “Tags” field.
- Add/remove tags then all tags should be updated in the ServiceNow platform as well as in the Vectra Detect.

- **Note** -Entity and Detection records cannot be updated or deleted from ServiceNow.

2.3.3. Automatic Security Incident Creation

- You can create a ServiceNow Security Incident automatically based on the Incident Creation criteria(Entity and Detection).
- If you have provided any conditions under “Incident creation criteria”, the app will create a Security Incident and link entities in the Security Incident based on those conditions.
- Entities fields are mapped to Security Incident fields based on the saved profile in the Field Mapping section of the Incident Profile.

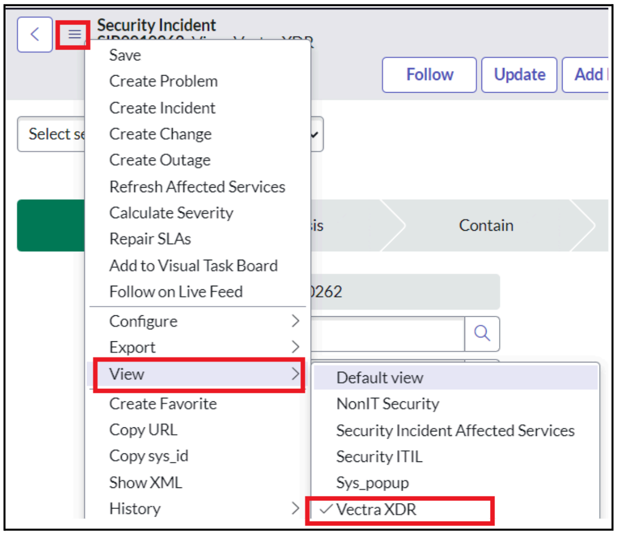
- If the specified condition does not match then no Security incident gets created.

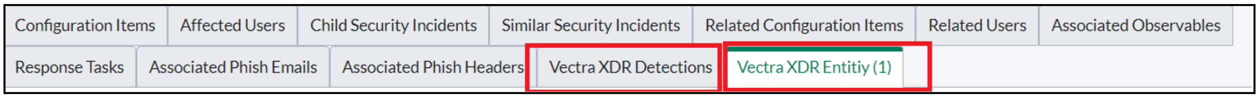
2.3.4. SOAR Actions

You can perform the actions from entities and Security incidents from the top menu. To view the Vectra entities and Detection in the Security Incident form view, have to enable the "Show All Related Lists". Change the view of Security Incident to enable tabs on the Security Incident form view under related list. And to do that follow below steps

Change the view to enable the tabs "Vectra entities" and "Vectra Detections"

- Click on the icon "Additional Action" and select the "View".
- Select "Vectra XDR" so it enables the tabs.





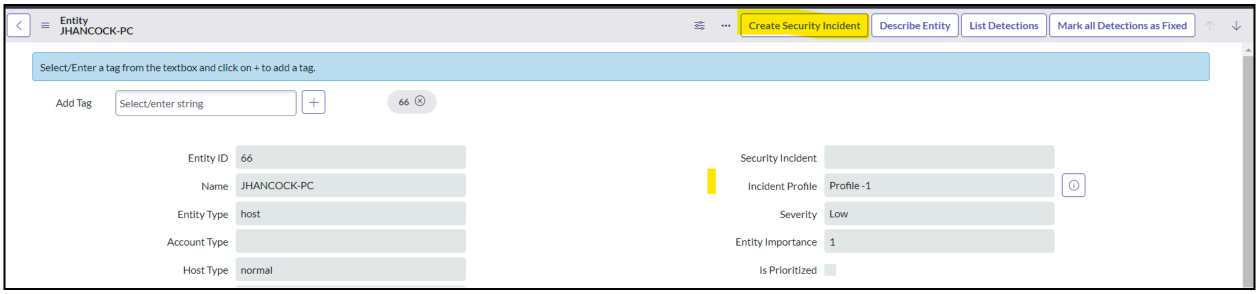
2.3.4.1. Manual Security Incident Creation

- You can create Security Incidents manually from an entity. A manually-created Incident's fields are populated based on the Field Mapping settings of the Incident Profile that ingested the entities.
- You can create Security Incidents only for an entity in an Active state.

Role Required: Vectra analyst

Procedure:

- Login to the ServiceNow instance.
- Navigate to Vectra > Entity



Select/Enter a tag from the textbox and click on + to add a tag.

Entity ID	66	Security Incident	
Name	JHANCOCK-PC	Incident Profile	Profile -1
Entity Type	host	Severity	Low
Account Type		Entity Importance	1
Host Type	normal	Is Prioritized	□

- Click to view any entity record in an Active state.
- Click on the Create Security Incident button (top/bottom).
- Clicking the "Create Security Incident" button creates the Security Incident for that entity, maps the entity fields to the Security Incident field, and displays the Security Incident ID in the entity record. You can navigate to the Security Incident by clicking "Preview this record".
- Open the Security Incident by clicking "Preview this record" > "Open record".
- To view the list of entities associated with a Security Incident, perform the following actions:
  - Scroll down on the Security Incident Page
  - Under "Related Links," click on "Show All Related Lists"
  - A new set of tabs will appear underneath.
  - Click on the "Entity" tab to view the list of entities associated with the Security Incident.
  - Click on the "Detection" tab to view the list of detections associated with Security Incidents.
- On the entity page, you can also relate an entity to a pre-existing Incident by clicking on the "Search" button next to the " Incident" field (i.e. "Looking using list").
- The Incident table gets opened in a new tab.
- Search and select any Incident to attach the entity to the Incident.
- You can then open the Incident from the reference provided as mentioned in the above steps.

2.3.4.2. Create Assignment

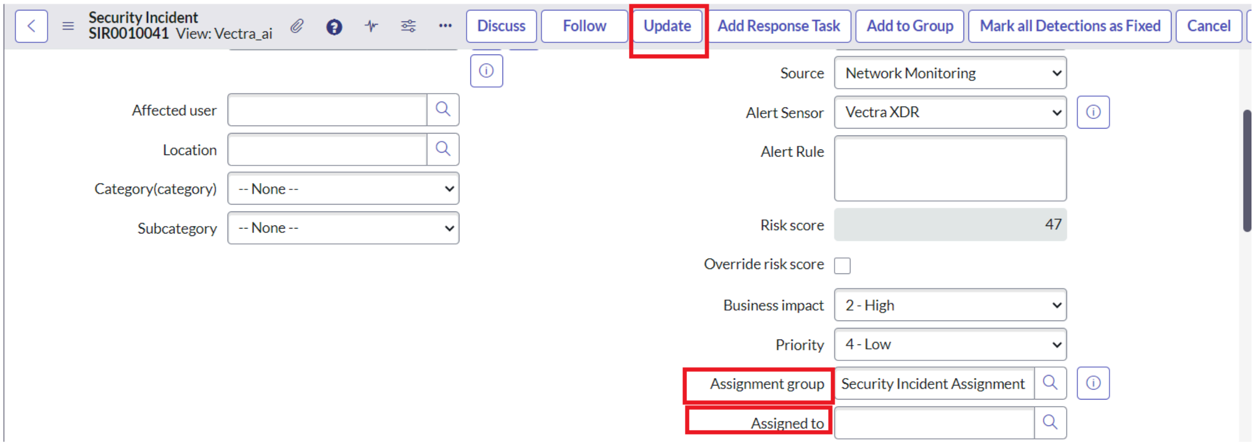
Can assign the user to the entity on the Vectra platform from Security Incident.

Role Required :Vectra analyst

Procedure:

- Login to the ServiceNow instance.
- Navigate to Vectra > Security Incident
- Open record
- Select the Group
- Select the User to whom want to assign entity on Vectra
- Click on the Update button to assign the user to the Entity.
- It will assign the selected user to the entity on Vectra platform

- If the selected user does not exist on the Vectra platform it shows an error message stating user does not exist on the Vectra platform and hence it assigns the user that is set as Fallback user in Incident profile.



Security Incident
SIR0010041 View: Vectra_ai

Affected user	
Location	
Category(category)	-- None --
Subcategory	-- None --
Source	Network Monitoring
Alert Sensor	Vectra XDR
Alert Rule	
Risk score	47
Override risk score	□
Business impact	2 - High
Priority	4 - Low
Assignment group	Security Incident Assignment
Assigned to	

Note: Create a user with ID, Name and email ID while creating user.

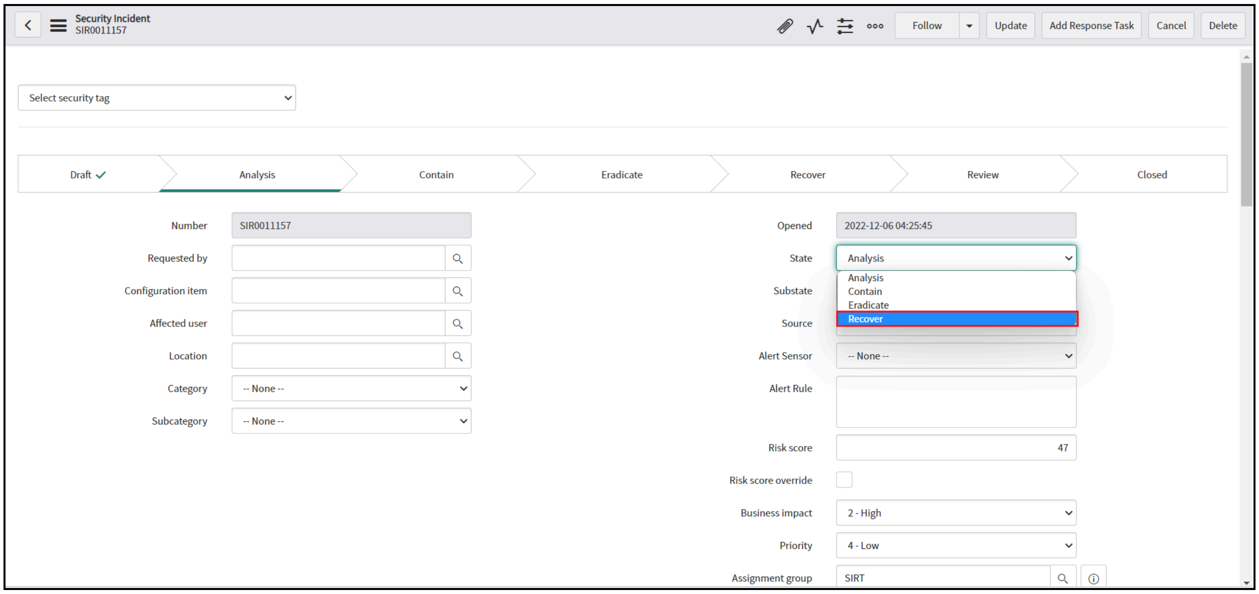
2.3.4.3. Close Security Incident

When close the Security Incident that has Entities or Detection linked to it. It wont close the Entities or detections.

