



SCOPE CERTIFIED APPLICATION INSTALLATION AND CONFIGURATION GUIDE

Snyk Security for Application Vulnerability Response (3.2.0)

VERSION CONTROL

#	Document Version	Date	Owner	Document Status	Comments
1	1.0.0	8th August, 2022	Crest Data Systems	Complete	<ul style="list-style-type: none"> Brand new integration for Snyk SCA vulnerability with ServiceNow AVR
2	1.1.0	10th Oct, 2023	Crest Data Systems	Complete	<ul style="list-style-type: none"> Bi-directional integration for triaging vulnerabilities and exception management from ServiceNow to Snyk New ability to close AVITs when the project gets deleted from Snyk Added CWE information from Snyk into ServiceNow Additional filtering options: IsUpgradable, IsPatchable, Source, Patched, Fixable, IsPinnable and IsFixed Added support of Utah and Vancouver ServiceNow versions
3	2.0.0	18th March, 2024	Crest Data System	Complete	<ul style="list-style-type: none"> Added SAST Integration support Added Support for the EU and AU regions Added filtering support for TargetReference and Status Updated source_scan_id mapping to latest_issue_counts.updated_at Added mapping for Exploit Maturity and cvss Score Added more granular triaging check in ServiceNow
4	2.1.0	03rd July, 2024	Crest Data	Complete	<ul style="list-style-type: none"> Added filtering support for Target Name, Environment, Tags, and Lifecycle Added mapping for SCA and SAST issue titles in source notes and description field of AVIT, respectively. Added mapping of target name of Snyk project in the correlation ID field of scanned application table Added feature for bulk ignored AVIT from the Remediation task Updated Target Reference filter label to Branch Updated user-agent

					<ul style="list-style-type: none"> Fixed disappeared SAST issue should get closed in ServiceNow AVIT Fixed approval business rule work for only Snyk AVIT
5	2.2.0	28th Nov 2024	Crest Data	Complete	<ul style="list-style-type: none"> Improved filtering for issues imported using the REST API by applying filter rules after import. Improved filtering to allow an "OR" condition when selecting multiple filters (the previous default only allowed "AND"). Improved bidirectional ignore feature such that AVITs manually closed in ServiceNow will add a permanent ignore in Snyk, or AVITs manually reopened will delete existing ignores in Snyk. Improved performance of large-scale issues import by giving customers the ability to set a system property to select the REST (more efficient) or V1 API for fetching SCA issues. Added support for Custom Snyk Base URL Bug fixes Added support for Xanadu
6	3.0.0	16th Dec 2024	Crest Date	Complete	<ul style="list-style-type: none"> Added filtering support for Project Type. Added IaC issues support in existing SCA integrations Mapped the Last opened as First found in AVIT Changed mapping of disclosureTime to first_detection_date in third-party.
7	3.1.0	Jun 24, 2025	Crest Data	Complete	<ul style="list-style-type: none"> Added AVIT close and reopen based on project status Restrict closing issue on Snyk if project is inactive Added v2 condition builder for project query Updated user agent to v3.1.0 Added event trigger to close AVIT on Snyk Updated API version to 2024-10-15 Added validation to restrict filtering for 1000 projects if V1 is in use.
8	3.2.0	8th Aug 2025	Crest Data	Complete	<ul style="list-style-type: none"> Added support of bidirectional updates from Exception rules. Added mapping of source_exploitability for REST SCA Minor Bug fixes

Contents

Contents	4
1. Overview	6
Snyk ServiceNow Application	6
1.1. Application features	6
1.2. Compatibility Matrix	6
2. Snyk App for Vulnerability Response	7
2.1. Pre-Requisites	7
2.2. ServiceNow Plugins	7
2.3. Application Installation	7
3. Configuration Instructions for New Installation AND Upgrades	8
3.1. Update Required After App Install/Upgrade – Snyk Base URL Change	8
3.2. Permission and Roles	9
3.3. Create Users	9
3.4. Global Setting	11
3.5. Run Scheduled Script (Mandatory Step for fresh Install, Upgrades, and Cloned instances)	14
3.6. Generate REST/OAuth Token	16
3.7. Add IaC Scan Type for IaC issues in AVIT Table (Only if you want to fetch IaC Issues)	18
4. Use Cases	21
4.1. Fetch Projects from Snyk platform	21
4.2. Vulnerability Filtering	25
4.3. Managing Exceptions in ServiceNow	36
4.4. Fetch SAST Issues from the Snyk platform.	38
4.5. Fetch SCA & IaC Issues from the Snyk platform(Only for the US region)	45
4.6. Fetch Issues from Snyk All Region SCA & IaC Vulnerability integration	55
4.7. Bulk ignore of Application Vulnerable Items (AVITs) using Remediation tasks	61
4.8. Unignore issues from ServiceNow to Snyk	63
4.9. Automatically Ignore and Unignore AVITs using Exception Rules	64
4.10. Snyk Risk Score Calculator	66
4.11. Snyk Dashboard	67
4.12. System properties (optional)	71
4.13. CI LookUp rule	71
4.14. Assignment Rule	77
4.15. Privacy Policy	81
5. Upgrade Behaviour (From 3.0.0)	83
5.1. Changed mapping of last opened in AVIT	83
5.2. Two false options in Vulnerability filtering (Perform the steps below to remove duplicate options)	85
6. Support, Troubleshooting, and Known Behaviors	89

6.1. Support	89
6.2. Troubleshooting	91
6.2.1. Unable to generate the token	91
6.2.2. Unable to install "Snyk VR Integration" from the ServiceNow Store	93
6.2.3. Unable to create a new user	93
6.2.4. Unable to install/activate the plugin in ServiceNow Instance	93
6.2.5. The user deletes the Application Registry default record	93
6.2.6. The user deletes the REST Message default record	93
6.2.7. The user deletes any of the Integrations records	93
6.2.8. Unable to search Lifecycle & Environment from AVIT	93
6.2.9. Unable to see CVE & CWE in the Third-party records	95
6.2.10. Organizations were not found, or you do not have permission to access them	96
6.2.11. Invalid Redirect URL error message while authorizing Snyk Application	96
6.2.12. Able to generate the token, but integration is failing.	96
6.2.13. Getting Reconcile-related errors while running integration.	96
6.2.14. Unable to ignore an issue from ServiceNow to Snyk. Getting 403 Error in Outbound HTTP Calls.	97
6.3. Known Behaviors	98
6.3.1. Vulnerability Integration fails when one integration is running and the second integration is executed.	98
6.3.2. The Snyk application vulnerable item is in the open state even if the Snyk issue is fixed in the Snyk platform.	98
6.3.3. The state of existing AVIT will not update from "Deferred" to Open when Triaging in ServiceNow is selected.	99
6.3.4. Recently Ignored issues on the Snyk side could take ~5 hours to reflect in SCA V1 API.	99
6.3.5. Additional comments and state updates on the Snyk side may take up to ~9 hours in the US region. Typical performance is right away.	99
6.3.6. Users must be added to the approver group for performing "Mark as False positive" and "Request Exception."	99
6.3.7. Users must initiate the Reapply calculator's UI action inside the VR scope.	100
6.3.8. Unable to "Mark as False positive" or "Request Exception" for IaC issues.	100
6.3.9. Use of "Move Project" V1 Snyk API can lead to unexpected results in SN Integration.	100
6.3.10. OAuth Process	100

1. Overview

Snyk is a Developer Security Platform that integrates directly into development tools and automation pipelines. Snyk makes it easy to find, prioritize, and fix security vulnerabilities in code, dependencies, containers, and infrastructure as code. Backed by industry-leading vulnerability intelligence and designed by developers for developers, Snyk fits into your development workflow to add security expertise to your toolkit.

Snyk ServiceNow Application

This application imports Snyk Projects and Snyk Issues data into ServiceNow as Application Release, Scanned Applications, Application Vulnerable Item, Vulnerability, Application Scan Summary, and Package in ServiceNow. It provides a user-friendly dashboard for data visualization and supports filtering issues to be ingested.

1.1. Application features

The main features of the integration include:

1. Deliver Snyk security insights on vulnerabilities in open-source dependencies seamlessly into a ServiceNow workflow
2. Provide visibility into your development team's application security risk on both platforms
3. Enable AppSec managers to create automated workflow processes to minimize risk and guide developer teams to focus on the highest priorities.
4. Synchronize vulnerability exceptions between ServiceNow and Snyk
5. Calculate vulnerability risk and determine prioritization using ServiceNow's vulnerability calculators combined with Snyk's industry-leading intelligence
6. Consolidate vulnerabilities and security outcomes, giving security teams visibility into end-to-end workflow management
7. Bidirectional functionality to ignore and unignore vulnerabilities using the ServiceNow exception or false positive workflows from ServiceNow to Snyk
8. Support the US, AU, and EU regions of Snyk

1.2. Compatibility Matrix

ServiceNow Version:

- Xanadu, Yokohama and Zurich

Snyk API Version:

- REST for projects and Organizations, SAST, SCA, IaC(US/AU/EU region)
- V1/reporting for SCA & IaC Issues(US region)

2. Snyk App for Vulnerability Response

This section describes the procedure for downloading and installing the Snyk Security for AppVR application from the store.

2.1. Pre-Requisites

1. The user should have an Enterprise license to the Snyk Platform.
2. Your ServiceNow Redirect URL
("https://YOUR-INSTANCE.service-now.com/oauth_redirect.do") must be set up on the Snyk side for the Snyk App to be authorized with ServiceNow.
Note: Contact servicenow@snyk.io to register your instance for the Snyk app. Please mention that the redirect URL needs to be added under ServiceNow Snyk Security for Application Vulnerability Response. This step is mandatory for new integration installations.

2.2. ServiceNow Plugins

The following ServiceNow plugins must be activated:

Vulnerability Response (com.snc.sn_vul) - min version(24.1.5)

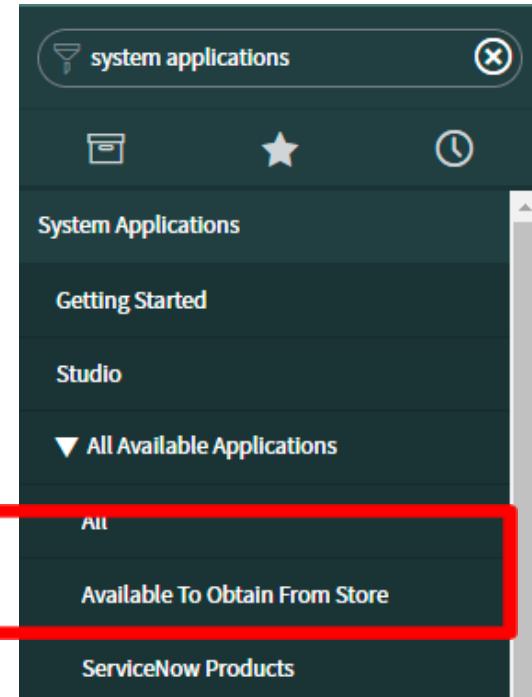
To install these plugins:

1. Log in to your instance with system admin credentials.
2. Navigate to "System Definition," and under it, select "Plugins" for your instance.
3. Search and install the above plugin.

2.3. Application Installation

Steps to install the application from the ServiceNow Store:

- Users with the System administrator(admin) role can install the application from the ServiceNow Store.
- Go to <https://store.servicenow.com>
- Search for the "Snyk Security for Application Vulnerability Response" on the search tab.
- Click on the Snyk Security for Application Vulnerability Response.
- Click on the "Get" button and enter the ServiceNow ID credentials.
- Once successfully added, open the instance and Navigate to Applications > All Available Applications > All.
- Find the application using the filter criteria and search bar.
- Next to the application listing, click Install.



3. Configuration Instructions for New Installation AND Upgrades

3.1. Update Required After App Install/Upgrade – Snyk Base URL Change

Background: Snyk has recently migrated its platform hosting for **new customers** to **AWS**. Existing customers will continue to be hosted on **Google Cloud Platform (GCP)**. New customer still has option to opt for GCP.

What's Changing in the ServiceNow App?

In this release of the ServiceNow Snyk Integration, the base URL will default to the new AWS URL: <https://app.us.snyk.io>

This means:

- If you are a new Snyk customer on AWS, you do not need to make any changes.
- If you are an existing or new Snyk customer on GCP, you need to update the base URL in your integration to continue syncing correctly.

If your Snyk organization is still hosted on GCP, follow these steps after upgrading the app:

- Open Global Settings and go to base URL and change URL to app.snyk.io for GCP

How to Know if You're on AWS or GCP?

If you're unsure which platform you're hosted on:

- Log in to your Snyk account and check the URL in your browser.
 - If it's app.us.snyk.io, you're on **AWS**.
 - If it's app.snyk.io, you're on **GCP**.

Important Note: Customers hosted in the us.snyk.io (AWS) region MUST use the REST APIs.

3.2. Permission and Roles

Note: By default `x_snyk2_snyk_vr_in.configure_integration` will be added under `sn_vul.app_configure_integrations`.

3.3. Create Users

Note: This step is optional. If you do not want to create a user, then System Admin can access the Snyk Application.

The ServiceNow platform admin creates the various users for the application.

Username (for example)	Description	Role to be assigned
App Admin	This user will access the Snyk App for Application Vulnerability Response application, fetch the Data, and access various application modules.	<ul style="list-style-type: none">● oauth_admin● sn_sec_cmn.admin● sn_vul.admin● sn_vul.app_exception_approver● sn_vul.app_false_positive_approver● sn_vul.app_manage_risk_score_configuration● sn_vul.app_read_assigned● sn_vul.app_configure_integrations● web_service_admin

Below is an example showing how to create an App Admin user and assign it to the "sn_vul.app_configure_integrations" role. Other users can be created similarly by giving them the appropriate roles.

Role Required: System Administrator (admin)

Procedure:

- Navigate to "Organization" and select "Users" under it.
- Click the Users module.



The screenshot shows the ServiceNow interface for managing users. The left sidebar contains a navigation tree with sections like Configuration, CI Lifecycle Management, CI State Registered Users, Password Reset, Blocked Users, Organization, and Users. The 'Users' item under the Organization section is highlighted with a red box. The main panel displays a list of users with columns for User ID, Name, Email, Active status, and creation/updated dates. There are 628 users listed, with page 1 of 100 shown.

- On the Users list that is displayed, click New. A new user form is displayed.

The screenshot shows the 'User' new record form. The 'User' tab is selected. The form includes fields for User ID (SnykAdmin), First name (Snyk), Last name (Admin), Title, Department, Password, Email, Language (None), Calendar integration (Outlook), Time zone (System (America/Los_Angeles)), Date format (System (yyyy-MM-dd)), Business phone, Mobile phone, and Photo (Click to add...). The 'Active' checkbox is checked. Other checkboxes for 'Password needs reset', 'Locked out', 'Web service access only', and 'Internal Integration' are unchecked. A 'Submit' button is at the bottom.

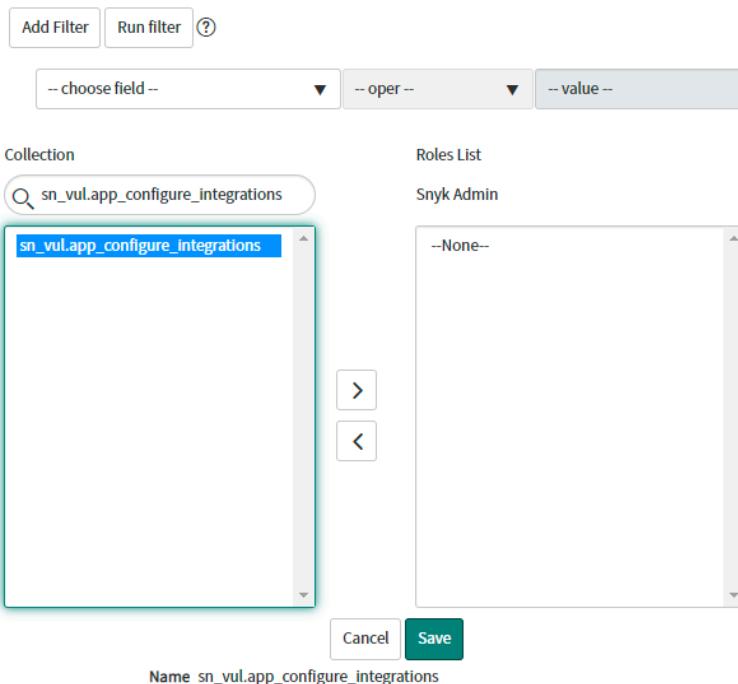
- Fill out the required details in the form.

Note: The values shown in the following table and figure are example values.

Field	Description
User ID	A unique user ID is required for the role in your ServiceNow Platform instance. An example is SnykAdmin

First Name	The person you are assigning
Last Name	The person you are assigning
Title	Job Title
Password	The unique password created for this user
Email	Unique email address

- Click Submit. Once submitted, you can assign the role.
- On the Users list, click on the name of the new user you created, such as Snyk Admin.
- In the user, the record goes to the Roles section, and click Edit.
- Select "sn_vul.app_configure_integrations" in the Collection column and move it to the Roles list. Similarly, users can add other roles to the user.



- Click Save.

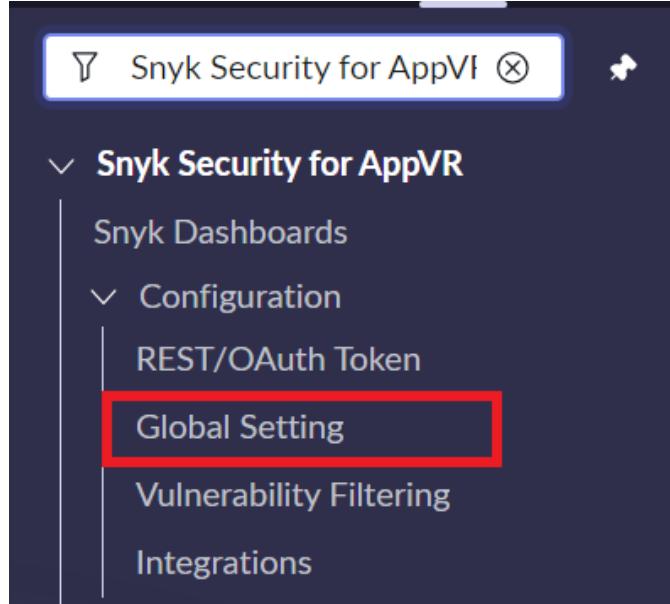
3.4. Global Setting

The global setting provides feasibility for defining project tag keys to populate Snyk projects into the CMDB table.

Role Required: x_snyk2_snyk_vr_in.configure_integration

Procedure:

1. Login to the ServiceNow instance.
2. Navigate to "Snyk Security for AppVR" and select "Configuration."
3. Click on "Global Setting."



4. The Global setting page gets opened with the below default values
 - "Base URL": <https://api.us.snyk.io> (Default)
 - Enter the Snyk BaseURL according to the region where your Snyk platform is deployed. Below are the valid BaseURLs
US region Snyk BaseURL for GCP users : <https://api.snyk.io>
US region Snyk BaseURL for AWS users : <https://api.us.snyk.io>
EU region Snyk BaseURL : <https://api.eu.snyk.io>
AU region Snyk BaseURL : <https://api.au.snyk.io>
TenantURL: <https://api.<tenant-name>.snyk.io>
 - "Project Tags": CMDBID
 - If a Snyk Project tag exists with the same key, such as "CMDBID," then the value of that tag is mapped with the source_app_id field in the CMDB table during the project import job.
 - If the tag is absent, then "project id"(unique ID) is mapped with the source_app_id field in the CMDB table.
 - "Page size for projects": 100
 - "Page size for SCA & IaC issues (US Region)": 1000
- Note:** "Page size for SCA & IaC issue" property will not be used in SAST and SCA & IaC Vulnerability Import (Rest API - All region) Integration.
- "Choose the API mechanism to fetch the SCA issues from Snyk(US region)."
 - **Important Note: Customers hosted in the us.snyk.io (AWS) region MUST use the REST APIs.**
 - There are two mechanisms for fetching SCA issues for the US region.

■ V1 API

- The V1 API has more options for filtering data to be imported, but it limits the number of projects that can be selected in the projects filter. You must use the REST API to apply a project filter for more than 1000 projects.

■ REST API

- Use this to fetch data for more than 1000 filtered projects.

- "Choose the API mechanism to fetch the IaC issues from Snyk(US region).

- **Important Note: Customers hosted in the us.snyk.io (AWS) region MUST use the REST APIs.**

- There are two mechanisms for fetching IaC issues for the US region.

■ V1 API

- The V1 API has more options for filtering data to be imported, but it limits the number of projects that can be selected in the projects filter. You must use the REST API to apply a project filter for more than 1000 projects.

■ REST API

- Use this to fetch data for more than 1000 filtered projects.

5. Provide the comma-separated project tag key to map the Snyk projects in the ServiceNow CMDB table. If a tag key is present on a project, that tag value will be used to map CI in discovered applications. For example, if "CMDBID: 1234" is present on a project, it will check scanned applications for any record with source_app_id as 1234. If found, it will map it to a newly created discovered application. Click the "save" button.

The screenshot shows the ServiceNow Global Setting page for the Snyk Vulnerability Integration. The left sidebar has a search bar with 'snyk' and a favorites section showing 'No Results'. The main content area has tabs for Favorites, History, Workspaces, Admin, and Global Setting. The Global Setting tab is active. It contains fields for 'Snyk base URL' (set to https://api.snyk.io), 'Project Tags' (set to CMDBID), 'Page size for Projects' (set to 100), 'Page size for SCA & IaC Issues(US Region)' (set to 1000), 'API mechanism for SCA issues' (set to V1), and 'API mechanism for IaC issues' (set to V1). A 'Save' button is at the bottom right.

3.5. Run Scheduled Script (Mandatory Step for fresh Install, Upgrades, and Cloned instances)

Note: Please follow the steps below to update the mandatory application registry details for authentication.

1. Navigate to System Definitions -> Scheduled Job.
2. Search for Update Oauth Registry And Integration Name.

Name	Active	Class	Updated	Run as
*Update Oauth Registry And Integration Name	Search	Search	Search	Search

3. Click on that record.
4. Click on the Execute Now button.

The screenshot shows the 'Update Oauth Registry And Integration Name' record in the 'Scheduled Script Execution' table. The 'Name' field is populated with the record's name. The 'Active' checkbox is checked. The 'Application' dropdown is set to 'Snyk Vulnerability Integration'. A note below the form states: 'For scheduled job types that require an entered time, you have the option to enter an associated time zone. If no time zone is selected, the job will run at the entered time in time zone of the user who entered the time. If 'Use System Time Zone' is selected, the entered time will run in the time zone of the instance running the job.' The 'Run' dropdown is set to 'On Demand'. The 'Run this script' section contains the following Groovy script:

```

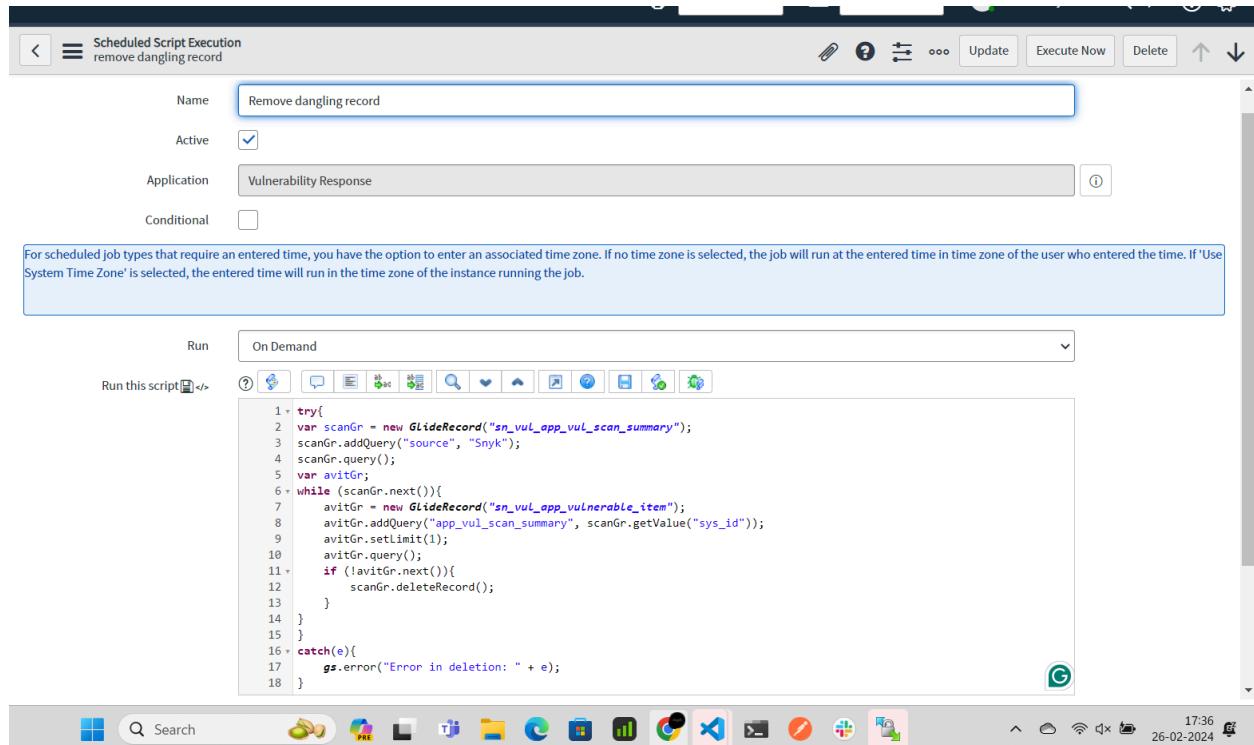
1  gs.info("Executing script to update Snyk oauth record.");
2  var authEntityGr = new GlideRecord("oauth_entity");
3  if (authEntityGr.getProperty("x_snyk2_snyk_vr_in.oauthEntitySysId")){
4      var redirectUrl = "https://" + gs.getProperty('instance_name') + ".service-now.com/oauth_redirect.do";
5      if (authEntityGr.redirect_url != redirectUrl){
6          authEntityGr.redirect_url = redirectUrl;
7      }
8      if (authEntityGr.client_id != gs.getProperty("x_snyk2_snyk_vr_in.clientId")){
9          authEntityGr.client_id = gs.getProperty("x_snyk2_snyk_vr_in.clientId");
10     }
11     if (authEntityGr.client_secret != gs.getProperty("x_snyk2_snyk_vr_in.clientSecret")){
12         authEntityGr.client_secret = gs.getProperty("x_snyk2_snyk_vr_in.clientSecret");
13     }
14 }

```

Note: the steps below are optional to delete dangling scan summary records from the table. From 2.0.0, we use `latest_issue_counts.update_at` from projects as scan summary id instead of introducedDate in the issue.

