

VECTRA XDR FOR ITSM - USER GUIDE

Vectra XDR for ITSM- (2.0.0)

Table of Contents

1. Overview	5
Architectural Diagram	6
1.1. Application Features	6
1.2. Compatibility Matrix	7
2. Vectra XDR for ITSM Integration	7
2.1.1. Installation	7
2.1.2. Application Download and Installation	7
2.1.2.1. Configure Application scope	8
2.1.2.2. Scheduled Jobs Activation	8
2.1.3. Permissions and Roles	9
System administrator	9
Vectra Admin (x_cdsp_vectra_c_it.vectra_admin+personalize_dictionary + itil)	9
Vectra Analyst (x_cdsp_vectra_c_it.vectra_user+Personalize dictionary + itil (to view the Incident))	10
2.1.4. Create Users	10
2.2. Configurations	15
2.2.1. Authentication Configuration	15
2.2.2. CI Lookup Rule	16
2.2.3. Incident Profiles	17
2.2.3.2. Incident Creation	18
2.2.3.3. Field Mapping	20
2.2.3.4. Scheduling	21
2.3. Use Cases	22

2.3.1. MSP Support	22
2.3.2. Entity and Detection Ingestion	25
2.3.3. Automatic Incident Creation	26
2.3.4. SOAR Actions	26
2.3.4.1. Manual Incident Creation	27
2.3.4.2. Create Assignment	28
2.3.4.3. Close Incident in ServiceNow	29
2.3.4.4. Download PCAP	30
2.3.4.5. Mark all detections as fixed for an entity	31
2.3.4.6. Mark/Unmark Detection as fixed	32
2.3.4.7. Describe Entity	33
2.3.4.8. Describe Detection	34
2.3.4.9. List Detection	34
2.3.4.10. Add to Group	35
2.3.4.11. Close detection	36
2.3.4.12. Re-open detection	37
2.3.4.13. Close Multiple Detections	38
2.3.4.14. Re-open Multiple Detections	39
2.3.4.15. Close Entity	40
2.3.5. Process Monitor	42
3. Upgradation	43
4. Uninstallation	43
5. Support, Troubleshooting, and Limitations	45
5.1. Support Contact	45
5.2. Troubleshooting	45
5.2.1. Application Logs	45
5.2.2. Unable to create a new user	45
5.2.5. Automatic Incident is not Created	46
5.2.7. Out-of-Sync data between Vectra and ServiceNow results in incorrect UI behavior	46
5.2.8. New notes added in Vectra are not reflected in existing ServiceNow Security incidents	47

1. Overview

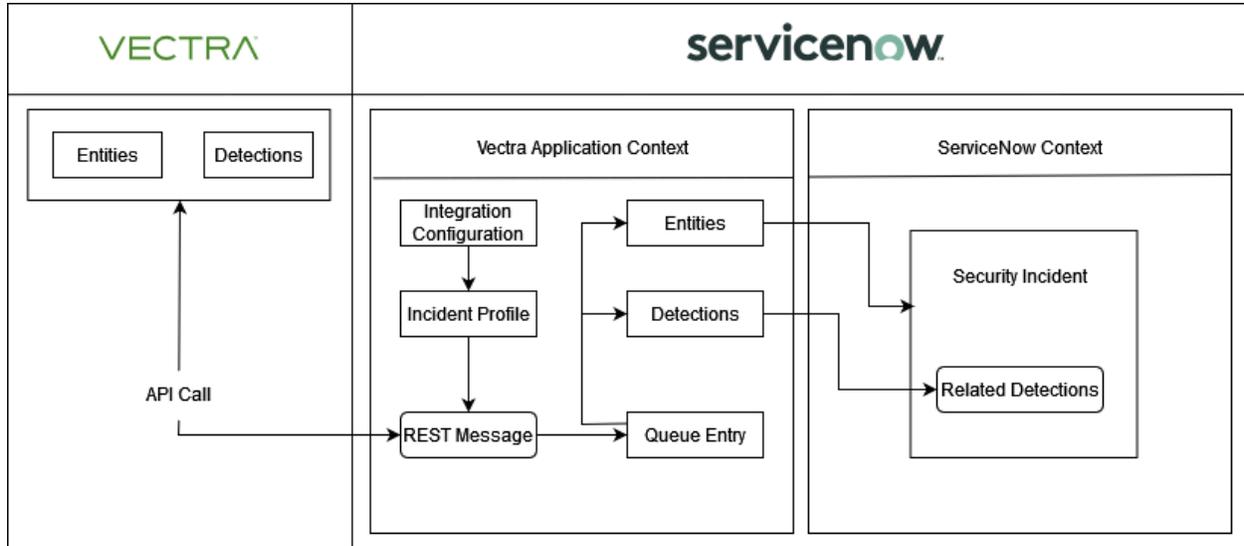
The Vectra threat detection & response platform captures packets and logs across your public cloud, SaaS, federated identity, and data center networks. It applies patented security-led AI to the surface, prioritizes threats, and integrates into your security stack for rapid response.

Vectra ServiceNow Application

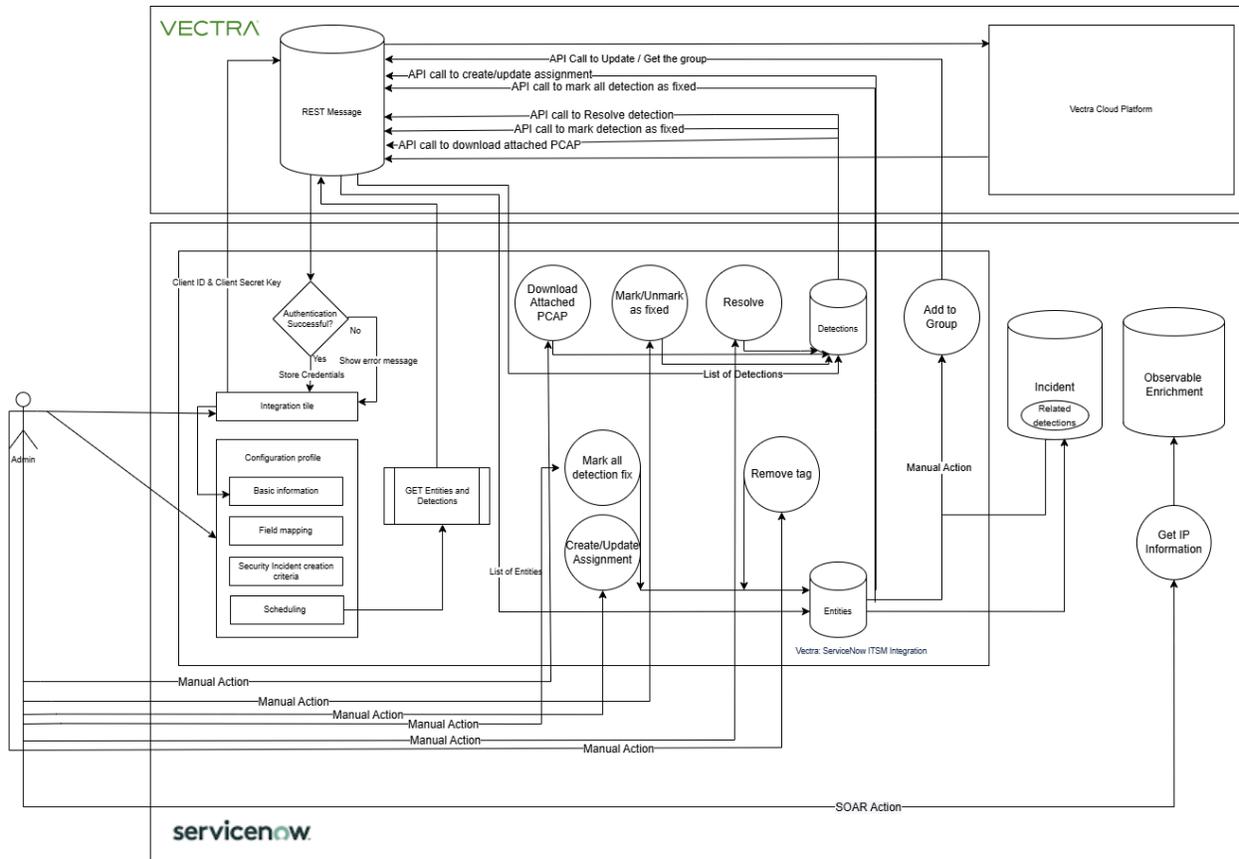
This application fetches Entities and Detections from the Vectra Detect based on the provided API filters and ingests data into the ServiceNow platform. It provides the capability of creating “ Incidents” based on the defined condition/criteria. It also provides support to perform some manual actions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

System Architecture

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 Incident creation criteria and create Incidents based on them.
- Set the CI Lookup Rules.
- Ability to map Entity fields with ServiceNow Incident fields.
- 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 resolve the detection.
- Ability Add/Update Assignment to Entity on Vectra Detect.
- 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 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:

- 3.4
- SOAR Actions: All APIs have current version 3.4 as of May. 27.

2. Vectra XDR for ITSM Integration

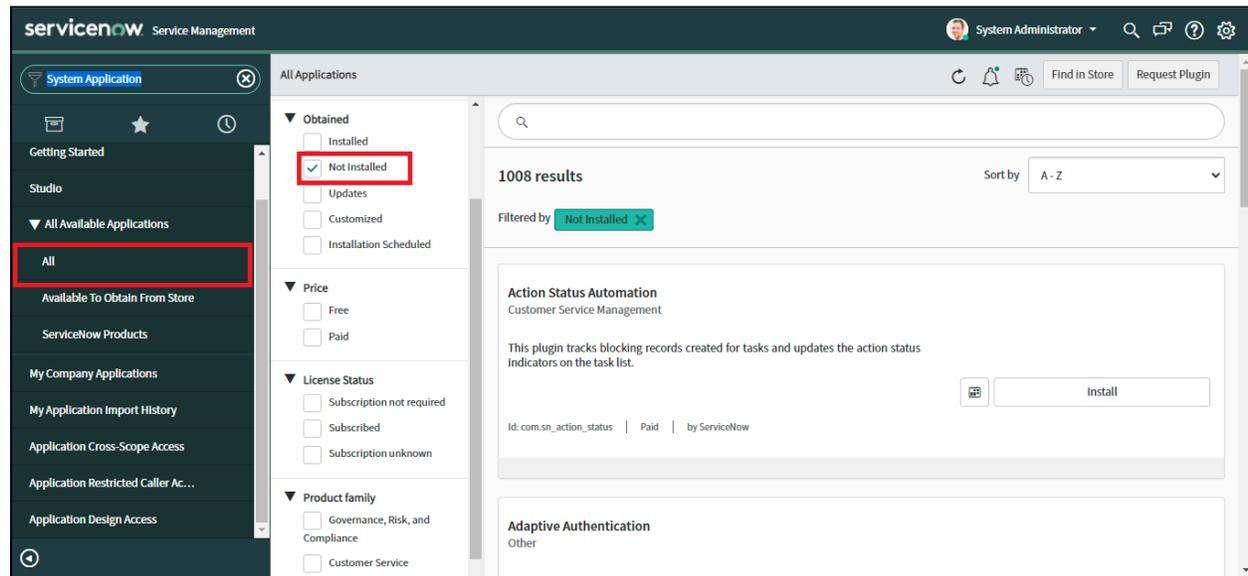
2.1.1. Installation

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

2.1.2. Application Download and Installation

- Download the Vectra XDR for ITSM Integration app from the ServiceNow app store on the ServiceNow instance and enter your user credentials.

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

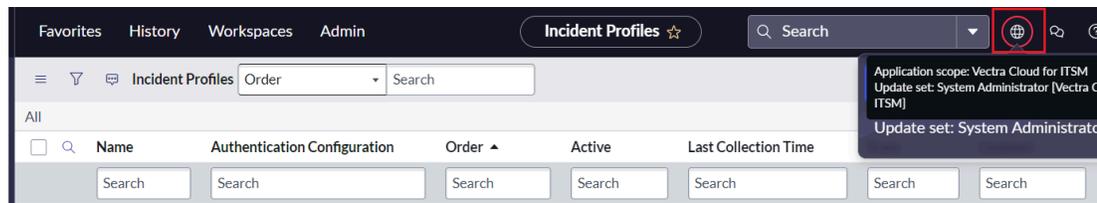


- Click on the “Not Installed tab”. A list of applications available for installation will be displayed.
- Locate the Vectra XDR for ITSM Integration app, select it, and click “Install”.
- The application will be installed on your instance.

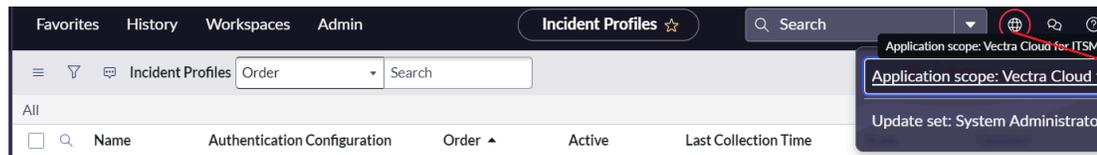
2.1.2.1. Configure Application scope

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

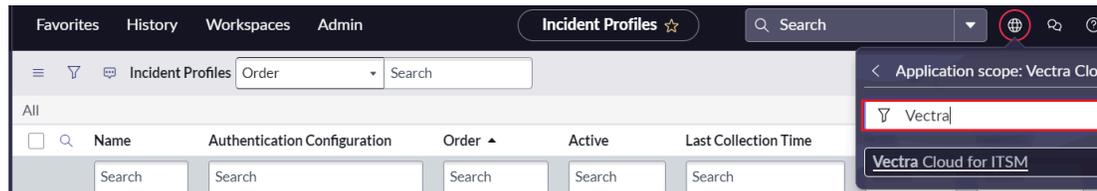
- Click on the “Application Scope” i



- Click on the arrow.



- Enter application name to search application scope.