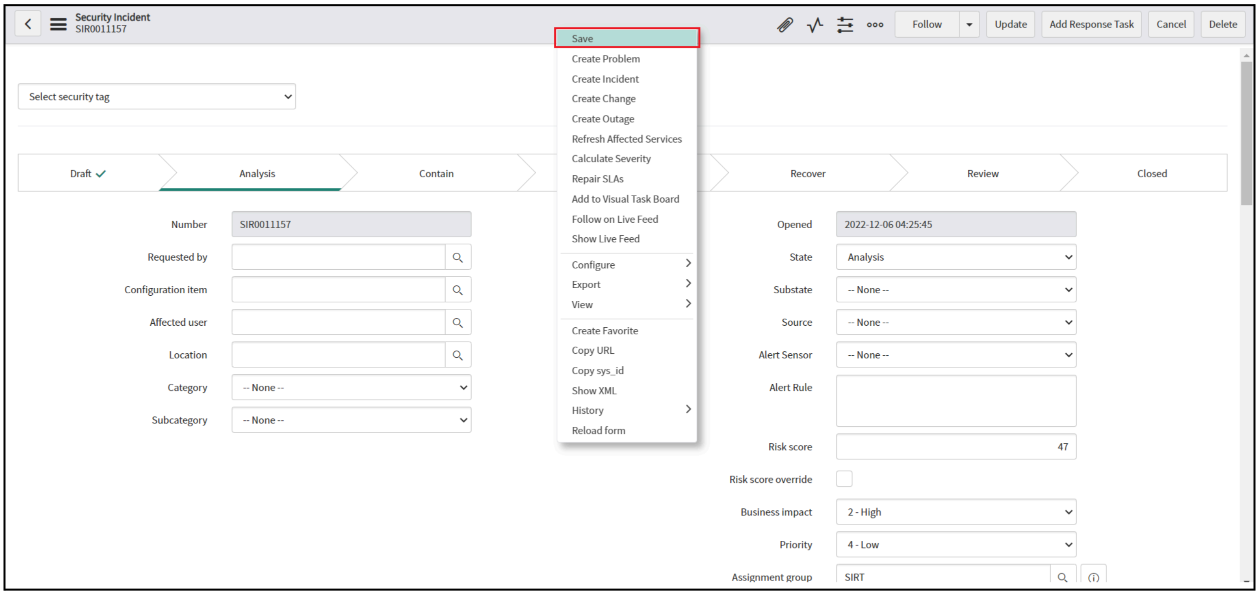
Role Required: Vectra analyst

Procedure:

- Login to the ServiceNow instance.
- Navigate to Security Incident > Show All Incidents.
- Select any Security Incident that has alerts linked to it.
- Go to the State field, select Recover, right-click on the security incident taskbar, and select the Save Option

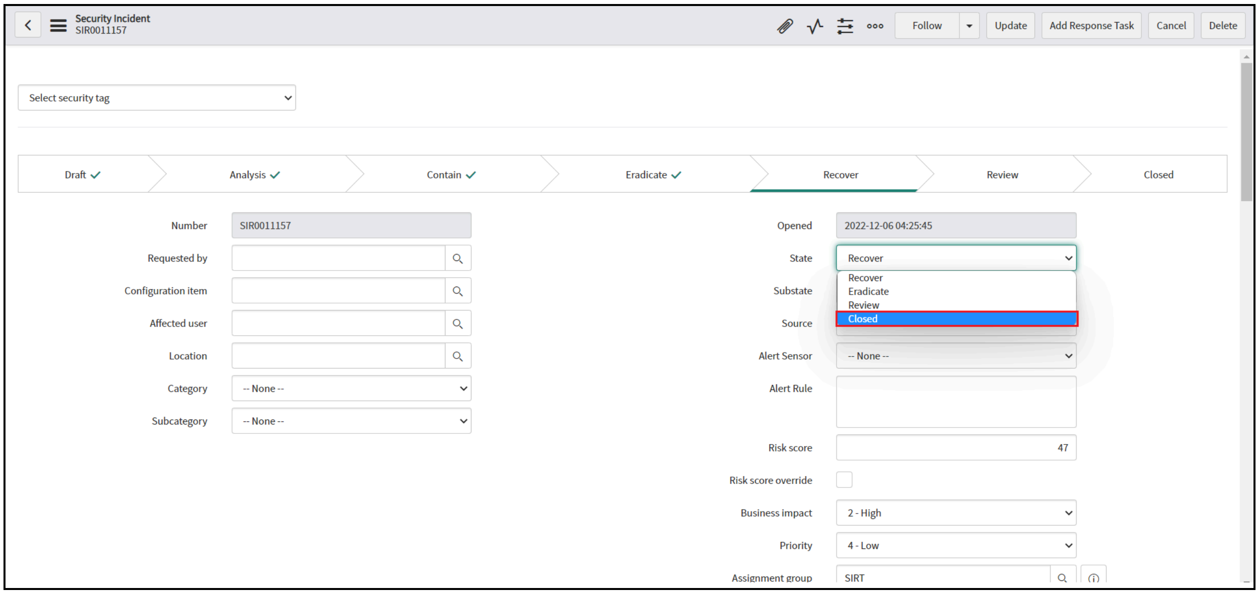


Number	SIR0011157	Opened	2022-12-06 04:25:45
Requested by		State	Analysis
Configuration item		Substate	
Affected user		Source	
Location		Alert Sensor	-- None --
Category	-- None --	Alert Rule	
Subcategory	-- None --		
		Risk score	47
		Risk score override	□
		Business impact	2 - High
		Priority	4 - Low
		Assignment group	SIRT



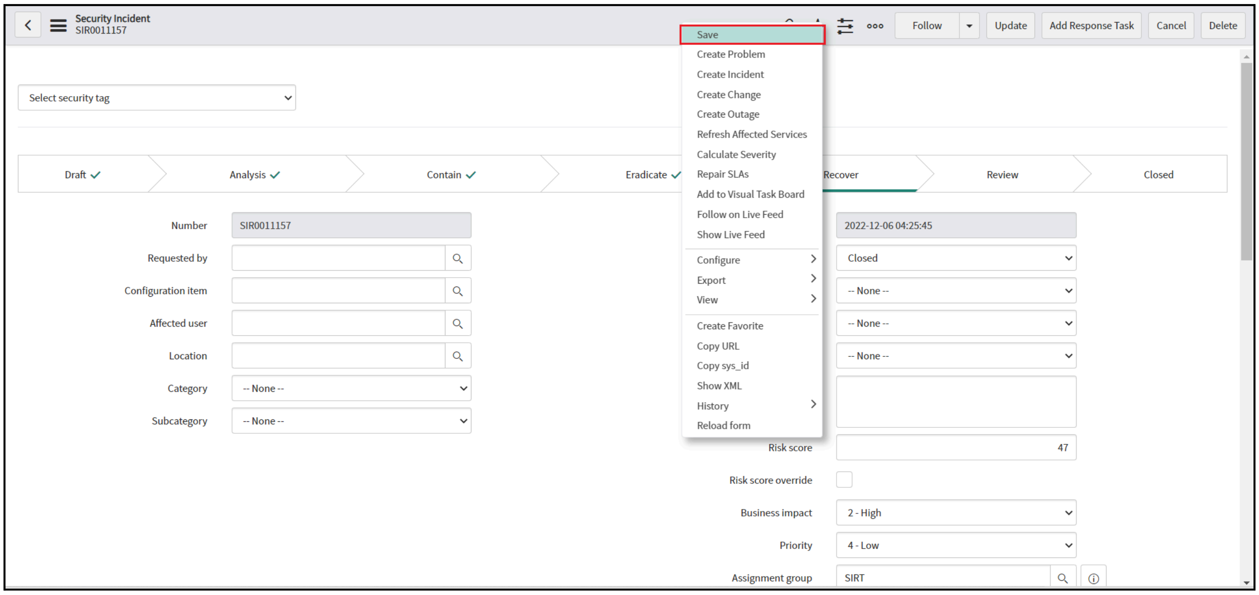
Number	SIR0011157	Opened	2022-12-06 04:25:45
Requested by		State	Analysis
Configuration item		Substate	-- None --
Affected user		Source	-- None --
Location		Alert Sensor	-- None --
Category	-- None --	Alert Rule	
Subcategory	-- None --		
		Risk score	47
		Risk score override	□
		Business impact	2 - High
		Priority	4 - Low
		Assignment group	SIRT

- For “State”, select “Closed”.



Number: SIR0011157
Requested by:
Configuration item:
Affected user:
Location:
Category: -- None --
Subcategory: -- None --
Opened: 2022-12-06 04:25:45
State: Recover
Substate:
Source:
Alert Sensor: -- None --
Alert Rule:
Risk score: 47
Risk score override: □
Business impact: 2 - High
Priority: 4 - Low
Assignment group: SIRT

- Provide a “Resolution code” and “Resolution note in Closure Information and right-click on the security incident taskbar and click the Save option.



Number: SIR0011157
Requested by:
Configuration item:
Affected user:
Location:
Category: -- None --
Subcategory: -- None --
2022-12-06 04:25:45
Closed
-- None --
-- None --
-- None --
Risk score: 47
Risk score override: □
Business impact: 2 - High
Priority: 4 - Low
Assignment group: SIRT

- After clicking Save, a consent form displays, allowing you to dismiss alerts of your choosing upon closing the Security Incident.

2.3.4.4. Download PCAP

Description: As a ServiceNow Vectra App Admin and Vectra Analyst, I should be able to download the PCAP file from the detection form viCreate Users

Role Required: Vectra_analyst

Procedure:

- Login to the ServiceNow instance.
- Save the Vectra Profile and start its data collection
- Select detection and click to open
- From the detection form view this action can be performed.
- Click on the "**Download PCAP" button to perform the action.**
- Once it downloads successfully the file should be attached to the detection and a note should be generated under the "**Activities**" inside the Notes Section.
- If the PCAP file is already attached and the user again clicks on "Download PCAP", then the new attachment should be appended with an old attachment after downloading.

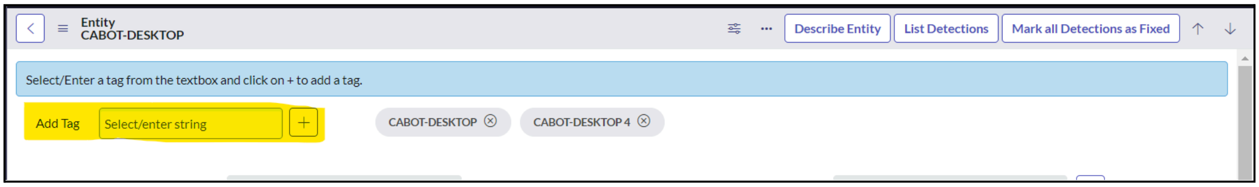
2.3.4.5. Update a tag (Add/ Remove) to Entity in Vectra Detect

As a ServiceNow Vectra App Admin and Vectra Analyst, I should be able to add/remove a tag/tags to an Entity on the ServiceNow platform and the changes in tags should also get reflected on the Vectra Detect.

Role Required: Vectra_analyst

Procedure:

- Login to the ServiceNow instance.
- Navigate to Vectra application > Entity
- Select any entity record which is active.
- Entity form view toolbar has a button "Add Tag".



Select/Enter a tag from the textbox and click on + to add a tag.

- The existing applied tags should be shown as tag pills in the toolbar on top of the form.
- To add a tag to any Entity enter the text so that suggestion appears if you want to select the suggested tag then click on add icon. But if the text came up as suggestions are not the one you want to make Tag then enter the text of your choice and click on add button.
- The applied tags (if any) shown as tag pills will have a cross icon.
- If the user clicks on the cross icon of the applied tag, the tag pill will be removed.
- Added and removed tags will get reflected on the Vectra Detect at the same time when added or removed on ServiceNow.
- While updating tags if an error occurs then the application will show the error message in the logs.

- **Note:** Duplicate tag entry is not allowed.