If upgrading the Snyk application from 1.x to 2.x, follow the steps below to delete dangling records of scan summaries after fetching the data from Snyk after upgrading the integration.

1. Navigate to System Definitions -> Scheduled Job
2. Create a new scheduled job
3. Fill in the other details based on the screenshot below. (**Ensure you create this script within the Vulnerability Response(VR) scope.**)



Here is the script

```

try{
  var scanGr = new GlideRecord("sn_vul_app_vul_scan_summary");
  scanGr.addQuery("source", "Snyk");
  scanGr.query();
  var avitGr;
  while (scanGr.next()){
    avitGr = new GlideRecord("sn_vul_app_vulnerable_item");
    avitGr.addQuery("app_vul_scan_summary", scanGr.getValue("sys_id"));
    avitGr.setLimit(1);
    avitGr.query();
    if (!avitGr.next()){
      scanGr.deleteRecord();
    }
  }
}
catch(e){
  gs.error("Error in deletion: " + e);
}

```

4. Click on the Execute Button to remove dangling scan summary records.

3.6. Generate REST/OAuth Token

Note: The steps below should be performed for AU and EU regions before generating a token.

1. Login to the ServiceNow instance.
2. Navigate to Snyk Security For AppVR -> Global Settings.
3. Please enter the base URL value according to the region of your Snyk platform.
4. Click on Save.

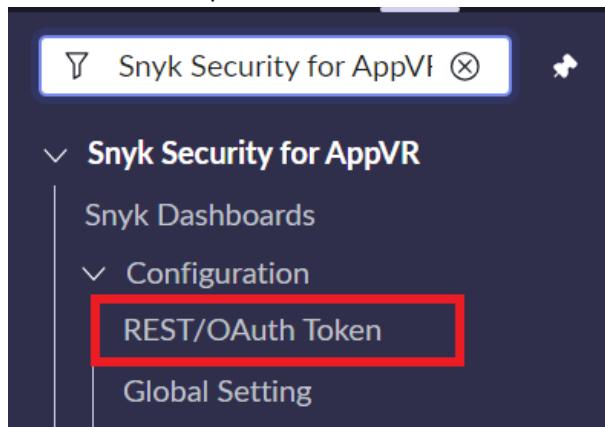
The screenshot shows the ServiceNow interface with the search bar containing 'snyk'. The left sidebar has a tree view under 'Snyk Security for AppVR' with nodes like 'Snyk Dashboards', 'Configuration', 'REST/OAuth Token', etc. The main content area is titled 'Global Setting' and contains several configuration fields. The 'Base URL' field is populated with 'https://api.snyk.io'. There are also fields for 'Project Tags' (CMDBID), 'Page size for Projects' (set to 100), 'Page size for SCA & IaC Issues (US Region)' (set to 1000), and dropdowns for 'SCA API mechanism' (set to V1) and 'IaC API mechanism' (set to V1). A 'Save' button is located at the bottom right of the form.

This section describes how to authorize Snyk Apps to fetch data from Snyk. This module will help the user generate the access token and regenerate a refresh token if either of the tokens expires.

Role Required: x_snyk2_snyk_vr_in.configure_integration, web_service_admin

Procedure:

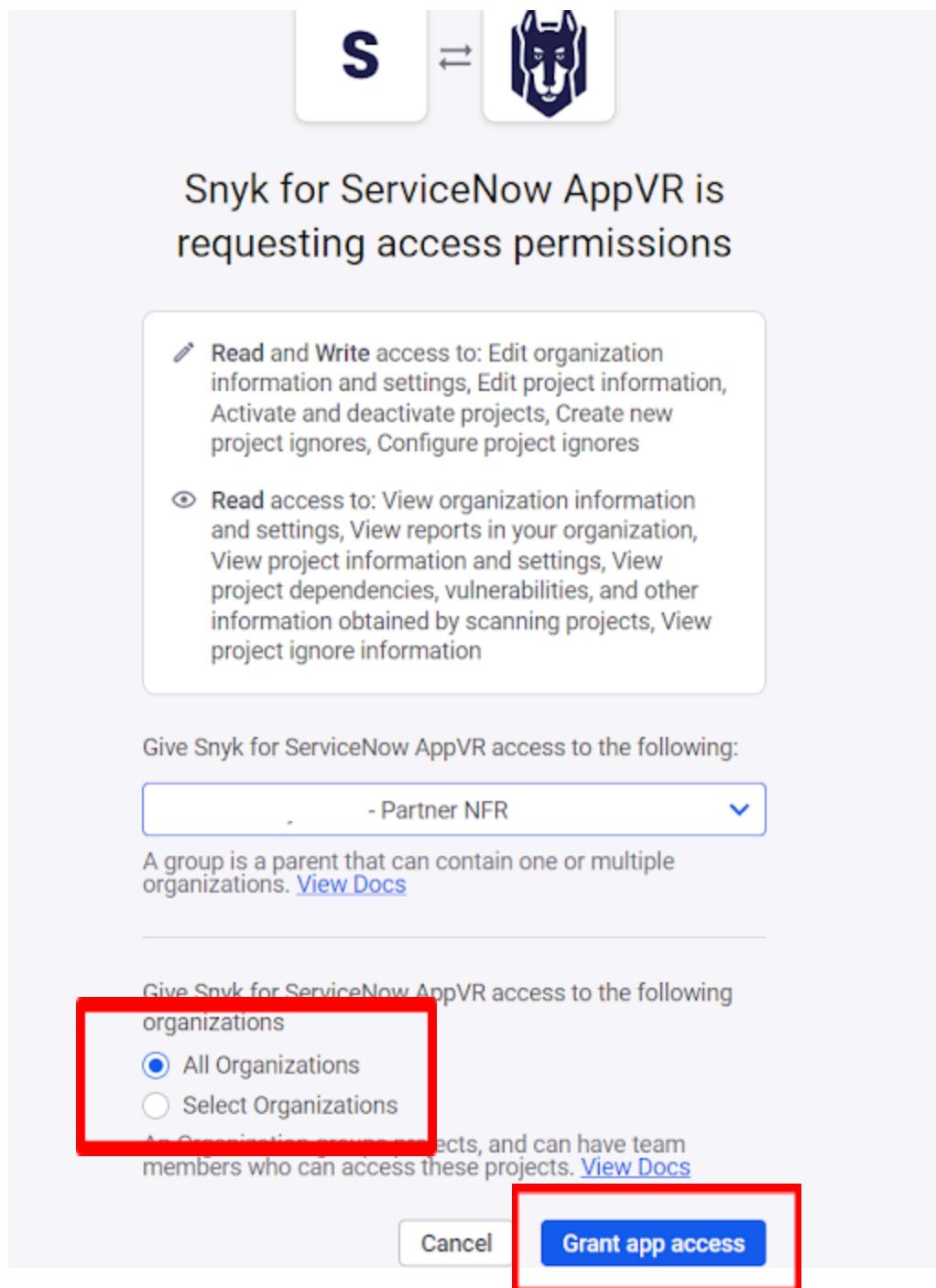
1. Login to the ServiceNow instance.
2. Navigate to "Snyk Security for AppVR."
3. Click on "Snyk Security for AppVR" under it, select "Configuration" and select "REST/OAuth Token" from the dropdown menu.



4. Click on the "Get OAuth Token" to generate the Access and Refresh tokens for the first time.
5. If the Refresh token expires, the user needs to follow all the steps from the beginning of this section to regenerate it.

The screenshot shows the 'REST Message' configuration page in ServiceNow. The 'Name' field is set to 'Snyk On Demand'. The 'Application' dropdown is set to 'Snyk VR Integration'. The 'Accessible from' dropdown is set to 'This application scope only'. The 'Endpoint' field contains the URL 'https://snyk.io/api/'. The 'Authentication' tab is selected, showing 'OAuth 2.0' as the authentication type and 'SnykOAuth default_profile' as the OAuth profile. A note states that authentication configured on the REST Message will automatically apply to child HTTP Methods. Below this, there is a 'Related Links' section with a red box around it, containing links for 'Get OAuth Token' and 'Get OAuth Token'.

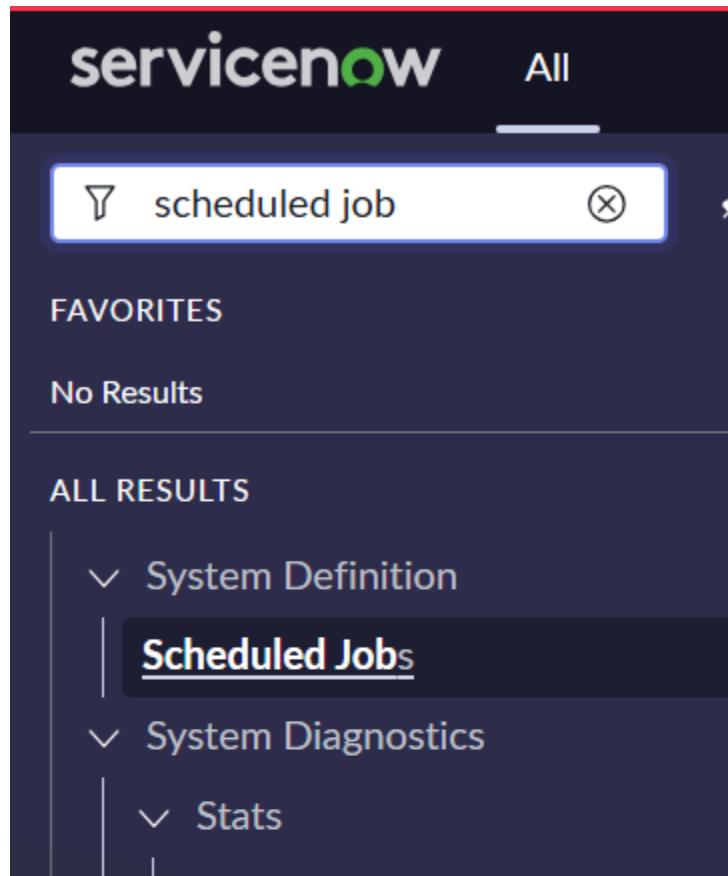
6. The system redirects the user to the Snyk App Authorization page after clicking "Get OAuth Token." Based on their requirements, users can provide access to all organizations or select a particular organization from the list.
7. To successfully authorize with Snyk Apps, the user must click "Grant app access."



Note: This screenshot is for illustrative purposes only, your tenant is not accessible by any third party.

3.7. Add IaC Scan Type for IaC issues in AVIT Table (Only if you want to fetch IaC Issues)

1. Navigate to Scheduled Jobs.

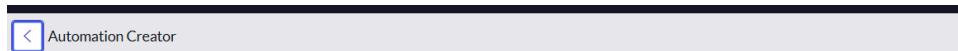


2. Click on the "New" button.

A screenshot of the ServiceNow web interface showing the "Scheduled Jobs" list. The top navigation bar includes "Favorites", "History", "Workspaces", "Admin", "Scheduled Jobs" (selected), and "New". The main content area shows a table with columns: Name, Active, Class, and Updated. The table lists several scheduled jobs:

Name	Active	Class	Updated
Active Learning	true	Scheduled Script Execution	2021-10-19 05:57:18
Activity Stream Reaper	true	Scheduled Script Execution	2020-05-14 04:41:59
ActSub - clean up activity stream	true	Scheduled Script Execution	2021-04-15 04:24:03
Add checkpoint descriptions	false	Scheduled Script Execution	2015-08-11 15:18:01
Add Identifier Fields In Recommended Rules	false	Scheduled Script Execution	2019-04-17 17:30:37

3. Click on Automatically run a script of your choosing.



4. Add details of every field as mentioned in the below image.

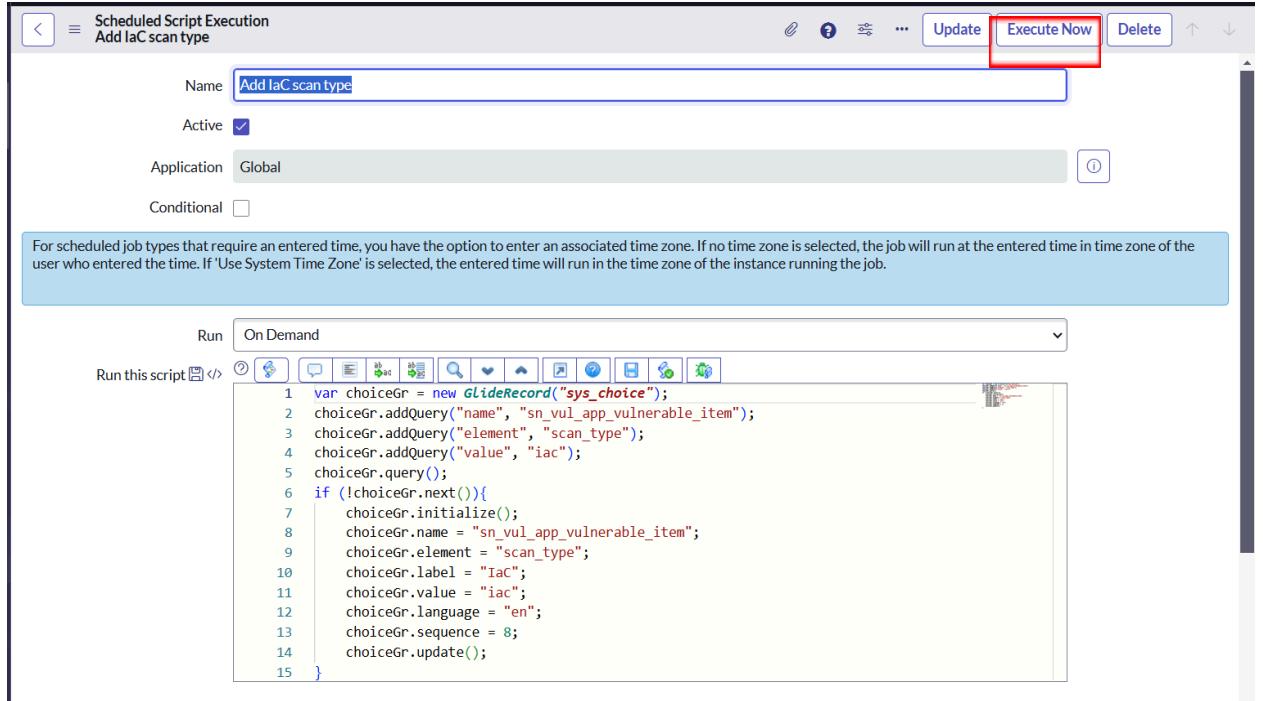
The screenshot shows the 'Scheduled Script Execution' page in ServiceNow. A yellow banner at the top says 'Please save record before pasting...'. The 'Name' field contains 'Add IaC scan type'. The 'Active' checkbox is checked. The 'Application' dropdown is set to 'Global'. The 'Conditional' checkbox is unchecked. The 'Run' dropdown is set to 'On Demand'. Below these settings is a 'Run this script' section with a copy icon. The script editor contains the following GlideScript code:

```
1 var choiceGr = new GlideRecord("sys_choice");
2 choiceGr.addQuery("name", "sn_vul_app_vulnerable_item");
3 choiceGr.addQuery("element", "scan_type");
4 choiceGr.addQuery("value", "iac");
5 choiceGr.query();
6 if (!choiceGr.next()){
7     choiceGr.initialize();
8     choiceGr.name = "sn_vul_app_vulnerable_item";
9     choiceGr.element = "scan_type";
10    choiceGr.label = "IaC";
11    choiceGr.value = "iac";
12    choiceGr.language = "en";
13    choiceGr.sequence = 8;
14    choiceGr.update();
15 }
```

5. Ensure the scope of your Application is **Global**.
6. Here is the script you can copy.

```
var choiceGr = new GlideRecord("sys_choice");
choiceGr.addQuery("name", "sn_vul_app_vulnerable_item");
choiceGr.addQuery("element", "scan_type");
choiceGr.addQuery("value", "iac");
choiceGr.query();
if (!choiceGr.next()){
    choiceGr.initialize();
    choiceGr.name = "sn_vul_app_vulnerable_item";
    choiceGr.element = "scan_type";
    choiceGr.label = "IaC";
    choiceGr.value = "iac";
    choiceGr.language = "en";
    choiceGr.sequence = 8;
    choiceGr.update();
}
```

7. Click on the Submit button.
8. Open the same scheduled job again and click on the Execute Now button.



4. Use Cases

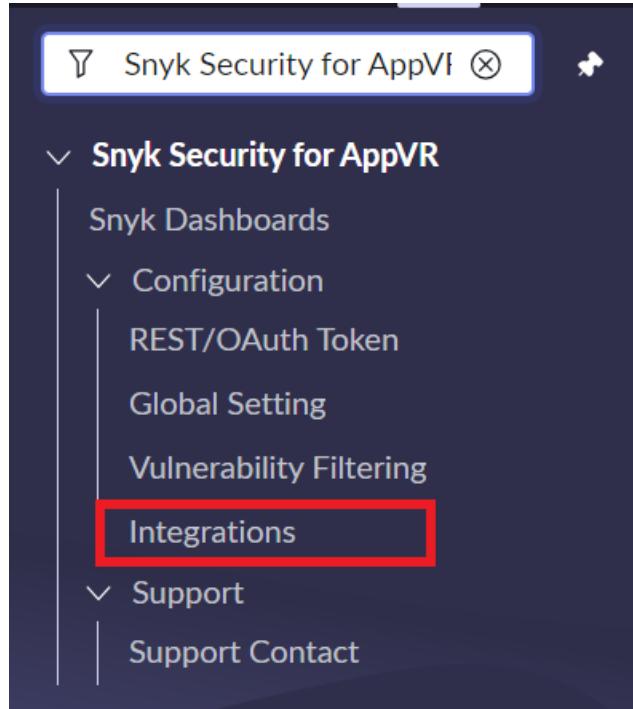
4.1. Fetch Projects from Snyk platform

"Snyk Security for AppVR" provides the functionality to fetch Projects from Snyk and populate them as an Application Release and Scanned Application in ServiceNow.

Role Required: x_snyk2_snyk_vr_in.configure_integration

Procedure:

1. Login to the ServiceNow instance.
2. Navigate to "Snyk Security for AppVR," and under it, select "Configuration."
3. Click on "Integrations."

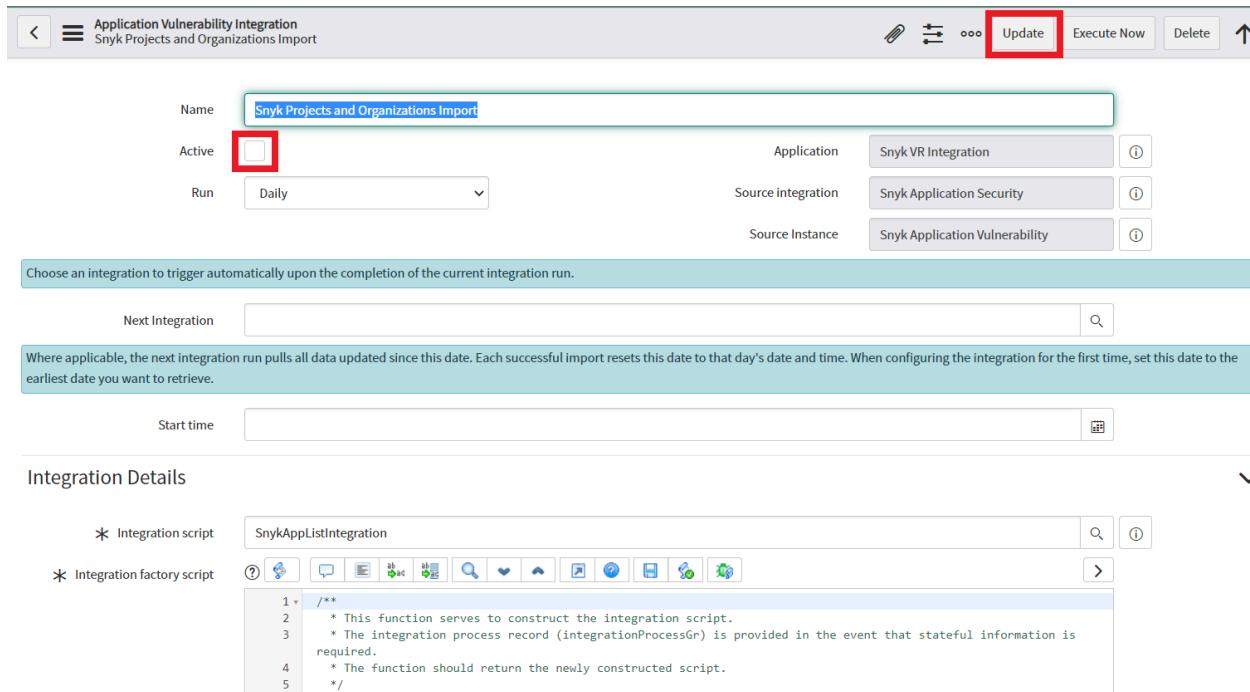


4. Select Integration with the name "Snyk Projects and Organizations Import" and the Source Instance value as the default provided by Integration Instance.

The screenshot shows a list view of 'Application Vulnerability Integrations' in ServiceNow. The table has the following columns:

Name	Active	Source Integration	Source Instance	Start time	Next Integration	Run as
Snyk Projects and Organizations Import	<input checked="" type="checkbox"/>	Snyk Application Security	Snyk Application Vulnerability	(empty)	(empty)	(empty)
Snyk SCA & IaC Fixed Vulnerabilities Import (US Region - V1 API)	<input type="checkbox"/>	Snyk Application Security	Snyk Application Vulnerability	2024-07-30 16:22:48	(empty)	(empty)
Snyk SCA & IaC Vulnerabilities Import (All Region - Rest API)	<input type="checkbox"/>	Snyk Application Security	Snyk Application Vulnerability	2024-12-17 00:00:00	(empty)	(empty)
Snyk SCA & IaC Vulnerabilities Import (US Region - V1 API)	<input type="checkbox"/>	Snyk Application Security	Snyk Application Vulnerability	2024-12-17 00:00:00	Snyk SCA & IaC Fixed Vulnerabilities Imp...	(empty)

5. Activate the checkbox "Active." Click on the button "Update."
6. There is no need for a Start time. This integration will always fetch all projects and organizations.