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

2.1.1.2.2. Scheduled Jobs Activation

Required roles: System administrator

The 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 ITSM -> Configuration -> Scheduled Jobs
- activate all the scheduled jobs listed here

Name	Active	Class	Updated
Entity Scheduler	false	Incident Scheduler	2025-05-21 23:53:31
Vectra Cloud Profile Invocation	false	Scheduled Script Execution	2025-05-21 23:53:31
Vectra Cloud Scheduled Data Import Queue Processor	false	Scheduled Script Execution	2025-05-21 23:53:31
Vectra Detections Scheduled Data Import 01	false	Scheduled Data Import	2024-04-04 05:21:50
Vectra Detections Scheduled Data Import 02	false	Scheduled Data Import	2024-04-04 05:21:44
Vectra Entity Scheduled Data Import 01	false	Scheduled Data Import	2024-04-04 05:21:39
Vectra Invalidate Process Monitor Job	false	Scheduled Script Execution	2025-05-21 23:53:31

2.1.1.3. Permissions and Roles

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

Role	Contains role	Permissions
System administrator	NA	<ul style="list-style-type: none"> • 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
	<ul style="list-style-type: none"> • x_cdsp_vectra_c_it.vectra_admin • x_cdsp_vectra_c_it.vectra_user 	<ul style="list-style-type: none"> • Can Install the application • Can configure the Authentication Configuration. • Can create Incident

<p>Vectra Admin (x_cdsp_vectra_c_it.vectra_admin+personalize_dictionary + itil)</p>		<p>Profile</p> <ul style="list-style-type: none"> • Can access Contact Support • Can access Log module • Can access Process monitor • Can run the SOAR actions
<p>Vectra Analyst (x_cdsp_vectra_c_it.vectra_user+Personalize dictionary + itil (to view the Incident))</p>	<ul style="list-style-type: none"> • x_cdsp_vectra_c_it.vectra_user • export_set_scheduler 	<ul style="list-style-type: none"> • Accessing the Application. • Read access to the Incident Profile module. • Can run the SOAR actions. • Process Monitor (Read Only) • Read Access to the Detections and Entities tables (Only Deeplink navigation access) • Can access Support Contact.
<p>MSP Admin</p>	<ul style="list-style-type: none"> • x_cdsp_vectra_c_it.vectra_admin • personalize_dictionary • itil • x_cdsp_vectra_c_it.msp_admin 	<p>Accessing tables</p> <ul style="list-style-type: none"> • Scheduled Data Import Pool • Data Source Pool • Entites Staging • Detection Staging

2.1.4. Create Users : Non - MSP

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

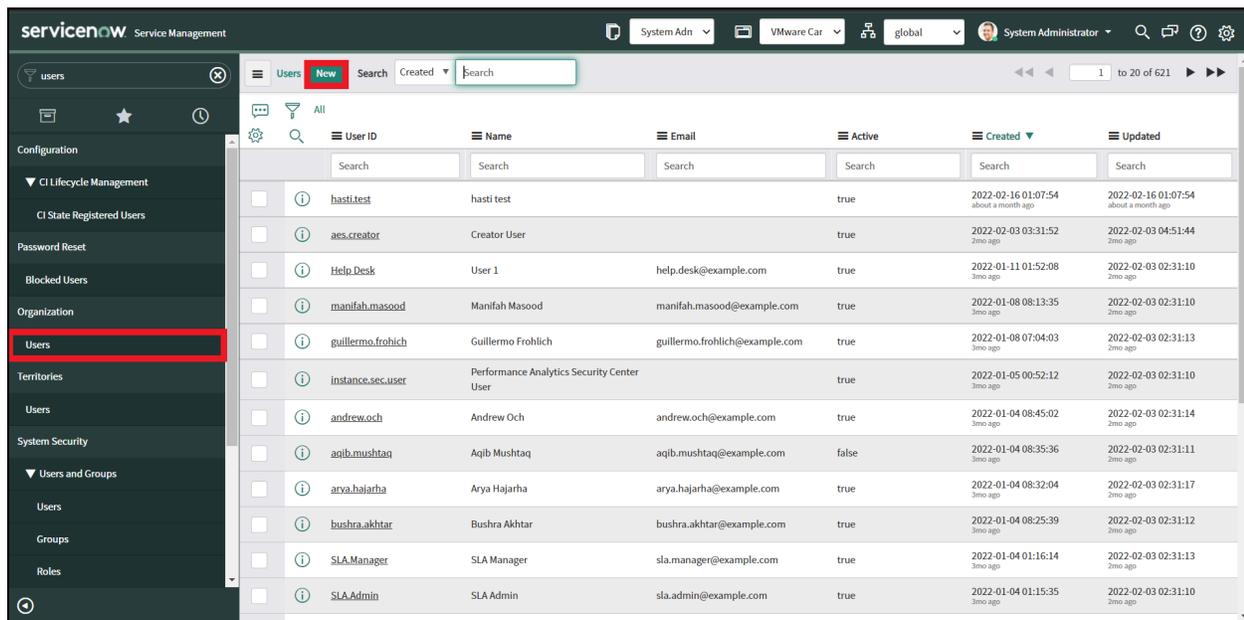
Username (for example)	Role to be assigned
Security Admin	x_cdsp_vectra_c_it.vectra_admin personalize_dictionary itil
Security Analyst	x_cdsp_vectra_c_it.vectra_user personalize_dictionary

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

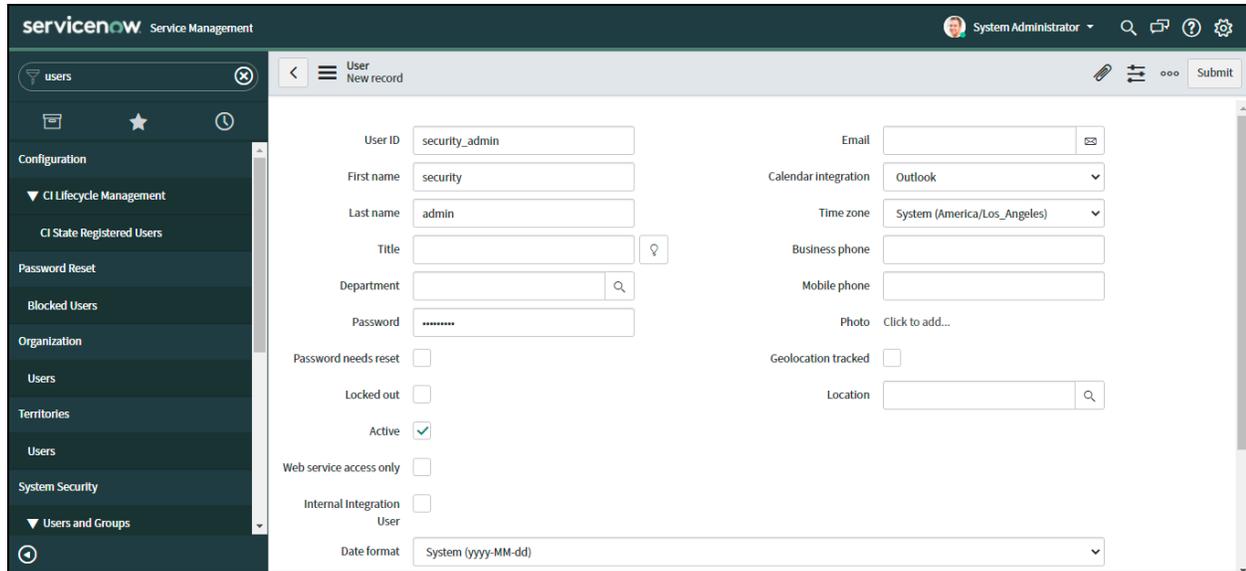
Role Required: [System Administrator](#)

Procedure:

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



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

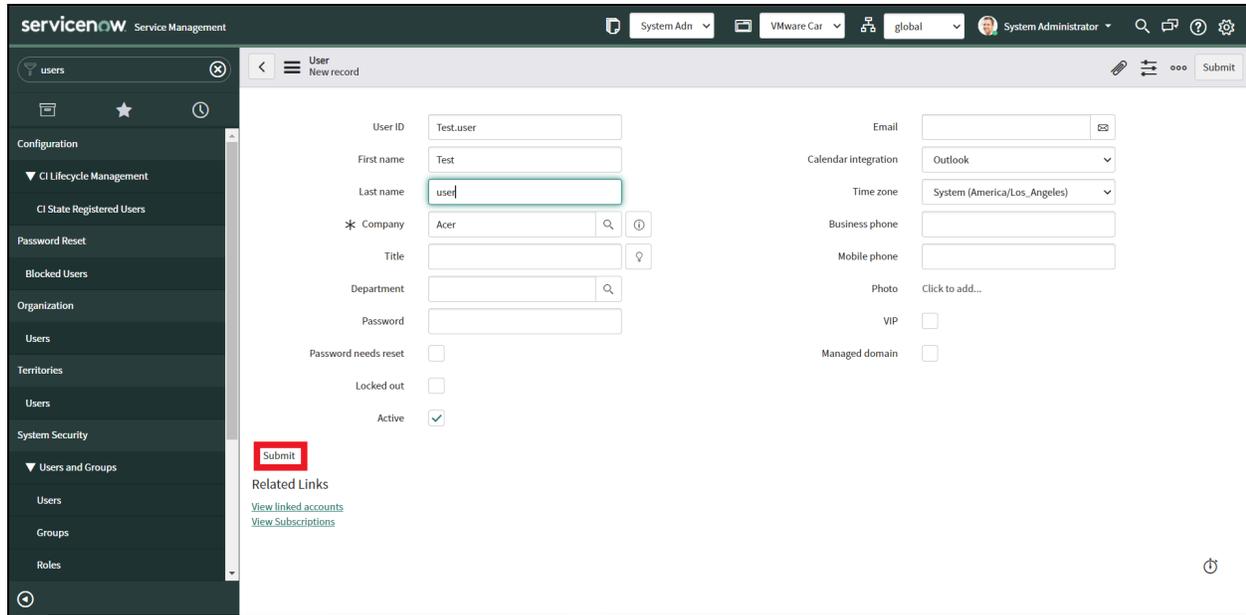


- Fill in the form.

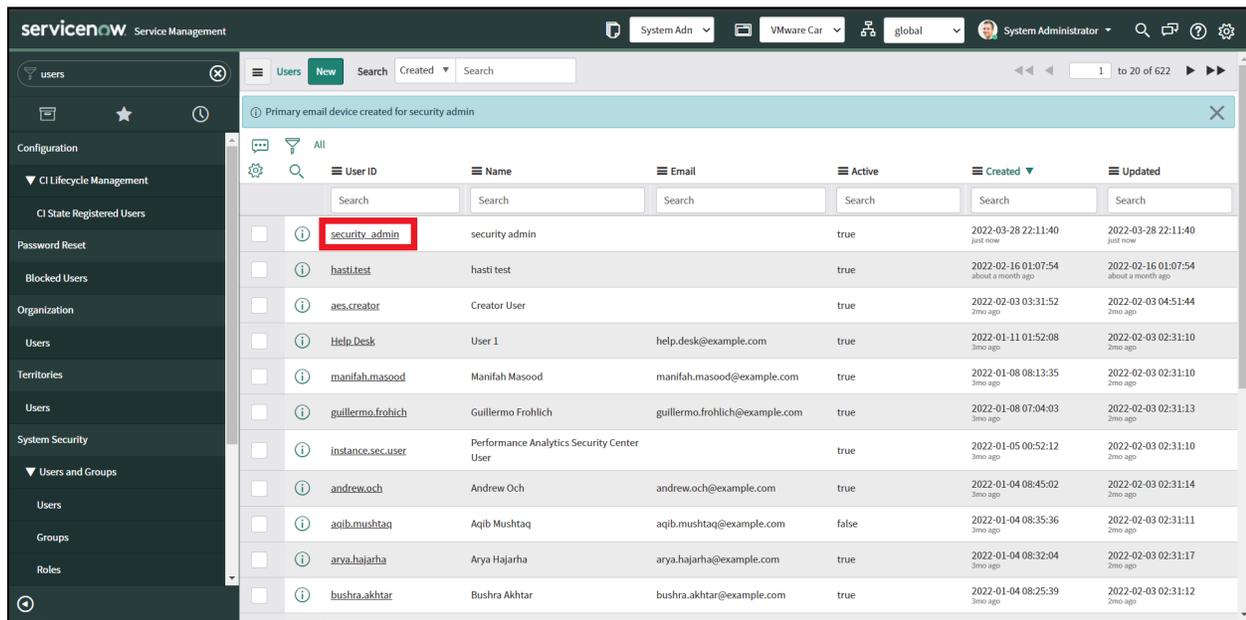
Note: Example values for the User ID title and email address are shown in the table below.

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

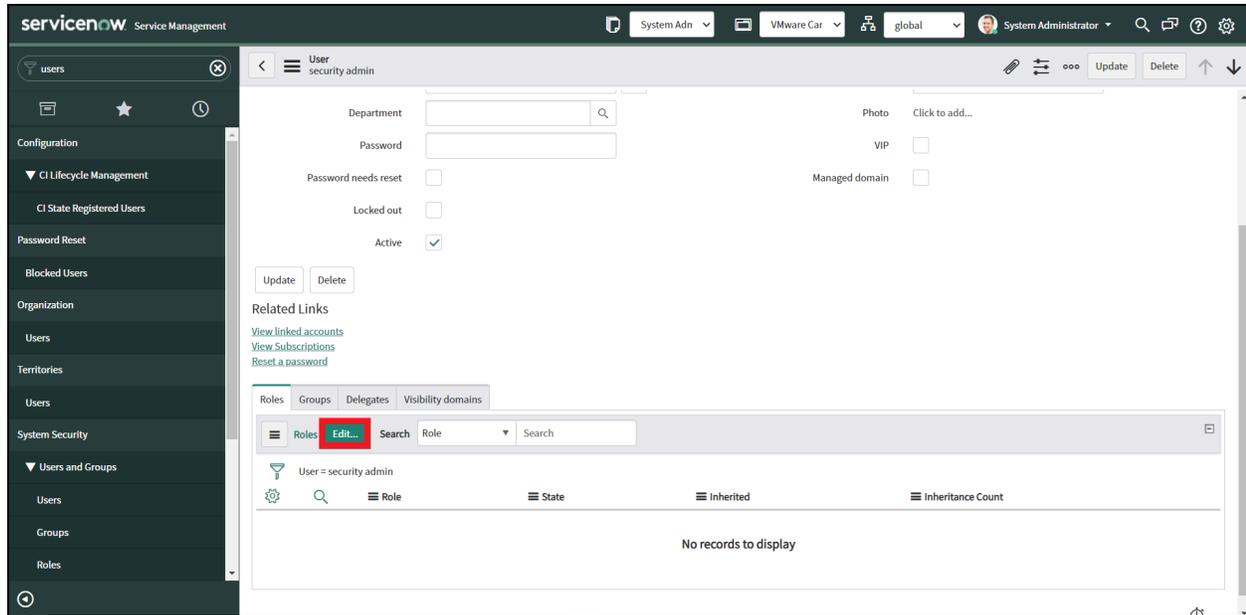
- Click “Submit.” Once submitted, you can assign the role.