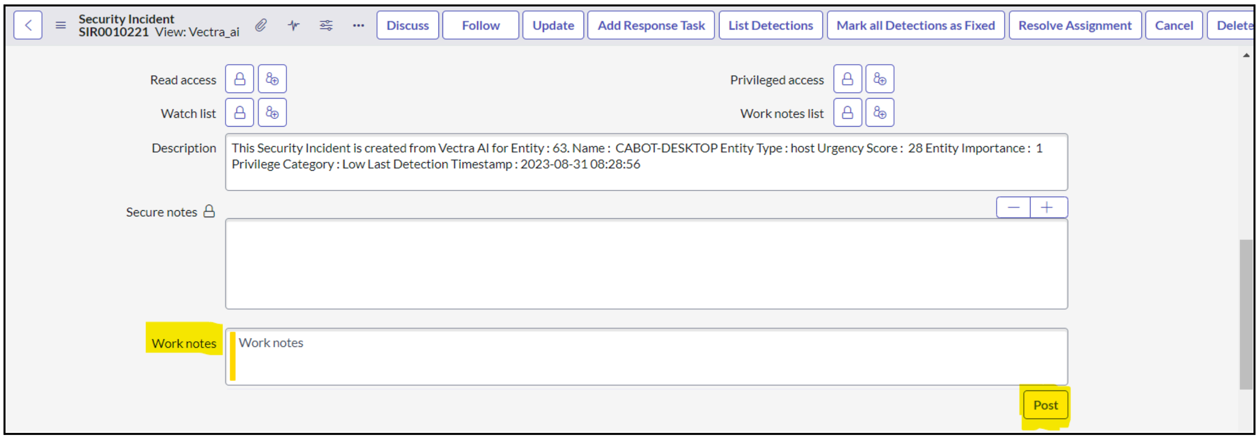
2.3.4.6. Add a note to Entity in Vectra Detect

As a ServiceNow Vectra App Admin and Vectra Analyst, I should be able to add a note to an Entity in ServiceNow, and the same changes should also get reflected in the Vectra Detect.

Role Required: Vectra_analyst

Procedure:

- Login to the ServiceNow instance.
- Navigate to Vectra application > Security Incident
- Select any Security incident.
- From the **Work notes add the notes and click on "Post"**



Description: This Security Incident is created from Vectra AI for Entity : 63. Name : CABOT-DESKTOP Entity Type : host Urgency Score : 28 Entity Importance : 1 Privilege Category : Low Last Detection Timestamp : 2023-08-31 08:28:56

Work notes: Work notes

- The notes should be added to the "Activities" and the same notes should be added to the Entity on to the Vectra Detect to which the current security incident is linked.
- Users should be able to add multiple notes to a particular Entity.

2.3.4.7. Mark all detections as fixed for an entity

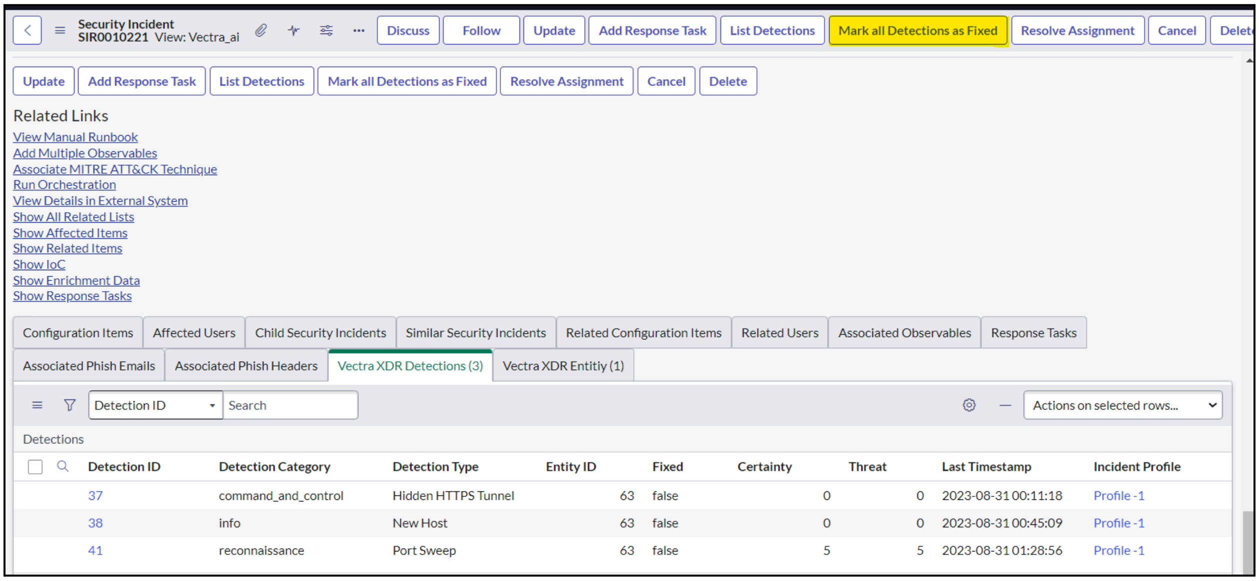
As a ServiceNow Vectra App Admin and Vectra Analyst, I should be able to mark all the Detections for specific Entity as fixed in ServiceNow and the same changes should also get reflected in the Vectra Detect.

Role Required: Vectra_analyst

Procedure:

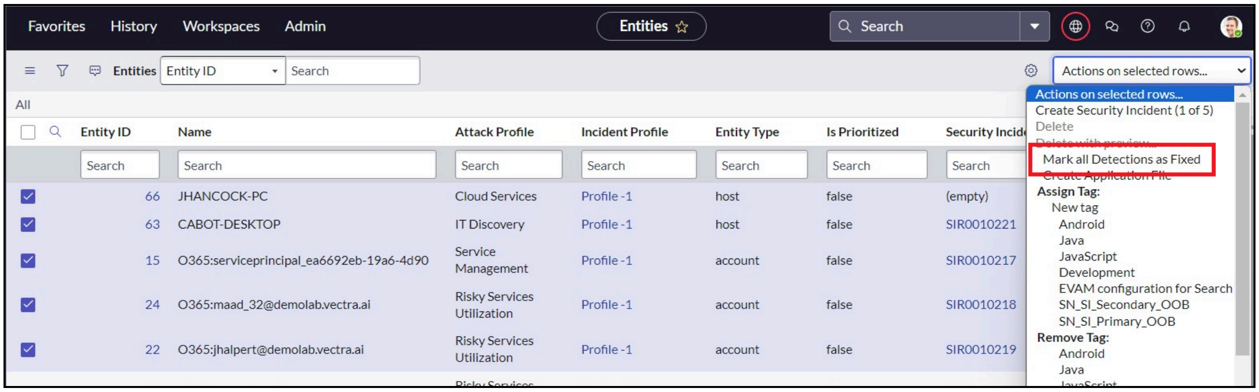
- Login to the ServiceNow instance.
- Navigate to Vectra application > Entity

- Open entity form view
- Click on "**Mark all Detections as Fixed**"



Detection ID	Detection Category	Detection Type	Entity ID	Fixed	Certainty	Threat	Last Timestamp	Incident Profile
37	command_and_control	Hidden HTTPS Tunnel	63	false	0	0	2023-08-31 00:11:18	Profile -1
38	info	New Host	63	false	0	0	2023-08-31 00:45:09	Profile -1
41	reconnaissance	Port Sweep	63	false	5	5	2023-08-31 01:28:56	Profile -1

- On the entity form view there will be a button of "**Mark all Detections as Fixed" if the** Detection is not fixed on the ServiceNow
- On the Entity list view select single or multiple entities and click on "Mark all Detections as Fixed". So it will fix all the detection on the ServiceNow as well as on the Vectra detect platform.



	Entity ID	Name	Attack Profile	Incident Profile	Entity Type	Is Prioritized	Security Incid
	Search	Search	Search	Search	Search	Search	Search
☑	66	JHANCOCK-PC	Cloud Services	Profile -1	host	false	(empty)
☑	63	CABOT-DESKTOP	IT Discovery	Profile -1	host	false	SIR0010221
☑	15	O365:serviceprincipal_ea6692eb-19a6-4d90	Service Management	Profile -1	account	false	SIR0010217
☑	24	O365:maad_32@demolab.vectra.ai	Risky Services Utilization	Profile -1	account	false	SIR0010218
☑	22	O365:jhalpert@demolab.vectra.ai	Risky Services Utilization	Profile -1	account	false	SIR0010219
			Risky Services				

- You can also perform an action from the Security Incident, open any incident, click on Entity Tab, select single or multiple Entity, and select the action "Mark all Detections as Fixed". So here it will mark Fix for the detections which are not fixed. E.g. you have selected 20 entities and of which 20 detections are there out of 20, 10 are fixed and 10 are not. So it will show the pop-up "" and run the action.
- The Detections should be reflected as marked as fixed in the Vectra Detect after marking fixed from ServiceNow and the "Fixed" checkbox should get checked in the form in ServiceNow.

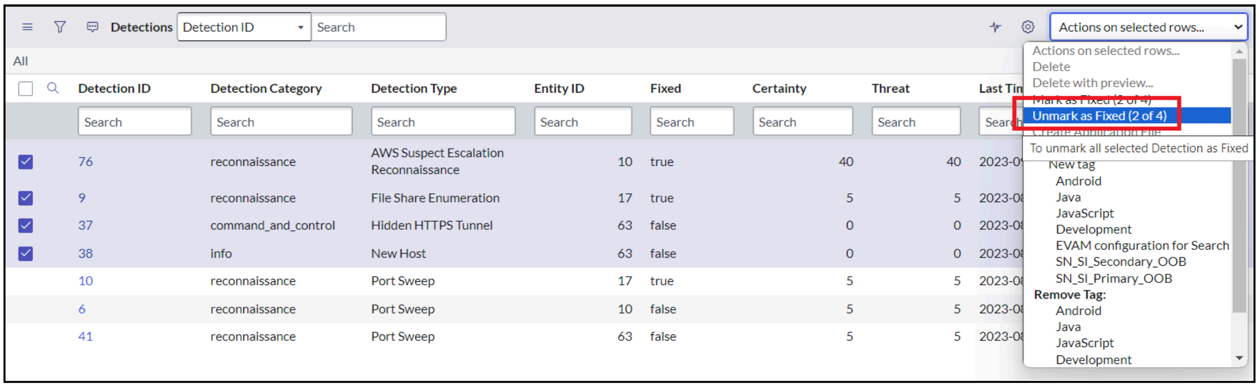
2.3.4.8. Mark/Unmark Detection as fixed

As a ServiceNow Vectra App Admin and Operation User, I should be able to mark or unmark a Detection as fixed in ServiceNow and the same changes should also get reflected in the Vectra XDR.

Role Required: Vectra_analyst

Procedure:

- Login to the ServiceNow instance.
- Navigate to Vectra application > Detection
- Open record to view
- Select detection to open
- “Mark as Fixed” is visible in the Detection form view when Detection is not fixed on ServiceNow.