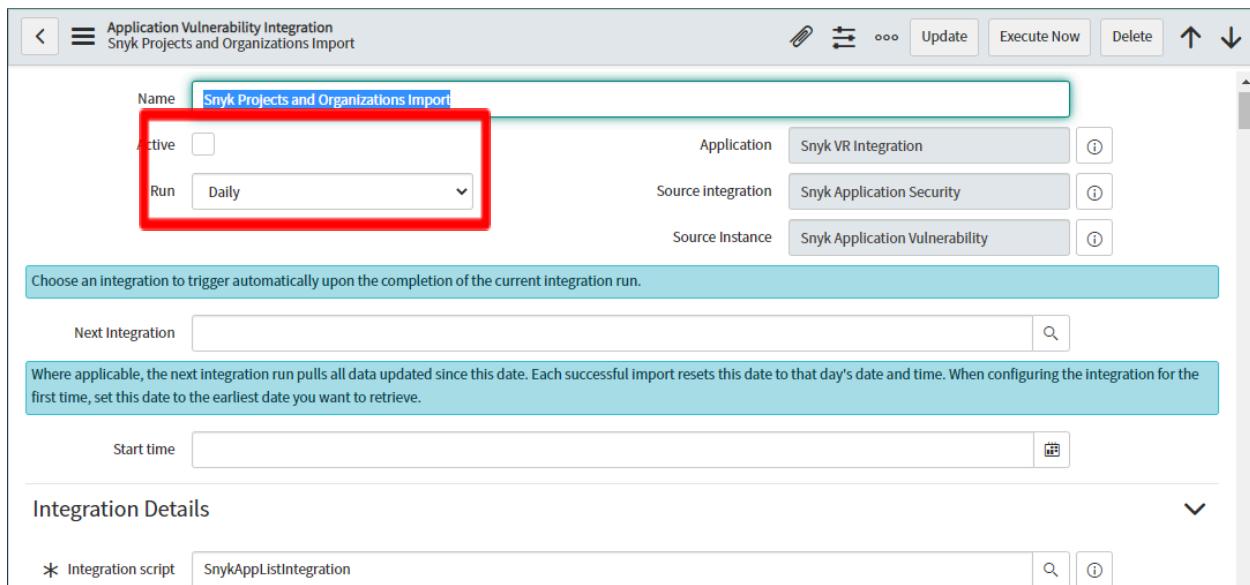
The screenshot shows the 'Application Vulnerability Integration' screen for 'Snyk Projects and Organizations Import'. The 'Update' button at the top right is highlighted with a red box. The 'Name' field contains 'Snyk Projects and Organizations Import'. The 'Active' checkbox is checked. The 'Run' dropdown is set to 'Daily'. The 'Application' is 'Snyk VR Integration', 'Source integration' is 'Snyk Application Security', and 'Source Instance' is 'Snyk Application Vulnerability'. A note below says: 'Choose an integration to trigger automatically upon the completion of the current integration run.' A 'Next Integration' search bar is present. A note below it says: 'Where applicable, the next integration run pulls all data updated since this date. Each successful import resets this date to that day's date and time. When configuring the integration for the first time, set this date to the earliest date you want to retrieve.' A 'Start time' input field is shown. The 'Integration Details' section shows the 'Integration script' is 'SnykAppListIntegration' with its code view:

```

/*
 * This function serves to construct the integration script.
 * The integration process record (integrationProcessGr) is provided in the event that stateful information is required.
 * The function should return the newly constructed script.
 */

```

- To fetch Projects according to a scheduled time interval, select the relevant option from the Run dropdown, set the Time, and click the "Update" button.



The screenshot shows the same integration configuration page. The 'Run' dropdown and 'Active' checkbox are highlighted with a red box. The rest of the interface is identical to the previous screenshot, including the 'Update' button at the top right.

- Open the Snyk Integration record. To fetch projects immediately, click on the "Execute Now" button.

Application Vulnerability Integration
Snyk Projects and Organizations Import

Name: Snyk Projects and Organizations Import

Active:

Run: Daily

Time: Hours 00 00 00

Application: Snyk VR Integration

Source integration: Snyk Application Security

Source Instance: Snyk Application Vulnerability

Choose an integration to trigger automatically upon the completion of the current integration run.

Next Integration:

Where applicable, the next integration run pulls all data updated since this date. Each successful import resets this date to that day's date and time. When configuring the integration for the first time, set this date to the earliest date you want to retrieve.

Start time:

Integration Details

* Integration script: SnykAppListIntegration

* Integration factory script:

```

1 /**
2  * This function serves to construct the integration script.
3  * The integration process record (integrationProcessGr) is provided in the event that stateful information is
4  * required.
5  * The function should return the newly constructed script.
6 */
(function(integrationProcessGr){

```

9. Imported projects will be visible as Application Release (sn_vul_app_release).
10. Users will have to provide the filter, as "Source" is "Snyk," and then click on "Run" to view all the projects fetched from Snyk.

Application Releases Search Application name ▼ Search

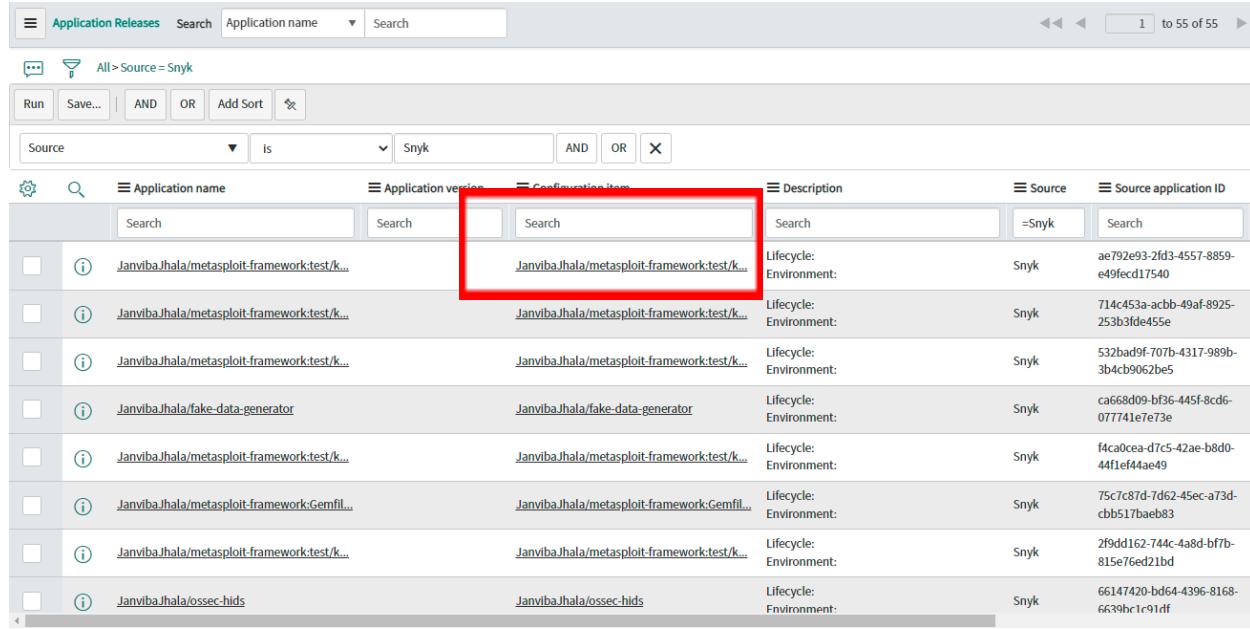
All > Source = Snyk

Run	Save...	AND	OR	Add Sort	✖
Source	Is	Snyk	ID	OR	✖

Application name Application version Configuration item Description Source Source application ID

JanvibaJhala/metasploit-framework:test/k...	JanvibaJhala/metasploit-framework:test/k...	Lifecycle: Environment:	Snyk	ae792e93-2fd3-45f7-8859-e49fec17540
JanvibaJhala/metasploit-framework:test/k...	JanvibaJhala/metasploit-framework:test/k...	Lifecycle: Environment:	Snyk	714c453a-acbb-49af-8925-253b3fde455e
JanvibaJhala/metasploit-framework:test/k...	JanvibaJhala/metasploit-framework:test/k...	Lifecycle: Environment:	Snyk	532bad9f-707b-4317-989b-3b4cb9062be5
JanvibaJhala/fake-data-generator	JanvibaJhala/fake-data-generator	Lifecycle: Environment:	Snyk	ca668d09-bf36-445f-8cd6-077741e7e73e
JanvibaJhala/metasploit-framework:test/k...	JanvibaJhala/metasploit-framework:test/k...	Lifecycle: Environment:	Snyk	f4ca0cea-d7c5-42ae-b8d0-44f1ef44ae49
JanvibaJhala/metasploit-framework:Gemfil...	JanvibaJhala/metasploit-framework:Gemfil...	Lifecycle: Environment:	Snyk	75c7c87d-7d62-45ec-a73d-cbb517baeb83
JanvibaJhala/metasploit-framework:test/k...	JanvibaJhala/metasploit-framework:test/k...	Lifecycle: Environment:	Snyk	2f9d162-744c-4a8d-bf7b-815e76ed21bd
JanvibaJhala/ossec-hids	JanvibaJhala/ossec-hids	Lifecycle: Environment:	Snyk	66147420-bd64-4396-8168-6639hr1c91nf

11. Click on Configuration Item to view the configuration item record.



The screenshot shows a ServiceNow search interface for 'Application Releases'. The search bar at the top has 'Search' and 'Application name' dropdowns. Below the search bar, there's a toolbar with 'Run', 'Save...', 'AND', 'OR', 'Add Sort', and a clear button. A filter bar below the toolbar shows 'All > Source = Snyk'. The main search results table has columns: 'Source' (dropdown), 'Is' (dropdown), 'Snyk' (text input), 'AND', 'OR', and a clear button. The results table has columns: 'Application name', 'Application version', 'Configuration item', 'Description', 'Source', and 'Source application ID'. The 'Source' column contains links to various Snyk findings. The 'Configuration item' column also contains links. The 'Source application ID' column shows unique identifiers. A red box highlights the 'Source' column header.

Source	Is	Snyk	AND	OR	X
Source	Is	Snyk	AND	OR	X
JanvibaJhala/metasploit-framework:test/k...	JanvibaJhala/metasploit-framework:test/k...	Search	Search	Search	Search
JanvibaJhala/metasploit-framework:test/k...	JanvibaJhala/metasploit-framework:test/k...	JanvibaJhala/metasploit-framework:test/k...	Lifecycle: Environment:	Snyk	ae792e93-2fd3-4557-8859-e49fec17540
JanvibaJhala/metasploit-framework:test/k...	JanvibaJhala/metasploit-framework:test/k...	JanvibaJhala/metasploit-framework:test/k...	Lifecycle: Environment:	Snyk	714c453a-acbb-49af-8925-253b3fde455e
JanvibaJhala/metasploit-framework:test/k...	JanvibaJhala/metasploit-framework:test/k...	JanvibaJhala/metasploit-framework:test/k...	Lifecycle: Environment:	Snyk	532bad9f-707b-4317-989b-3b4cb9062be5
JanvibaJhala/fake-data-generator	JanvibaJhala/fake-data-generator	JanvibaJhala/fake-data-generator	Lifecycle: Environment:	Snyk	ca668d09-bf36-445f-8cd6-077741e7e73e
JanvibaJhala/metasploit-framework:test/k...	JanvibaJhala/metasploit-framework:test/k...	JanvibaJhala/metasploit-framework:test/k...	Lifecycle: Environment:	Snyk	f4ca0cea-d7c5-42ae-b8d0-44f1ef44ae49
JanvibaJhala/metasploit-framework:Gemfil...	JanvibaJhala/metasploit-framework:Gemfil...	JanvibaJhala/metasploit-framework:Gemfil...	Lifecycle: Environment:	Snyk	75c7c87d-7d62-45ec-a73d-cbb517baeb33
JanvibaJhala/metasploit-framework:test/k...	JanvibaJhala/metasploit-framework:test/k...	JanvibaJhala/metasploit-framework:test/k...	Lifecycle: Environment:	Snyk	2f9dd162-744c-4a8d-bf7b-815e76ed21bd
JanvibaJhala/ossec-hids	JanvibaJhala/ossec-hids	JanvibaJhala/ossec-hids	Lifecycle: Environment:	Snyk	66147420-bd64-4396-8168-6639hr1r91nf

4.2. Vulnerability Filtering

This section describes how to use filters to define which categories of issues to be imported from Snyk.

Note: The filters below do not work for Snyk Projects and Organizations Import integration.

Role Required: x_snyk2_snyk_vr_in.configure_integration

Filters:

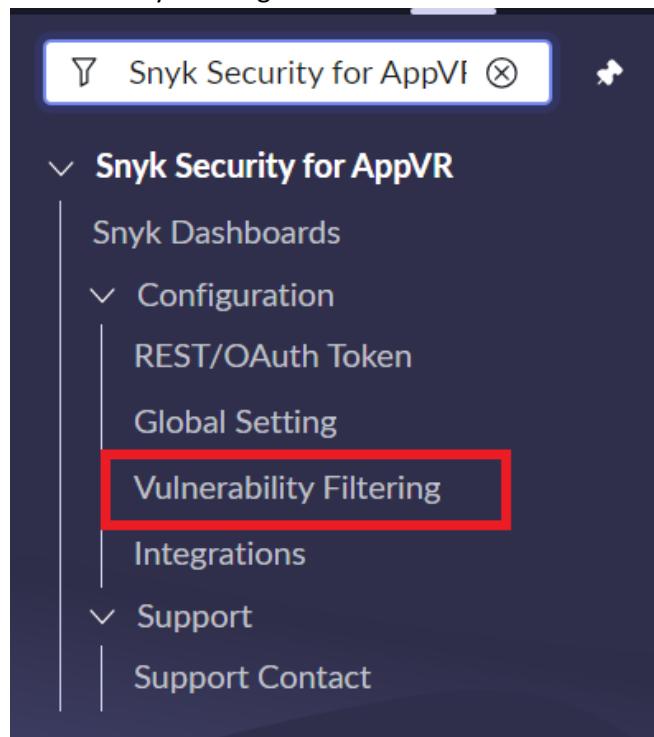
- 1) Organization
- 2) Projects
- 3) Projects Query
- 4) Project Type
- 5) Lowest Severity
- 6) Ignored
- 7) Minimum Priority Score
- 8) Maximum Priority Score
- 9) IsUpgradable
- 10) IsPatchable
- 11) IsFixed
- 12) Branch
- 13) Target Name
- 14) Environment
- 15) Lifecycle
- 16) Languages

- 17) Exploit Maturity
- 18) Source
- 19) Tags
- 20) Patched
- 21) Fixable
- 22) IsPinnable
- 23) Status
- 24) SCA IsFixable Condition

Note: If you're transitioning Snyk from version 1.1.0 to 3.x, it's necessary to execute the Snyk Projects and Organizations Import to access the benefits of the **Branch, Target Name, Environment, Lifecycle, and Tags** filter.

Procedure:

1. Login to the ServiceNow instance.
2. Navigate to "Snyk Security for AppVR" and select "Configuration."
3. Click on "Vulnerability Filtering."



4. The Vulnerability Filtering form view gets opened with a default value for Lowest Severity as "Low," and a default value for Ignored, IsUpgradable, IsPatchable, Patched, Fixable, IsPinnable, IsFixed as "All," and the "Status" field is used for the SAST type issues/Vulnerability.
5. For the SAST integration, Ignored, Severity, and Status fields are used to filter the issues/Vulnerability.

The screenshots illustrate the configuration of the Snyk Security for Application Vulnerability Response integration in ServiceNow. Both screens show the 'Vulnerability Filtering' page, which was created on 2022-07-13 00:14:09.

Top Screenshot (Detailed Filtering):

- Filtering capabilities for each integrations are as below:**
 - Snyk Projects and Organizations Import integration will obtain all projects and organizations from Snyk based on the access privileges assigned during the OAuth token generation process.
 - Snyk SCA & IaC Fixed Vulnerabilities Import (US Region - V1 API) supports: Organizations, Lowest Severity, Projects, Branch, Target Name, Environment, Lifecycle, Source, Tags, Minimum priority score, Maximum priority score, IsPatchable, Ignored, IsPinnable, IsUpgradable, IsFixed, patched, Fixable, Exploit Maturity, Languages. IaC Issues do not support Languages and Exploit Maturity filter.
 - Snyk SCA & IaC Vulnerabilities Import (All Region - Rest API) supports: Organizations, Lowest Severity, Projects, Branch, Target Name, Environment, Lifecycle, Source, Tags, Minimum priority score, Maximum priority score, IsPatchable, Ignored, IsUpgradable, IsFixableManually, IsFixableSnyk, IsFixableUpstream
 - Snyk SAST Vulnerabilities Import supports: Organizations, Lowest Severity, Projects, Branch, Target Name, Environment, Lifecycle, Source, Tags, Ignored, Status
 - Note: If you want to get data from ALL Organizations or ALL Projects or ALL Languages or ALL Exploit Maturity categories, do NOT select all values within the filter. This logic is applicable to all the filters. When multiple filters are applied, they adhere to an AND condition, whereas the same filter with distinct values follows an OR condition.
- Filtering Options:**
 - Organizations:** Projects Query, Add Filter Condition, Add "OR" Clause, choose field, oper, value.
 - Projects:** Branch, Project Type, Languages, Exploit Maturity, Target Name, Environment, Lifecycle.
 - Other Filters:** Lowest Severity (Low), Ignored (All), Minimum Priority Score, Maximum Priority Score, IsUpgradable (All), IsPatchable (All), IsFixed (All).

Bottom Screenshot (Simplified Filtering):

- Filtering Options:**
 - Minimum Priority Score, Maximum Priority Score, IsUpgradable (All), IsPatchable (All), IsFixed (All), IsPinnable (All), Patched (All), Status (All).
 - SCA IsFixable Condition:** Add Filter Condition, Add "OR" Clause, choose field, oper, value.
 - Manage exceptions in ServiceNow:** Manage exceptions in ServiceNow checkbox.
 - Manage false positives in ServiceNow:** Manage false positives in ServiceNow checkbox.

6. Users can reset the filters by clicking on the **Reset to Default** button.

The screenshot shows the ServiceNow interface with the search bar containing 'snyk'. The left sidebar is expanded, showing the 'Snyk Security for AppVR' integration under 'ALL RESULTS'. The main area displays the 'Vulnerability Filtering' record, which was created on 2022-07-13 00:14:09. The record details the filtering capabilities for Snyk integrations, mentioning various import types and their supported fields like Organizations, Projects, Branch, Target Name, Environment, Lifecycle, Source, Tags, Languages, and Exploit Maturity. The 'Update' button at the top right of the record view is highlighted with a red box.

7. Users can update the existing record. Change the existing details and click on the update button.

This screenshot is identical to the one above, showing the 'Vulnerability Filtering' record in ServiceNow. The 'Update' button is again highlighted with a red box, indicating the step where users change existing details and click to update the record.

8. Organizations, Projects, Languages, Branch, Target Name, Environment, Lifecycle, Exploit Maturity, Tags, and Source Filters can be modified by clicking the Lock button.

The screenshot shows the ServiceNow interface with the search bar containing 'snyk'. The left sidebar has a 'Snyk Security for AppVR' section expanded, showing various integration options like 'Snyk Dashboards', 'Configuration', 'Support', 'Privacy Policy', etc. The main content area is titled 'Vulnerability Filtering - Created 2022-07-13 00:14:09'. It includes a note about filtering capabilities and a form for setting filters. The 'Organizations' dropdown in the filter section is highlighted with a red box and contains a lock icon.

9. If users want to select a single organization or project from the list, they must click on the icon below.

This screenshot is similar to the previous one but focuses on the 'Select target record' buttons. Two red boxes highlight these buttons for both the 'Organizations' and 'Projects' dropdowns. These buttons also feature lock icons, indicating they are reference fields.

10. Clicking on the above icon will open up the list of organizations and projects from which users can select organizations and projects one at a time.

11. Select a value from the Target reference to filter the Vulnerable item ingestion.

The screenshot shows a ServiceNow interface titled 'Snyk Organizations'. The search bar at the top contains the query 'Crest Data Systems NFR - Shared'. Below the search bar, the results are displayed in a table with two columns: 'Organization Name' and 'Organization Id'. The first result, 'Crest Data Systems NFR - Shared', is highlighted with a red box.

Organization Name	Organization Id
Crest Data Systems NFR - Shared	8f793725-eddf-4c7b-81e7-aa8546bd7df9
Crest Test Org #1	63782260-073a-4bb6-9e5f-8c74804ec79e
Crest Test Org #3	10d65a79-2862-4093-94f1-51b7e34d83fc
Crest Test Org #2	b37c6d78-198f-411d-9958-8b5dd07f99ca

12. The selected organization and project will be visible to the user on the Vulnerability Filtering page as below.
13. If you want to fetch issues from all organizations and projects, leave the value empty. If selecting the projects filter, ensure it does not exceed 1000 projects. Refer to this [link](#) for more information about the issue API filtering.

The screenshot shows the 'Vulnerability Filtering' page. At the top, there is a note: 'Filtering capabilities for each integrations are as below.' Below this, a list of supported imports is provided. Further down, there are two dropdown menus: 'Organizations' and 'Projects'. The 'Organizations' dropdown is expanded, showing a list of organizations. The entry 'Crest Data Systems NFR - Shared' is highlighted with a red box.

Filtering capabilities for each integrations are as below.

- Snyk Projects and Organizations Import integration will obtain all projects and organizations from Snyk based on the access privileges assigned during the OAuth token generation process.
- Snyk SCA & IaC/SCA & IaC Fixed Vulnerabilities Import (US Region - V1 API) supports: Organizations, Lowest Severity, Projects, Branch, Target Name, Environment, Lifecycle, Source, Tags, Minimum priority score, Maximum priority score, Ispatchable, Ignored, Ispinable, IsUpgradable, IsFixed, patched, Fixable, Exploit Maturity, Languages. IaC issues do not support Languages and Exploit Maturity filter.
- Snyk SCA & IaC Vulnerabilities Import (All Region - Rest API) supports: Organizations, Lowest Severity, Projects, Branch, Target Name, Environment, Lifecycle, Source, Tags, Minimum priority score, Maximum priority score, Ispatchable, Ispinable, Ignored, IsUpgradable, IsFixableManually, IsFixableSnyk, IsFixableUpstream
- Snyk SAST Vulnerabilities Import supports: Organizations, Lowest Severity, Projects, Branch, Target Name, Environment, Lifecycle, Source, Tags, Ignored, Status
- Note: If you want to get data from ALL Organizations or ALL Projects or ALL Languages or ALL Exploit Maturity categories, do NOT select all values within the filter. This logic is applicable to all the filters. When multiple filters are applied, they adhere to an AND condition, whereas the same filter with distinct values follows an OR condition.

14. If users want to select multiple organizations or projects from the list, they must click the icon below.

Filtering capabilities for each integrations are as below.

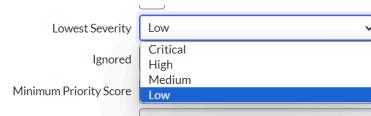
- Snyk Projects and Organizations Import integration will obtain all projects and organizations from Snyk based on the access privileges assigned during the OAuth token generation process.
- Snyk SCA & IaC/SCA & IaC Fixed Vulnerabilities Import (US Region - V1 API) supports: Organizations, Lowest Severity, Projects, Branch, Target Name, Environment, Lifecycle, Source, Tags, Minimum priority score, Maximum priority score, Ispatchable, Ignored, Ispinable, IsUpgradable, IsFixed, patched, Fixable, Exploit Maturity, Languages. IaC issues do not support Languages and Exploit Maturity filter.
- Snyk SCA & IaC Vulnerabilities Import (All Region - Rest API) supports: Organizations, Lowest Severity, Projects, Branch, Target Name, Environment, Lifecycle, Source, Tags, Minimum priority score, Maximum priority score, Ispatchable, Ispinable, Ignored, IsUpgradable, IsFixableManually, IsFixableSnyk, IsFixableUpstream
- Snyk SAST Vulnerabilities Import supports: Organizations, Lowest Severity, Projects, Branch, Target Name, Environment, Lifecycle, Source, Tags, Ignored, Status
- Note: If you want to get data from ALL Organizations or ALL Projects or ALL Languages or ALL Exploit Maturity categories, do NOT select all values within the filter. This logic is applicable to all the filters. When multiple filters are applied, they adhere to an AND condition, whereas the same filter with distinct values follows an OR condition.