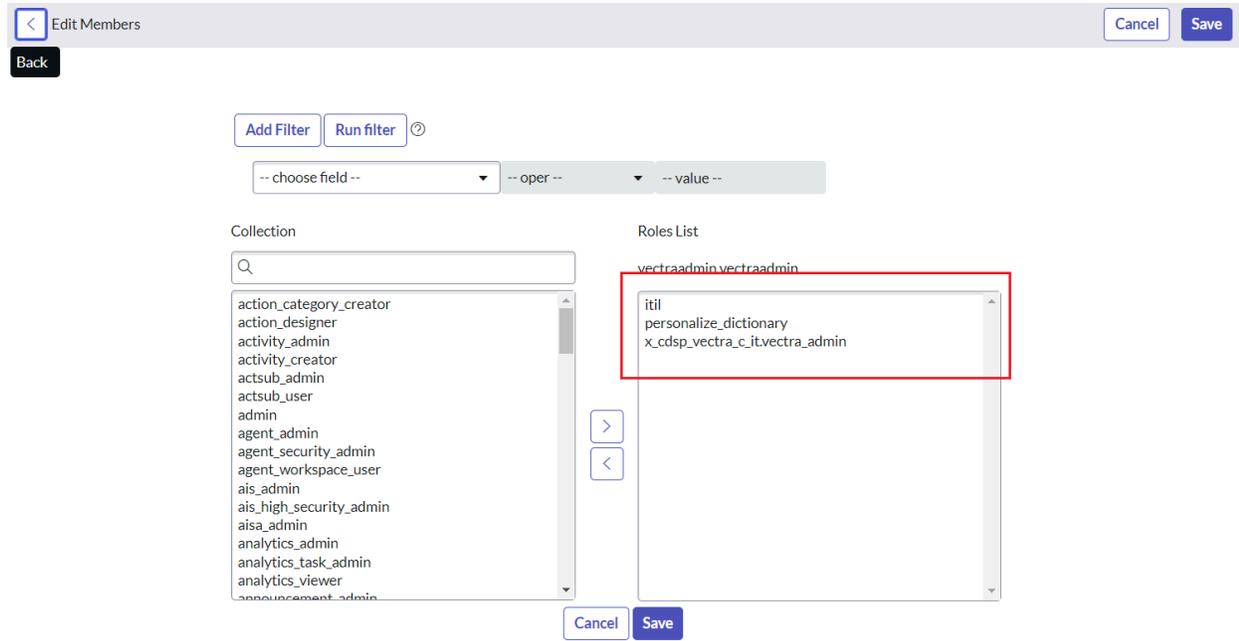
- Click the name of the new user you created.



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



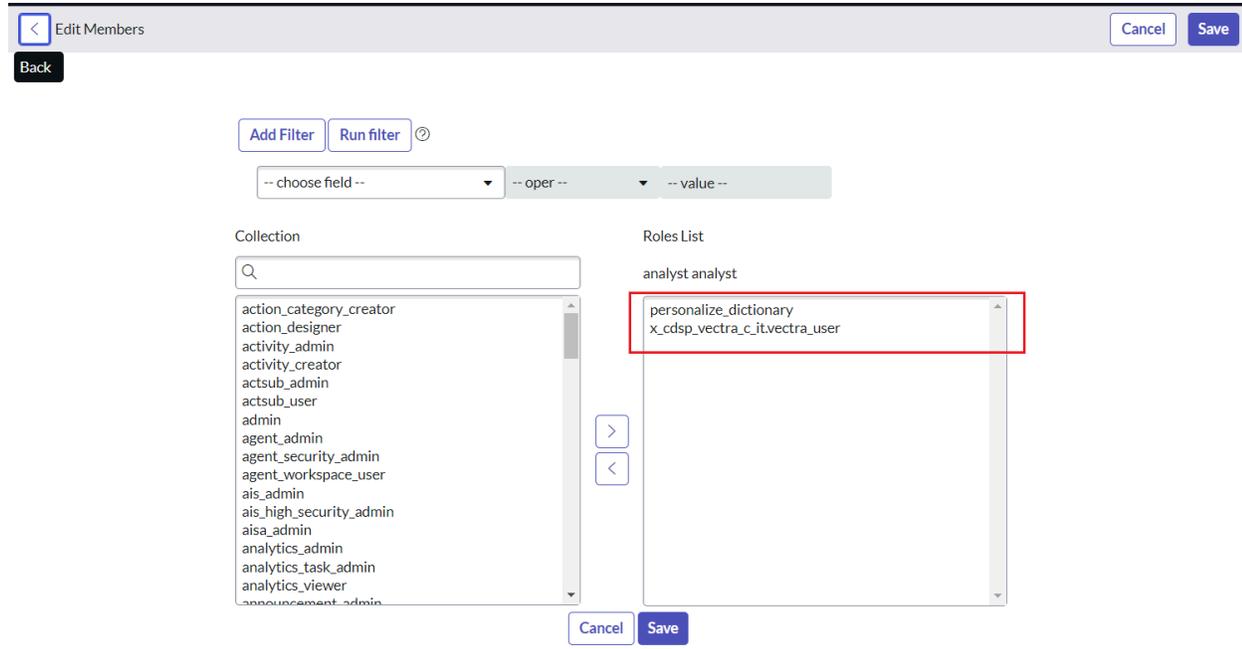
- When the Edit Members form displays, enter `x_cdsp_vectra_c_it.vectra_admin` in the Collection field.
- In the Collection column, select `x_cdsp_vectra_c_it.vectra_admin` and move to the Roles list.
- Click the Save button.
- Scroll down and open the role: “`x_cdsp_vectra_c_it.vectra_admin`”
- Scroll 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.



- When the Edit Members form displays, enter sn_si.admin and export_set_scheduler in the Collection field.
- In the Collection column, select x_cdsp_vectra_c_it.vectra_admin and move 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. x_cdsp_vectra_c_it.vectra_user.



2.1.1.5. Create Users: MSP

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

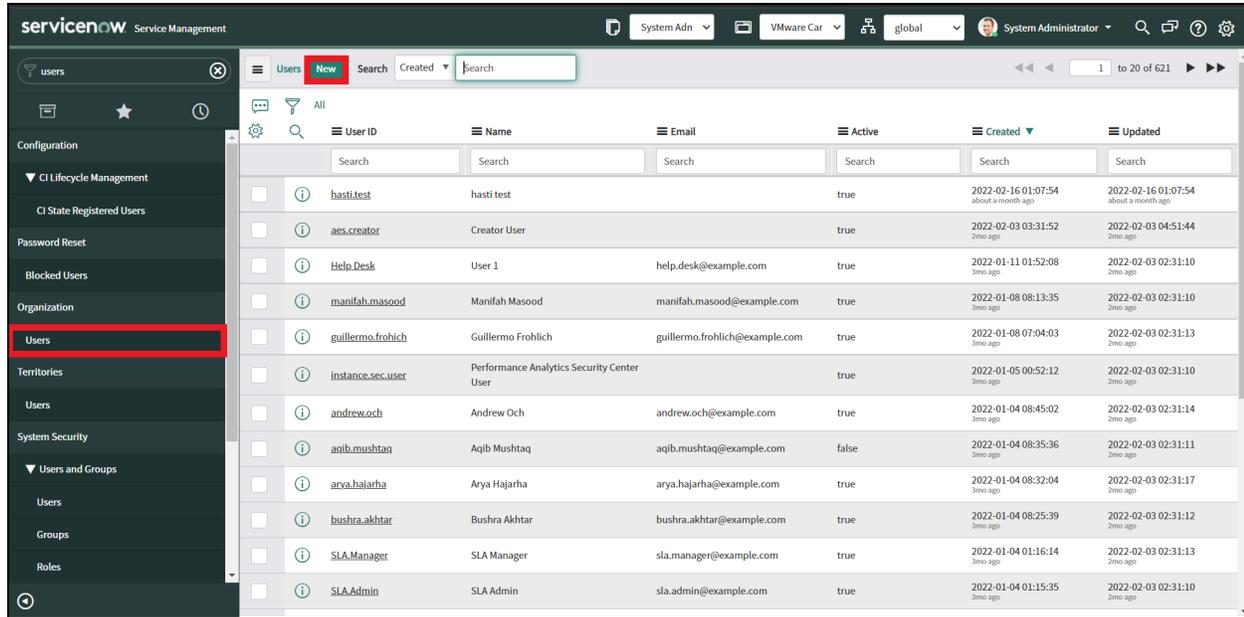
Username (for example)	Role to be assigned
Security Admin	x_cdsp_vectra_c_it.vectra_admin personalize_dictionary itil
Security Analyst	x_cdsp_vectra_c_it.vectra_user personalize_dictionary
MSP Admin	x_cdsp_vectra_c_it.vectra_admin personalize_dictionary itil x_cdsp_vectra_c_it.msp_admin

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

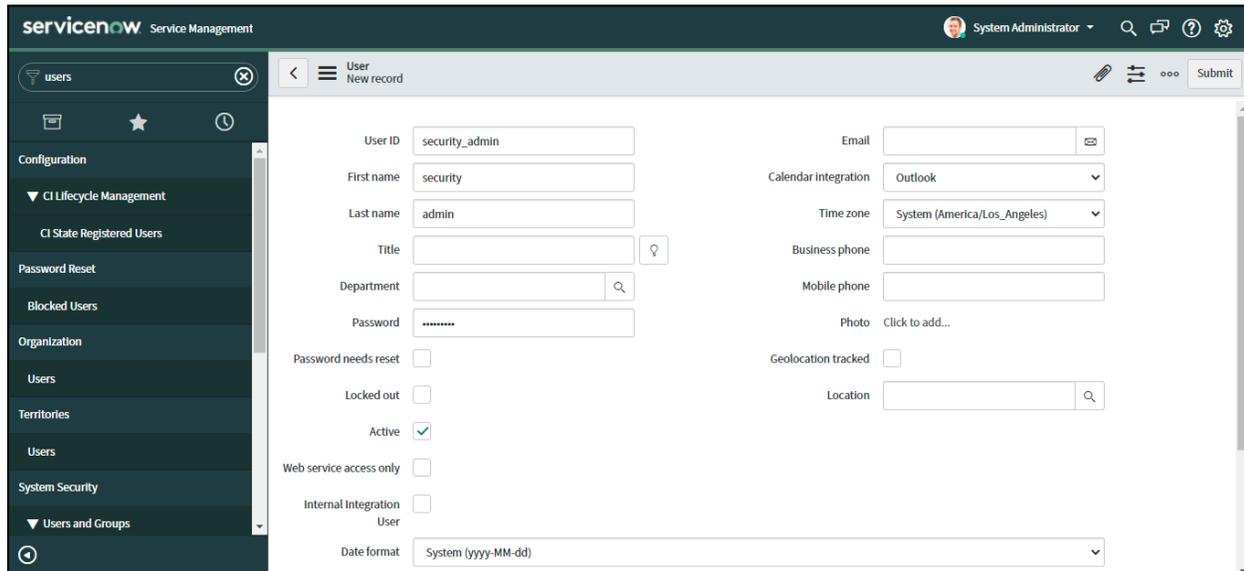
Role Required: [System Administrator](#)

Procedure:

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



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

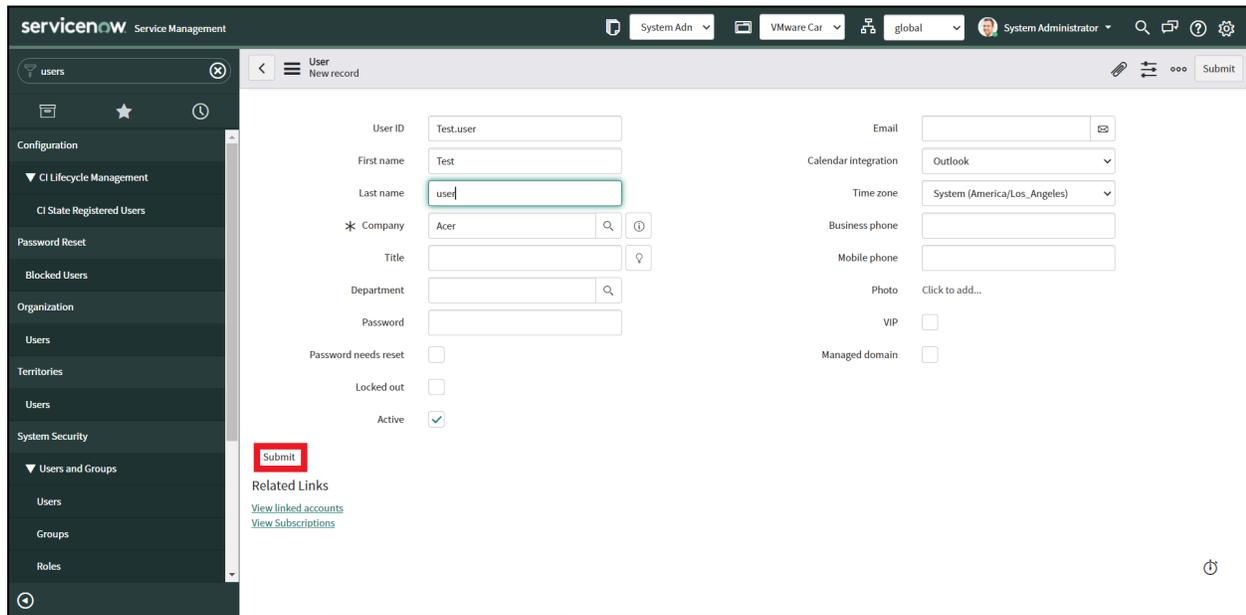


- Fill in the form.