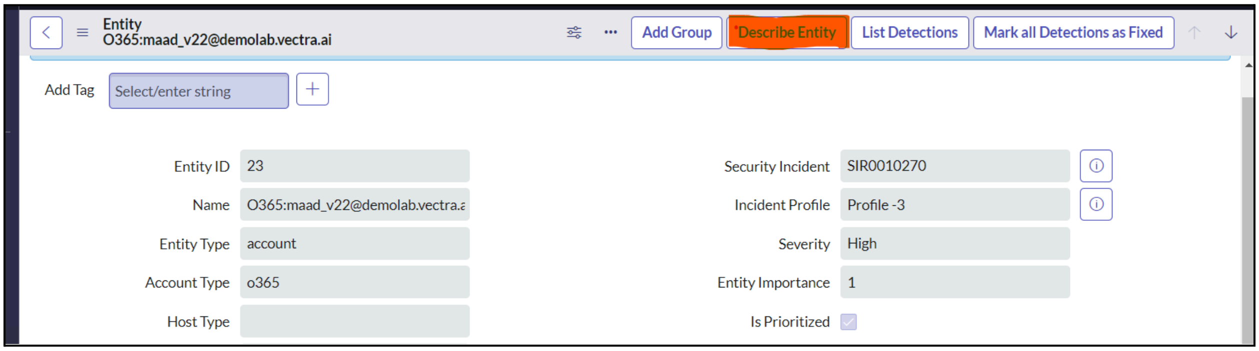


☐	Detection ID	Detection Category	Detection Type	Entity ID	Fixed	Certainty	Threat	Last Tin
	Search	Search	Search	Search	Search	Search	Search	Search
☑	76	reconnaissance	AWS Suspect Escalation Reconnaissance	10	true	40	40	2023-0
☑	9	reconnaissance	File Share Enumeration	17	true	5	5	2023-0
☑	37	command_and_control	Hidden HTTPS Tunnel	63	false	0	0	2023-0
☑	38	info	New Host	63	false	0	0	2023-0
	10	reconnaissance	Port Sweep	17	true	5	5	2023-0
	6	reconnaissance	Port Sweep	10	false	5	5	2023-0
	41	reconnaissance	Port Sweep	63	false	5	5	2023-0

- Unmark as Fixed” is visible in the Detection form view when Detection is fixed on ServiceNow.
- Based on the detection status Fixed/Not Fixed, the application shows the button “Mark as Fixed /Unmark as FIxed”.
- Click on the button to perform the action, Mark as Fixed, so a confirmation pop-up will be displayed.
- Click on the “Yes” button on the confirmation pop-up then that particular Detection will be marked as fixed on the Vectra Detect. Moreover, it will add the notes in ServiceNow detection, based on action (Mark as Fixed/Unmark as Fixed).
- Now select the detection which is fixed so the button “Unmark as Fixed” is visible now click on the button so it shows the pop up when click on Yes, it will mark all the selected detections as Not fixed on ServiceNow and on Vectra Detect. Moreover, it will add the notes in ServiceNow detection, based on action (Mark as Fixed/Unmark as Fixed).
- When clicking on “No” on the confirmation pop-up, the application will not perform the action.

2.3.4.9. Describe Entity

- Login to the ServiceNow instance.
- Navigate to Vectra application > Search for the Entity table
- Open the record and you will see the button “Describe Entity”.
- Click on the button
- It will fetch the latest updated details of the entity from the Vectra platform and update the entity details in the ServiceNow.

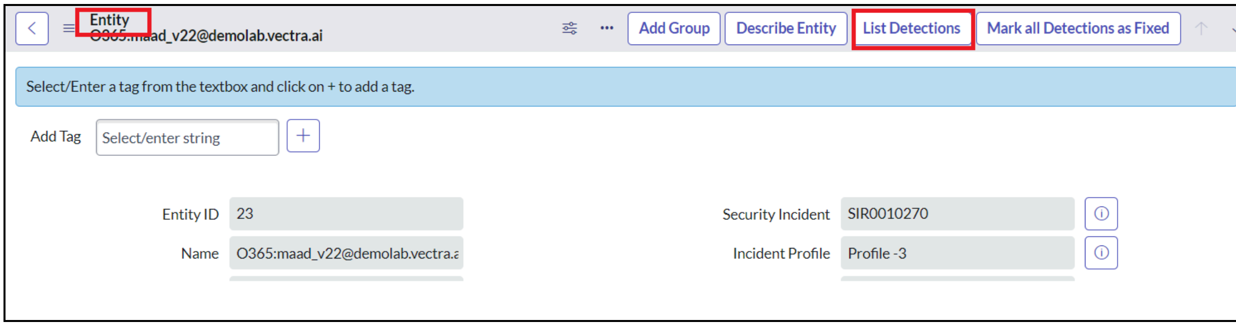


Entity ID	23	Security Incident	SIR0010270
Name	O365:maad_v22@demolab.vectra.a	Incident Profile	Profile -3
Entity Type	account	Severity	High
Account Type	o365	Entity Importance	1
Host Type		Is Prioritized	☑

Note: If the Incident profile is deleted then the action button will not be visible on the entity form view.

2.3.4.10. List Detection

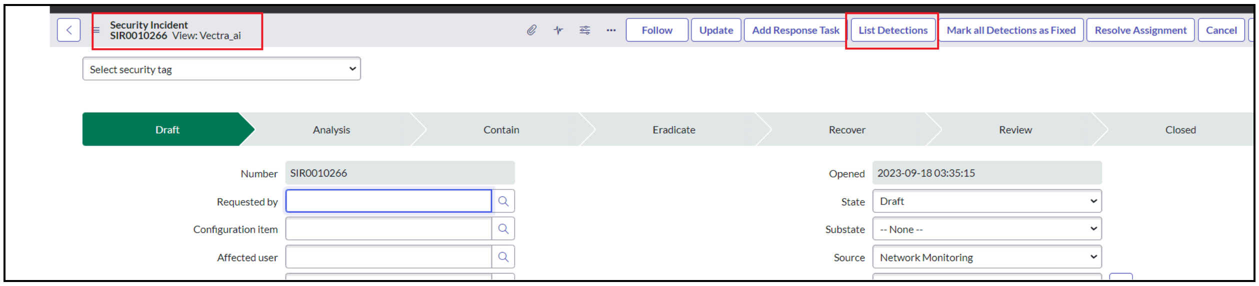
- Login to the ServiceNow instance.
- Navigate to Vectra application > Search for the Entity table/Security Incident table (This action can be performed from Entity and Incident table also).
- Open the Entity/Security Incident record to run the action.
- On the form view you will see the “List Detection” button



Select/Enter a tag from the textbox and click on + to add a tag.

Entity ID	23	Security Incident	SIR0010270
Name	O365:maad_v22@demolab.vectra.a	Incident Profile	Profile -3

- Now click on the button.
- So it will fetch all the detections which are linked with Entity.
- Can Perform List Detection from the Security Incident Form view also.
- **Note**: If the Incident profile is deleted then the action button will not be visible on the entity and Security Incident form view.

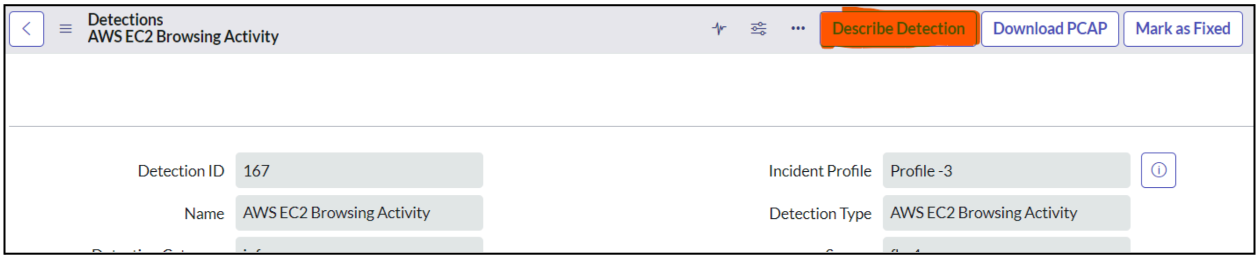


Security Incident
SIR0010266 View: Vectra_ai

Number	SIR0010266	Opened	2023-09-18 03:35:15
Requested by		State	Draft
Configuration Item		Substate	-- None --
Affected user		Source	Network Monitoring

2.3.4.11. Describe Detection

- Login to the ServiceNow instance.
- Navigate to Vectra application > Search for the detection table
- Now open the record and click on the button " Describe Detection".
- It will fetch the latest updated details of Detection from the Vectra platform and update into the ServiceNow.



Detections
AWS EC2 Browsing Activity

Detection ID	167	Incident Profile	Profile -3
Name	AWS EC2 Browsing Activity	Detection Type	AWS EC2 Browsing Activity

Note: If the Incident profile is deleted then the action button will not be visible on the entity form view.

2.3.4.12. Add to Group

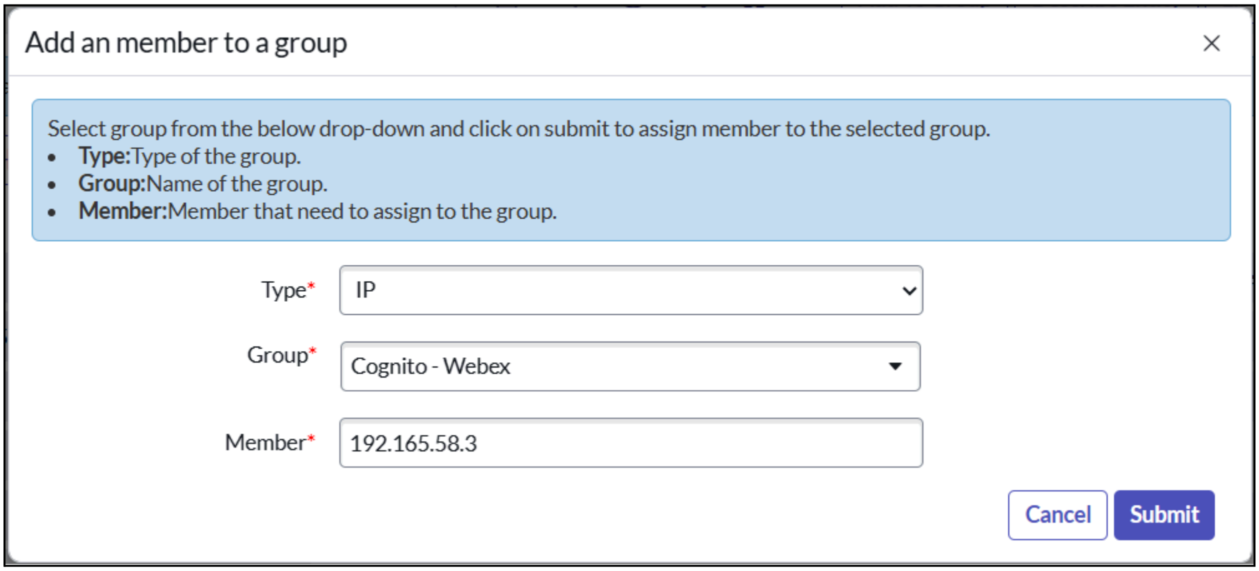
Description: As a ServiceNow Vectra app Admin and Operation User, I should be able to add members in the Group from the Entity and security Incident from using "Add to Group" UI action and the same changes should also get reflected on the Vectra platform.

Role: Vectra Admin, Vectra Analyst

Procedure:

- Login to the ServiceNow instance.
- Navigate to Vectra application > Search for the Security Incident or entity table.
- This action can be performed from the Security Incident as well from the entities form view.
- Now open the record and click on the button " Add to Group".
- It opens the pop up to select the Type.
- Then select the relevant Type and group i.g. for Account type entities , select the group that belongs to the Account type entity.

- Now enter value in the Member field e.g. If the type is Account then enter the value e.g. uuid or ID.
- Members are added to the “members” list in the body. The member value added depends on the group type. Below mentioned the type and accepted value.
    - Account Members: Add by uuid or entity ID(Integer)
    - Host Members: Add by name or url(String) and ID(Integer)
    - IP Members: Add by IP address (String)
    - Domain Members: Add by domain(String)
- Now click on the “Submit” button to assign the Group and “Cancel” to not to assign the Group.
- When clicked on Submit, It assigns the group to the entity on the Vectra Platform and shows the information message on the UI and the application log.
-


Add an member to a group

Select group from the below drop-down and click on submit to assign member to the selected group.