15. Users can select multiple values from the list on the left-hand side, click on ">" to move them into the selected list, and then click on the Save button, and vice versa.

16. Users can use the Project Query filter to define conditions based on Organizations, Projects, Branch, Source, Target Name, Environment, Lifecycle, and Tags. Dot-walking to reference fields is also supported.

The screenshot shows the 'Vulnerability Filtering' page in ServiceNow. At the top, there's a note about Snyk API support and a note about ignoring all values. Below that, there are two tabs: 'Organizations' and 'Projects'. Under 'Projects Query', there's a search bar with 'Demo #1' and a dropdown menu for 'Organization Name' which is currently set to 'Organization Name'. To the right, there's a note about activating Windows.

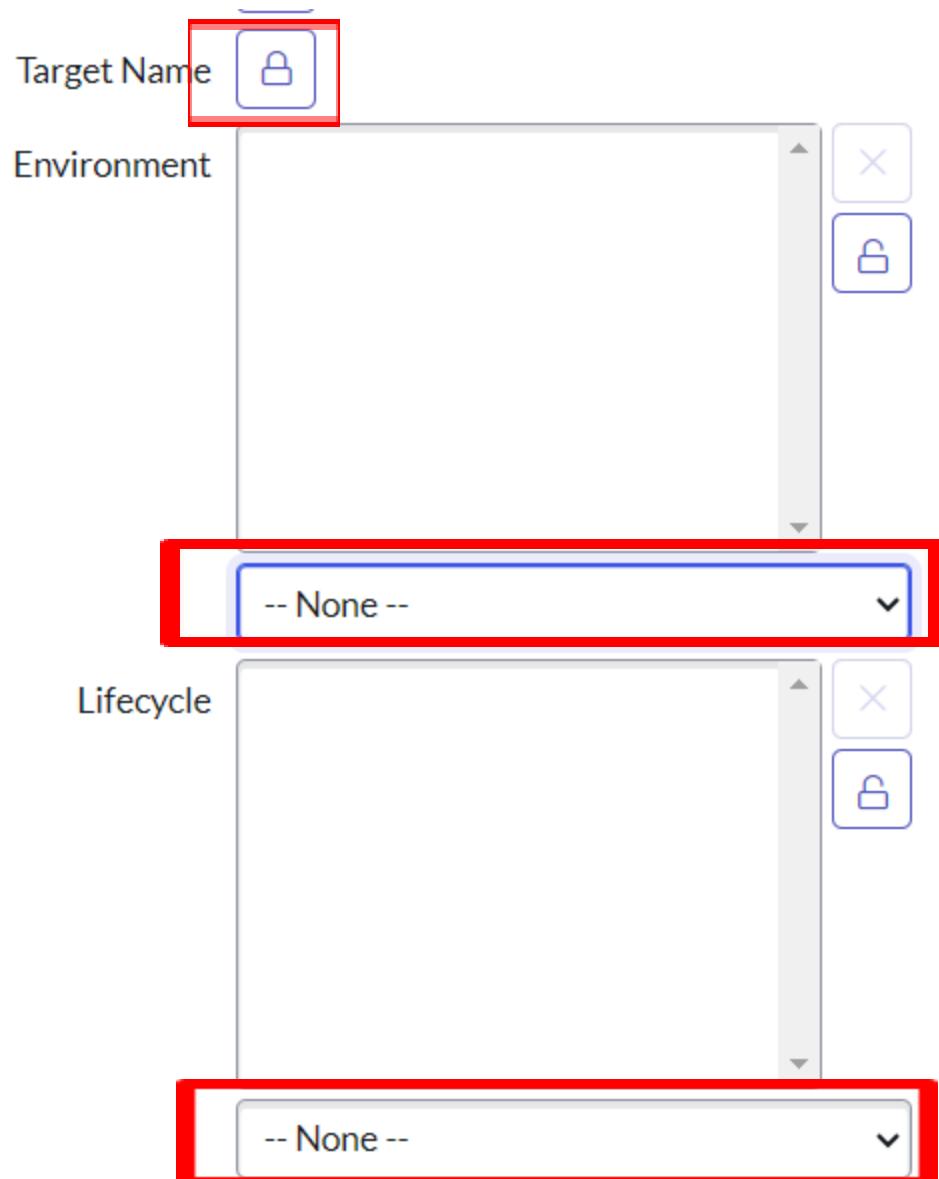
17. Users can select the severity from the dropdown of the lowest severity by clicking on the dropdown list.



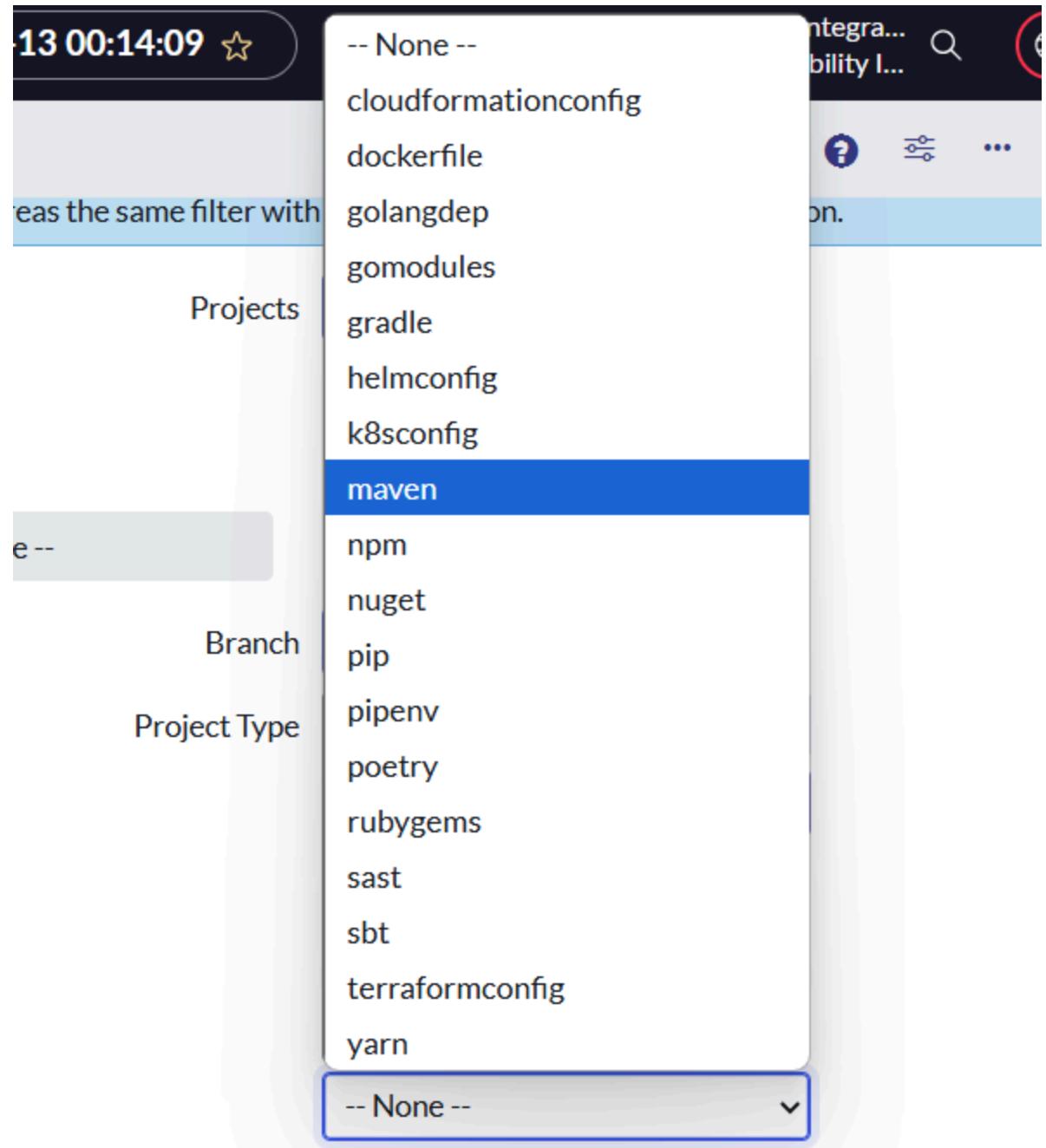
18. Users can select the Ignore, IsUpgradable, IsPatchable, Patched, Fixable, IsPinnable, and IsFixed values from the dropdown by clicking on the dropdown list.



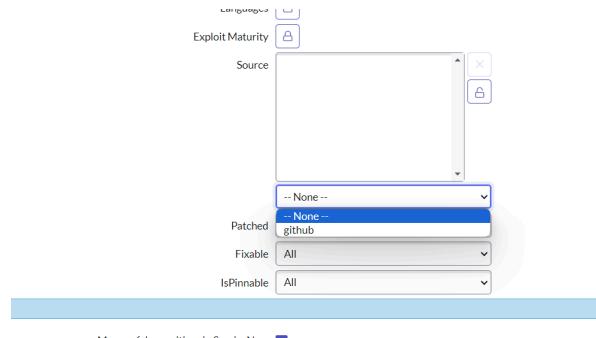
19. Users can select the Branch, Target Name, Environment, and Lifecycle value from the choices.



20. Users can select the Project Type value from the Project Type choices by clicking on the list.

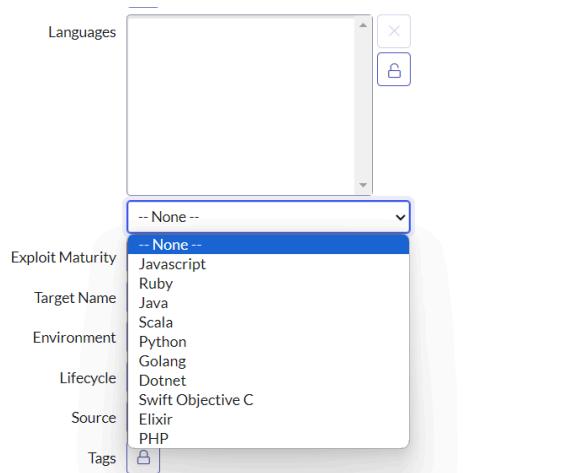


21. Users can select the Source value from the Source choices by clicking on the list.

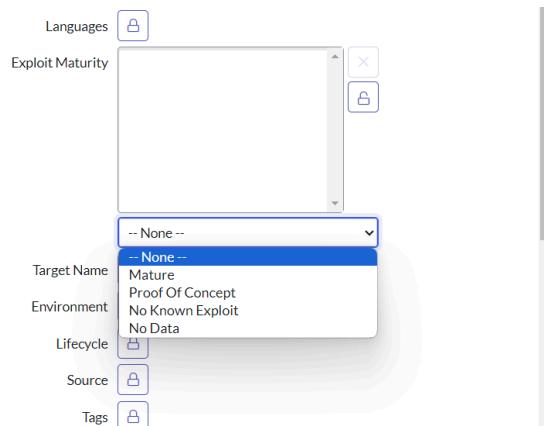


22. Users can provide values in Minimum Priority Score and Maximum Priority Score based on their requirements.
23. Users can select the Languages value from the Languages choices by clicking on the Choices list.

Note: If the languages are not selected, the integration will fetch data for all the languages shown in the dropdown.



24. Users can select the Exploit Maturity value from the choices of Exploit Maturity by clicking on the Choices list.



25. Users can select one of the isFixable types to filter when using the SCA REST Integration.

Note: Only the "is" operator is allowed.

The screenshot shows a configuration screen for 'SCA IsFixable Condition'. At the top, there are buttons for 'Add Filter Condition' and 'Add "OR" Clause'. Below these are dropdown menus for 'choose field', 'oper', and 'value'. A search bar is present. A dropdown menu is open, showing options like 'IsFixableManually', 'IsFixableSnyk', and 'IsFixableUpstream'. A checkbox 'Manage false positives in ServiceNow' is checked. The background shows other configuration sections like 'Manage exceptions in ServiceNow'.

26. If the Filtering has more than 1000 projects and User is using V1 API than Configuration will throw an error “The selected filter includes more than 1,000 projects. Please update the filter or use the REST mechanism to retrieve SCA and IaC issues.”

The screenshot shows the 'Vulnerability Filtering' configuration page. It includes a header with 'Created 2022-07-13 00:14:09' and buttons for 'Update' and 'Reset to Default'. Below the header are two error messages: 'The selected filter includes more than 1,000 projects. Please update the filter or use the REST mechanism to retrieve SCA and IaC issues' and 'Invalid update'. A note below explains filtering capabilities: 'Filtering capabilities for each integrations are as below.' It lists supported imports for Snyk Projects, SCA & IaC, and SAST, noting that IaC issues do not support Languages and Exploit Maturity filters. It also notes that if multiple filters are applied, they adhere to an AND condition, whereas the same filter with distinct values follows an OR condition. The main configuration area shows fields for 'Organizations' and 'Projects', with a 'Projects Query' section containing dropdowns for 'choose field', operators, and values, along with 'OR' and 'AND' buttons. Other filters include 'Lowest Severity', 'Branch', 'Project Type', and an 'Activate Windows' link.

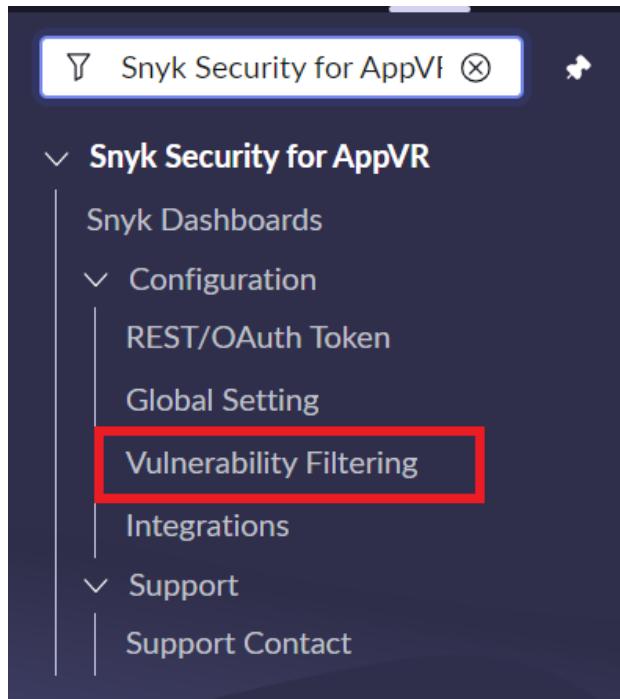
4.3. Managing Exceptions in ServiceNow

This section describes how to use "Managing in ServiceNow" to define the state of issues to be imported from Snyk.

Role Required: x_snyk2_snyk_vr_in.configure_integration

Procedure:

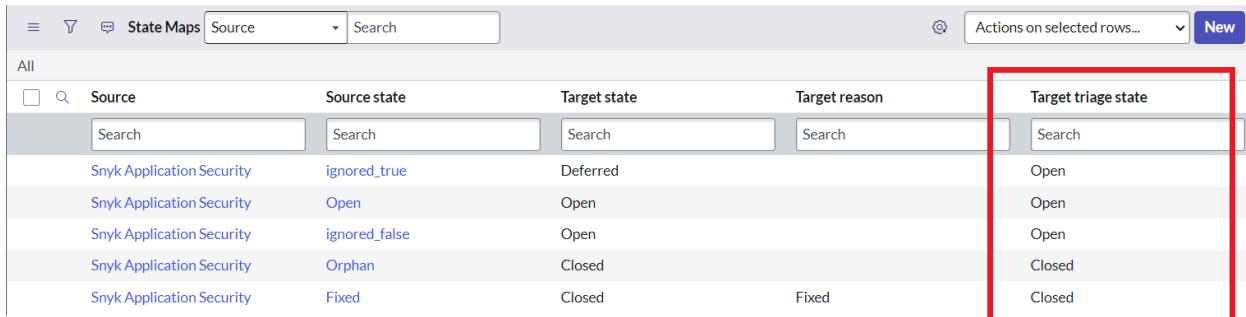
1. Login to the ServiceNow instance.
2. Navigate to "Snyk Security for AppVR" and select "Configuration."
3. Click on "Vulnerability Filtering."



4. Users can select "Manage exceptions in ServiceNow" and "Manage false positives in ServiceNow" by clicking on the checkbox and selecting the update button to update the vulnerability filtering form, as shown below.

The screenshot shows the 'Vulnerability Filtering' configuration page. At the top, it displays the title 'Vulnerability Filtering' and the creation date 'Created 2022-07-13 00:14:09'. Below the title are several filter options: 'Minimum Priority Score' (text input), 'Maximum Priority Score' (text input), 'IsUpgradable' (dropdown: All), 'IsPatchable' (dropdown: All), 'IsFixed' (dropdown: All), 'IsPinnable' (dropdown: All), 'Patched' (dropdown: All, with 'Organizations' selected), 'Status' (dropdown: All), 'Languages' (button with lock icon), 'Exploit Maturity' (button with lock icon), 'Target Name' (button with lock icon), 'Environment' (button with lock icon), 'Lifecycle' (button with lock icon), 'Source' (button with lock icon), 'Tags' (button with lock icon), and 'Fixable' (dropdown: All). Below these filters are buttons for 'Add Filter Condition' and 'Add "OR" Clause'. A note at the bottom says 'Select these options to manage exceptions and false positives in ServiceNow.' At the bottom of the page are two checkboxes: 'Manage exceptions in ServiceNow' (checked) and 'Manage false positives in ServiceNow' (checked). There are also 'Update' and 'Reset to Default' buttons.

5. If the user selects the "Manage exceptions in ServiceNow" checkbox and imports an issue, then the AVIT created will have the state mapping for the "Target triage state" as shown below:



The screenshot shows a ServiceNow State Maps interface. The top navigation bar includes 'State Maps', 'Source' (selected), and a search bar. On the right, there are buttons for 'Actions on selected rows...' and 'New'. The main area is titled 'All' and contains a table with columns: Source, Source state, Target state, Target reason, and Target triage state. A red box highlights the 'Target triage state' column, which lists 'Open', 'Open', 'Open', 'Closed', and 'Closed' corresponding to the rows.

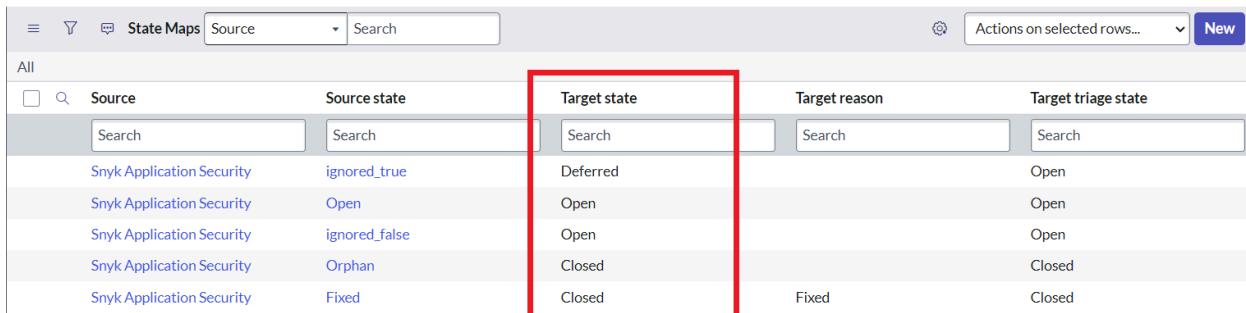
Source	Source state	Target state	Target reason	Target triage state
Snyk Application Security	ignored_true	Deferred		Open
Snyk Application Security	Open	Open		Open
Snyk Application Security	ignored_false	Open		Open
Snyk Application Security	Orphan	Closed		Closed
Snyk Application Security	Fixed	Closed	Fixed	Closed

- If the user does not select the "Manage exceptions in ServiceNow" checkbox and imports an issue, the AVIT created will have the state mapping for "Target state," as shown below.

7. Approve requests in the Vulnerability:

- "Manage exceptions in ServiceNow" and "Manage false positives" in ServiceNow. These options are available under Vulnerability Filtering. If the checkboxes are selected, buttons will be visible on the Vulnerability Item form to initiate the action. Once clicked on the button to run the action, a request is sent for approval to the user/group defined in the approval workflow.
- Please review the link for more information - <https://docs.servicenow.com/bundle/washingtondc-security-management/page/product/vulnerability-response/task/vr-ws-approve-requests.html>.

- Note: The functional details are mentioned in sections 6.3.3 and 6.3.4



The screenshot shows a ServiceNow State Maps interface. The top navigation bar includes 'State Maps', 'Source' (selected), and a search bar. On the right, there are buttons for 'Actions on selected rows...' and 'New'. The main area is titled 'All' and contains a table with columns: Source, Source state, Target state, Target reason, and Target triage state. A red box highlights the 'Target state' column, which lists 'Deferred', 'Open', 'Open', 'Closed', and 'Closed' corresponding to the rows.

Source	Source state	Target state	Target reason	Target triage state
Snyk Application Security	ignored_true	Deferred		Open
Snyk Application Security	Open	Open		Open
Snyk Application Security	ignored_false	Open		Open
Snyk Application Security	Orphan	Closed		Closed
Snyk Application Security	Fixed	Closed	Fixed	Closed

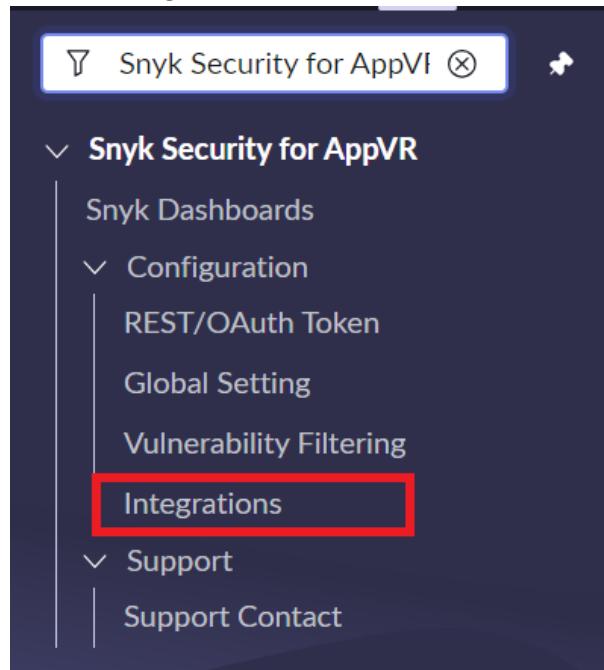
4.4. Fetch SAST Issues from the Snyk platform.

Note: This integration is standard for fetching SAST data from any region, i.e., AU, EU, or US. "Snyk Security for AppVR" provides the functionality to fetch SAST Issues and their details from Snyk and populate them as Vulnerability, Application Vulnerable Item, and Application Scan Summary in ServiceNow.

Role Required: x_snyk2_snyk_vr_in.configure_integration

Procedure:

1. Login to the ServiceNow instance.
2. Navigate to "Snyk Security for AppVR," and under it, select "Configuration."
3. Click on "Integrations."



4. Select Integration with the name "Snyk SAST Vulnerabilities Import" and Source Instance value as default provided integration instance.

Application Vulnerability Integrations							
	Name	Active	Source integration	Source Instance	Start time	Next Integration	Run as
All > Source integration = Snyk Application Security							
<input type="checkbox"/>	Search	<input type="button" value="Search"/>	<input type="button" value="=Snyk Application Secr"/>	<input type="button" value="Search"/>	<input type="button" value="Search"/>	<input type="button" value="Search"/>	<input type="button" value="Search"/>
	Snyk Projects and Organizations Import	false	Snyk Application Security	Snyk Application Vulnerability	(empty)	(empty)	(empty)
<input checked="" type="checkbox"/>	Snyk SAST Vulnerabilities Import	false	Snyk Application Security	Snyk Application Vulnerability	2024-07-30 16:22:48	(empty)	(empty)
	Snyk SCA & IaC Fixed Vulnerabilities Import (US Region - V1 API)	false	Snyk Application Security	Snyk Application Vulnerability	2024-12-17 00:00:00	(empty)	(empty)
	Snyk SCA & IaC Vulnerabilities Import (All Region - Rest API)	false	Snyk Application Security	Snyk Application Vulnerability	(empty)	(empty)	(empty)
	Snyk SCA & IaC Vulnerabilities Import (US Region - V1 API)	false	Snyk Application Security	Snyk Application Vulnerability	2024-12-17 00:00:00	Snyk SCA & IaC Fixed Vulnerabilities Imp...	(empty)

5. Activate the checkbox "Active." Click on the button "Update."
6. You must change the start time system property if you want to change the start time. By default, it will fetch all the code issues from Snyk.