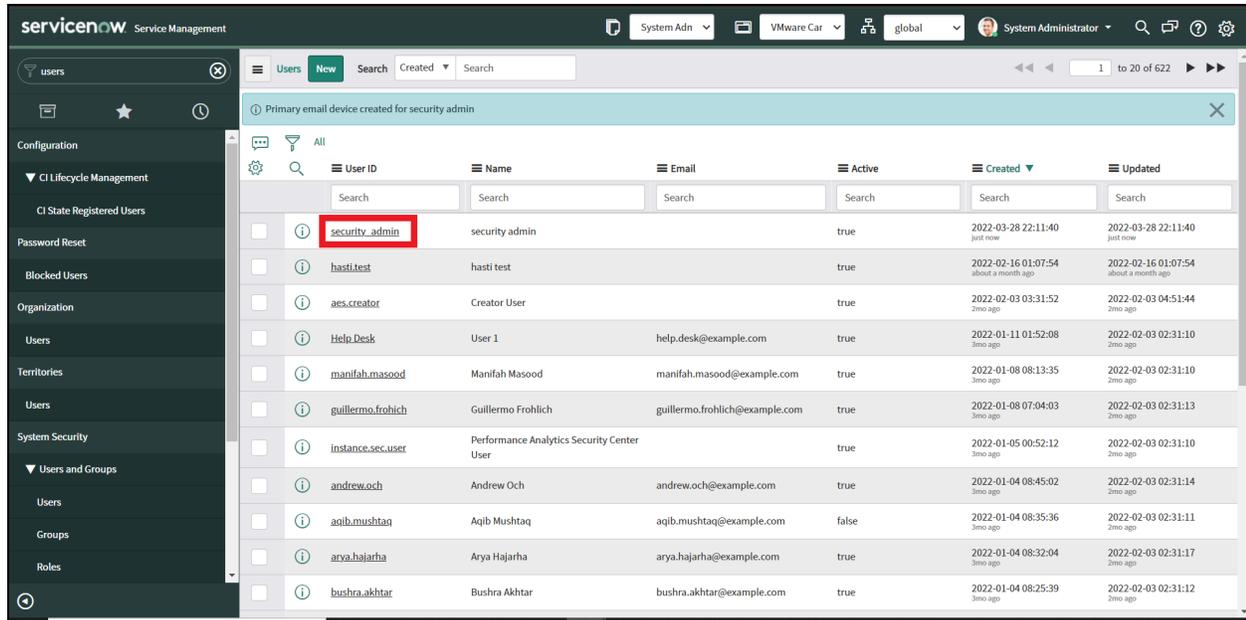
Note: Example values for the User ID title and email address are shown in the table below.

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

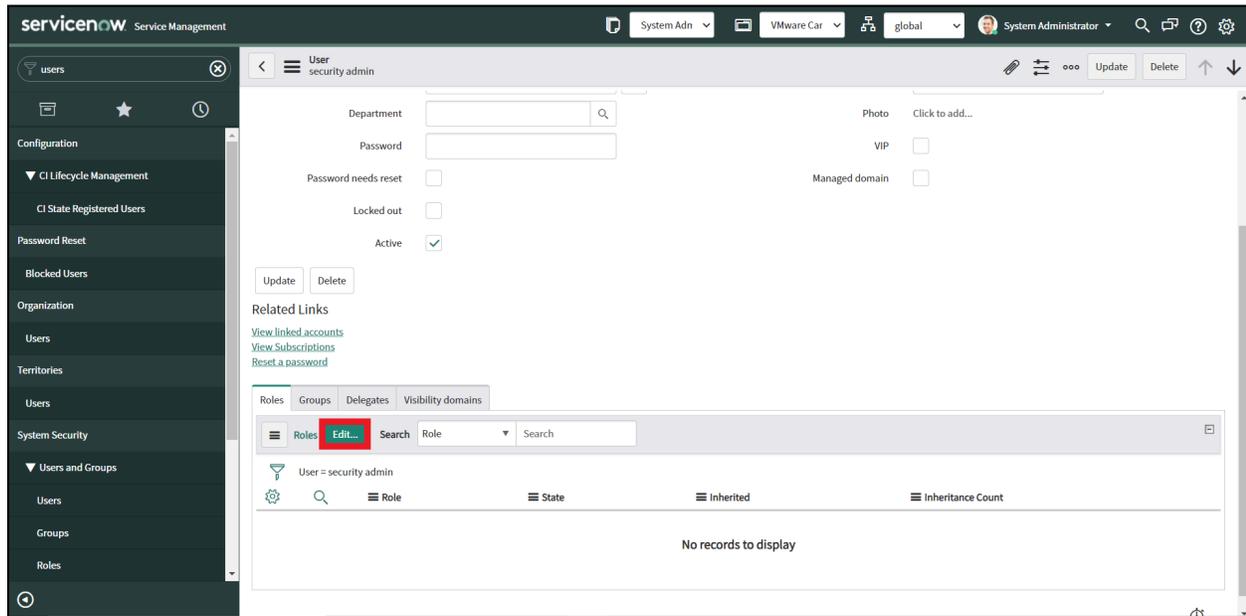
- Click "Submit." Once submitted, you can assign the role.



- Click the name of the new user you created.

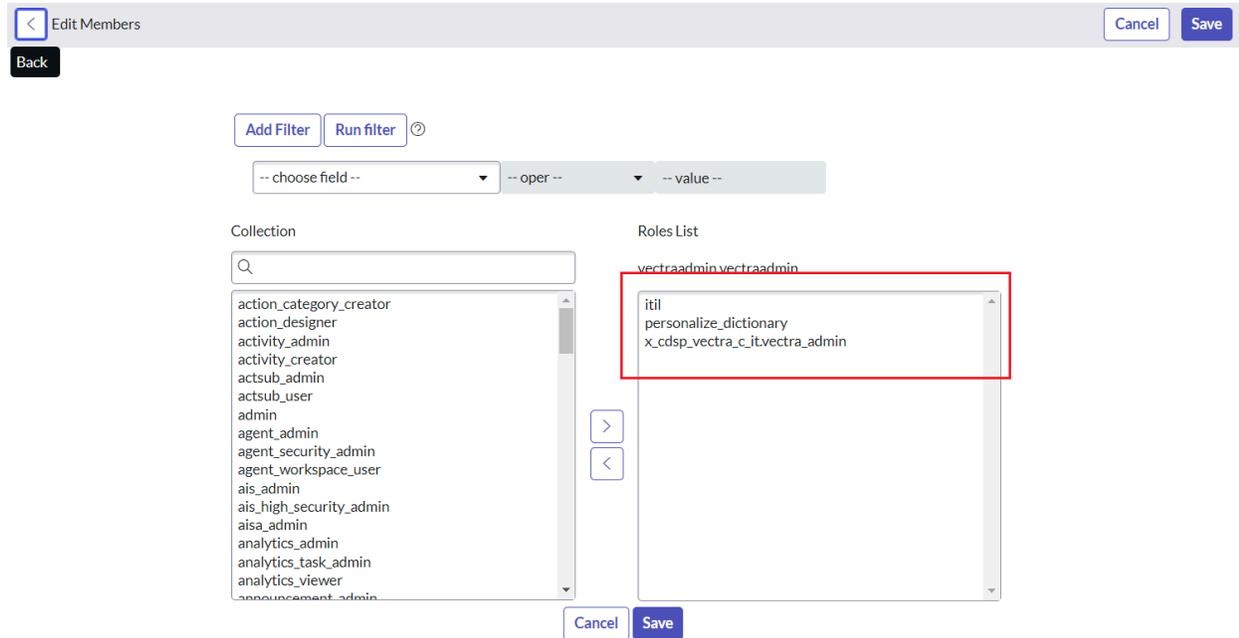


- Once the record is open, scroll down and go to the Roles section, and click "Edit".



- When the Edit Members form displays, enter `x_cdsp_vectra_c_it.vectra_admin` in the Collection field.
- In the Collection column, select `x_cdsp_vectra_c_it.vectra_admin` and move to the Roles list.
- Click the Save button.
- Scroll down and open the role: " `x_cdsp_vectra_c_it.vectra_admin`"

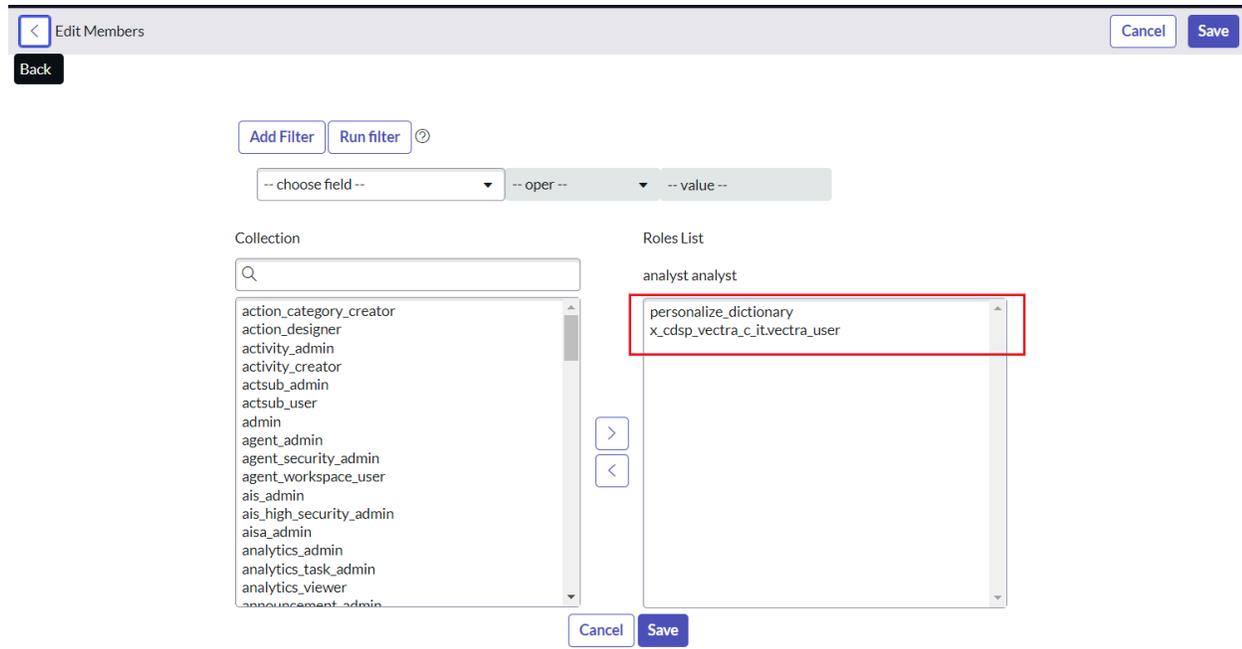
- Scroll down and click on the “Edit” button.
- Search the roles to be added.
- Select the roles and move it to “Contains Roles List” by either double-clicking on the role or clicking on the right arrow.



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

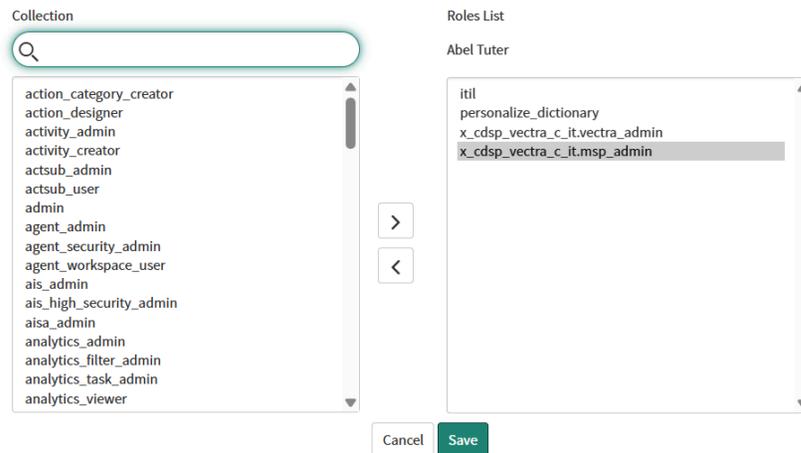
2. Create Analyst User

- All of the steps for creating admin users are applicable for analyst users also, but you must add roles specific to analyst i.e. x_cdsp_vectra_c_it.vectra_user.



3. 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_it.msp_admin.



2.2. Configurations

2.2.1. Authentication Configuration

Required roles: Application admin OR System administrator

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

- Users should be able to see the ServiceNow Incident Response Integration with Vectra SAAS Authentication Configuration by navigating to
 - All
 - Vectra XDR for ITSM
 - Authentication Configurations.

Open the Vectra Cloud for Authentication Configurations 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.

The screenshot shows the 'Authentication Configuration' form for a record named 'Auth-2'. At the top, there are 'Update' and 'Delete' buttons. Below is a blue informational box with the following text: 'This authentication configuration record is used to connect to the Vectra XDR platform'. It lists four fields: Name, Vectra XDR URL, Client ID, and Client Secret Key, each with a brief description. A note specifies the format for the Vectra XDR URL: 'https://00000000000.xyz.portal.vectra.ai'. The form fields are:

- Name: 'Auth-2' (highlighted with an asterisk)
- Vectra XDR URL: 'https://308714519558.cc1.portal.vectra.ai' (highlighted with an asterisk and has a lock icon)
- Client ID: (empty, highlighted with an asterisk)
- Client Secret Key: (masked with dots, highlighted with an asterisk)

 At the bottom of the form, there are 'Update' and 'Delete' buttons.

- ❖ Client Secret Key: Password type field where the user will enter a Client secret key.
- ❖ All the fields are mandatory and are highlighted with an asterisk.

2.2.2. CI Lookup Rule

Based on the configured CI Lookup rules, it will attach the CI records that exist in the CMDB and link with the Incident.

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

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

Vectra Cloud CI Lookup Rule Rule-1

- Name:** The name of the rule
- Order:** The order in which this rule should be evaluated relative to other rules
- Lookup method:** The method used for matching which is either a custom script or selecting a table and field in the CMDB
- Active:** The flag that indicates whether the rule is active or disabled
- Source field:** The specific source field from Vectra Cloud Finding data that is being used as input to this rule

* Name: * Order:

Lookup Method: Active:

Define the source field from Vectra Cloud Finding data for the lookup rule

* Source Field:

Description:

For Field matching rules, specify the table and field to search within the CMDB. 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 Table: * Search On Field:

- 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.