- **Type:**Type of the group.
- **Group:**Name of the group.
- **Member:**Member that need to assign to the group.

Type* IP

Group* Cognito - Webex

Member* 192.165.58.3

Note: If the Incident profile is deleted then the action button will not be visible on the entity form view.

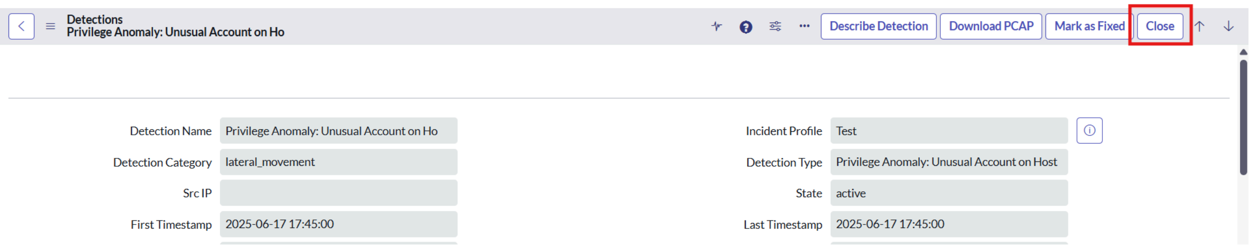
2.3.4.13. Close detection

The user can close the detection with an appropriate reason in ServiceNow, and the same changes will be reflected on the Vectra XDR detection.

Role Required: Vectra analyst

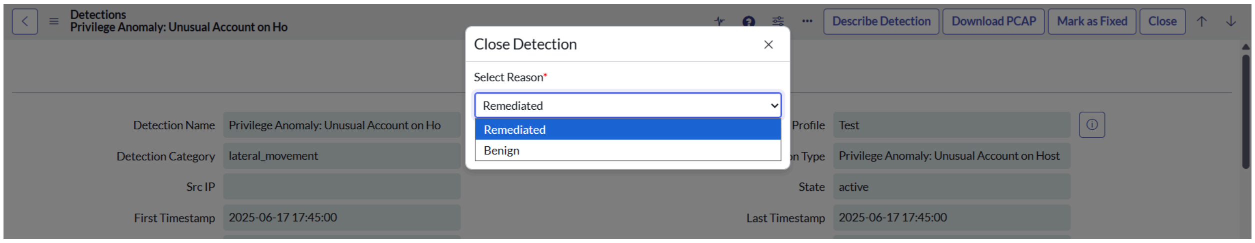
Procedure:

- Login to the ServiceNow instance.
- Navigate to Vectra application > Detections
- Open detection record which is active & have fixed & is_triaged - false
- Click on the “Close” button.



Detection Name: Privilege Anomaly: Unusual Account on Ho
Incident Profile: Test
Detection Category: lateral_movement
Detection Type: Privilege Anomaly: Unusual Account on Host
Src IP:
State: active
First Timestamp: 2025-06-17 17:45:00
Last Timestamp: 2025-06-17 17:45:00

- It should open modal, select the reason for resolution & click submit.



Select Reason*: Remediated

Detection Name: Privilege Anomaly: Unusual Account on Ho
Profile: Test
Detection Category: lateral_movement
n Type: Privilege Anomaly: Unusual Account on Host
Src IP:
State: active
First Timestamp: 2025-06-17 17:45:00
Last Timestamp: 2025-06-17 17:45:00

- If the operation is successful, an info message will be displayed on the detection form : **“Successfully closed detection as <Reason> on the Vectra XDR platform.”**, a note will be added to the detection record & the reason value will be set as the given reason value. If the selected reason is benign, is Triaged field will be checked, or if the selected reason is Remediated the Fixed will be checked.
- After closing detection, if there are no remaining active and open detections linked to the entity, then the entity’s state will be changed to **inactive**.
- If the operation fails, an appropriate error message should be displayed on the detection form & related failure notes will be added to the note of detection record.

Notes:

- If user close detection or entity from the Vectra XDR portal, that detection or entity details won’t be synced in the servicenow because only active entities are fetched from the Vectra portal into the servicenow.
- If a user closes a single detection or single active detection or all detections present for any entity from servicenow, that entity and detection’s latest details won’t be synced in the servicenow because only active entities are fetched from the Vectra portal into the servicenow.
- If a user closes an entity from the servicenow, that entity and its related detections latest state/details won’t be synced in the servicenow because only active entities are fetched from the Vectra portal into the servicenow.

For all these above scenarios, user can perform the **Describe Entity** and **Describe Detection** action to sync the entity and detection latest details.

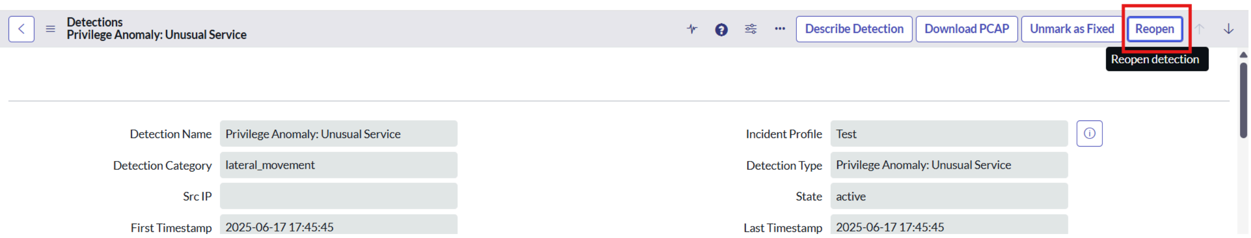
2.3.4.14. Re-open detection

The user can Re-open the closed detection in ServiceNow, and the same changes will be reflected on the Vectra XDR detection.

Role Required: Vectra analyst

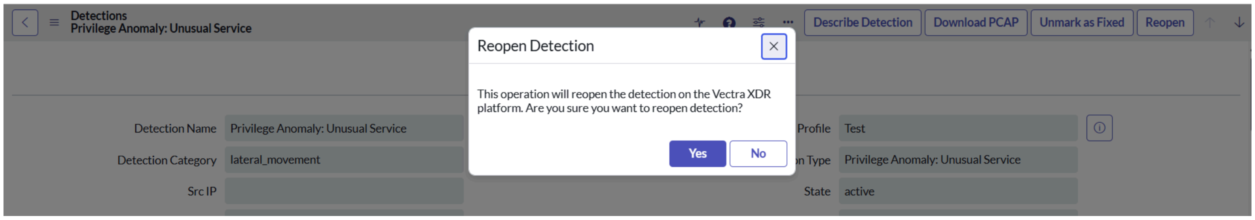
Procedure:

- Login to the ServiceNow instance.
- Navigate to Vectra application > Detections
- Open detection record which is active & have either of fixed or is_triaged - true
- Click on the “Reopen” button.



Detection Name: Privilege Anomaly: Unusual Service
Detection Category: lateral_movement
Src IP:
First Timestamp: 2025-06-17 17:45:45
Incident Profile: Test
Detection Type: Privilege Anomaly: Unusual Service
State: active
Last Timestamp: 2025-06-17 17:45:45

- It should open the modal for confirmation, click on the “Yes” button.



Reopen Detection

This operation will reopen the detection on the Vectra XDR platform. Are you sure you want to reopen detection?

Detection Name: Privilege Anomaly: Unusual Service
Detection Category: lateral_movement
Src IP:
Profile: Test
n Type: Privilege Anomaly: Unusual Service
State: active

- If the operation is successful, an info message will be displayed on the detection form : **"Successfully opened detection on the Vectra XDR platform.",** a note will be added to the detection record & is Triaged and Fixed fields will be unchecked & the reason field will be cleared.
- After reopening a detection, the entity’s state will be changed to active.
- If the operation fails, an appropriate error message will be displayed on the detection form & related failure notes will be added to the note of detection record.

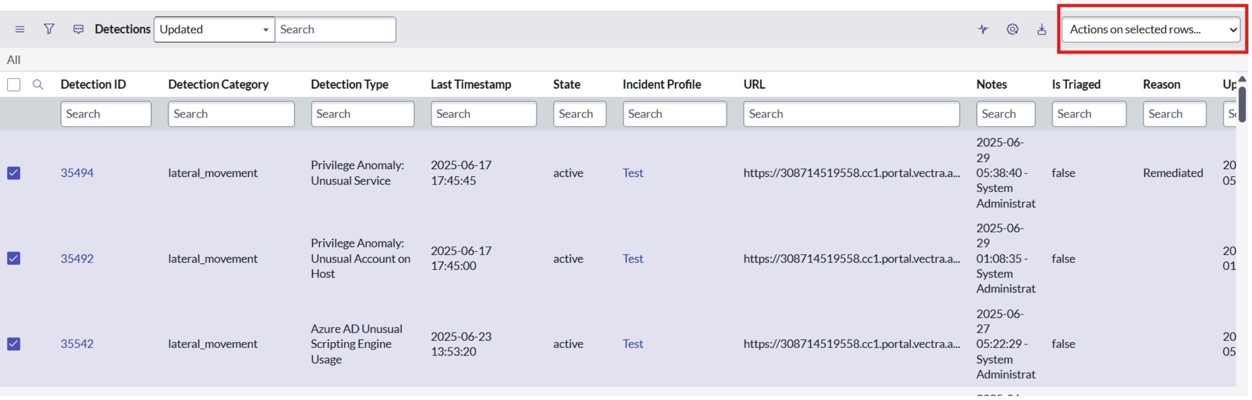
2.3.4.15. Close Multiple Detections

The user can close multiple detection at once from list view in ServiceNow, and the same changes will be reflected on the Vectra XDR detection.

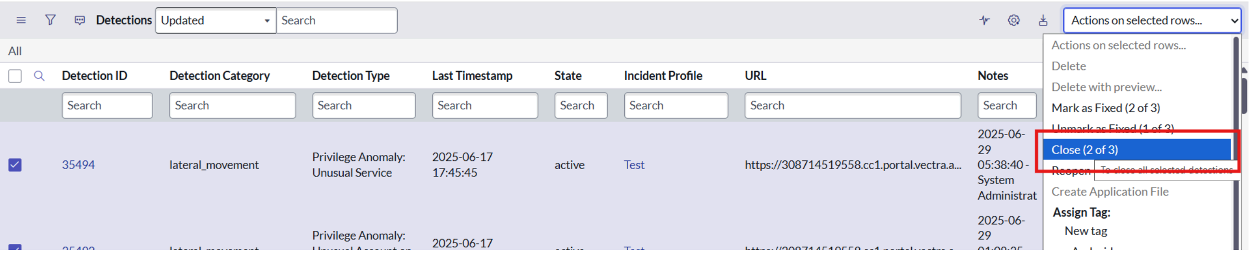
Role Required: Vectra analyst

Procedure:

- Login to the ServiceNow instance.
- Navigate to Vectra application > Detections
- Select one or more detections & click on the **“Actions on selected rows”** button at the top-right side of the list view, you should be able see the “Close” UI action in the dropdown, click on it.