The screenshot shows the 'Application Vulnerability Integration' screen. At the top, there are buttons for Back, Forward, Refresh, and a toolbar with icons for Update, Execute Now, Delete, and others. A message at the top says 'You are editing this record in update set Hima Javiya (cancel)'. Below this, the 'Name' field is set to 'Snyk SAST Vulnerabilities Import'. The 'Active' checkbox is unchecked. The 'Run' dropdown is set to 'Daily'. On the right, there are fields for 'Application' (Snyk Vulnerability Integration), 'Source integration' (Snyk Application Security), and 'Source Instance' (Snyk Application Vulnerability). A note below says 'Choose an integration to trigger automatically upon the completion of the current integration run.' A 'Next Integration' search bar is present. A detailed note states: 'Where applicable, the next integration run pulls all data updated since this date. Each successful import resets this date to that day's date and time. When configuring the integration for the first time, set this date to the earliest date you want to retrieve.' Under 'Integration Details', there is a section for 'Integration script' named 'SnykSastVulnIntegration' and a larger section for 'Integration factory script' containing the following code:

```

1+ /**
2 * This function serves to construct the integration script.
3 * The integration process record (integrationProcessGr) is provided in the event that stateful information is
4 * required.
5 * The function should return the newly constructed script.

```

7. Open the Snyk SAST Integration record. To fetch issues currently, click on the "Execute Now" button.

This screenshot is identical to the one above, showing the 'Application Vulnerability Integration' screen for the 'Snyk SAST Vulnerabilities Import' record. The 'Execute Now' button is highlighted with a red box, indicating the action to be taken.

8. To fetch issues within a specific interval, select the relevant option from the Run dropdown, set the time, and click the "Update" button.

Note: The default time is 4:00 for SCA integration, which is 2 hours later than the Project and Orgs integration time so that tokens can be generated without token conflicts.

The screenshot shows the 'Application Vulnerability Integration' configuration page for 'Snyk SAST Vulnerabilities Import'. Key fields include:

- Name:** Snyk SAST Vulnerabilities Import
- Active:** Unchecked
- Run:** Daily (highlighted with a red box)
- Application:** Snyk Vulnerability Integration
- Source integration:** Snyk Application Security
- Source Instance:** Snyk Application Vulnerability

Below these, there's a note about choosing an integration to trigger automatically upon completion. A 'Next Integration' field is present, followed by a note about setting the start date. The 'Integration Details' section shows the 'Integration script' set to 'SnykSastVulnIntegration' and the 'Integration factory script' set to a script that constructs the integration script. The script content is as follows:

```
1+ /**
2+ * This function serves to construct the integration script.
3+ * The integration process record (integrationProcessGr) is provided in the event that stateful information is
4+ * required.
5+ * The function should return the newly constructed script.
```

9. To view collected issues, navigate to "Application Vulnerability Response," under it click on "Vulnerable Items" and under it select "All."

The screenshot shows the ServiceNow mobile application interface. At the top, there is a search bar with the text "Application vulnerability". Below the search bar, the title "ALL RESULTS" is displayed. A hierarchical menu is shown under "ALL RESULTS":

- Application Vulnerability Response
 - My Approvals
 - Remediation Tasks
 - Active
 - Assigned to Me
 - Assigned to My Groups
 - All
 - Vulnerable Items
 - Active
 - Assigned to Me
 - Assigned to My Groups
 - Missed Remediation Commi...
 - Multiple Deferrals
 - Unassigned
 - All
- Penetration Test Assessmen...
 - Active
 - Assigned to Me

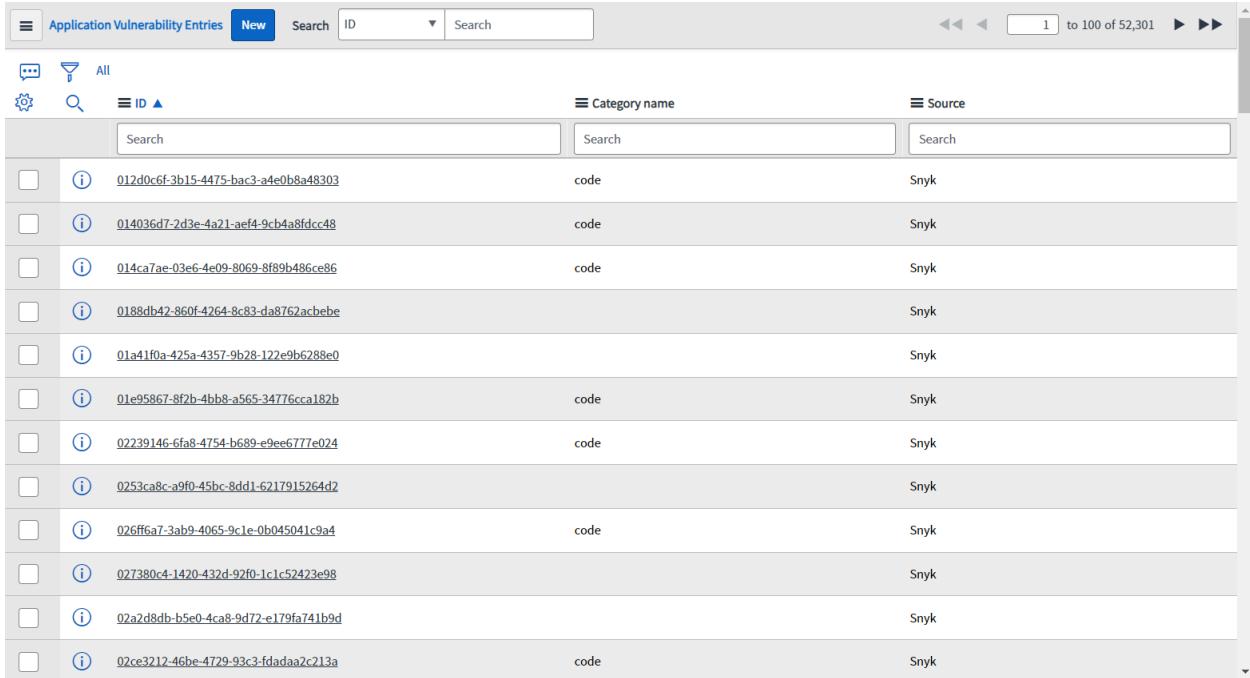
10. Users will have to provide the filter as "Source" "is" "Snyk" AND "Scan Type" "is" "Static." Then click "Run" to view all the SAST issues retrieved from Snyk.

	Number	Summary	Discovered Applications	Source AVIT ID	Source	Risk score	Risk rating	State	Remediation target	Remediation status	Vulnerability
	Search	Search	Search	Search	=Snyk	Search	Search	Search	Search	Search	Search
<input type="checkbox"/>	AVIT0029546	carwin/juice-shop	94938d90-d142-4226-a23a-48bc8e7863c5	Snyk	● 0	5 - None	Deferred	(empty)	No Target		0b5f21db-1815-9767-cbee949c2
<input type="checkbox"/>	AVIT0029748	carwin/juice-shop	f810b1be-f11b-4fcf-9077-2407cabd2319	Snyk	● 0	5 - None	Open	(empty)	No Target		108789b3-3816-4798-a4f2-9f63a07a984
<input type="checkbox"/>	AVIT0029753	carwin/juice-shop	feb7feeb-3846-4ae8-9dd6-d446f924a2e	Snyk	● 0	5 - None	Open	(empty)	No Target		965241b7-b412-4bec-bc85-d7f488028a24
<input type="checkbox"/>	AVIT0029752	carwin/juice-shop	fd2a1dc2-df06-4e17-a839-ee5a70fa9a91	Snyk	● 0	5 - None	Open	(empty)	No Target		e5814119-25da-4e68-a8c8-e0b49c5cd2e3a
<input type="checkbox"/>	AVIT0029749	carwin/juice-shop	f83aef62-6cae-4135-9fe9-35778696b7a0	Snyk	● 0	5 - None	Open	(empty)	No Target		43cdd0c0-3aa8-4d80-aad4-149e3a1d45b0
<input type="checkbox"/>	AVIT0029754	carwin/juice-shop	ff6312b5-b6d2-405b-8f9e-cbea818d9a93	Snyk	● 0	5 - None	Open	(empty)	No Target		53a1df66-78ec-bcd5-7d6240fc2
<input type="checkbox"/>	AVIT0029747	carwin/juice-shop	f7fb17460-7f34-4734-b22a-5127824d4aeb	Snyk	● 0	5 - None	Open	(empty)	No Target		9e780a14-f6ad-47db-832f-1cbf04ac479f

11. Change the view to "Snyk" to view the Snyk mapping fields in the AVIT table.

12. Third-party vulnerabilities will be visible in the list view of the "Application Vulnerability Entries (sn_vul_app_vul_entry)."

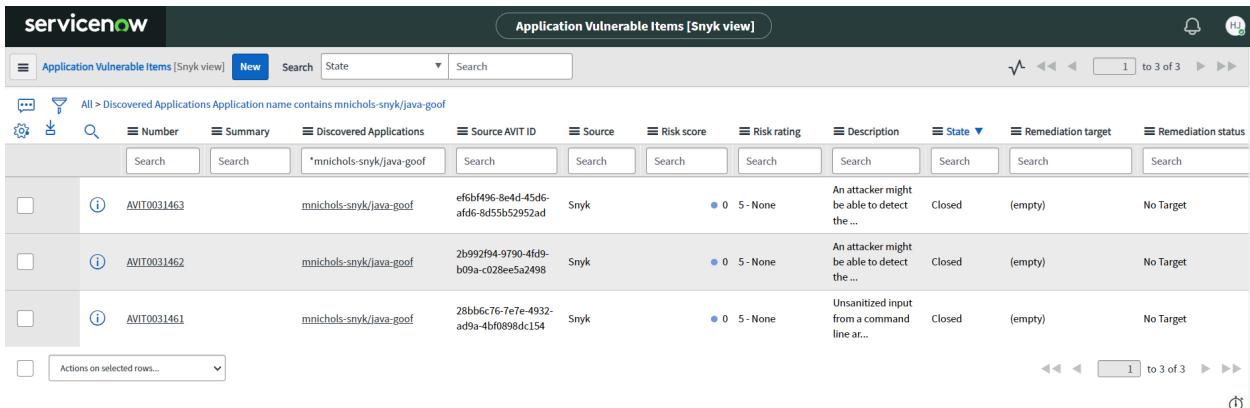
Note: Third-party vulnerability will only contain CWE as part of the SAST issue.



This screenshot shows a list of application vulnerability entries in ServiceNow. The columns include ID, Category name, and Source. Most entries are categorized as 'code' and sourced from 'Snyk'. The list is long, indicating many vulnerabilities found.

ID	Category name	Source
012d0c6f-3b15-4475-bac3-a4e0b8a48303	code	Snyk
014036d7-2d3e-4a21-aeef4-9cb4a8fdcc48	code	Snyk
014ca7ae-03e6-4e09-8069-8f89b486ce86	code	Snyk
0188db42-860f-4264-8c83-dab762acbebe		Snyk
01a41f0a-425a-4357-9b28-122e9b6288e0		Snyk
01e95867-8f2b-4bb8-a565-34776cca182b	code	Snyk
02239146-6fa8-4754-b689-e9ee6777e024	code	Snyk
0253ca8c-a9f0-45bc-8dd1-6217915264d2		Snyk
026ff6a7-3ab9-4065-9c1e-0b045041c9a4	code	Snyk
027380c4-1420-432d-92f0-1c1c52423e98		Snyk
02a2d8db-b5e0-4ca8-9d72-e179fa741b9d		Snyk
02ce3212-46be-4729-93c3-fdadada2c213a	code	Snyk

13. If a project is deleted or deactivated after the AVIT is created, the AVIT state will be closed with a proper note in the Description in the subsequent ingestion of issues.



This screenshot shows a list of application vulnerable items in ServiceNow, filtered by the Snyk source. The columns include Number, Summary, Discovered Applications, Source AVIT ID, Source, Risk score, Risk rating, Description, State, Remediation target, and Remediation status. The first two items have a risk score of 0 and a risk rating of 5 - None. The third item has a risk score of 0 and a risk rating of 5 - None, with a note in the Description field stating 'Unsanitized input from a command line ar...'. All items are currently in a Closed state.

Number	Summary	Discovered Applications	Source AVIT ID	Source	Risk score	Risk rating	Description	State	Remediation target	Remediation status
AVIT0031463	mnichols-snyk/java-goof	ef6bf496-8e4d-45d6-afdf-8d55b52952ad	Snyk	0	5 - None	An attacker might be able to detect the ...	Closed	(empty)	No Target	
AVIT0031462	mnichols-snyk/java-goof	2b992f94-9790-4f69-b09a-c028ee5a2498	Snyk	0	5 - None	An attacker might be able to detect the ...	Closed	(empty)	No Target	
AVIT0031461	mnichols-snyk/java-goof	28bb6c76-7e7e-4932-ad9a-4fb0f898dc154	Snyk	0	5 - None	Unsanitized input from a command line ar...	Closed	(empty)	No Target	

14. If the user marks an AVIT as "Mark as False Positive" or "Request Exception," the AVIT state will be set to "In Review." Once the request is approved, the "Additional comment," "Until date," "Reason," and "Additional comment" in the request exception added by the user will be added to the Snyk platform user interface. The AVIT state will be set to "Closed" after an approver approves the request.

Note: The "Mark as False Positive" and "Request Exception" buttons will only be visible when the "Manage Exception in ServiceNow" & "Manage False Positive in ServiceNow" flag are set to "true" in the Vulnerability Filtering section. Selecting "Mark as False Positive" will permanently ignore the issue in Snyk.

Once the AVIT is "Approved" and the state is changed, the user can see the "Additional information" added to the issue on the Snyk platform. Users must click on the "Source link" in the AVIT's Findings, redirecting them to the Snyk platform on the Issues page. Then, the user needs to add an "ignored" parameter in the filter.

Users will be able to see the issue with the comment. The comment will include the AVIT Number with the reason added from the ServiceNow side.

AVIT closed on ServiceNow due to project inactive/deleted will not close issue on Snyk Platform.

4.5. Fetch SCA & IaC Issues from the Snyk platform(Only for the US region)

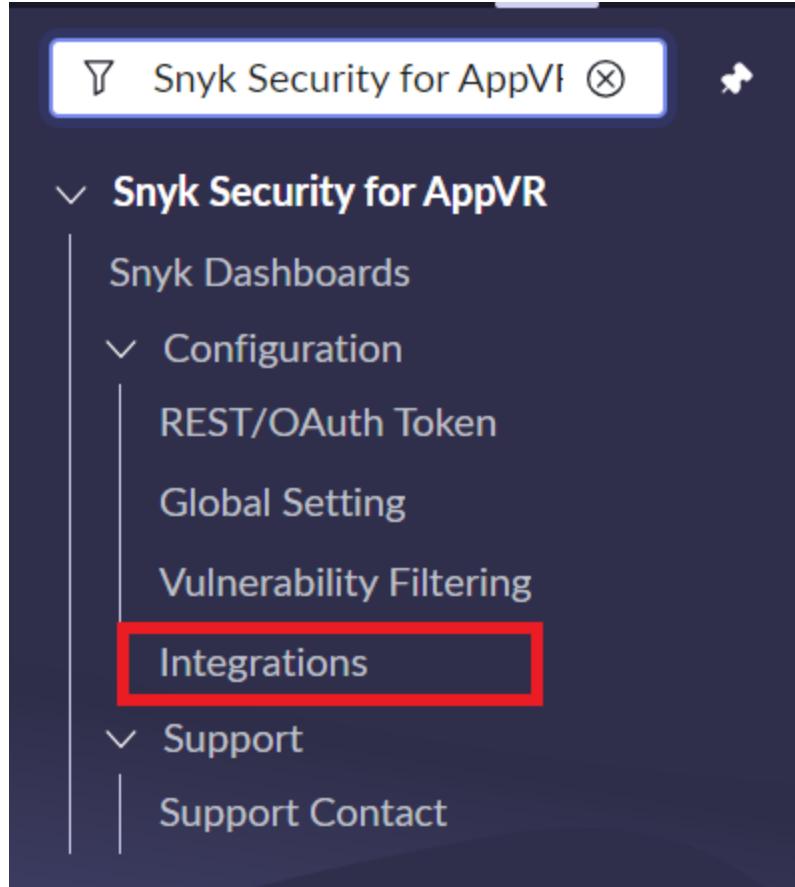
"Snyk Security for AppVR" provides the functionality to fetch Issues and their details from Snyk and populate them as Vulnerability, Application Vulnerable Item, Application Scan Summary, and Package in ServiceNow.

Important Note: Customers hosted in the us.snyk.io (AWS) region MUST use the REST APIs.

Role Required: x_snyk2_snyk_vr_in.configure_integration

Procedure:

1. Login to the ServiceNow instance.
2. Navigate to "Snyk Security for AppVR," and under it, select "Configuration."
3. Click on "Integrations."



4. Select Integration with the name "Snyk SCA & IaC Vulnerabilities Import(US Region - V1 API)" and Source Instance value as default provided integration instance.

The screenshot shows a ServiceNow list view for 'Application Vulnerability Integrations'. The header includes 'All', 'Favorites', 'History', 'Workspaces', and the current page title 'Application Vulnerability Integrations'. A search bar is present at the top. The table has columns: 'Name', 'Active', 'Source integration', 'Source Instance', 'Start time', 'Next Integration', and 'Run as'. There are several rows listed, and the last row, which is 'Snyk SCA & IaC Vulnerabilities Import(US Region - V1 API)', is highlighted with a red rectangular box around its entire row.

Name	Active	Source integration	Source Instance	Start time	Next Integration	Run as
Search	<input type="button" value="Search"/>	=Snyk Application Secur	<input type="button" value="Search"/>	<input type="button" value="Search"/>	<input type="button" value="Search"/>	<input type="button" value="Search"/>
Snyk Projects and Organizations Import	false	Snyk Application Security	Snyk Application Vulnerability	(empty)	(empty)	(empty)
Snyk SAST Vulnerabilities Import	false	Snyk Application Security	Snyk Application Vulnerability	2024-07-30 16:22:48	(empty)	(empty)
Snyk SCA & IaC Fixed Vulnerabilities Import (US Region - V1 API)	false	Snyk Application Security	Snyk Application Vulnerability	2024-12-17 00:00:00	(empty)	(empty)
Snyk SCA & IaC Vulnerabilities Import (All Region - V1 API)	false	Snyk Application Security	Snyk Application Vulnerability	(empty)	(empty)	(empty)
Snyk SCA & IaC Vulnerabilities Import(US Region - V1 API)	<input checked="" type="checkbox"/>	Snyk Application Security	Snyk Application Vulnerability	2024-12-17 00:00:00	Snyk SCA & IaC Fixed Vulnerabilities Imp...	(empty)

5. Activate the checkbox "Active." Click on the button "Update."
6. You must change the start time system property to change the start time. By default, it will take 90 days from the current time if the integration start time is blank.

The screenshot shows the 'Application Vulnerability Integration' record in ServiceNow. The integration is named 'Snyk SCA & IaC Vulnerabilities Import (US Region - V1 API)'. The 'Active' checkbox is checked. The 'Update' button is highlighted with a red box. Other fields shown include 'Run Daily' for the schedule, 'Snyk Vulnerability Integration' as the application, and 'Snyk Application Security' as the source integration.

7. Open the Snyk Integration record. To Fetch issues immediately, click on the "Execute Now" button.

The screenshot shows the same integration record with the 'Active' checkbox checked. The 'Run' dropdown is set to 'Daily'. The 'Time' field shows 'Hours: 01, 00, 00'. The 'Update' button is highlighted with a red box. The integration details section shows the same script content as the previous screenshot.

8. To fetch issues according to a scheduled time interval, select the relevant option from the Run dropdown, set the time, and click the "Update" button.

The screenshot shows the ServiceNow integration configuration interface. At the top, the title bar reads "Application Vulnerability Integration - Snyk SCA & IaC Vulnerabilities Import (US Region - V1 API)". Below the title, there's a "Name" field containing "Snyk SCA & IaC Vulnerabilities Import (US Region - V1 API)". On the right side, there are tabs for "Application", "Source integration", and "Source Instance". Under "Application", it says "Snyk Vulnerability Integration". Under "Source integration", it says "Snyk Application Security". Under "Source Instance", it says "Snyk Application Vulnerability". A red box highlights the "Run" and "Time" settings. The "Run" dropdown is set to "Daily", and the "Time" field shows "Hours: 01", "Minutes: 00", and "Seconds: 00". Below the main configuration area, there's a section titled "Integration Details" which displays the integration script code:

```

/* Integration script
 * SnykAppVullIntegration
 */
/*
 * This function serves to construct the integration script.
 * The integration process record (integrationProcessGr) is provided in the event that stateful information
 * is required.
 * The function should return the newly constructed script.
 */
(function(integrationProcessGr){

```

- "Snyk SCA & IaC Fixed Vulnerabilities Import(US Region - V1 API)" by default will be provided in the subsequent Integration for "Snyk SCA & IaC Vulnerabilities Import(US Region - V1 API)," which means it will trigger automatically once the "Snyk SCA & IaC Vulnerabilities Import(US Region - V1 API)" finishes its execution.

Note: The default time for SCA integration is 1:00, which is one hour later than the Project and Orgs integration time so that the token can be generated without any token conflicts.

- To view collected issues, navigate to "Application Vulnerability Response." Under it, click "Vulnerable Items," and under it, select "All."

The screenshot shows the ServiceNow mobile interface with a search bar at the top containing the text "Application vulnerability". Below the search bar, the title "ALL RESULTS" is displayed. A hierarchical list of search filters is shown, with some items expanded to reveal further options. A red rectangular box highlights the "All" option under the "Vulnerable Items" section.

- ▽ Application Vulnerability Resp...
- My Approvals
- ▽ Remediation Tasks
 - Active
 - Assigned to Me
 - Assigned to My Groups
 - All
- ▽ Vulnerable Items
 - Active
 - Assigned to Me
 - Assigned to My Groups
 - Missed Remediation Commi...
 - Multiple Deferrals
 - Unassigned
 - All**
- ▽ Penetration Test Assessmen...
- Active
- Assigned to Me

11. Users will have to provide the filter as "Source" "is" "Snyk" and then click on "Run" to view all the issues that are fetched from the Snyk.

AVIT ID	Location	Priority Score	Status	Remediation Target
AVIT0174919	carwin/snyk-goof:Dockerfile	100	Open	(empty)
AVIT0177181	carwin/k8s-goof:package.json	100	Open	(empty)
AVIT0173539	carwin/k8s-goof:Dockerfile	100	Open	(empty)
AVIT0173550	JanvibaJhala/VulnWhisperer:Dockerfile	100	Open	(empty)
AVIT0173521	JanvibaJhala/goof:Dockerfile	100	Open	(empty)

12. Change the view to "Snyk" to view the "Snyk Priority Score" in the AVIT table.

13. Third-party vulnerabilities will be visible in the list view of the "Application Vulnerability Entries (sn_vul_app_vul_entry)."

Note: A third-party vulnerability will only be created when the Snyk issue does not contain CVEs. IaC issues will always create a third-party vulnerability.

The screenshot shows a list of application vulnerabilities. The columns are: ID, Category name, Source, and Created. The data includes various npm packages like 'npm:sanitize-html', 'SNYK-JS-HANDLEBARS', and 'npm:tunnel-agent' with their respective details and creation dates.

ID	Category name	Source	Created
npm:sanitize-html:20160801	vuln	Snyk	2022-11-23 03:17:13
SNYK-JS-HANDLEBARS-534988	vuln	Snyk	2022-11-23 03:17:17
npm:marked:20170815_1	vuln	Snyk	2022-11-23 03:17:13
SNYK-JS-HANDLEBARS-174183	vuln	Snyk	2022-11-23 03:17:16
npm:marked:20170815	vuln	Snyk	2022-11-23 03:17:12
SNYK-JS-EXPRESSFILEUPLOAD-473997	vuln	Snyk	2022-11-23 03:17:13
SNYK-JS-HANDLEBARS-567742	vuln	Snyk	2022-11-23 03:17:17
SNYK-JS-EJS-1049328	vuln	Snyk	2022-11-23 03:17:10
npm:tunnel-agent:20170305	vuln	Snyk	2022-11-23 03:17:26
SNYK-JS-TAR-1536758	vuln	Snyk	2022-11-23 03:17:22

14. Packages will be visible in the list view of the "Package (sn_vul_app_package)" table.

15. Users will have to provide the filter as "Source" "is" "Snyk" and then click on "Run" to view all of the packages that are fetched from Snyk.