Vectra XDR CI Lookup Rule Intitech

- Active:** The flag that indicates whether the rule is active or disabled
- Source field:** The specific source field from Vectra XDR Finding data that is being used as input to this rule

* Name: * Order:

Lookup Method: Active:

Define the source field from Vectra XDR Finding data for the lookup rule

* Source Field:

Description:

For Field matching rules, specify the table and field to search within the CMDB. 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

```

17 var gr = new GlideRecord("cmdb_ci_hardware");
18 gr.addQuery("name", sourceValue);
19 gr.addQuery("sys_domain", "c94122494a362312007f2ce5bd78768f");
20 // OR gr.addQuery("sys_domain", rule.sys_domain);
21 gr.query();
22 if (gr.next()) {
23     return gr.getValue("sys_id");
24 }
25 return null;
26 })(rule, sourceValue, sourcePayload);
    
```

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 like when a Vectra entity should generate ServiceNow Incidents in an automated way.

Role Required: Vectra admin/System admin

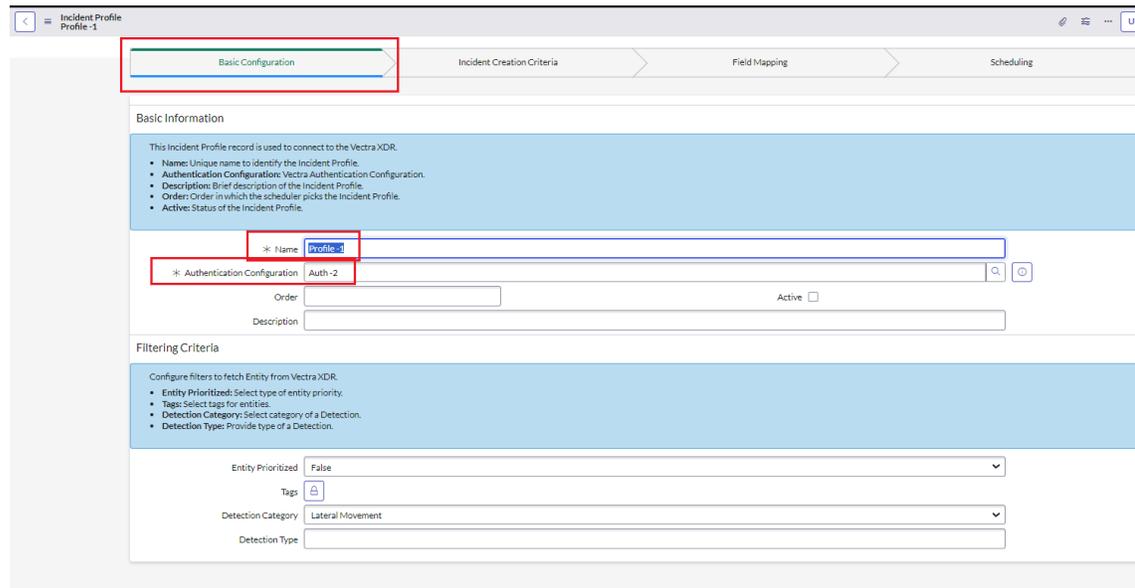
- As ServiceNow Vectra App Admin, I should be able to configure the profile to control the Vectra Detect data flow. I should be able to control what data to fetch from the Vectra Detect and convert it to Incidents in ServiceNow.

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.
- Entity Prioritized is default set to “True” so select value accordingly.
- Provide the value in the “Entity Urgency” field. Entity Urgency accepts a value between 0 to 100.



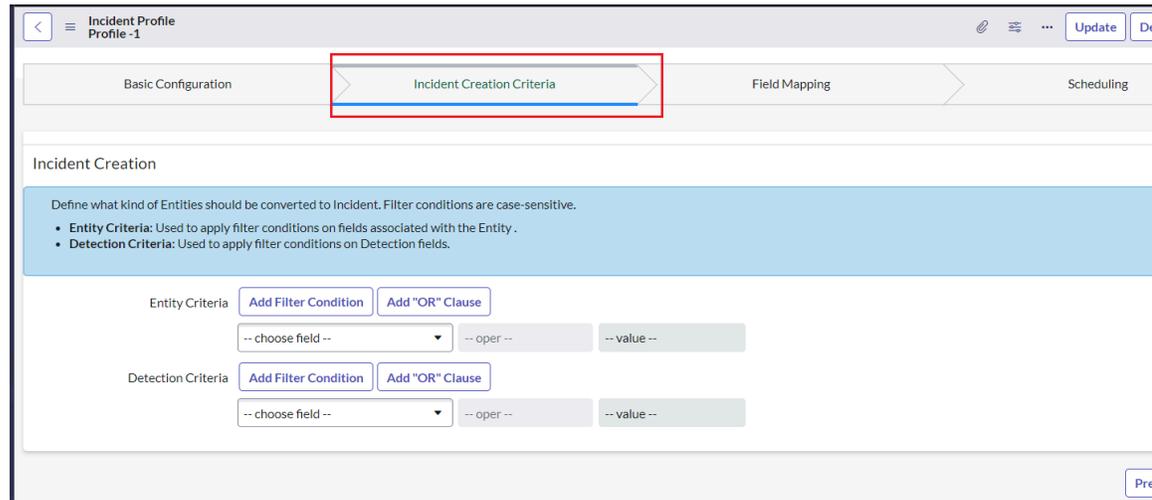
- Select the Value for “Entity Prioritized”. The default value is “All”.
- Provide a “Tag” to filter data tag-wise.(Tag populates in the list after one successful job run).
- Select “Detection Category” and provide “Detection Type” to filter data and based on the Detection filters, it fetches the detections.
- Now click on the Next button to move to the Incident CreationCriteria tab.

2.2.3.2. Incident Creation

Procedure:

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

- Complete the Basic Configuration.
- Click on Next to move to “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 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 Incident.
- 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 based on that, Incidents should be created.
- Select “AND” or “OR” to add multiple conditions.
- Note: “OR” condition applies between Entity Criteria and Detection so if any of the conditions match, the 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 Incident is 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 should be displayed.

- When assigning the user from the 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 Vectra entity.

Incident Creation

Define what kind of Entities should be converted to 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

Entity Type is host

Detection Criteria

Fallback User

By default "Assigned to" field of a 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

2.2.3.3. Field Mapping

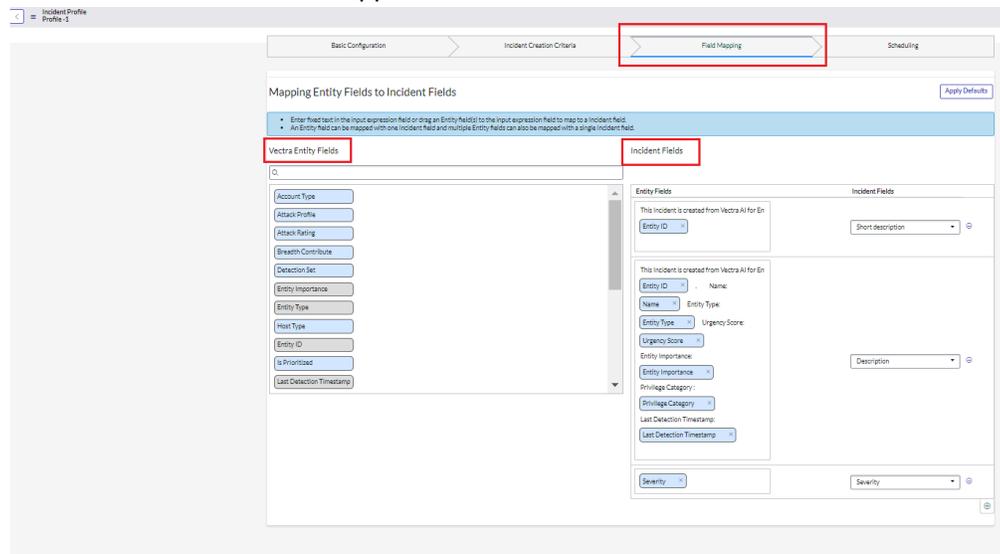
This section shows how to map Vectra Entity fields with ServiceNow ITSM Incident fields.

Role Required: [Vectra admin](#)

Procedure:

- Login to the ServiceNow instance.
- Navigate to Vectra application > Incident Profile.
- Complete the Basic Configuration and 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 " Incidents".
- Provide which fields of Entities get mapped with which fields of 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 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 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 Incident fields by clicking on the remove (minus)/add (plus) buttons.
- Different Incident fields can be selected from the dropdown list as needed.
- To map default fields click on the “Apply Defaults” button on the right side of the “Mapping Entity Fields to Incident Fields” heading in the “Field Mapping” tab. When it is clicked the default field mapping should 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](#)

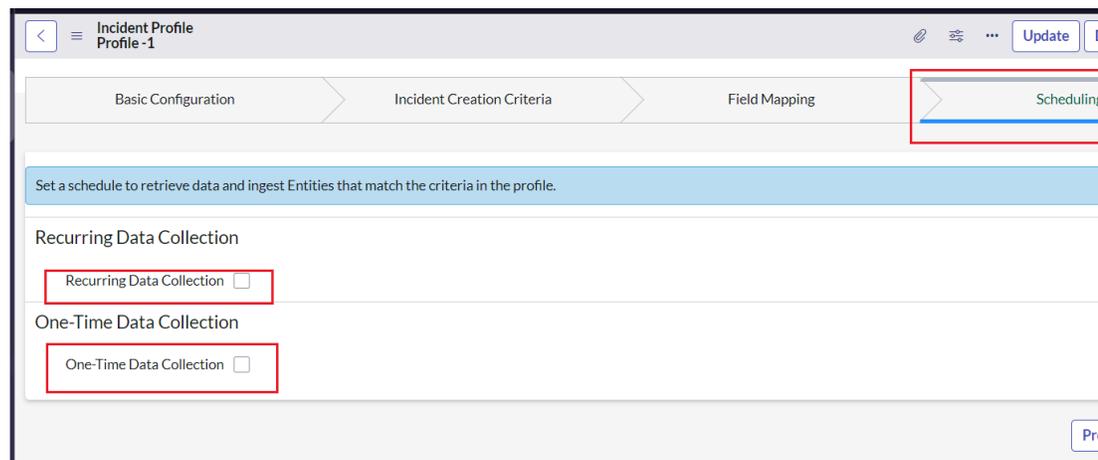
Procedure:

- Login to the ServiceNow instance.
- Navigate to Vectra application > Incident Profile.
- Complete the Basic Configuration, 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 on 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 different sources..
- Inactive profile can make active by selecting the checkbox of Active from the Basic Configuration tab while editing/updating the profile.

Notes:

- If a user deletes the Authentication Configuration source which is configured in the profile then that source will get deleted from the profile also and it will not run the scheduler.

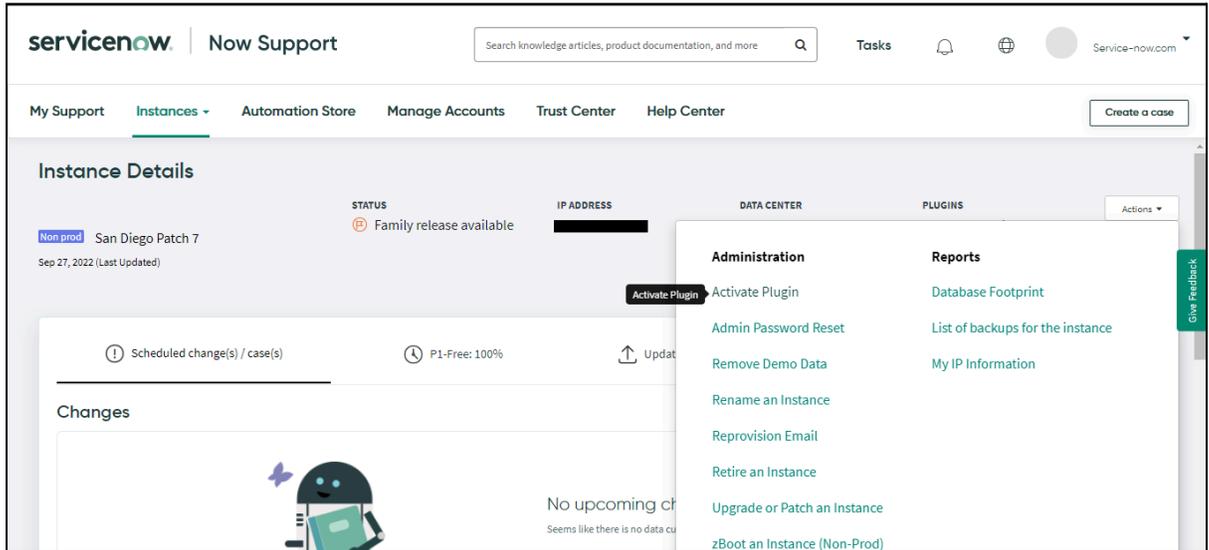


2.3. Use Cases

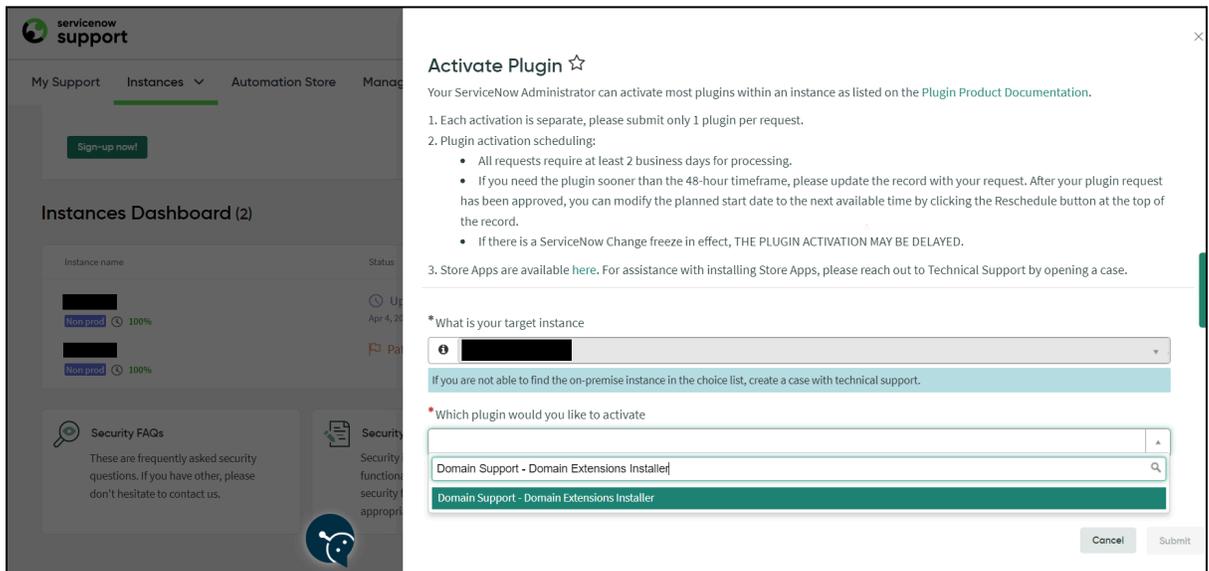
2.3.1. MSP Support

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.