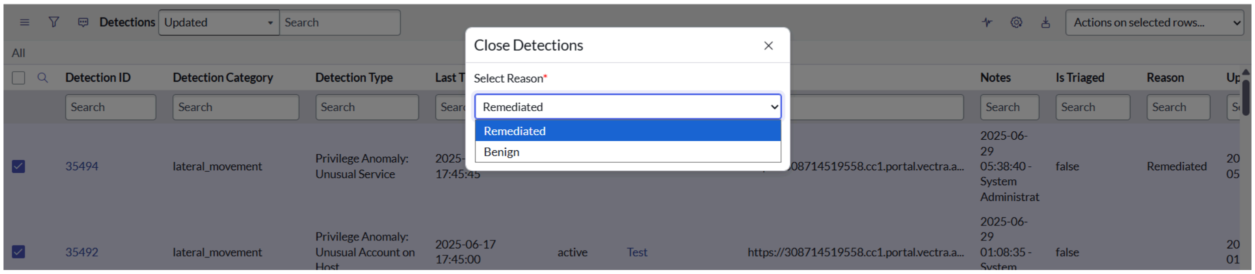


Detection ID	Detection Category	Detection Type	Last Timestamp	State	Incident Profile	URL	Notes	Is Triaged	Reason	Up
Search	Search	Search	Search	Search	Search	Search	Search	Search	Search	S
☑ 35494	lateral_movement	Privilege Anomaly: Unusual Service	2025-06-17 17:45:45	active	Test	https://308714519558.cc1.portal.vectra.a...	2025-06-29 05:38:40 - System Administrat	false	Remediated	20 05
☑ 35492	lateral_movement	Privilege Anomaly: Unusual Account on Host	2025-06-17 17:45:00	active	Test	https://308714519558.cc1.portal.vectra.a...	2025-06-29 01:08:35 - System Administrat	false		20 01
☑ 35542	lateral_movement	Azure AD Unusual Scripting Engine Usage	2025-06-23 13:53:20	active	Test	https://308714519558.cc1.portal.vectra.a...	2025-06-27 05:22:29 - System Administrat	false		20 05



Detection ID	Detection Category	Detection Type	Last Timestamp	State	Incident Profile	URL	Notes
Search	Search	Search	Search	Search	Search	Search	Search
☑ 35494	lateral_movement	Privilege Anomaly: Unusual Service	2025-06-17 17:45:45	active	Test	https://308714519558.cc1.portal.vectra.a...	2025-06-29 05:38:40 - System Administrat

- It should open modal, select the reason for resolution & click submit.



Select Reason* Remediated

Detection ID	Detection Category	Detection Type	Last T	URL	Notes	Is Triaged	Reason	Up
☑ 35494	lateral_movement	Privilege Anomaly: Unusual Service	2025- 17:45:45	...08714519558.cc1.portal.vectra.a...	2025-06-29 05:38:40 - System Administrat	false	Remediated	20 05
☑ 35492	lateral_movement	Privilege Anomaly: Unusual Account on Host	2025-06-17 17:45:00	https://308714519558.cc1.portal.vectra.a...	2025-06-29 01:08:35 - System	false		20 01

- If the operation is successful a note : **"Successfully closed detection as <Reason> on the Vectra XDR platform."** will be added to the detection record & the reason value will be set as given reason value. If the selected reason is benign, is Triaged field will be checked, or if the selected reason is Remediated the Fixed will be checked.
- After closing detections, if there are no remaining active and open detections linked to the entity, then the entity's state will be changed to **inactive**.
- If the operation fails, an appropriate error note will be added to the note of detection record.

Notes:

- If user close detection or entity from the Vectra XDR portal, that detection or entity details won't be synced in the servicenow because only active entities are fetched from the Vectra portal into the servicenow.
- If a user closes a single detection or single active detection or all detections present for any entity from servicenow, that entity and detection's latest details won't be synced in

the servicenow because only active entities are fetched from the Vectra portal into the servicenow.

- If a user closes an entity from the servicenow, that entity and its related detections latest state/details won't be synced in the servicenow because only active entities are fetched from the Vectra portal into the servicenow.

For all these above scenarios, user can perform the **Describe Entity** and **Describe Detection** action to sync the entity and detection latest details.

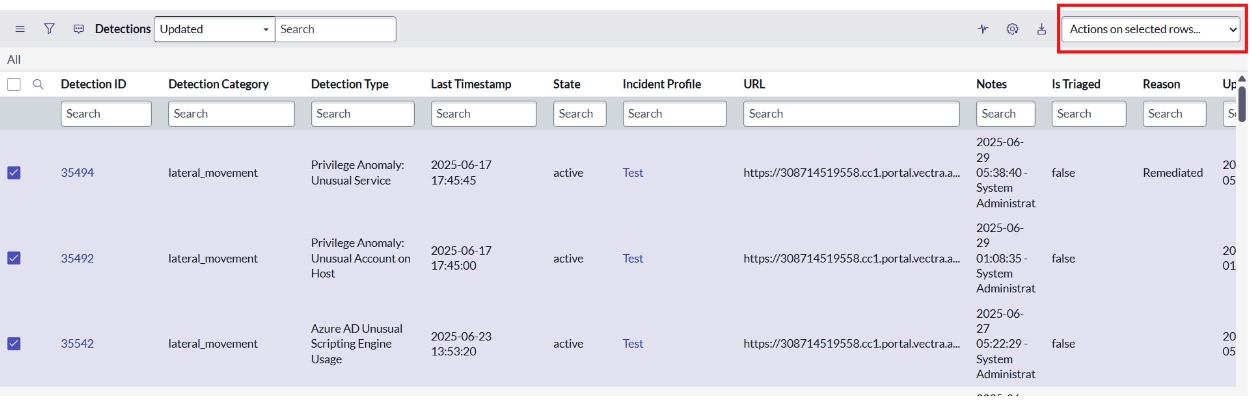
2.3.4.16. Re-open Multiple Detections

The user can Re-open multiple detections from list view in ServiceNow, and the same changes will be reflected on the Vectra XDR detection.

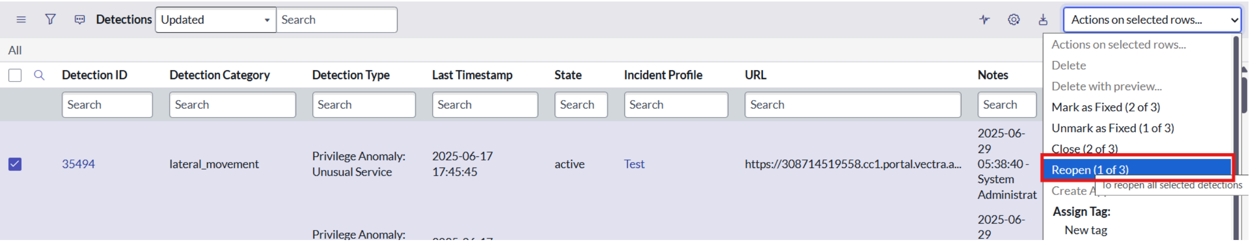
Role Required: Vectra analyst

Procedure:

- Login to the ServiceNow instance.
- Navigate to Vectra application > Detections
- Select one or more detections & click on the **"Actions on selected rows"** button at the top-right side of the list view, you should be able see the "Reopen" UI action in the dropdown, click on it.

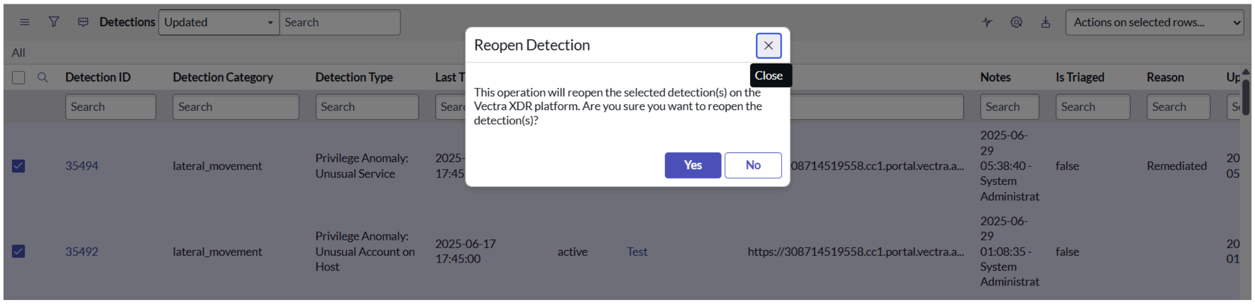


☐	Detection ID	Detection Category	Detection Type	Last Timestamp	State	Incident Profile	URL	Notes	Is Triaged	Reason	Up
	Search	Search	Search	Search	Search	Search	Search	Search	Search	Search	S
☑	35494	lateral_movement	Privilege Anomaly: Unusual Service	2025-06-17 17:45:45	active	Test	https://308714519558.cc1.portal.vectra.a...	2025-06-29 05:38:40 - System Administrat	false	Remediated	20 05
☑	35492	lateral_movement	Privilege Anomaly: Unusual Account on Host	2025-06-17 17:45:00	active	Test	https://308714519558.cc1.portal.vectra.a...	2025-06-29 01:08:35 - System Administrat	false		20 01
☑	35542	lateral_movement	Azure AD Unusual Scripting Engine Usage	2025-06-23 13:53:20	active	Test	https://308714519558.cc1.portal.vectra.a...	2025-06-27 05:22:29 - System Administrat	false		20 05



☐	Detection ID	Detection Category	Detection Type	Last Timestamp	State	Incident Profile	URL	Notes
	Search	Search	Search	Search	Search	Search	Search	Search
☑	35494	lateral_movement	Privilege Anomaly: Unusual Service	2025-06-17 17:45:45	active	Test	https://308714519558.cc1.portal.vectra.a...	2025-06-29 05:38:40 - System Administrat
			Privilege Anomaly:					2025-06-29

- It should open modal for confirmation.



Reopen Detection

This operation will reopen the selected detection(s) on the Vectra XDR platform. Are you sure you want to reopen the detection(s)?

Yes No

Detection ID	Detection Category	Detection Type	Last T				Notes	Is Triaged	Reason	Up
35494	lateral_movement	Privilege Anomaly: Unusual Service	2025- 17:45			08714519558.cc1.portal.vectra.a...	2025-06-29 05:38:40 - System Administrat	false	Remediated	20 05
35492	lateral_movement	Privilege Anomaly: Unusual Account on Host	2025-06-17 17:45:00	active	Test	https://308714519558.cc1.portal.vectra.a...	2025-06-29 01:08:35 - System Administrat	false		20 01

- If the operation is successful a note : **“Successfully opened detection on the Vectra XDR platform.”** will be added to each detection record & is Triaged and Fixed fields will be unchecked & the reason field will be cleared.
- After reopening detections, the entity’s state will change to **active**.
- If the operation fails, an appropriate error note will be added to the note of detection record.

2.3.4.17. Close Entity

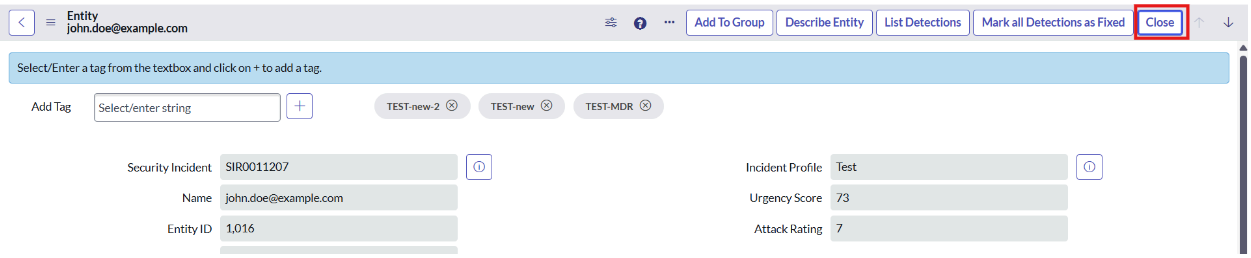
The user can close the entity in ServiceNow, which will close all its active detection in ServiceNow and changes will be reflected on the Vectra XDR detection.