The screenshot shows a search interface for packages. The search bar has 'Snyk' entered. Below it, there's a 'Run' button highlighted with a red box. The main table lists various packages like 'acorn', 'adm-zip', and 'ajv' with their details and source information.

Vendor	Unique ID	Source
acorn	5.7.1	Language: js Package Manager: npm
adm-zip	0.4.7	Language: js Package Manager: npm
adm-zip	0.4.11	Language: js Package Manager: npm
ajv	6.10.2	Language: js Package Manager: npm
ansi-regex	2.1.1	Language: js Package Manager: npm
apk-tools/apk-tools	2.10.6-r0	Language: linux Package Manager: alpine:...
apr-util/libaprutil1	1.5.4-1	Language: linux Package Manager: debian:8
apr-util/libaprutil1	1.5.4-3	Language: linux Package Manager: debian:9

16. If a project is deleted or deactivated after the AVIT is created, the AVIT state will be closed with a proper note in the Description.

The screenshot shows two main sections of the ServiceNow interface:

- Snyk Projects:** A form for a project named "carwin/goof:image-app/package.json". Fields include Type (empty), Id (37d70022-9c65-44e0-9a41-20ee92227825), Name (carwin/goof:image-app/package.json), Created (empty), Origin (github), Organization (Crest Data Systems NFR - Shared), and Is Deleted (checked). The Organization field is highlighted with a red box.
- Application Vulnerable Items:** A grid view showing a list of items. The columns are: Number, Summary, Discovered Applications, Risk score, Risk rating, Remediation target, Remediation status, Vulnerability, and Assignment. Several rows are highlighted with red boxes, specifically focusing on the "Risk rating" column which contains entries like "5 - None" and "1 - Critical".

17. If the user marks an AVIT as "Mark as False Positive" or "Request Exception," the AVIT state will be set to "In Review." Once the request is approved, the "Additional

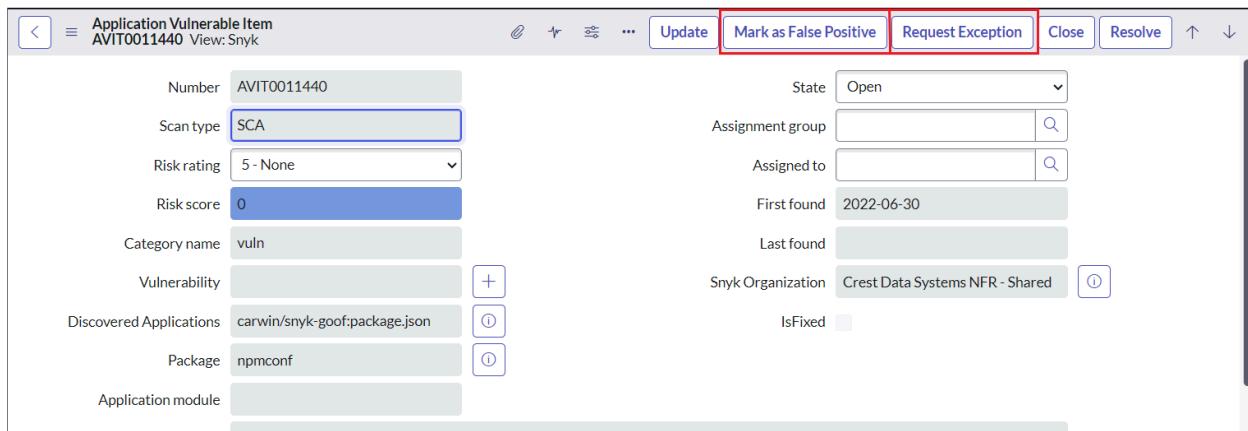
The screenshot shows the configuration of an integration:

- Name:** Snyk SCA & IaC Vulnerabilities Import (All Region - Rest API)
- Active:**
- Run:** Daily
- Application:** Snyk Vulnerability Integration
- Source integration:** Snyk Application Security
- Source Instance:** Snyk Application Vulnerability
- Integration Details:** Integration script is set to "SnykSastVulnIntegration".

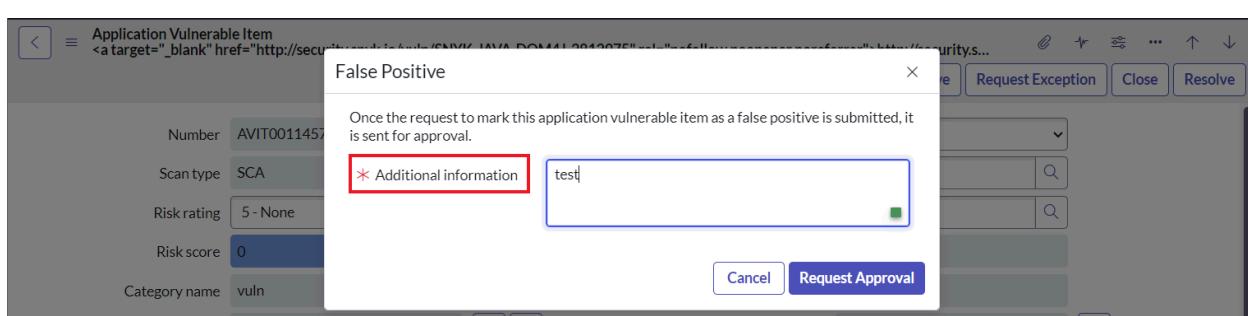
comment," "Until date," "Reason," and "Additional comment" in the request exception

added by the user will be added to the Snyk platform user interface. The AVIT state will be set to "Closed" after an approver approves the request.

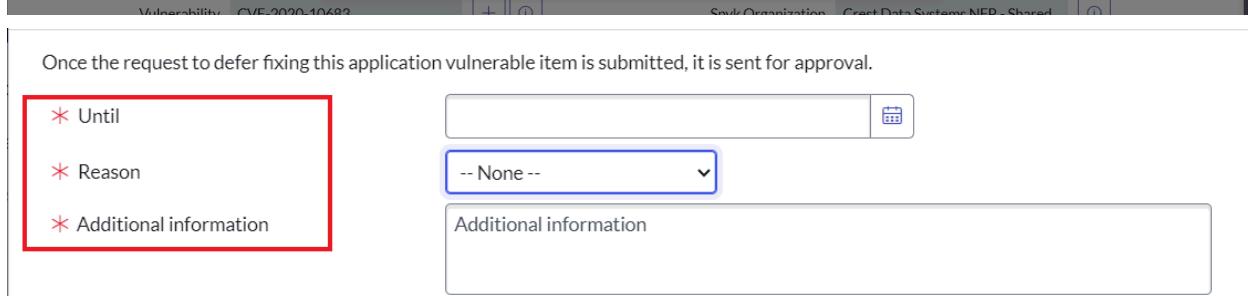
Note: The "Mark as False Positive" and "Request Exception" buttons will only be visible when the "Manage Exception in ServiceNow" & "Manage False Positive in ServiceNow" flag are set to "true" in the Vulnerability Filtering section.



The screenshot shows the ServiceNow interface for managing application vulnerabilities. The top navigation bar includes 'Update', 'Mark as False Positive' (highlighted with a red box), and 'Request Exception' (highlighted with a red box). Below the navigation, various fields are displayed: Number (AVIT0011440), Scan type (SCA), Risk rating (5 - None), Risk score (0), Category name (vuln), Vulnerability (+), Discovered Applications (carwin/snyk-goof:package.json), Package (npmconf), Application module, Location, State (Open), Assignment group, Assigned to, First found (2022-06-30), Last found, Snyk Organization (Crest Data Systems NFR - Shared), and IsFixed.



A modal dialog titled 'False Positive' is open, containing the message: 'Once the request to mark this application vulnerable item as a false positive is submitted, it is sent for approval.' It features a red box around the 'Additional information' field, which contains the value 'test'. Buttons for 'Cancel' and 'Request Approval' are at the bottom.



A modal dialog titled 'Request Approval' is open, containing the message: 'Once the request to defer fixing this application vulnerable item is submitted, it is sent for approval.' It features a red box around the 'Until' field (a date picker) and the 'Reason' dropdown menu, both of which are currently empty. A large red box also surrounds the 'Additional information' text area.



The screenshot shows the 'Requested Approvals' list view. It includes tabs for 'Requested Approvals (1)' and 'State Change Approvals (2)'. The main table has columns: State, Approver, Comments, Approval for, and Created. One row is shown with the 'State' column highlighted with a red box, showing the value 'Approved'. The 'Approver' column shows 'System Administrator', 'Comments' is '(empty)', 'Approval for' is '(empty)', and 'Created' is '2023-09-12 22:31:42'.

Once the AVIT is "Approved" and the state is changed, the user will be able to see the "Additional information" added to the issue on the Snyk platform. Users need to click on the "Source link" in the Findings of the AVIT, which will redirect to the Snyk platform on the Issues page. Then the user needs to add an "ignored" parameter in the filter.

The screenshot shows the Snyk Issues page with a search bar containing 'SNYK-JS-MONGOOSE-472486'. The results table has the following data:

Severity	Priority Score	Fixability	Exploit Maturity	Status	Count
>	0 of 91 issues	Sort by highest priority score			
> SEVERITY					
> PRIORITY SCORE					
FIXABILITY					
<input type="checkbox"/> Fixable	49				
<input type="checkbox"/> Partially fixable	14				
<input type="checkbox"/> No fix available	27				
> EXPLOIT MATURITY					
> STATUS					
<input checked="" type="checkbox"/> Open	90				
<input type="checkbox"/> Patched	0				
<input type="checkbox"/> Ignored	1				

A 'Did you know...' card is displayed on the right, suggesting prioritized fix pull requests for GitHub integration. The message reads: 'You can reduce the backlog of existing vulnerabilities at a manageable pace with prioritized fix pull requests - enable for your GitHub integration.' An illustration of three people is shown next to the card.

No results found.

Users will be able to see the issue with the comment. The comment will include the AVIT Number with the reason added from the ServiceNow side.

H dicer - Denial of Service (DoS)

VULNERABILITY | CVSS 7.5 HIGH | SNYK-JS-DICER-2311764 | IGNORED

Introduced through express-fileupload@1.1.10 Exploit maturity MATURE

Show more detail ▾

Ignored seconds ago by	N	Ignored path	*
Type	Not vulnerable	Expires	in 89 days
Reason	Vulnerability ignored from ServiceNow AVIT number: AVIT0004401 with reason: Test Sample Message		

4.6. Fetch Issues from Snyk All Region SCA & IaC Vulnerability integration

"Snyk Security for AppVR" provides the functionality to fetch Issues from other regions (besides the US) and populates them as Vulnerability, Application Vulnerable Item, and Application Scan Summary in ServiceNow.

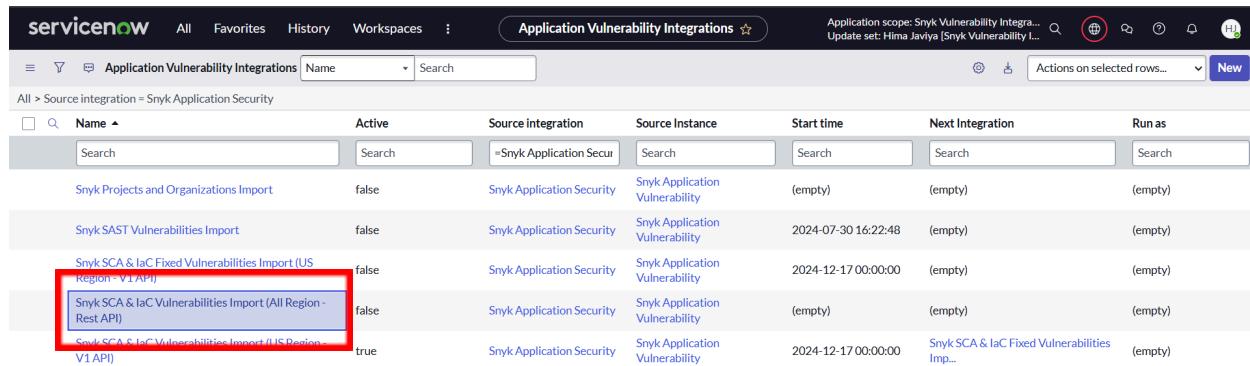
Role Required: x_snyk2_snyk_vr_in.configure_integration

Procedure:

1. Login to the ServiceNow instance.
2. Navigate to "Snyk Security for AppVR" and select "Configuration."
3. Click on "Integrations."



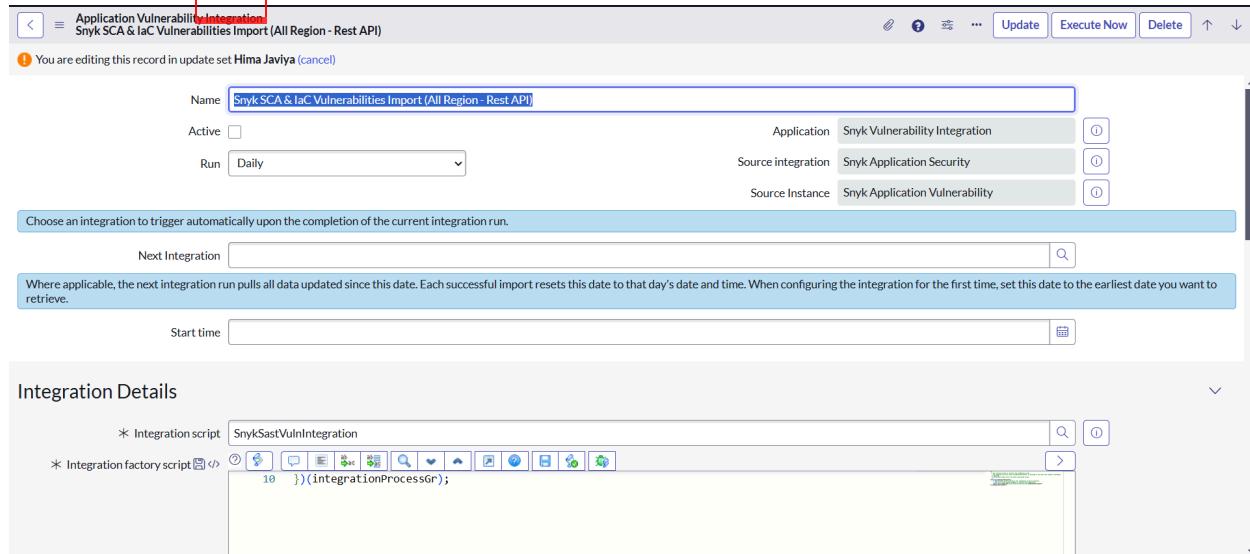
4. Click on the "Snyk SCA & IaC Vulnerability Import (All Region - Rest API)" integration.



Name	Active	Source integration	Source Instance	Start time	Next Integration	Run as
Snyk Projects and Organizations Import	false	Snyk Application Security	Snyk Application Vulnerability	(empty)	(empty)	(empty)
Snyk SAST Vulnerabilities Import	false	Snyk Application Security	Snyk Application Vulnerability	2024-07-30 16:22:48	(empty)	(empty)
Snyk SCA & IaC Fixed Vulnerabilities Import (US Region - V1 API)	false	Snyk Application Security	Snyk Application Vulnerability	2024-12-17 00:00:00	(empty)	(empty)
Snyk SCA & IaC Vulnerabilities Import (All Region - Rest API)	false	Snyk Application Security	Snyk Application Vulnerability	(empty)	(empty)	(empty)
Snyk SCA & IaC Vulnerabilities Import (US Region - V1 API)	true	Snyk Application Security	Snyk Application Vulnerability	2024-12-17 00:00:00	Snyk SCA & IaC Fixed Vulnerabilities Imp...	(empty)

5. Activate the checkbox "Active." Click on the button "Update."

6. Open the Snyk Vulnerabilities Import (Only for EU and AU region) record. To fetch issues, click on the "Execute Now" button.



Application Vulnerability Integration
Snyk SCA & IaC Vulnerabilities Import (All Region - Rest API)

You are editing this record in update set Hima Javiya (cancel)

Name	Snyk SCA & IaC Vulnerabilities Import (All Region - Rest API)	Application	Snyk Vulnerability Integration
Active	<input type="checkbox"/>	Source integration	Snyk Application Security
Run	Daily	Source Instance	Snyk Application Vulnerability

Choose an integration to trigger automatically upon the completion of the current integration run.

Next Integration

Where applicable, the next integration run pulls all data updated since this date. Each successful import resets this date to that day's date and time. When configuring the integration for the first time, set this date to the earliest date you want to retrieve.

Start time

Integration Details

* Integration script: SnykSastVulnIntegration

* Integration factory script: (IntegrationProcessGr);

7. To fetch issues according to a scheduled time interval, select the relevant option from the Run dropdown, set the time, and click the "Update" button.

The screenshot shows the ServiceNow integration configuration interface for "Application Vulnerability Integration". The integration is named "Snyk SC & IaC Vulnerabilities Import (All Region - Rest API)". Key settings include:

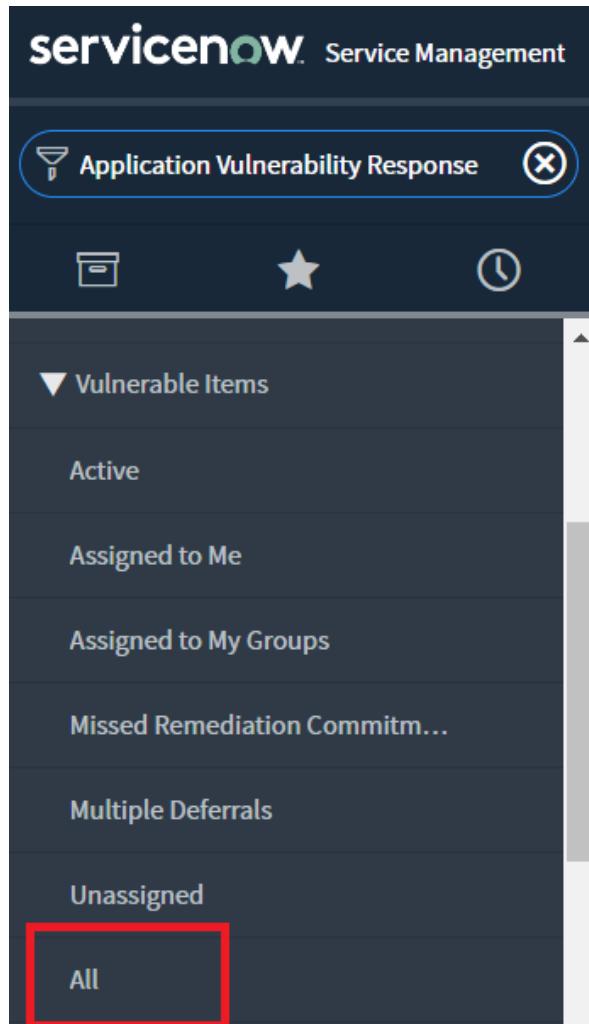
- Run:** Daily (highlighted with a red box)
- Time:** Hours 03 | 00 | 00
- Application:** Snyk Vulnerability Integration
- Source integration:** Snyk Application Security
- Source Instance:** Snyk Application Vulnerability

Below these settings, there is a note: "Choose an integration to trigger automatically upon the completion of the current integration run." A search bar for "Next Integration" is present, along with a note: "Where applicable, the next integration run pulls all data updated since this date. Each successful import resets this date to that day's date and time. When configuring the integration for the first time, set this date to the earliest date you want to retrieve." A "Start time" field with a calendar icon is also shown.

Integration Details

- * Integration script: SnykSastVulnIntegration
- * Integration factory script: `10 }){(integrationProcessGr);`

8. To view imported issues, navigate to "Application Vulnerability Response." Expand "Vulnerable Items," and under it select "All."



9. Users will have to provide the filter, as "Source" is "Snyk," and then click on "Run" to view all the issues fetched from Snyk.

Application Vulnerable Items [Snyk view]											
<input type="button" value="New"/> <input type="button" value="Search"/> <input type="text" value="Created"/> <input type="button" value="▼"/> <input type="text" value="Search"/> 1 to 100 of 2,007 											
<input type="button" value="Run"/> <input type="button" value="Save..."/> <input type="button" value="AND"/> <input type="button" value="OR"/> <input type="button" value="Add Sort"/> <input type="button" value="X"/>											
<input type="button" value="Source"/> <input type="button" value="▼"/> <input type="button" value="is"/> <input type="button" value="Snyk"/> <input type="button" value="AND"/> <input type="button" value="OR"/> <input type="button" value="X"/>											
	Number	Summary	Discovered Applications	Source AVIT ID	Source	Risk score	Risk rating	Description	State	Remediation target	Remediation status
<input type="checkbox"/>	AVIT0136968	mnichols-snyk/nodejs-goof/package.json	SNYK-JS-MINIMIST-2429795 CVE-2021-44906	Snyk	● 50 3 - Medium			Open (empty)	No Target		
<input type="checkbox"/>	AVIT0136965	mnichols-snyk/nodejs-goof/package.json	npm:ms:20170412 CVE-2017-20162	Snyk	● 25 4 - Low			Open (empty)	No Target		
<input type="checkbox"/>	AVIT0136967	mnichols-snyk/nodejs-goof/package.json	npm:debug:20170905 CVE-2017-16137	Snyk	● 50 3 - Medium			Open (empty)	No Target		
<input type="checkbox"/>	AVIT0136964	mnichols-snyk/nodejs-goof/package.json	npm:mime:20170907 CVE-2017-16138	Snyk	● 25 4 - Low			Open (empty)	No Target		
<input type="checkbox"/>	AVIT0136969	mnichols-snyk/nodejs-goof/package.json	SNYK-JS-KINDOF-537849 CVE-2019-2049	Snyk	● 50 3 - Medium			Open (empty)	No Target		
<input type="checkbox"/>	AVIT0136970	mnichols-snyk/nodejs-goof/package.json	SNYK-JS-HBS-1566555 CVE-2021-32822	Snyk	● 25 4 - Low			Open (empty)	No Target		

10. Change the view to "Snyk" to view the "Snyk Priority Score" in the AVIT table.

View	Default view		New	Search	Created	▼	Search	1 to 100 of 2,007 ►		
Filters	<input checked="" type="checkbox"/> Snyk									
Group By	>									
Show	<input type="checkbox"/> ID <input type="checkbox"/> OR <input type="checkbox"/> Add Sort <input type="checkbox"/>									
Refresh List										
Create Favorite										
				is	Snyk	AND	OR	X		
Number	Summary	Discovered Applications	Source AVIT ID	Source	Risk score	Risk rating	Description	State	Remediation target	Remediation status
	Search	Search	Search	=Snyk	Search	Search	Search	Search	Search	Search
<input type="checkbox"/>	(i) AVIT0136968	mnichols-snyk/nodejs-goof/package.json	SNYK-JS-MINIMIST-2429795 CVE-2021-44906	Snyk	● 50	3 - Medium	Open	(empty)	No Target	
<input type="checkbox"/>	(i) AVIT0136965	mnichols-snyk/nodejs-goof/package.json	npm:ms:20170412 CVE-2017-20162	Snyk	● 25	4 - Low	Open	(empty)	No Target	
<input type="checkbox"/>	(i) AVIT0136967	mnichols-snyk/nodejs-goof/package.json	npm:debug:20170905 CVE-2017-16137	Snyk	● 50	3 - Medium	Open	(empty)	No Target	
<input type="checkbox"/>	(i) AVIT0136964	mnichols-snyk/nodejs-goof/package.json	npm:mime:20170907 CVE-2017-16138	Snyk	● 25	4 - Low	Open	(empty)	No Target	
<input type="checkbox"/>	(i) AVIT0136969	mnichols-snyk/nodejs-goof/package.json	SNYK-JS-KINDOF-537849 CVE-2019-20149	Snyk	● 50	3 - Medium	Open	(empty)	No Target	
<input type="checkbox"/>	(i) AVIT0136970	mnichols-snyk/nodejs-goof/package.json	SNYK-JS-HBS-1566555 CVE-2021-32822	Snyk	● 25	4 - Low	Open	(empty)	No Target	

11. Third-party vulnerabilities will be visible in the list view of the "Application Vulnerability Entries (sn_vul_app_vul_entry)."