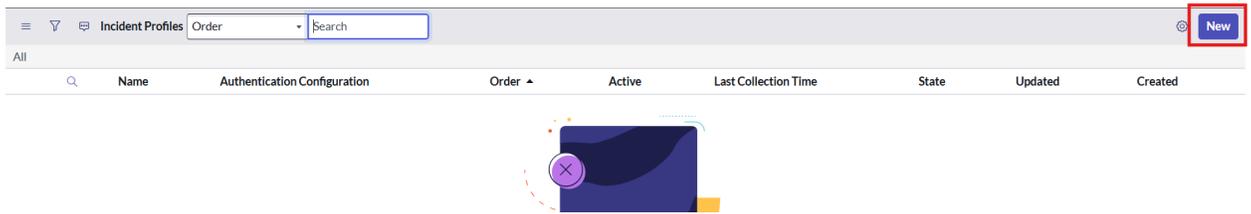


- e. Once the plugin is activated on the instance, you can install the application.

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.

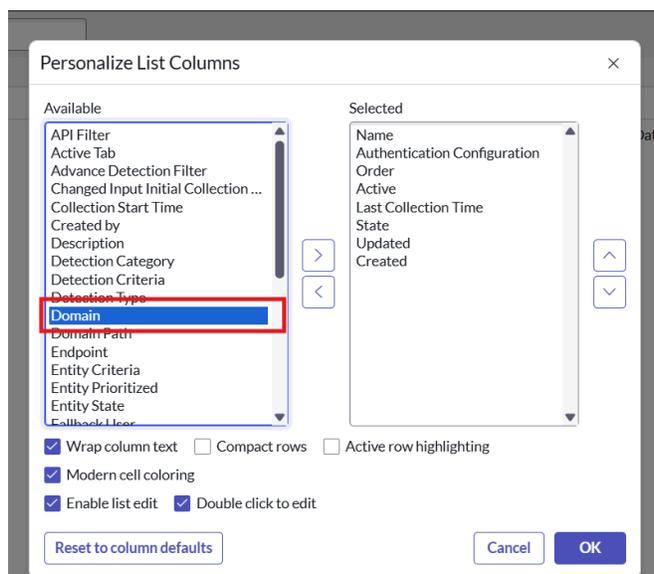
- create a new incident profile click the button on the top right corner.



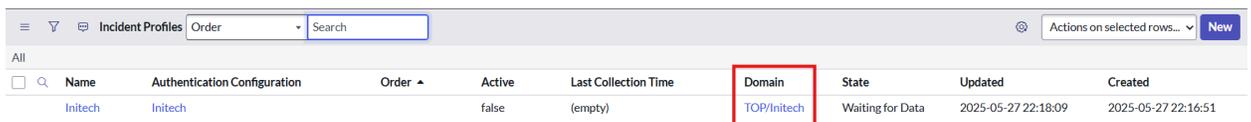
- Once the profile is created users may change the layout using the gear icon on the top right corner to see the domain column.



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



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



- Now if any entity, detection, incident is pulled/created by these profiles 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:

- Login to the ServiceNow instance.
- Navigate to Vectra ITSM> Select Incident Profile
- Provide the Incident creation criteria
- Navigate to the Entities table.
- Open any record to view the details
- See associated detection in the related list.
- Now navigate to the Detection table
- Both the tables are now populated with data.
- Open any record to view the details
- See the associated entity in the related list

2.3.2.1. Detection:

- All the fetched detections will be listed under the Detection table.
- Open any detection record to view, all fields will be read-only except .
- 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 attach the file to the detection record.
- Note - Users should not be able to create detection records manually from ServiceNow.

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.

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

2.3.3. Automatic Incident Creation

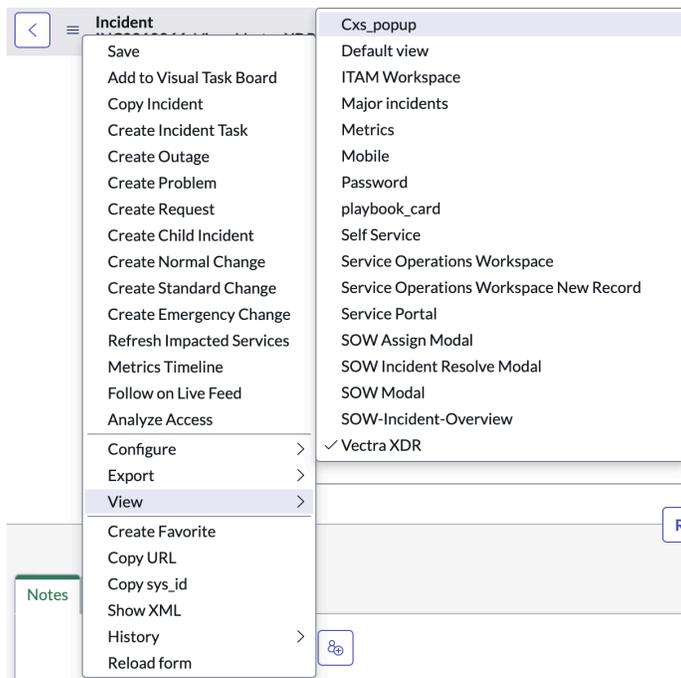
- You can create a ServiceNow Incident automatically based on the Incident Creation criteria(Entity and Detection).
- If you have provided any conditions under” Incident creation criteria”, the app will create an Incident and link entities in the Incident based on those conditions.
- Entities fields are mapped to 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 incident gets created.

2.3.4. SOAR Actions

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

Change the view to enable the tabs “Vectra XDR Entity” and “Vectra XDR Detections”

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



Configuration Items	Affected Users	Child Security Incidents	Similar Security Incidents	Related Configuration Items	Related Users	Associated Observables
Response Tasks	Associated Phish Emails	Associated Phish Headers	Vectra XDR Detections	Vectra XDR Entity (1)		

2.3.4.1. Manual Incident Creation

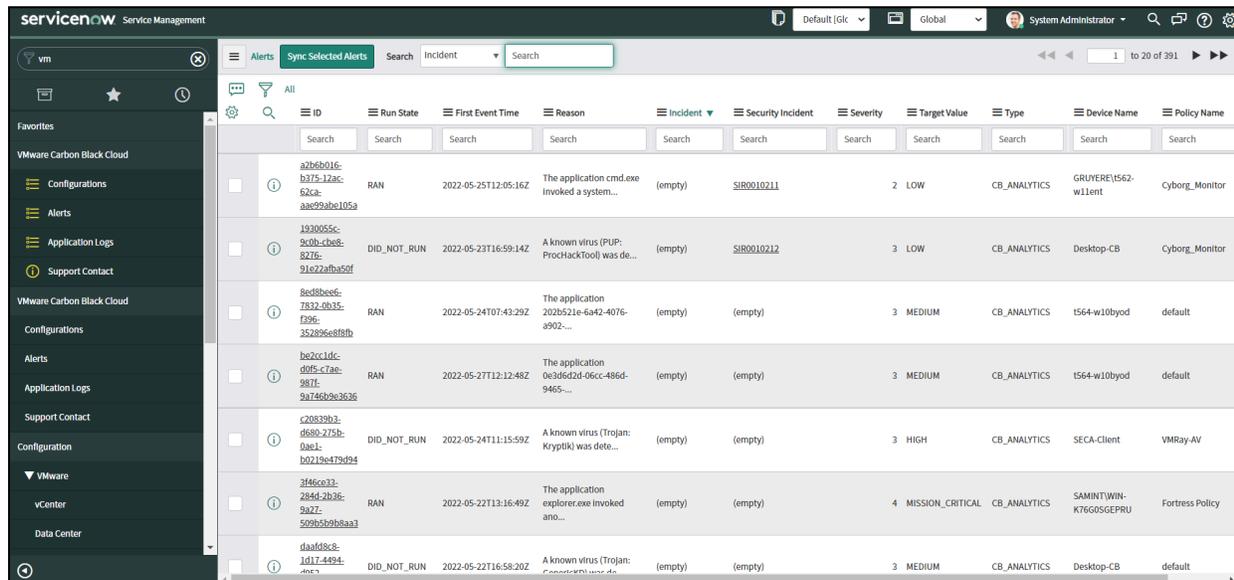
You can create Incidents manually from an entity. A manually-created Incident’s fields are populated based on the Field Mapping settings of the Incident Profile that ingested the entities.

You can create Incidents only for an entity in an Active state.

Role Required: [Vectra analyst](#)

Procedure:

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



- Click to view any entity record in an Active state.
- Click on the Create Incident button (top/bottom).
- Clicking the “Create Incident” button creates the Incident for that entity, maps the entity fields to the Incident field, and displays the Incident ID in the entity record. You can navigate to the Incident by clicking “Preview this record”.
- Open the Incident by clicking “Preview this record” > “Open record”.
- To view the list of entities associated with an Incident, perform the following actions:

- Scroll down on the 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 Incident.
- Click on the “Detection” tab to view the list of detections associated with the Incident.
- 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 will be 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.

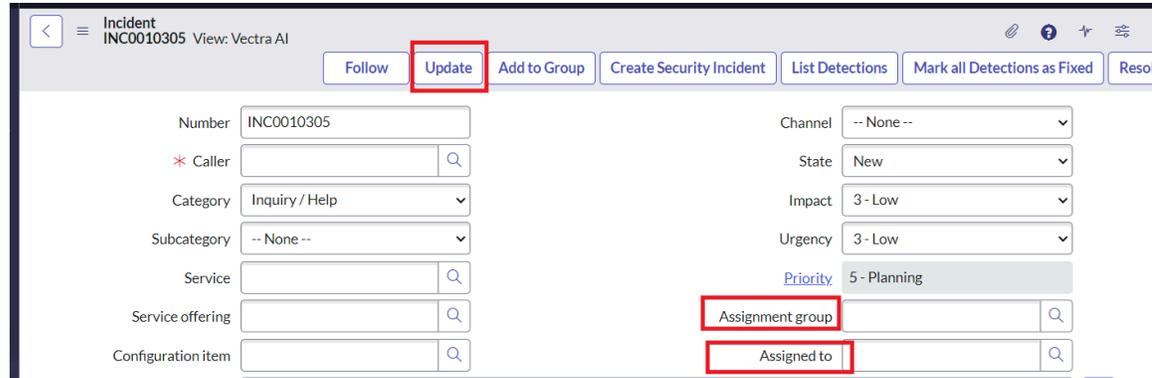
2.3.4.2. Create Assignment

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

Role Required: [Vectra analyst](#)

Procedure:

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



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

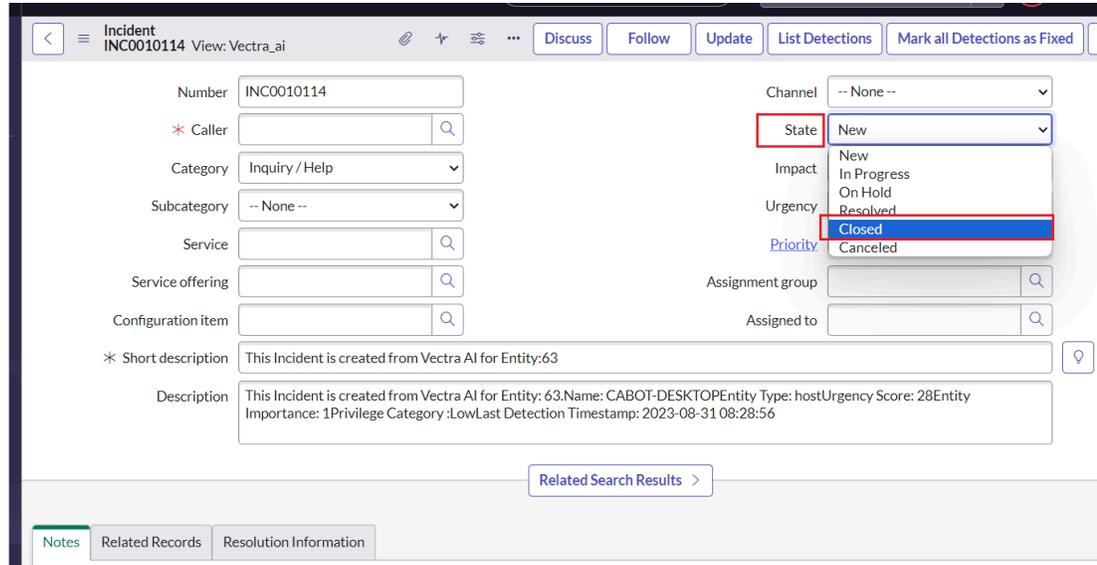
2.3.4.3. Close Incident in ServiceNow

If you close an Incident with detections associated with it, then that incident gets closed in ServiceNow only, it won't get synced with the Vectra entity.