Role Required: Vectra analyst

Procedure:

1. **From entity**

- Login to the ServiceNow instance.
- Navigate to Vectra application > Entities
- Open any active entity record.
- Click on the **“Close”** button.

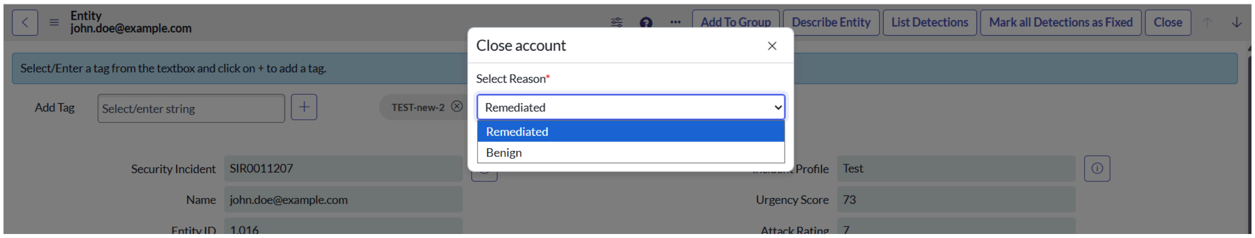


Select/Enter a tag from the textbox and click on + to add a tag.

Add Tag: Select/enter string

Security Incident	SIR0011207	Incident Profile	Test
Name	john.doe@example.com	Urgency Score	73
Entity ID	1,016	Attack Rating	7

- It should open modal, select the reason for resolution & click submit.



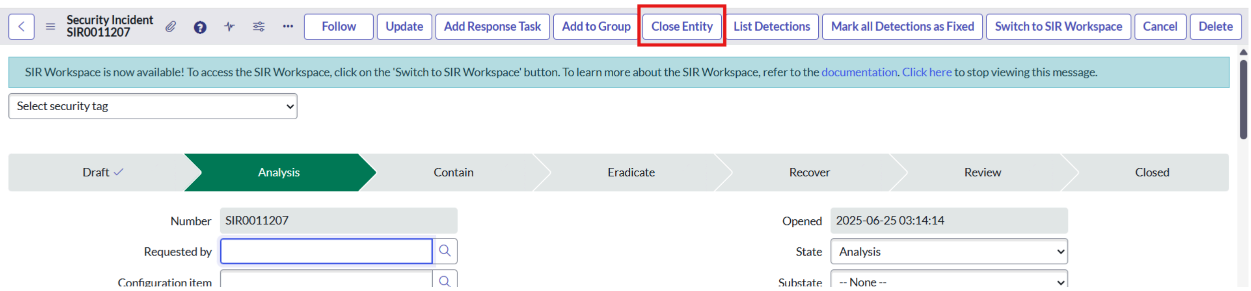
Select/Enter a tag from the textbox and click on + to add a tag.

Security Incident: SIR0011207
Name: john.doe@example.com
Entity ID: 1016
Profile: Test
Urgency Score: 73
Attack Rating: 7
Select Reason*: Remediated

- If the operation is successful, an info message will be displayed : **"Successfully closed <entityType> as <reason> on the Vectra XDR platform."** . A note will be added to related security incident records & and based on the response returned from the Vectra XDR platform, the corresponding detections will be closed in SNOW with the given reason. If the selected reason is **Benign**, the **Is Triaged** field will be checked; if the reason is **Remediated**, the **Fixed** field will be checked.
- After closing the entity, it should be marked as **inactive.**
- If the operation fails, an appropriate error message will be displayed & a note will be added to the note of security Incident record.

2. From Security Incident

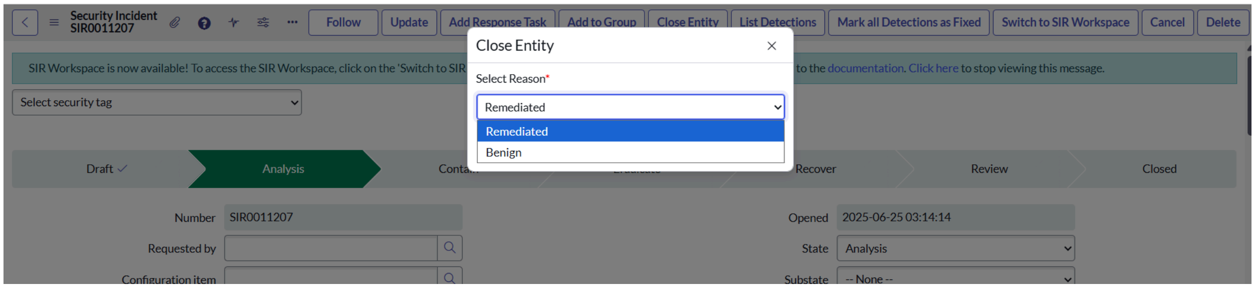
- Login to the ServiceNow instance.
- Navigate to Vectra application > Entities
- Open any active entity's security incident record.
- Click on the **"Close Entity"** button.



SIR Workspace is now available! To access the SIR Workspace, click on the 'Switch to SIR Workspace' button. To learn more about the SIR Workspace, refer to the documentation. Click here to stop viewing this message.

Number: SIR0011207
Requested by:
Configuration item:
Opened: 2025-06-25 03:14:14
State: Analysis
Substate: -- None --

- It should open modal, select the reason for resolution & click submit.



Number: SIR0011207
Opened: 2025-06-25 03:14:14
State: Analysis
Substate: -- None --
Select Reason*: Remediated

- If the operation is successful, an info message will be displayed : **"Successfully closed <entityType> as <reason> on the Vectra XDR platform."** . A note will be added to the security incident record & and based on the response returned from the Vectra XDR platform, the corresponding detections will be closed in SNOW with the given reason.

If the selected reason is **Benign**, the **Is Triaged** field will be checked; if the reason is **Remediated**, the **Fixed** field will be checked.

- After closing the entity, it should be marked as **inactive.**
- If the operation fails, an appropriate error message will be displayed & a note will be added to the note of security Incident record.

Notes:

- If user close detection or entity from the Vectra XDR portal, that detection or entity details won't be synced in the servicenow because only active entities are fetched from the Vectra portal into the servicenow.
- If a user closes a single detection or single active detection or all detections present for any entity from servicenow, that entity and detection's latest details won't be synced in the servicenow because only active entities are fetched from the Vectra portal into the servicenow.
- If a user closes an entity from the servicenow, that entity and its related detections latest state/details won't be synced in the servicenow because only active entities are fetched from the Vectra portal into the servicenow.

For all these above scenarios, user can perform the **Describe Entity** and **Describe Detection** action to sync the entity and detection latest details.

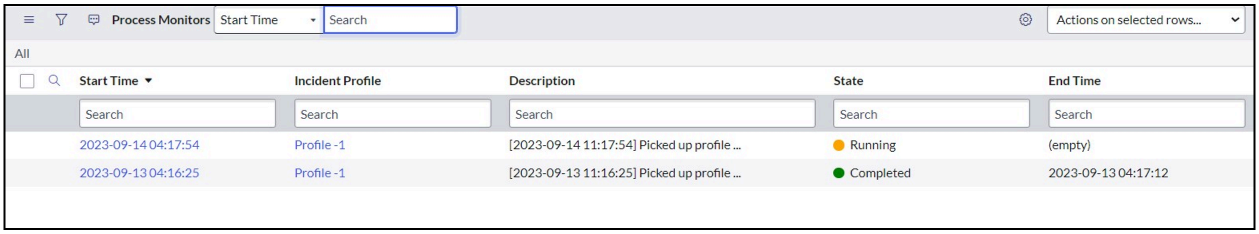
2.3.5. Process Monitor

Description: As a ServiceNow Vectra App Admin and Application analyst, I should see the ongoing ingestion process of Entity and the Security Incident creation in the process monitor.

Role Required: Vectra_analyst

Procedure:

- Login to the ServiceNow instance.
- Navigate to Vectra application > Process monitor
- All the fields which are present in the Process monitor are read-only.
- The process state field will be changed to **'New'** once the incident profile is picked for the ingestion.
- The process state field will be changed to **'Running'** once the data collection process is started and the ingestion process is started.



Start Time ▼	Incident Profile	Description	State	End Time
Search	Search	Search	Search	Search
2023-09-14 04:17:54	Profile -1	[2023-09-14 11:17:54] Picked up profile ...	● Running	(empty)
2023-09-13 04:16:25	Profile -1	[2023-09-13 11:16:25] Picked up profile ...	● Completed	2023-09-13 04:17:12

- Process's state field will be changed to **'Completed'** once all Entities are fetched and associated security incidents have been created.
- The process state field will be changed to **'Failed'** if an error occurs while fetching any entity or detection.
- The process state field will be changed to **'Complete with Error**' if an error occurs after all data is fetched successfully but another process like security incident creation fails.

3. Upgradation

This section describes the process of upgrading from the old version of the application to the newer version.

Role Required: System Administrator

1. Navigate to "System Applications" ⍰ "All Available applications" ⍰ "All".
2. Mark Check the "Installed" checkbox. A list of applications installed in the instance is displayed.
3. Locate the Vectra XDR for SIR application and click "Update".
4. The application will be updated in your instance.

Note:

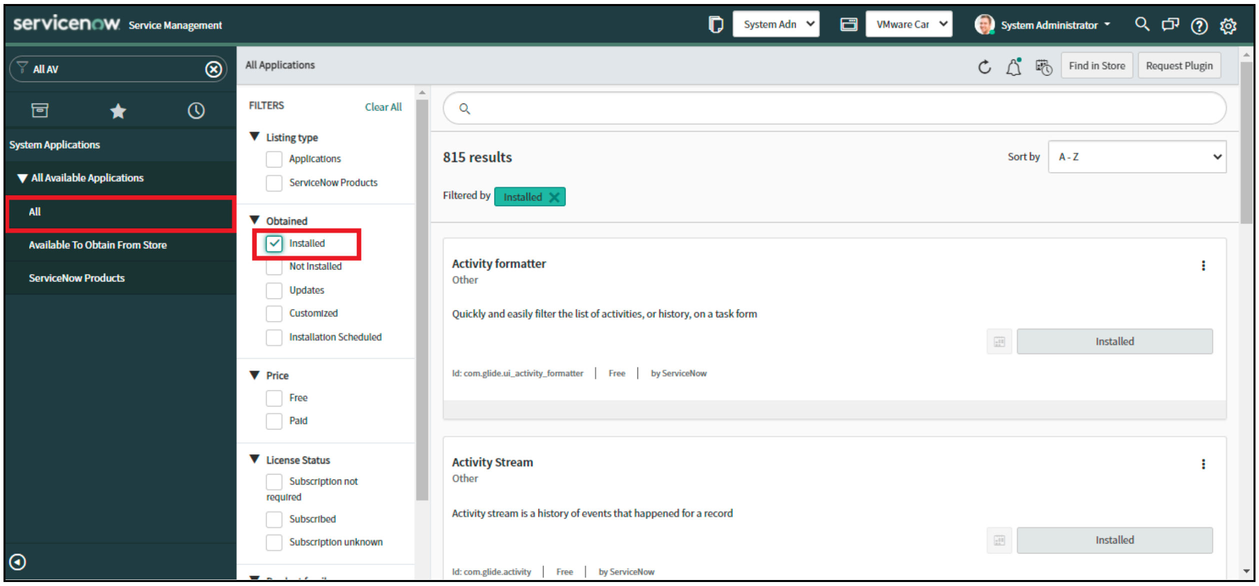
Scheduled Jobs: All scheduled jobs will be reset to their default configurations during the upgrade process. You must review, update, and reconfigure these jobs as needed after completing the update.