Note: Third-party vulnerability will only be created when the Snyk issue does not contain CVEs in the identifiers.

	ID	Category name	Source	Created
<input type="checkbox"/>	SNYK-DEBIAN9-GDKPIXBUF-345019		Snyk	2024-03-08 01:01:20
<input type="checkbox"/>	SNYK-DEBIAN9-BINUTILS-403912		Snyk	2024-03-08 01:01:20
<input type="checkbox"/>	SNYK-DEBIAN9-IMAGEMAGICK-402686		Snyk	2024-03-08 01:01:21
<input type="checkbox"/>	SNYK-DEBIAN9-IMAGEMAGICK-400039		Snyk	2024-03-08 01:01:21
<input type="checkbox"/>	SNYK-DEBIAN9-IMAGEMAGICK-402574		Snyk	2024-03-08 01:00:48
<input type="checkbox"/>	SNYK-DEBIAN9-SQLITE3-570321		Snyk	2024-03-08 01:00:48
<input type="checkbox"/>	SNYK-DEBIAN9-FREETYPE-1019584		Snyk	2024-03-08 01:00:48
<input type="checkbox"/>	SNYK-JS-MINIMIST-2429795		Snyk	2024-03-08 01:01:05
<input type="checkbox"/>	SNYK-DEBIAN9-OPENEXR-1090122		Snyk	2024-03-08 01:01:04
<input type="checkbox"/>	SNYK-DEBIAN9-OPENEXR-1318915		Snyk	2024-03-08 01:01:04
<input type="checkbox"/>	SNYK-DEBIAN9-IMAGEMAGICK-401160		Snyk	2024-03-08 01:01:24
<input type="checkbox"/>	SNYK-DEBIAN9-BINUTILS-403852		Snyk	2024-03-08 01:01:24

12. Packages will be visible in the list view of the "Package (sn vul app package)" table.

13. Users will have to provide the filter as "Source" is "Snyk" and then click on "Run" to view all the packages fetched from Snyk.

14. If the user marks an AVIT as "Mark as False Positive" or "Request Exception," the AVIT state will be set to "In Review." Once the request is approved, the "Additional comment," "Until date," "Reason," and "Additional comment" in the request exception added by the user will be added to the Snyk platform user interface. The AVIT state will be set to "Closed" after the request is approved.

Note: The "Mark as False Positive" and "Request Exception" buttons will only be visible when the "Manage Exception in ServiceNow" & "Manage False Positive in ServiceNow" flags are set to "true" in the Vulnerability Filtering section. **AVITs created for IaC issues using the REST Integration do not support Mark as False Positive and Request Exception.**

Application Vulnerable Item
AVIT0011440 View: Snyk

Number	AVIT0011440	State	Open
Scan type	SCA	Assignment group	
Risk rating	5 - None	Assigned to	
Risk score	0	First found	2022-06-30
Category name	vuln	Last found	
Vulnerability	carwin/snyk-goof:package.json	Snyk Organization	Crest Data Systems NFR - Shared
Discovered Applications	npmconf	IsFixed	
Package			
Application module			
Location			

Once the request to mark this application vulnerable item as a false positive is submitted, it is sent for approval.

* Additional information: test

Cancel Request Approval

Once the request to defer fixing this application vulnerable item is submitted, it is sent for approval.

* Until:

* Reason: -- None --

* Additional information:



The screenshot shows a ServiceNow Approvals grid. At the top, there are two tabs: "Requested Approvals (1)" and "State Change Approvals (2)". Below the tabs is a search bar with a dropdown menu set to "State". A red box highlights the "State" column header. The main table has columns: Approvals, State, Approver, Comments, Approval for, and Created. One row is visible, showing an approval from "System Administrator" with status "Approved" (indicated by a green dot). The "Created" field shows the date and time as "2023-09-12 22:31:42". At the bottom of the grid, there is a navigation bar with icons for back, forward, and search, followed by the text "1 to 1 of 1".

Once the AVIT is "Approved" and the state is changed, the user can see the "Additional information" added to the issue on the Snyk platform. Users must click on the "Source link" in the AVIT's Findings, redirecting them to the Snyk platform on the Issues page. Then, the user needs to add an "ignored" parameter in the filter.

Note:

- 1) The Vulnerability Filters that work for this integration are Projects, Organizations, Ignored, and Status.
- 2) The fixed Snyk SCA & IaC Fixed Vulnerabilities Import will not work for this integration.
- 3) The default run time is 00:00 for this integration.

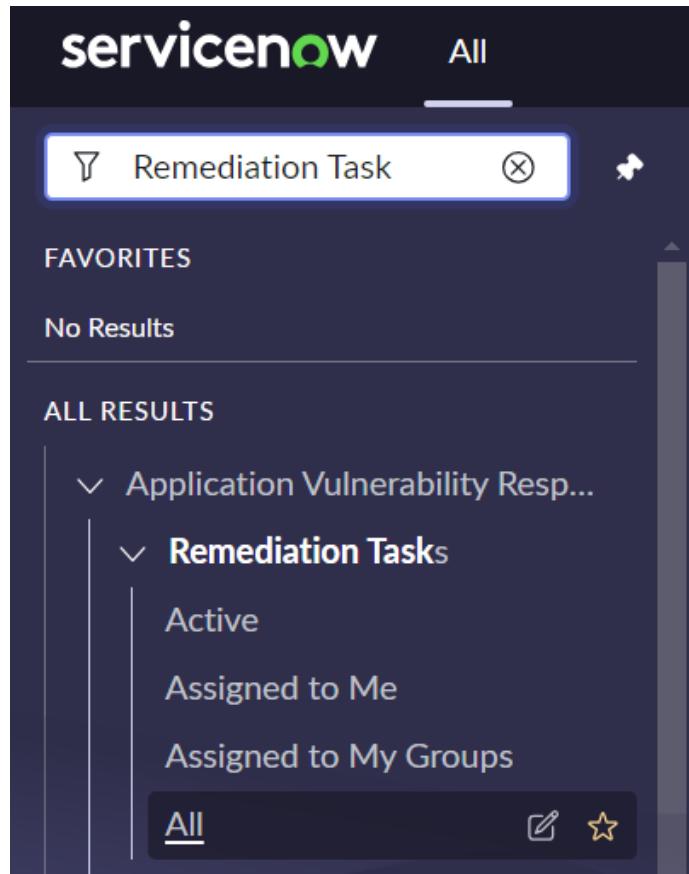
4.7. Bulk ignore of Application Vulnerable Items (AVITs) using Remediation tasks

This section describes how to use a Remediation task to ignore a group of Snyk issues from ServiceNow to Snyk.

Role Required: x_snyk2_snyk_vr_in.configure_integration

Procedure:

1. Login to the ServiceNow instance.
2. Navigate to Remediation Task under Application Vulnerability Response.



3. Click on All.
4. Click on the Create New button to create a new remediation task.

A screenshot of the "Application Remediation Task" creation form in ServiceNow. The top header says "Application Remediation Task New record". The form fields include:

- Number: AVUL0010007
- Risk rating: 5 - None
- Risk score: 0
- Configuration item: (empty)
- State: Open
- Assignment group: (empty)
- Assigned to: (empty)
- Created: (empty)
- Updated: (empty)

Below these fields is a "Short description" field containing "Test remediation task for Snyk". There are also "Description" and "Vulnerability" fields, both of which are currently empty.

At the bottom of the form is a "Group Configuration" tab, which is selected. It contains:

- Grouping method: -- None --
- Automatically update related application vulnerable items: A tooltip below this checkbox states: "Related application vulnerable items are automatically updated whenever the application vulnerable item condition is updated, or when the next scheduled job is invoked."

At the very bottom of the form is a "Submit" button.

5. Fill in the mandatory fields. Check all field descriptions [here](#)
6. Choose the Grouping method based on your requirements. Click on the submit button to create the record.
7. Open the newly created Remediation Task.

The screenshot shows the 'Application Remediation Task' form in ServiceNow. The task number is AVUL0010008. The risk rating is set to '5 - None'. The state is 'Open'. The configuration item is listed. The description field contains 'Test remediation task for Snyk'. The grouping method section shows a condition: 'Snyk Priority Score greater than 800'. The notes tab is also visible.

Field	Value
Number	AVUL0010008
Risk rating	5 - None
Risk score	0
Configuration item	[redacted]
State	Open
Assignment group	[redacted]
Assigned to	[redacted]
Created	2024-06-17 08:02:24
Updated	2024-06-17 08:02:24
* Short description	Test remediation task for Snyk
Description	[redacted]
Vulnerability	[redacted]

Remediation Status tab selected. **Group Configuration** tab is active. **Notes** tab is visible.

Grouping method: Filter

Application Vulnerable item condition:

- Snyk Priority Score greater than 800

Preview button is highlighted.

8. To permanently ignore all the issues, select "Mark as False Positive." Otherwise, click on Request Exception with a specific period.
9. Once the button to run the action is clicked, the request is sent for approval to the approver user/group.
10. To approve the exception, an approver has to approve the request. Please review the link for more information - <https://docs.servicenow.com/bundle/washingtondc-security-management/page/product/vulnerability-response/task/vr-ws-approve-requests.html>

Note: IaC AVIT fetched from REST Integration does not support Bulk ignore issues.

4.8. Unignore issues from ServiceNow to Snyk

This section describes how to unignore a Snyk issue from ServiceNow to Snyk that has been previously ignored in ServiceNow.

Role Required: x_snyk2_snyk_vr_in.configure_integration

Procedure:

1. Navigate to Applications Vulnerability Response > Vulnerable Items > All.
2. Select the Closed AVIT you want to reopen in ServiceNow.

3. Click on Reopen, and the issue will be unignored in Snyk..

The screenshot shows two overlapping ServiceNow pages. The top page is titled 'Application Vulnerable Item - AVIT0169490' and displays various details about the item, including its number, scan type, risk rating, and status. A red box highlights the 'Reopen' button in the top right corner of this page. The bottom page is also titled 'Application Vulnerable Item - AVIT0169490' and shows the 'Findings' tab selected. It includes fields like Source AVIT ID, Source severity, Snyk Priority Score, and a prominent 'Source link' field which contains a URL. A red box highlights this 'Source link' field.

4. Click on the Source link to verify the ignored has been removed in Snyk.

Note: AVITs for Iac Issues fetched using the REST Integration do not support Unignoring issues.

4.9. Automatically Ignore and Unignore AVITs using Exception Rules

Exception rules let you automate the deferral of vulnerable items that cannot be remediated immediately. By defining specific conditions – such as affected vulnerabilities, configuration items (CIs), or VIs, these rules automatically defer matching items for a defined period. More details about exception rules can be found [here](#).

This section describes how to automatically ignore & unignore a list of Snyk issues (AVITs) from ServiceNow to Snyk using Exception rules.

Role Required : sn_vul.app_manage_auto_exception_rule

Procedure :

1. Navigate to All > Application Vulnerability Response > Administration > Exception Rules.
2. Create a new Exception rule specify the filter conditions submit & Approve it.

3. Once the exception rule is approved, a remediation task is created in a deferred state. Starting from the "**Valid from**" to "**Valid to**" date, the exception rule runs on all the AVITs that are
 - a. newly created
 - b. moved from the Closed to the Open state.
 - c. If "execute on existing data" is enabled then a scheduled job runs once on the existing data on the "Valid from" date.
 After the "**Deferred until**" date the exception rule expires and all the AVITs are moved to open state again.
4. When an AVIT is moved to the **Deferred** state by an exception rule, it is also automatically **marked as "ignored"** in the Snyk platform, with the **expiration date** set to the "**Deferred Until**" date defined in the exception rule.
5. When an AVIT is moved to **open** state from **deferred** due to expiration of the exception rule, the same ignore is unignored from the Issue in Snyk platform.

Note: After version 26.0.11 of VR, exception rules no longer create remediation tasks. Instead, VITs are deferred directly without being associated with a remediation task.

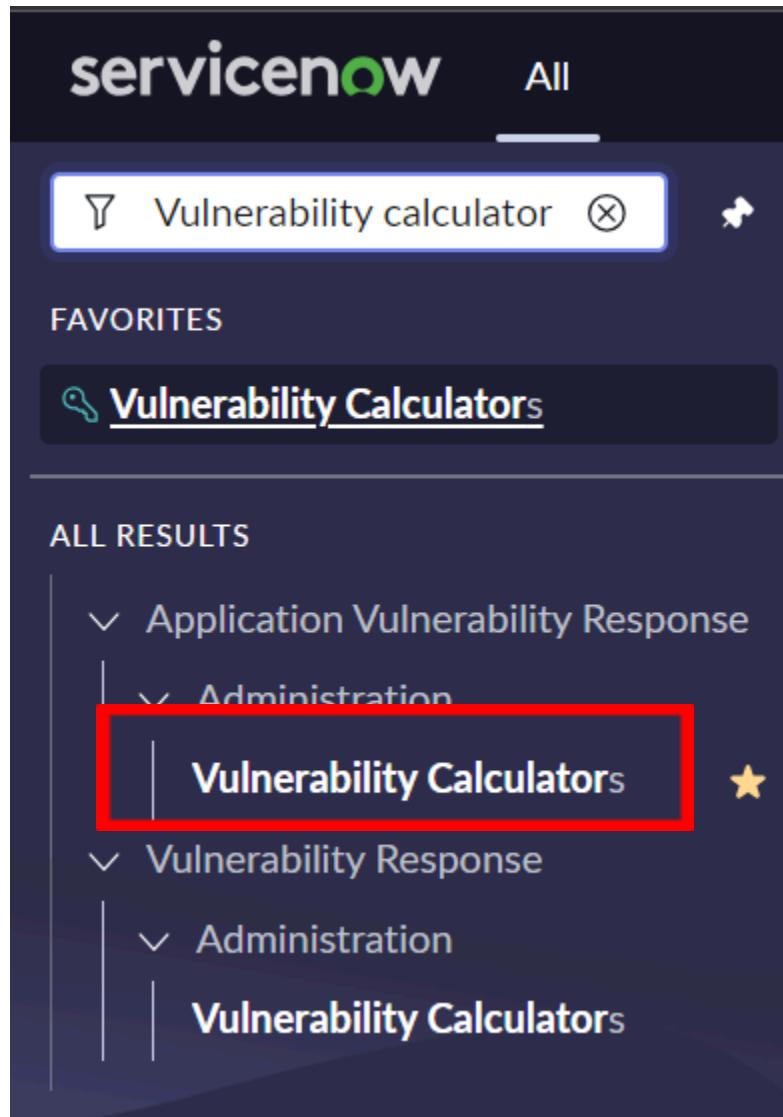
4.10. Snyk Risk Score Calculator

The Snyk risk score calculator calculates the risk rating and risk score based on the Snyk priority score. It can be used to define a risk score for an AVIT when automatically generating AVITs from vulnerabilities identified by Snyk.

Role Required: sn_vul.app_manage_risk_score_configuration

Procedure:

1. Login to the ServiceNow instance.
2. Navigate to the "Application Vulnerability Response"
3. Click "Administrator" and select "Vulnerability Calculator" from the dropdown menu.



4. Select "Snyk Calculator."

Name		Description	Table	Target field	Active
	Name	Description	Table	Target field	Active
<input type="checkbox"/>	Advanced Risk Calculator	Calculate the risk score based on multiple values, the vulnerability severity, vulnerability mapped to OWASP top 10 or SANs Top 25, business criticality and others. Open the Advanced Risk Score calculator rule to adjust which values are used, and how much weight to give each of these values.	Application Vulnerable Item [sn_vul_app_vulnerable_item]	risk_score	false
<input type="checkbox"/>	Snyk Calculator	Calculates the risk score for application vulnerable items using the Snyk Priority Score	Application Vulnerable Item [sn_vul_app_vulnerable_item]	risk_score	false
<input type="checkbox"/>	Basic Risk Calculator	Calculates the risk score for application vulnerable items using the normalized vulnerability severity	Application Vulnerable Item [sn_vul_app_vulnerable_item]	risk_score	false
	Actions on selected rows...				

5. Activate the Snyk calculator by clicking the active checkbox and then update the record.

* Name	Snyk Calculator	Application	Snyk Vulnerability Integration	<input type="checkbox"/>
Table	Application Vulnerable Item [sn_vul_app_vulnerable_item]	* Target field	Risk score	<input type="checkbox"/>
Description	Calculates the risk score for application vulnerable items using the Snyk Priority Score			
Active	<input checked="" type="checkbox"/>			
<input type="button" value="Update"/>	<input type="button" value="Delete"/>			

Vulnerability Calculator Rules																							
<input type="button" value="New"/>	<input type="button" value="New Risk Rule"/>	Search	Order	Search																			
<table border="1"> <thead> <tr> <th>Calculator = Snyk Calculator</th> <th>Name</th> <th>When this condition is met</th> <th>Set these values</th> <th>Order ▲</th> <th>Active</th> </tr> </thead> <tbody> <tr> <td><input type="checkbox"/></td> <td><input type="checkbox"/> Snyk Risk Rule</td> <td>Active = true .and. Source = Snyk</td> <td>Risk rule</td> <td>100</td> <td>true</td> </tr> <tr> <td></td> <td colspan="2">Actions on selected rows...</td><td></td><td></td><td></td></tr> </tbody> </table>						Calculator = Snyk Calculator	Name	When this condition is met	Set these values	Order ▲	Active	<input type="checkbox"/>	<input type="checkbox"/> Snyk Risk Rule	Active = true .and. Source = Snyk	Risk rule	100	true		Actions on selected rows...				
Calculator = Snyk Calculator	Name	When this condition is met	Set these values	Order ▲	Active																		
<input type="checkbox"/>	<input type="checkbox"/> Snyk Risk Rule	Active = true .and. Source = Snyk	Risk rule	100	true																		
	Actions on selected rows...																						

6. Note: Activating the Snyk risk score calculator will only calculate the risk score of AVITs whose source is Snyk. If the user wants to calculate the risk score of AVITs for other sources, they can create a new risk rule for them in the Snyk calculator or create a new calculator.

7. If you want to create your own calculator or modify the existing calculator, then click [this](#).

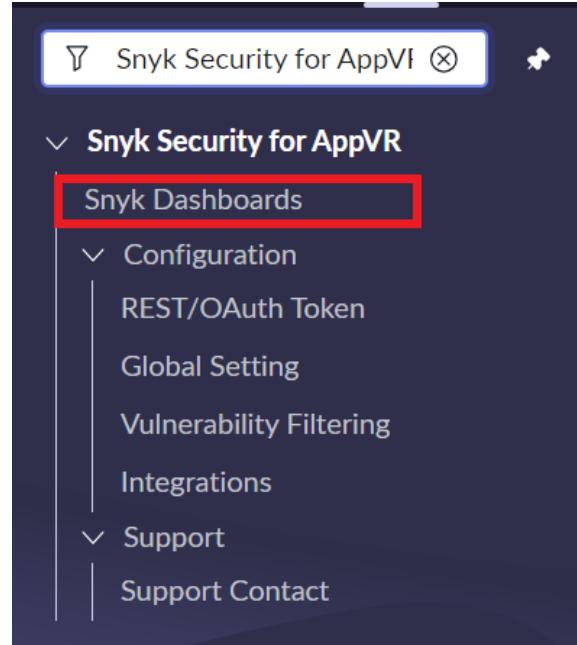
4.11. Snyk Dashboard

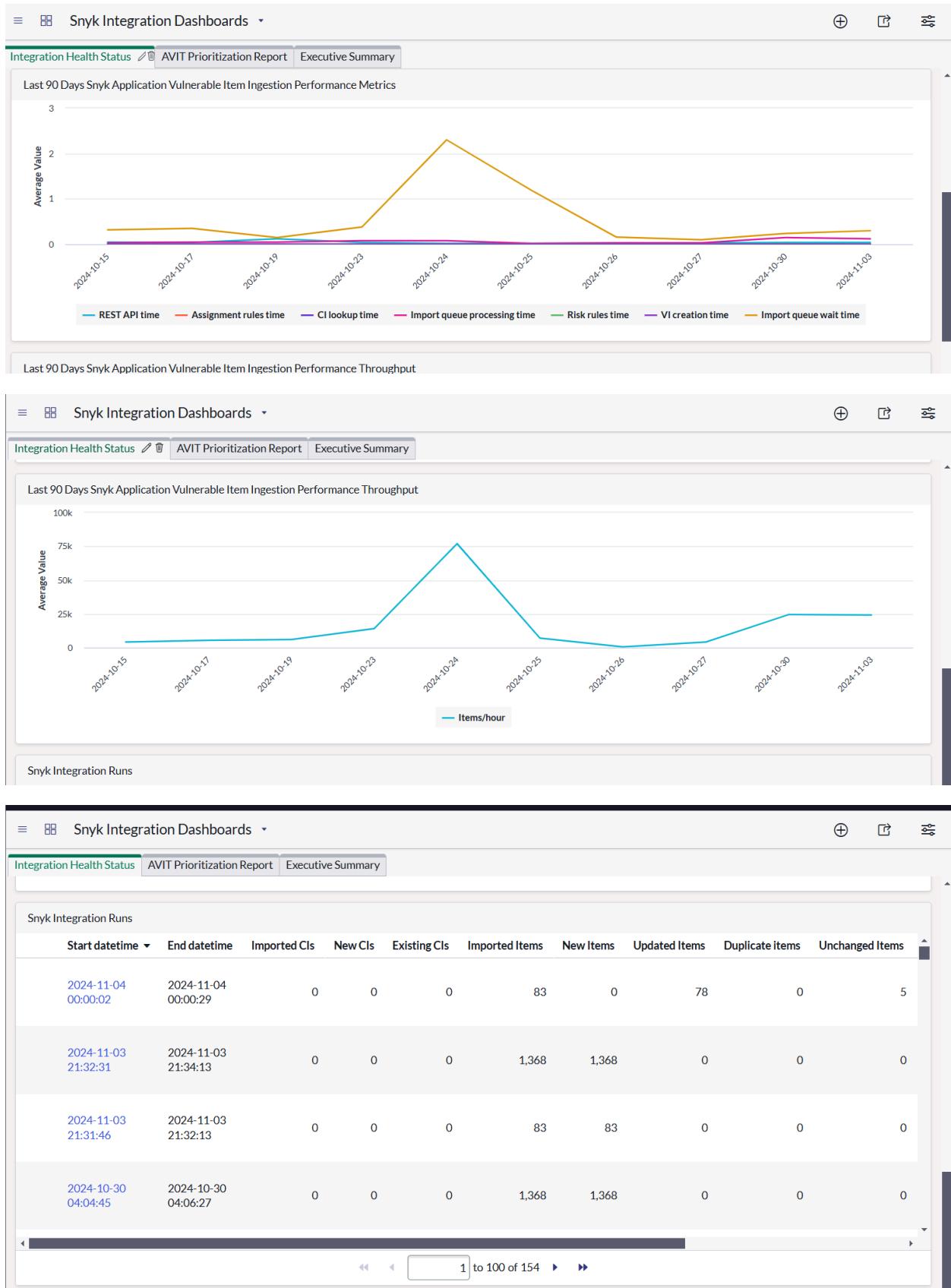
"Snyk Security for AppVR" provides the functionality to view the dashboard and provide an overview of the data.

Role Required: x_snyk2_snyk_vr_in.configure_integration, sn_vul.configure_integrations, sn_vul.app_read_assigned

Procedure:

1. Login to the ServiceNow instance.
2. Navigate to "Snyk Security for AppVR."
3. Click on "Snyk Security for AppVR," and under it select "Snyk Dashboards."





Last 90 Days Snyk AVITs By Severity

Discovered Applications	carwin/goof:package.json (1e42329f9321565046db352efaba107b)	carwin/k8s-goof:package.json (ed42fe5f9321565046db352efaba103b)	carwin/snyk-goof:package.json (1a42329f9321565046db352efaba107c)
Source severity			
critical	3	2	3
high	52	44	54
low	6	6	8
medium	47	40	48
Count	108	92	113
			1

Last 90 Days Snyk Unchanged AVITs: 16,288

Last 90 Days Snyk Updated AVITs: 248

Last 90 Days Snyk New AVITs: 19,291

Snyk Integration Dashboards

Integration Health Status | AVIT Prioritization Report | **Executive Summary**

Last 90 Days Snyk Fixed AVITs: 0

Last 90 Days Snyk Resolved AVITs: 0

4.12. System properties (optional)

Role required: System Administrator

Update the values in the system properties only if required. Changing values of system property can impact the integration. Below are the details of the system properties. Users can go to system properties by typing sys_properties.LIST and the filtering properties with app scope.