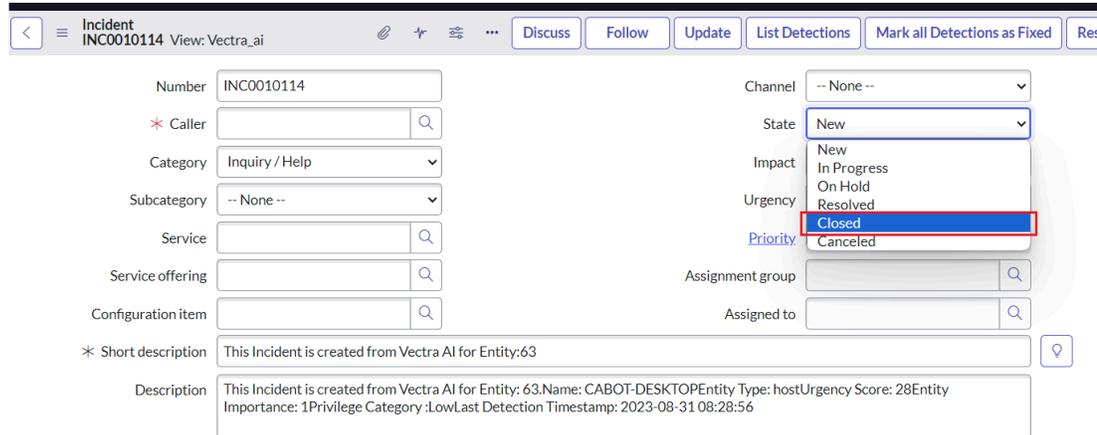
Role Required: [Vectra analyst](#)

Procedure:

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



- For “State”, select “Closed”.



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

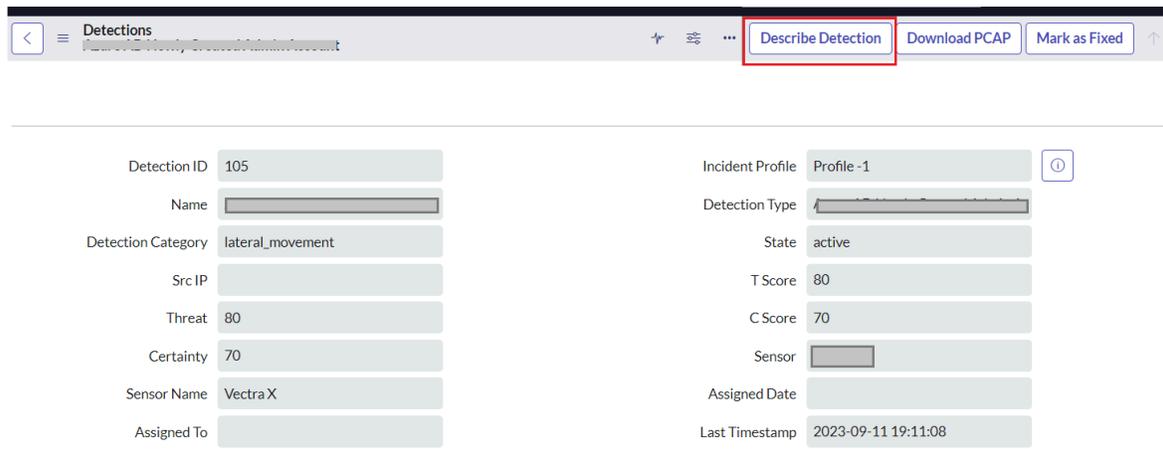
2.3.4.4. Download PCAP

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

Role Required: [Vectra analyst](#)

Procedure:

- 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. 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”**
- 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

- 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.
- You can also perform an action from the 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

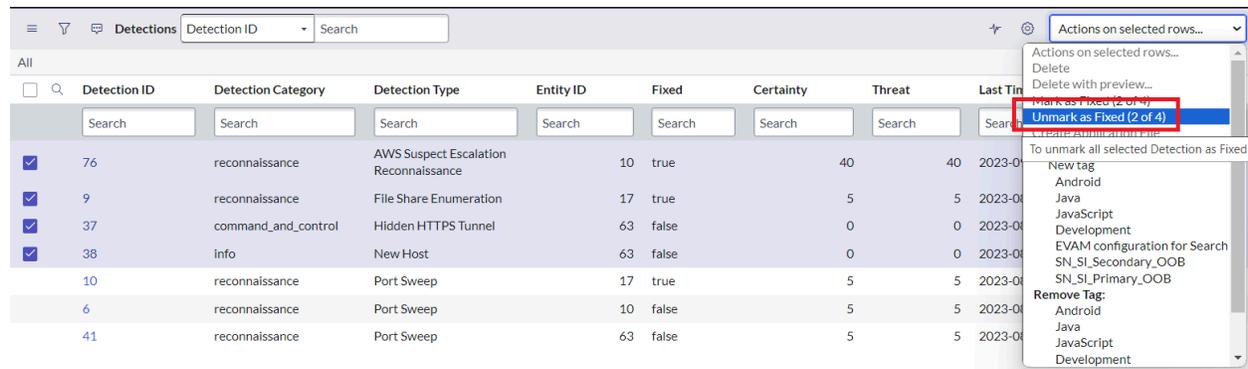
2.3.4.6. Mark/Unmark Detection as fixed

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 > 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.

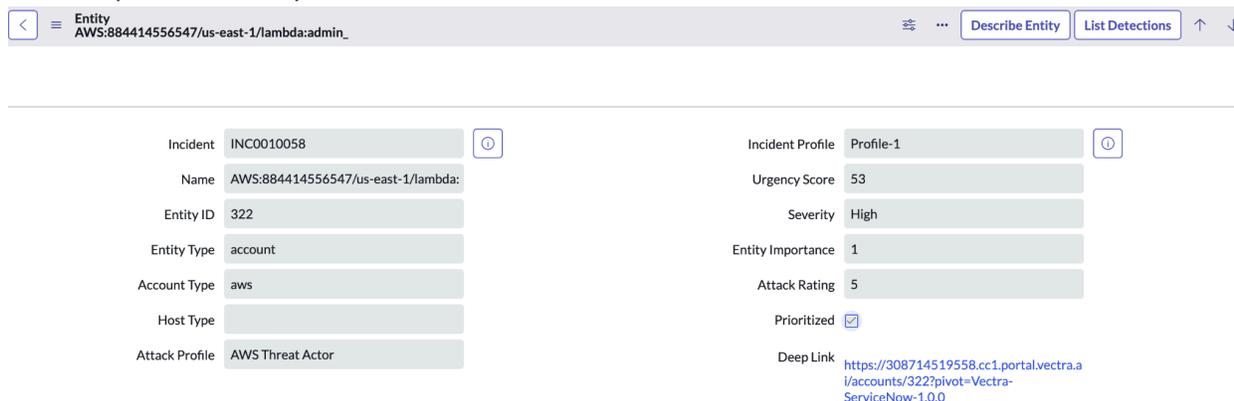


- Unmark as Fixed” is visible in the Detection form view when Detection is fixed on ServiceNow.
- Based on the detection status Fixed/Not Fixed, the application shows the button “Mark as Fixed /Unmark as Fixed”.
- Click on the button to perform the action, Mark as Fixed, so a confirmation pop-up will be displayed.
- Click on the “Yes” button on the confirmation pop-up then that particular Detection will be marked/unmarked 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.

2.3.4.7. Describe Entity

Role Required: [Vectra analyst](#)

- 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.



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

2.3.4.8. Describe Detection

Role Required: [Vectra analyst](#)

- 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.



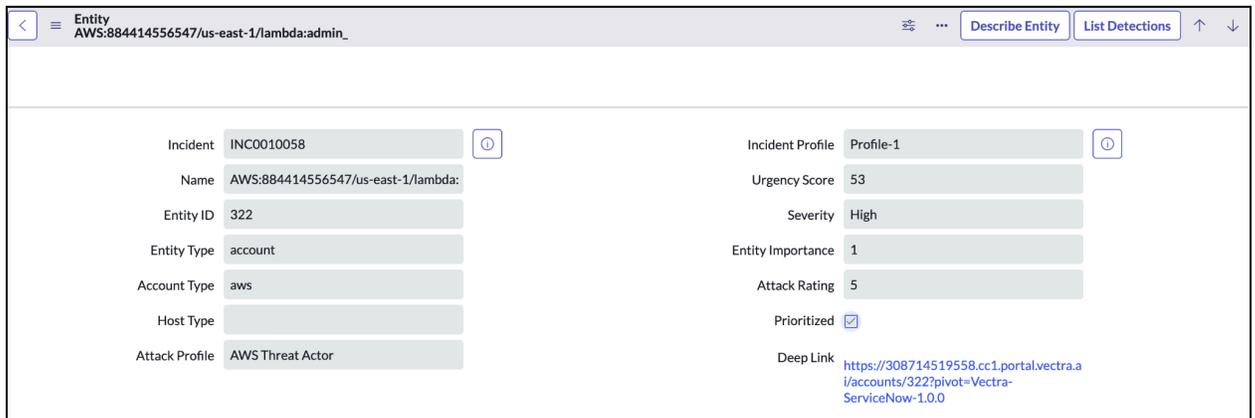
Detection ID	167	Incident Profile	Profile-3	
Name	AWS EC2 Browsing Activity	Detection Type	AWS EC2 Browsing Activity	

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

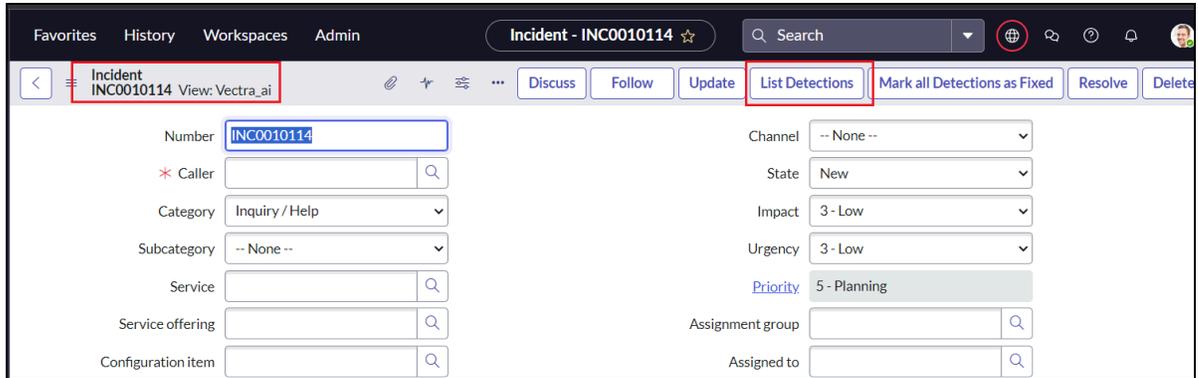
2.3.4.9. List Detection

Role Required: [Vectra analyst](#)

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



Note: This action can perform from the Incident form view also.



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

2.3.4.10. 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 Incident from using “Add to Group” UI action, and the same changes should also get reflected on the Vectra platform.

Role: [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 are the types and accepted values.
 - 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*

Group*

Member*

Note: If the Incident profile is deleted, then the action button will not be visible on the entity form view also nor visible in the associate Incident form view.

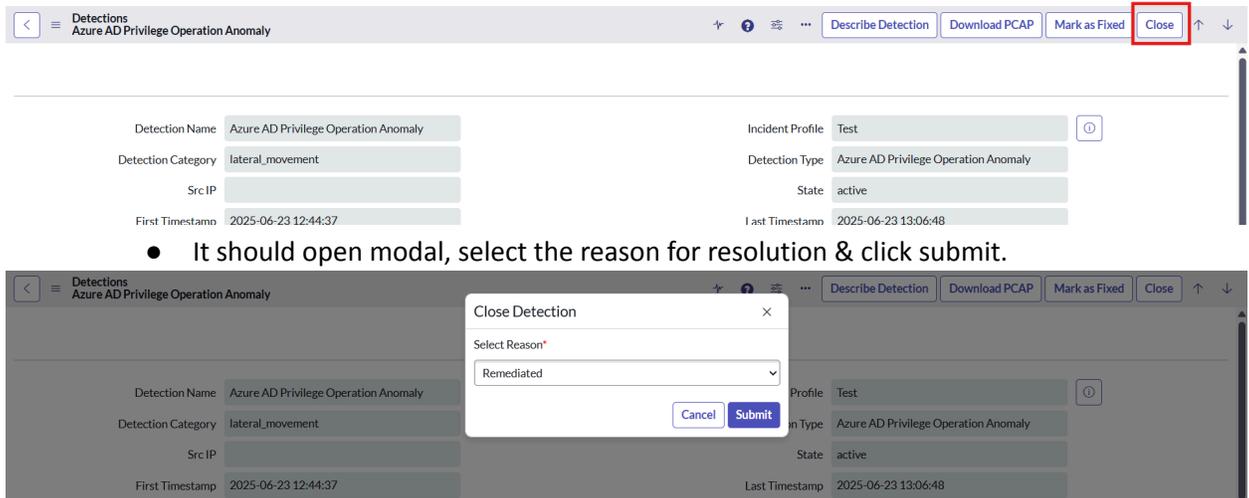
2.3.4.11. Close detection

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.



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

- 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 field 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.

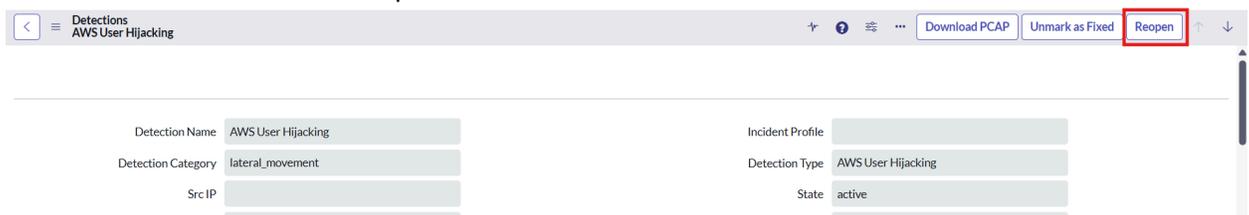
2.3.4.12. Re-open detection

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

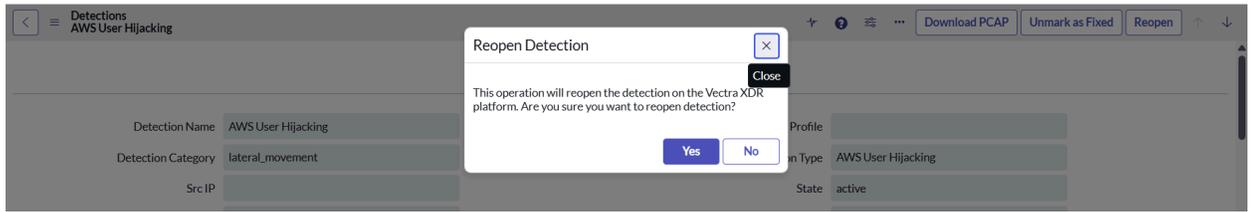
Role Required: [Vectra analyst](#)

Procedure:

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



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



- 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.