4. Uninstallation

This section describes how to uninstall the Vectra XDR for SIR application from a ServiceNow instance.

Role Required: System Administrator

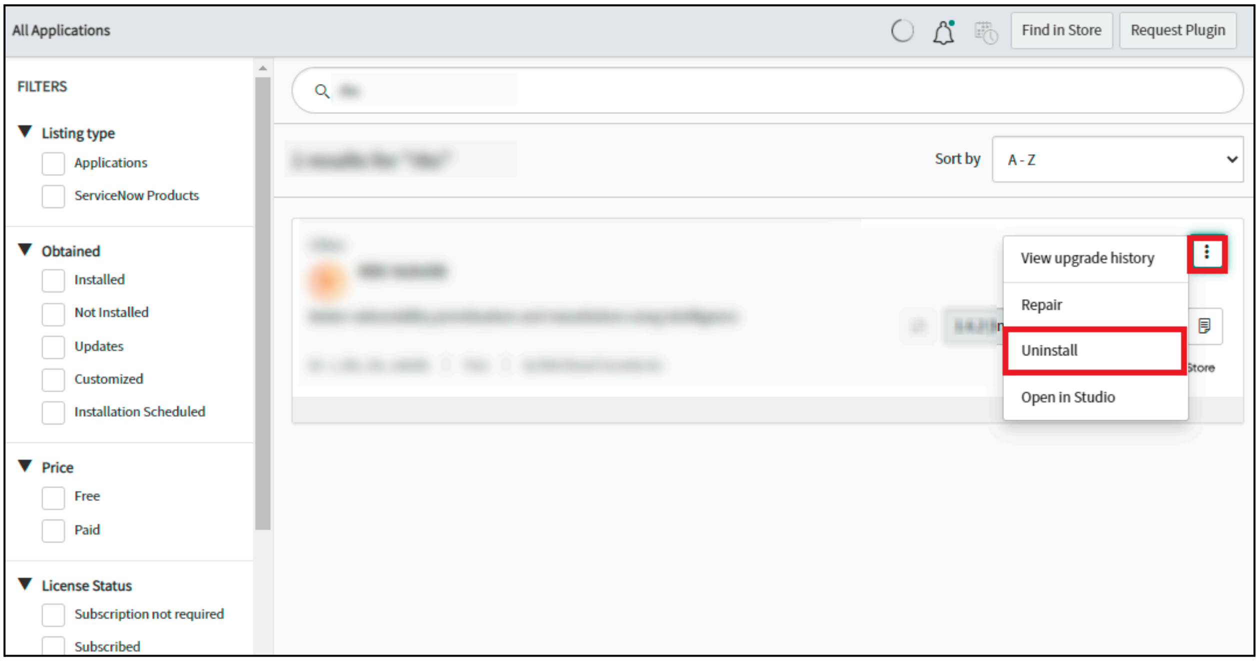
- Navigate to System Applications > All Available Applications > All
- Check the Installed checkbox in the Obtained dropdown.



Quickly and easily filter the list of activities, or history, on a task form

Activity stream is a history of events that happened for a record

- Search for the application in the Search Bar.
- Once you locate the application, click “Uninstall” from the three dots on the right side.



5. Support, Troubleshooting, and Limitations

5.1. Support Contact

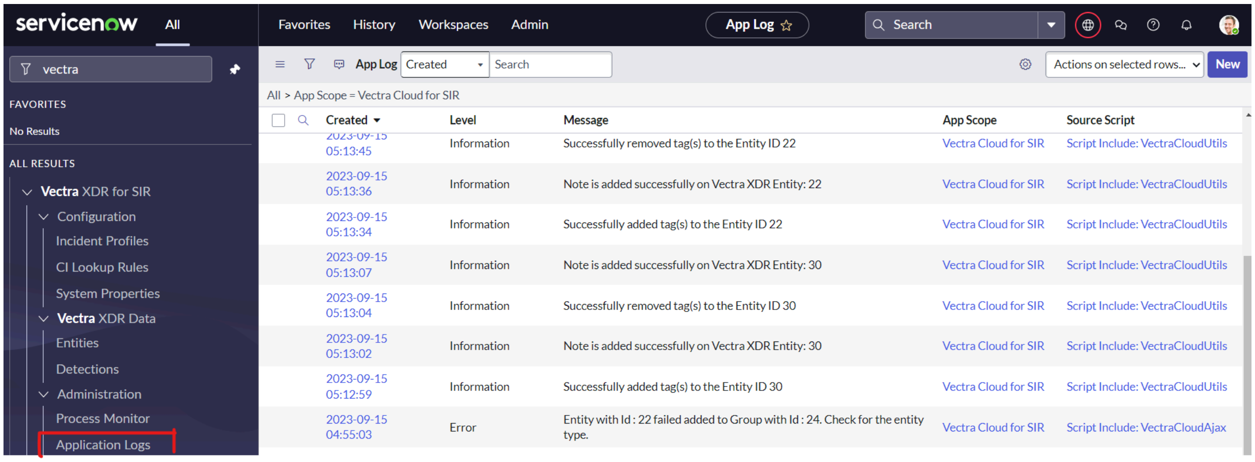
- Any user with “Vectra analyst” privileges can access the Support Contact page for any issues related to “Vectra XDR ServiceNow SecOps”.

5.2. Troubleshooting

5.2.1. Application Logs

Role Required: System Administrator

- If you experience any errors, check the application logs to get information about the error and how to resolve it.
- Navigate to System Logs > System Log > Application Logs or Vectra XDR for SIR > Application Logs



All > App Scope = Vectra Cloud for SIR

Created	Level	Message	App Scope	Source Script
2023-09-15 05:13:45	Information	Successfully removed tag(s) to the Entity ID 22	Vectra Cloud for SIR	Script Include: VectraCloudUtils
2023-09-15 05:13:36	Information	Note is added successfully on Vectra XDR Entity: 22	Vectra Cloud for SIR	Script Include: VectraCloudUtils
2023-09-15 05:13:34	Information	Successfully added tag(s) to the Entity ID 22	Vectra Cloud for SIR	Script Include: VectraCloudUtils
2023-09-15 05:13:07	Information	Note is added successfully on Vectra XDR Entity: 30	Vectra Cloud for SIR	Script Include: VectraCloudUtils
2023-09-15 05:13:04	Information	Successfully removed tag(s) to the Entity ID 30	Vectra Cloud for SIR	Script Include: VectraCloudUtils
2023-09-15 05:13:02	Information	Note is added successfully on Vectra XDR Entity: 30	Vectra Cloud for SIR	Script Include: VectraCloudUtils
2023-09-15 05:12:59	Information	Successfully added tag(s) to the Entity ID 30	Vectra Cloud for SIR	Script Include: VectraCloudUtils
2023-09-15 04:55:03	Error	Entity with Id : 22 failed added to Group with Id : 24. Check for the entity type.	Vectra Cloud for SIR	Script Include: VectraCloudAjax

5.2.2. Unable to create a new user

Problem Statement: Unable to create a new user in the ServiceNow instance.

- Review the following link and execute the steps.

  https://docs.servicenow.com/bundle/rome-platform-administration/page/administer/users-and-groups/task/t_CreateAUser.html

5.2.3. **Problem Statement:** CIs are not getting linked to the Security Incident.

Solution: The CMDB table should have a configuration item that exists before running the job in ServiceNow to fetch entities and detections from the Vectra platform. If there are no CIs that exist in the CMDB table that is selected in the CI Lookup rule to look up then the Incident will not have any Configuration Items linked to it.

5.2.4. **Problem statement:** Integration Profile is Inactive and try performing the actions

Solution : If the Incident Profile associated with Entity is inactive then a proper error message should be displayed in the pop-up frame of the current window.

5.2.5. **Problem Statement :**State of Job got stuck in state "New" OR "Running" for a long time.

Solution : If the job is running and the state got stuck e.g "Running " state then after 24 hrs it will auto go in "Failed" state.

5.2.6. Unable to install/activate the plugin in ServiceNow instance

Problem Statement: Unable to install/activate the plugin in ServiceNow instance.

- Review the following link and execute the steps.

  https://docs.servicenow.com/bundle/rome-platform-administration/page/administer/plugins/task/t_ActivateAPlugin.html

5.2.7. Automatic Security Incident is not Created

Problem Statement: Incident Creation Criteria are set to escalate certain entities to Security Incidents, but the Security Incident is not created according to the criteria.

- Open the Configuration profile.
- Go to the Incident Creation tab.
- Check the value of the Condition, it should be correct if not then change its value to the correct one.
- Save the Configuration and start the Data Collection.
- Check whether the Security Incidents are created or not.

5.2.8. Out-of-Sync data between Vectra and ServiceNow results in incorrect UI behavior

Problem Statement : This issue can occur when there is a data synchronization issue or mismatch between the Vectra platform and ServiceNow. Specifically, if changes are made directly in Vectra but those changes are not yet reflected in ServiceNow.

Solution :

To resolve data inconsistency between Vectra & ServiceNow use the following UI actions, these actions manually sync the entity & detections from Vectra to ServiceNow.

1. **Describe Entity**
2. **Describe Detection**
3. **List Detections**

Example Scenario:

1. An entity with 5 active detections is ingested into ServiceNow.
2. One detection is manually closed in Vectra, but this change has not yet been synced with ServiceNow.
3. The user clicks **Close Entity** in ServiceNow. As per API implementation it closes the remaining 4 detections in Vectra.
4. These 4 detection closures are successfully reflected in ServiceNow through the workflow.
5. Vectra now marks the entity as inactive, since all active detections were closed.

6. However, ServiceNow still shows 1 active detection (the one closed manually in Vectra earlier), because this closure was not yet synced.
7. On the next ingestion cycle, the entity is not ingested again from Vectra (since it is now inactive), so the remaining detection in ServiceNow is never updated, causing it to remain open, and the related entity also stays active.
8. This causes the **Close Entity** UI action to remain visible, even though the entity is already inactive in Vectra.

To resolve this inconsistency, users can manually sync the affected entity and its detections using the following UI actions:

- Describe Entity
- List Detections

Once these actions are triggered:

- The latest detection statuses are fetched directly from Vectra.
- Any closed detections not previously synced will be updated in ServiceNow.
- If no active detections remain, the entity will be correctly marked as inactive.
- This will ensure the Close Entity UI action is hidden as expected.

5.2.9. New notes added in Vectra are not reflected in existing ServiceNow Security incidents

Problem Statement : The integration is designed to add notes to a ServiceNow Security incident only when the related entity is first ingested as new. This means:

- When an entity is initially created in ServiceNow, all its notes (up to the latest 10 - because the API used to fetch entities from Vectra returns only the 10 latest notes per entity.) from Vectra are added to the Security incident.
- However, if new notes are added later in Vectra to an existing entity, these notes will not be added to the corresponding Security incident in ServiceNow during subsequent ingestion cycles.
- This behavior occurs because the integration only adds notes during the initial creation of the entity record in ServiceNow, not on updates.