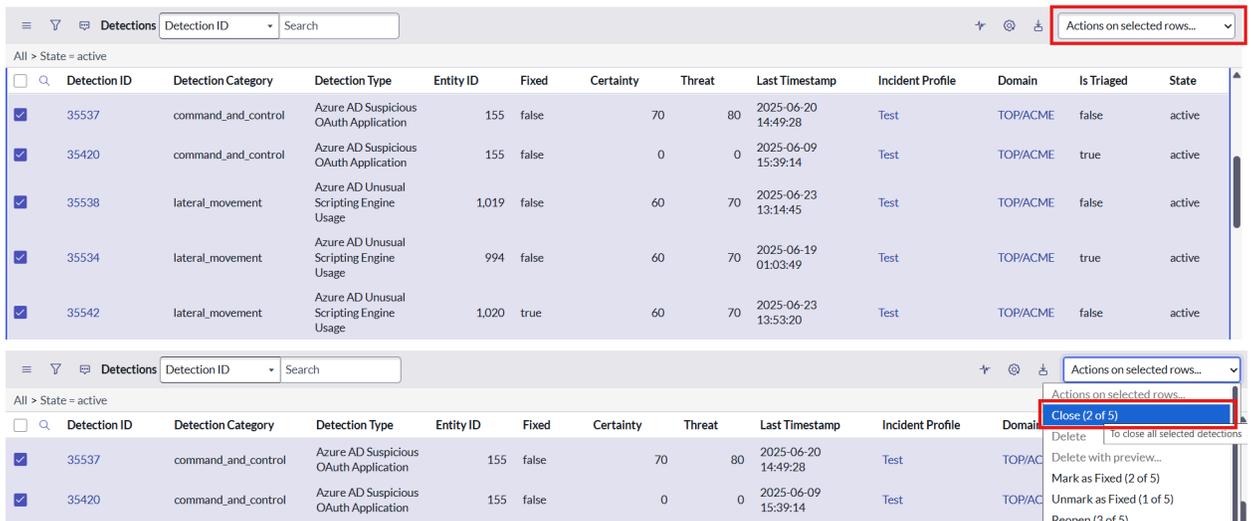
2.3.4.13. Close Multiple Detections

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.

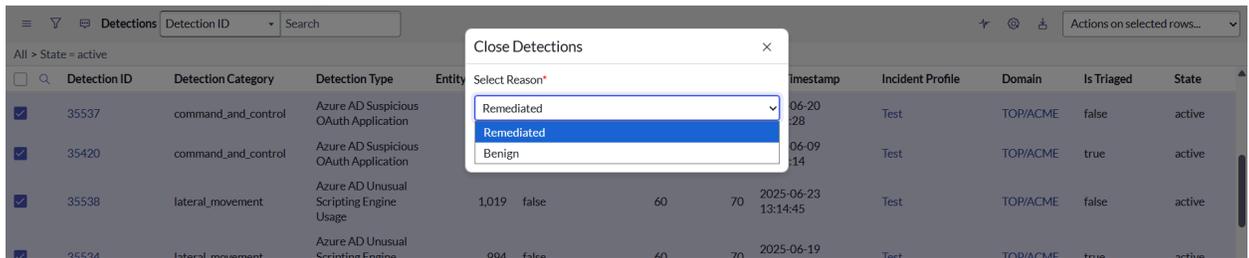
Role Required: [Vectra analyst](#)

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.



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



- 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 field 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.

2.3.4.14. 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.

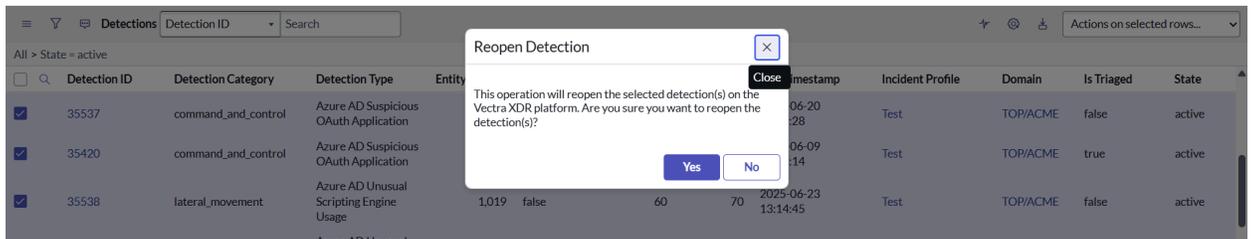
Role Required: [Vectra analyst](#)

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.



- It should open modal for confirmation.



- 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.

2.3.4.15. 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:

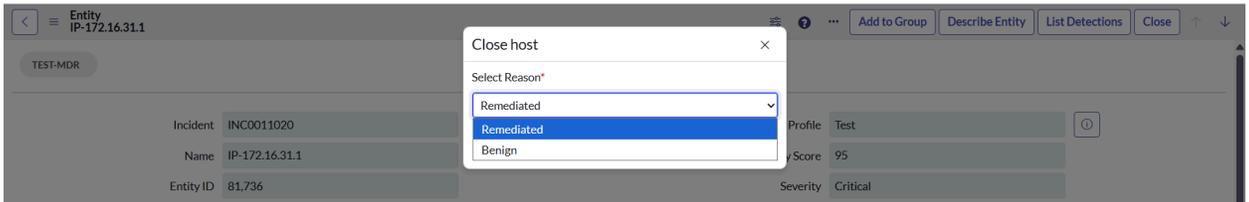
1. From entity

- Login to the ServiceNow instance.

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



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



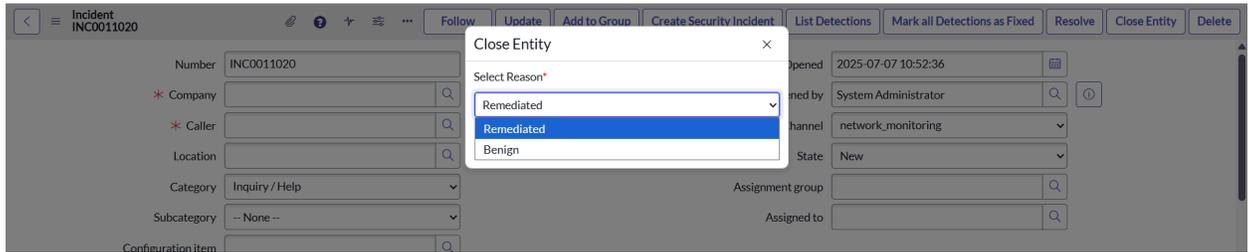
- If the operation is successful, an info message will be displayed : **“Successfully closed <entityType> as <reason> on the Vectra XDR platform.”**. A note will be added to related incident records & based on the response returned from the Vectra XDR platform, the corresponding detections will be closed in SNOW with the given reason. If the selected reason is **Benign**, the **Is Triage**d 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 Incident

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



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



- 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 incident record & 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 Incident creation in the process monitor.

Role: [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
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 **'Complete'** once all Entities are fetched and associated 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 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 ITSM application and click "Update".
4. The application will be updated in your instance.

Note:

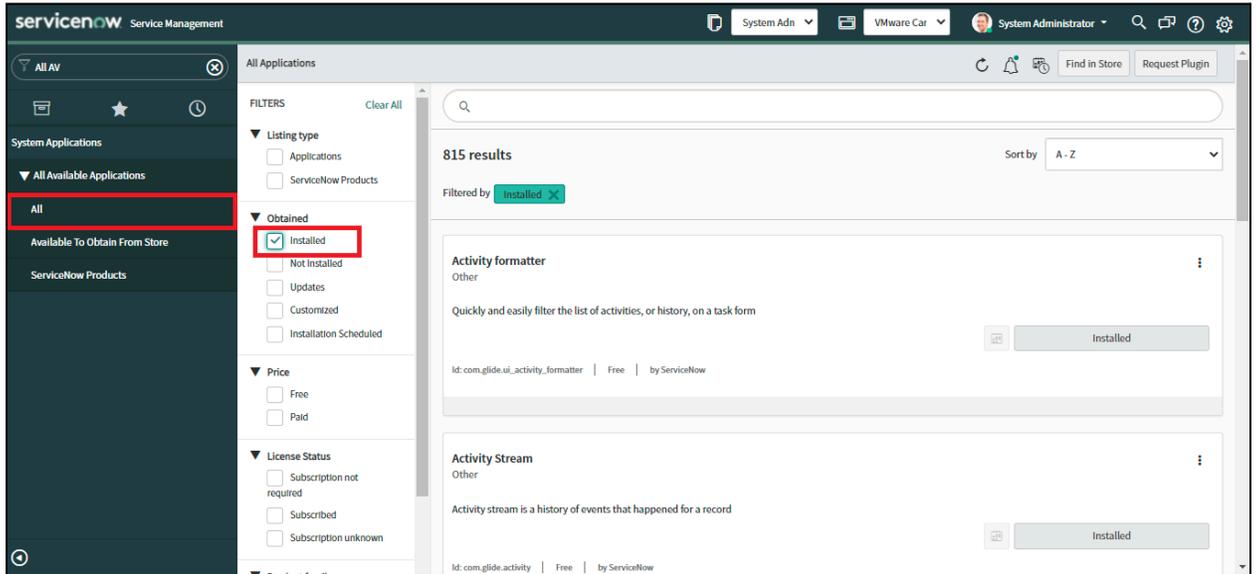
Scheduled Jobs: All scheduled jobs will be reset to their default configurations during the upgrade process. You must review, update, and reconfigure these jobs as needed after completing the update.

4. Uninstallation

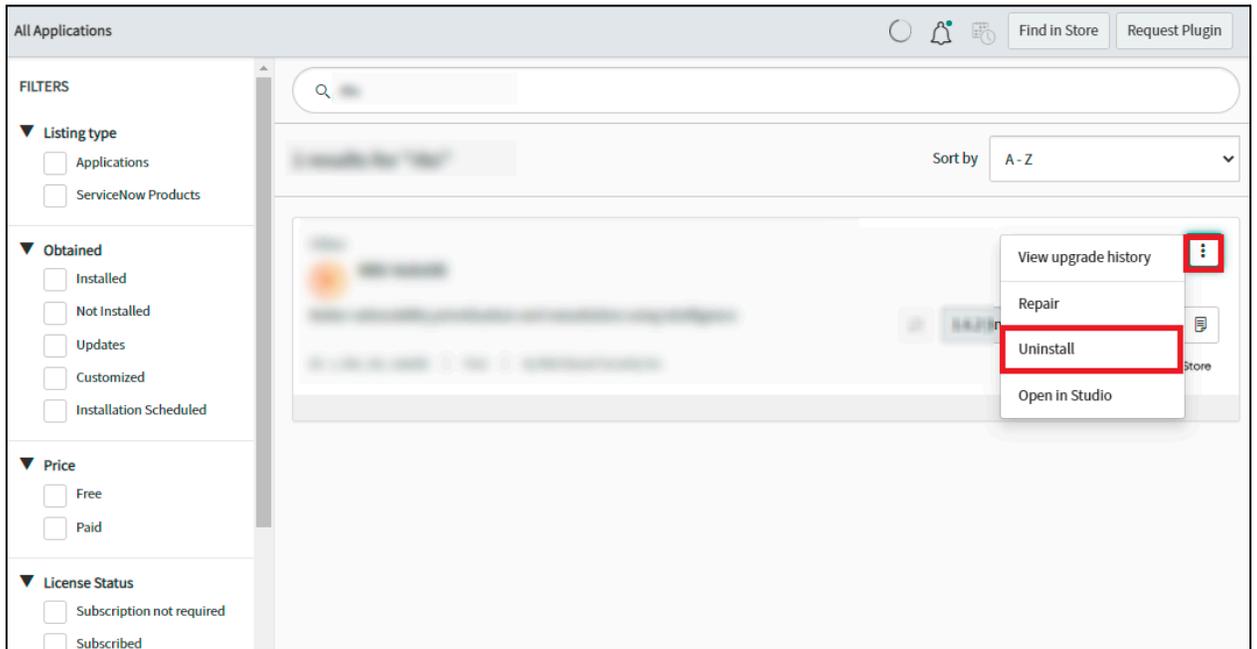
This section describes how to uninstall the Vectra XDR ITSM Integration application from a ServiceNow instance.

Role Required: [System Administrator](#)

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



- 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 ITSM”.

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 ITSM” > Application Logs

Created	Level	Message	App Scope	Source Script
2023-09-20 05:43:35	Information	Data collection has been completed successfully for incident profile : Profile -1'.	Vectra Cloud for ITSM	Script Include: VectraCloudProfile
2023-09-20 05:43:31	Information	Recurring data collection has been initiated for incident profile : Profile -1	Vectra Cloud for ITSM	Script Include: VectraCloudProfile
2023-09-20 05:43:31	Information	Initiated the background flow for Entity ingestion for profile 'Profile -1.	Vectra Cloud for ITSM	Script Include: VectraCloudProfile
2023-09-20 05:42:23	Information	Data collection has been completed successfully for incident profile : Profile -1'.	Vectra Cloud for ITSM	Script Include: VectraCloudProfile
2023-09-20 05:42:19	Information	Initiated the background flow for Entity ingestion for profile 'Profile -1.	Vectra Cloud for ITSM	Script Include: VectraCloudProfile
2023-09-20 05:42:19	Information	Recurring data collection has been initiated for incident profile : Profile -1	Vectra Cloud for ITSM	Script Include: VectraCloudProfile
2023-09-20 05:41:10	Information	Data collection has been completed successfully for incident profile : Profile -1'.	Vectra Cloud for ITSM	Script Include: VectraCloudProfile
2023-09-20 05:41:07	Information	Recurring data collection has been initiated for incident profile : Profile -1	Vectra Cloud for ITSM	Script Include: VectraCloudProfile

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:** 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.

5.2.4. **Problem Statement:** CIs not getting linked to the 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.

5.2.5. Automatic Incident is not Created

Problem Statement: Incident Creation Criteria are set to escalate certain entities to Incidents, but the 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 Incidents are created or not.

5.2.6. **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.

5.2.7. 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.

5.2.8. [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.