Properties	Use Case
x_snyk2_snyk_vr_in.pageSize	Page size for SCA & IaC Issues for V1 Integration
x_snyk2_snyk_vr_in.pageSizeProjects	Page size for Projects
x_snyk2_snyk_vr_in.request_timeout	When making a Snyk API request, this time will be utilized to wait for a response (in seconds).
x_snyk2_snyk_vr_in.retry	The API call will be retried this many times.
x_snyk2_snyk_vr_in.until_date	This will be implemented when updating the state from ServiceNow to Snyk. If the "AVIT Request Exception until date" exceeds 365 days, the issue will be ignored permanently. The default value is set to 365 days, but you can adjust it to a value below 365 days as needed.
x_snyk2_snyk_vr_in.waitTime	Wait time for subsequent API calls if a timeout error occurs in Snyk API (in milliseconds).

4.13. CI LookUp rule

- Below are the steps to follow if your ServiceNow instance stores Snyk Applications in the "sn_vul_app_scanned_application" table and you want to create or use existing CIs (Configuration Items) when creating Discovered Applications for Snyk applications.
- Make sure the system property (**sn_vul.use_product_model**) is false. For verification, follow the steps below.
 - Navigate to **sys_properties.LIST**
 - Search for **sn_vul.use_product_model**

The screenshot shows the ServiceNow sys_properties LIST view. The search bar at the top has 'Name contains use_product_model'. A single row is displayed in the list:

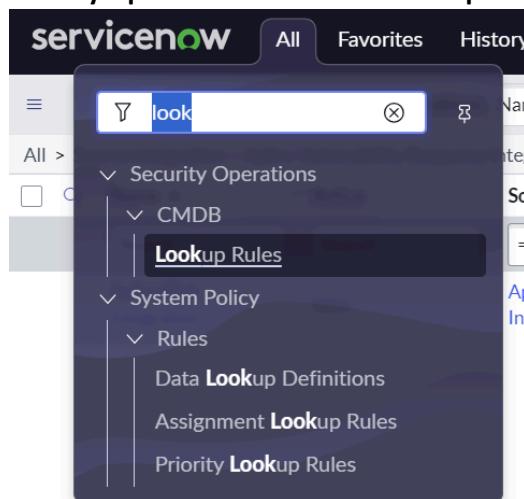
Name	Type	Description	Updated	Updated by
*use_product_model	true false	Vulnerability Response	2024-01-11 04:55:59	himajaviya

- The value should be **false**. If not, change it to **false**.

- If the **sn_vul.use_product_model** value is true, it will create a product model. If you choose that approach, you must create a Lookup rule with a lookup target Product Model.

Note: If your ServiceNow instance stores Snyk projects in a CMDB class other than the "**sn_vul_app_scanned_application**" table, then you need to create your own look-up rule but ensure you keep the source field as **source_app_id**. (**Note:** If you're using tags to match the record, then it will consider the tag value of the tag mentioned in the global settings module of the integration; otherwise, it will consider the project ID.) Follow the steps below to create the Lookup rule.

- Navigate to **Security Operations -> CMDB -> Lookup Rules**.



- Click on the New button to create a new Lookup rule.

The screenshot shows the 'Lookup Rule' creation form. At the top, there is a header with back, forward, and save buttons, and a 'Submit' button on the right. Below the header is a help panel with instructions for fields: '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', and 'Product model or CI - the method used for searching either on product model or CI'. The main form area has fields for 'Name' (with a red asterisk), 'Order' (with a red asterisk), 'Lookup method' (set to 'Field matching'), 'Active' (checkbox checked), and 'Description'. Below this is a section titled 'Define the source and source field for the lookup rule.' with fields for 'Source' (set to 'Snyk Application Security') and 'Source field' (empty). There is also a 'Description' field and a 'Lookup target' dropdown set to 'Product model'. At the bottom of the form is a note: '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.' At the very bottom are 'Search on product model table' (dropdown set to 'Application Model [cmdb_application]'), 'Search on product model field' (dropdown set to '--None--'), and a 'Submit' button.

- Give a Unique **Name**—for example, "Snyk Product Rule."

- Select "Field matching" in the **Lookup Method**. Use a custom script if the table is not present in the list.
- Select **Source** as Snyk Application Security.
- Select **Lookup target** as Product Model or Configuration item based on requirement.
- Select the Table name where your ServiceNow stored application data is **Search on the product table**.
- In the **Source field**, give the product table a unique name that should map to the application field name. (Application fields: app_name, source_app_id)
- Click on the **Update** Button.
- Similarly, users can create CI lookups for other CMDB tables if needed.
- Make sure your CMDB matching field has the exact same value as the Snyk project tags value/project ID to map correct Cls.
- **Note:** Any customization to the existing lookup rule or new lookup rule that is created will never override in future upgrades, as ServiceNow doesn't override customer updates by default.
- Refer to the link below for more info about creating CI Look-up rule:
<https://docs.servicenow.com/bundle/washingtondc-security-management/page/product/security-operations-common/task/create-ci-identifier-rules.html>.
- From **v3.1.0 onwards**, the **sourcepayload** will include **full project details from the API**, enabling more advanced and specific **CI lookup rule matching**.

The payload contains comprehensive project metadata, including:

- Project ID, name, and type
- Latest issue and dependency counts
- Target file and Git reference
- Origin and status
- Organization and target relationships (including URLs)
- Importer info
- Project attributes (e.g., lifecycle, environment, tags)

Payload Example:

```
{  
  "type": "project",  
  "id": "50f158ef-6a8c-4c51-830c-baf16ed5d5a8",  
  "meta": {  
    "latest_issue_counts": {  
      "updated_at": "2025-06-01T19:05:42.202Z",  
      ...  
    },  
    ...  
  },  
  ...  
}
```

```
"critical": 0,  
"high": 0,  
"medium": 0,  
"low": 0  
,  
"latest_dependency_total": {  
    "updated_at": "2025-06-01T19:05:42.202Z",  
    "total": 0  
}  
,  
"attributes": {  
    "name": "mnichols-snyk/strapi:package.json",  
    "type": "yarn",  
    "target_file": "package.json",  
    "target_reference": "develop",  
    "origin": "github",  
    "created": "2024-11-20T16:06:20.419Z",  
    "status": "active",  
    "business_criticality": [],  
    "environment": [],  
    "lifecycle": [],  
    "tags": [],  
    "read_only": false,  
    "settings": {  
        "recurring_tests": {  
            "frequency": "daily"  
        },  
        "pull_requests": {}  
    },  
    "build_args": {
```

```
"root_workspace": "."
}

},
"relationships": {
  "organization": {
    "data": {
      "type": "org",
      "id": "8f793725-eddf-4c7b-81e7-aa8546bd7df9"
    },
    "links": {
      "related": "/rest/orgs/8f793725-eddf-4c7b-81e7-aa8546bd7df9"
    }
  },
  "target": {
    "data": {
      "id": "3f997c18-0004-49a7-83f7-1b518b49d996",
      "type": "target",
      "attributes": {
        "display_name": "mnichols-snyk/strapi",
        "url": "https://github.com/mnichols-snyk/strapi"
      }
    },
    "meta": {
      "integration_data": {
        "id": 891598420,
        "name": "strapi",
        "owner": "mnichols-snyk"
      }
    }
  }
},
"links": {
```

```
"related": "/rest/orgs/8f793725-eddf-4c7b-81e7-aa8546bd7df9/targets/3f997c18-0004-49a7-83f7-1b518b49d996"  
}  
},  
"importer": {  
    "data": {  
        "type": "user",  
        "id": "ae8daca3-9df9-4275-b6dc-a3260a804aa3"  
    },  
    "links": {  
        "related": "/rest/orgs/8f793725-eddf-4c7b-81e7-aa8546bd7df9/users/ae8daca3-9df9-4275-b6dc-a3260a804aa3"  
    }  
},  
},  
"source_app_id": "50f158ef-6a8c-4c51-830c-baf16ed5d5a8",  
"name": "mnichols-snyk/strapi:package.json",  
"short_description": "Lifecycle\nEnvironment:",  
"correlation_id": "mnichols-snyk/strapi",  
"last_policy_compliance_check_date": "NULL"  
}
```

Example Usecase

To match **Container Repository Entries** with **Projects** based on Repository URL with name of CI.

Create a Lookup rule with Lookup method as Script, type as Custom and Select Parent attribute if field is nested like in this example url is nested as `relationships.target.data.attributes.url`.

Below is screenshot of CI Lookup Record.

Script:

```
var cmdbGr = new GlideRecord('cmdb_ci_container_repository_entry');  
  
if (cmdbGr.get('name',  
sourcePayload.relationships.target.data.attributes.url))  
  
    return cmdbGr.getUniqueValue();
```

```
return null;
```

The screenshot shows the 'Lookup Rule' configuration page in ServiceNow. The rule is titled 'Test' and is set to have an order of 10. It is marked as 'Active'. The 'Lookup method' is set to 'Script' and the 'Type' is 'Custom'. The 'Source' is 'Snyk Application Security' and the 'Source field' is 'relationships'. The 'Lookup target' is 'Configuration Item'. A note at the bottom of the form states: '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.' Below this note is a script editor containing the following code:

```

/*
 * CI Lookup Rule Script
 */
// Available variables:
// - sourceValue: The value of the source field from incoming data that is used for lookup
// - rule: Reference to the lookup rule that is being evaluated
// - sourcePayload: All the fields from incoming data that can be used for matching CI
//
// Return either:
// - the sysid of the CI that was matched by the rule
// - null if there were no CI records that matched
// -----
var cmdbGr = new GlideRecord('cmdb_ci_container_repository_entry');
if (cmdbGr.get('name', sourcePayload.relationships.target.data.attributes.url))
    return cmdbGr.getUniqueValue();
return null;
})(rule, sourceValue, sourcePayload);

```

4.14. Assignment Rule

- The Snyk application has two assignment rules by default in an inactive state: 1) Snyk Assignment Rule and 2) Snyk Assignment Rule Based On Project Tags for assigning AVIT to users/groups.
- Navigate to Application Vulnerability Response > Administration > Assignment Rules for more information.**

Name	Condition	Assign using	Assignment value	Execution order	Active	Reapply
Snyk assignment rule	Source = Snyk.and. Active = true	Script	Assigned by script	100	false	No
Snyk Assignment Rule Based On Project Tags	Source = Snyk.and. Active = true	Script	Assigned by script	100	false	Yes

1. Snyk Assignment Rule Based On Project Tags

- If you want to assign AVIT based on project tags, use this assignment rule. To use this assignment rule, you need to make below changes.

```
// 1. Declare tags key and values
var tags = {
    "CMDBID" : ["java-goof", "democheck1234"]
}; // Add key value pair of tags. for example:
"<tags-key>": ["tags-value1", "<tags-value2>"]

// 2. two option available for assigning avit group and user. By default it will check for user.
var whomToAssign = "user"; // Replace with group if you want to assign AVIT to group

// 3. Mapping of tags value and sys id of user/group.
var sysIdOfUserOrGroupBasedOnTags = {
    "java-goof": "afdf1ee287d9421015f3c91e0ebb357a",
    "democheck1234": "afdf1ee287d9421015f3c91e0ebb357a"
}; // If you want to assign user to AVIT which has <tag-value> in discovered application/projects. then delcare it in above dict like "<tag-value>" : "<sys-id of user/group>"

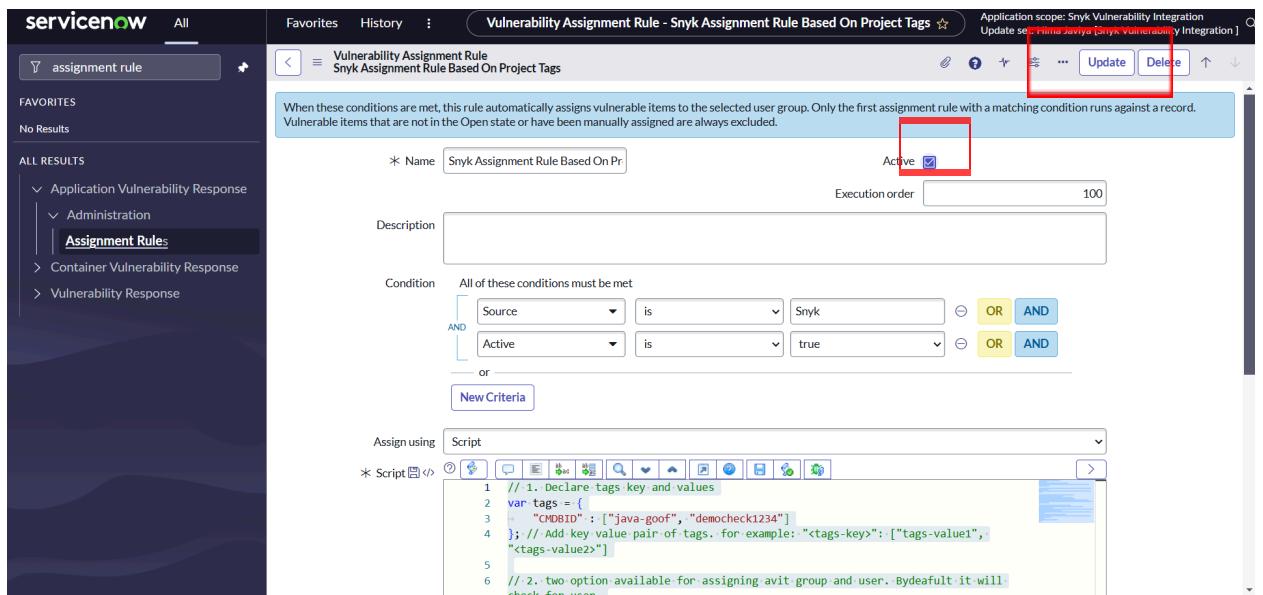
// 4. Logic to map appropriate user/group to AVIT
```

```

var sourceDict =
current.application_release.source_additional_info;
for (var key in tags) {
    if (sourceDict[key] !== undefined &&
tags[key].indexOf(sourceDict[key]) != -1) {
        if (whomToAssign == "user") {
            current.assigned_to =
sysIdOfUserOrGroupBasedOnTags[sourceDict[key]];
        }
        else if (whomToAssign == "group") {
            current.assignment_group =
sysIdOfUserOrGroupBasedOnTags[sourceDict[key]];
        }
        break; // match found
    }
}

```

- b. Check comments in the code and update the codebase accordingly so it works seamlessly with your data and mark it as active.



2. Snyk assignment rule

- a. This assignment rule verifies the presence of any business application record with tag values corresponding to a Business App name. If such a record exists, it will associate the managed by group of the business application to the AVIT. Change the code below according to your requirements.

```
// 1. Declare tag keys and tag values here.  
var tagValuesMap = {  
    "CMDBID": ["java-goof", "democheck1234"], //  
    "<tag-key>": ["<tag-value1>", "<tag-value2>"]  
};  
  
for (var tagkey in tagValuesMap) {  
    var baGr = new GlideRecord("cmdb_ci_business_app");  
    // 2. you can change table as per your requirements  
    var values = tagValuesMap[tagkey].join(",");  
    baGr.addQuery("name", "IN", values); // Make sure  
    your record is present with tag values as name. If tag  
    value is present in another field then change  
    accordingly.  
    baGr.query();  
    var match = false;  
    while (baGr.next() && !match) {  
        if  
(current.application_release.source_additional_info[tag  
key] == baGr.getValue("name")) {  
            match = true;  
            current.assignment_group =  
baGr.managed_by_group + " ";  
            break;  
        }  
    }  
    if (match)  
        break;  
}
```

- b. Change the tag key and tag values according to your environment and check other comments. After changing, mark active as true for this assignment rule.

The screenshot shows the ServiceNow interface for creating a new assignment rule. The left sidebar shows a tree view under 'Assignment Rules' with 'Administration' selected. The main panel shows the 'Vulnerability Assignment Rule - Snyk assignment rule' configuration. The 'Active' checkbox is highlighted with a red box. The 'Condition' section defines a rule where 'Source' is 'Snyk' AND 'Active' is 'true'. The 'Assign using' section contains a script block:

```

    * Script </>
    1 // 1. Declare tag keys and tag values here.
    2 var tagValuesMap = [
    3     "CMDID": ["java-goof", "demochek1234"], // <tag-key>: [<tag-value1>,
    4     "<tag-value2>"]
    5 ];
    6
  
```

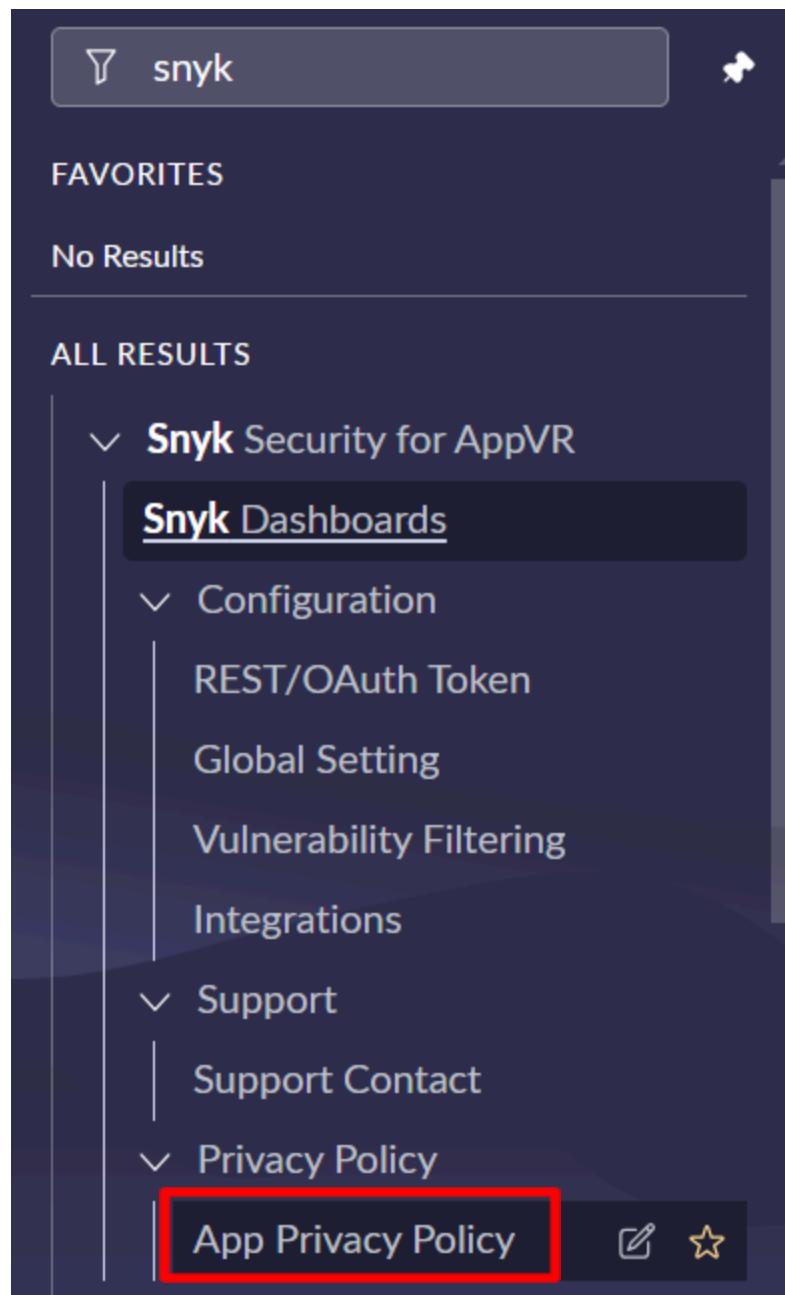
C. Apply the changes to run the assignment rule for existing AVITs.

The screenshot shows the 'Vulnerability Assignment Rules' list page. The table displays two rules: 'Snyk assignment rule' and 'Snyk Assignment Rule Based On Project Tags'. The 'Apply Changes' button at the top right is highlighted with a red box.

Name	Condition	Assign using	Assignment value	Execution order	Active	Reapply
Snyk assignment rule	Source = Snyk.and. Active = true	Script	Assigned by script	100	false	No
Snyk Assignment Rule Based On Project Tags	Source = Snyk.and. Active = true	Script	Assigned by script	100	true	Yes

4.15. Privacy Policy

- Navigate to "Snyk Security for AppVR."
- To check the privacy policy related to the application, navigate to "Snyk Security for AppVR," and under it, look for "Privacy policy" and select "App Privacy Policy" from the dropdown menu.



The screenshot shows the ServiceNow header with links for Favorites, History, Workspaces, Admin, and the ServiceNow logo. Below the header is a search bar and various navigation icons. The main content area is titled "Privacy Notice for the Snyk Security for Application Vulnerability Response integration with ServiceNow". It contains two sections: "1. Data Transfer" and "2. Data Usage".

1. Data Transfer

- From Snyk to ServiceNow**

When the integration is enabled, ServiceNow imports Organizations and Projects from Snyk. Users choose which Snyk Groups and Organizations they want to retrieve data from. In addition, users can configure the integration to retrieve SCA and SAST issues. For clarity, Snyk does not send personal data to ServiceNow via the integration.
- From ServiceNow to Snyk**

When configured by the user, Application Vulnerable Items (AVIT) granted an approved "Exception" or "False Positive" status or closed manually in ServiceNow, the ServiceNow system will update the "Ignored" setting on the corresponding issue in Snyk with a note of ServiceNow AVIT id.

2. Data Usage

- By Snyk**

Snyk uses, transfers, stores, and secures the above data in accordance with any agreements in effect between the user and Snyk and our [Privacy Notice](#). Specifically, with respect to the data Snyk receives from ServiceNow as a result of the integration, Snyk may (i) collect, analyze, and otherwise process the data internally for its business purposes, including for the purposes of security and analytics, to improve and enhance the services, or for other development, diagnostic and corrective purposes in connection with the services or other Snyk products or services, and (ii) publicly disclose the data only in an aggregated and/or de-identified form in connection with its business in a manner that does not identify customers or users.
- By ServiceNow**

This Privacy Notice does not cover ServiceNow's usage of data. Please see ServiceNow's documentation and applicable privacy notice(s) for details with respect to how ServiceNow treats data transferred to it from Snyk.

5. Upgrade Behaviour (From 3.0.0)

5.1. Changed mapping of last opened in AVIT

- In previous versions, the "disclosure Time" of SCA issues was mapped to the "last opened" field of an AVIT. That behavior is now changed to "First detection date" in the third-party table as it is a more logical mapping for the integration.
- To see the "disclosure time" in ServiceNow, navigate to Application Vulnerable Items.
- Open any SCA AVIT that is fetched from V1 integration.

Application Vulnerable Item
AVIT0166163 View: Snyk

Number	AVIT0166163	State	Closed
Scan type	SCA	Reason	Fixed
Risk rating	5 - None	Assignment group	
Risk score	0	Assigned to	
Recommendation		First found	2024-11-20
Category name	vuln	Last found	2024-11-27
Vulnerability	CVE-2024-38828	Last opened	2024-11-20
Discovered Applications	mnhols-snyk/spring-integration-s	Closed	2024-12-19 22:25:23
Package	org.springframework:spring-webm	Closed by	VR System
Application module		Snyk Organization	Crest Data Systems NFR - Shared
Source exploitability	no-known-exploit	IsFixed	<input checked="" type="checkbox"/>
Description			
Location			
Summary			

- Now copy the Source AVIT ID of the same AVIT. (Exclude content after pipe(| for example, if Source AVIT ID is SNYK-JAVA-ORGSPRINGFRAMEWORK-8384234 | CVE-2024-38828, then copy only SNYK-JAVA-ORGSPRINGFRAMEWORK-8384234).
- Now Navigate to Third-party.
- Search with copied ID.

third-party

Favorites History Workspaces Admin Application Vulnerability Entries

All > ID contains SNYK-JAVA-ORGSPRINGFRAMEWORK-8384234

ID	Category name	Source
*SNYK-JAVA-ORGSPRINGFRAMEWORK-8384234	Search	Search
SNYK-JAVA-ORGSPRINGFRAMEWORK-8384234		Snyk

The screenshot shows the 'Application Vulnerability Entry' screen. At the top, there are fields for 'ID' (SNYK-JAVA-ORGSPRINGFRAMEV), 'Source' (Snyk), and 'Severity' (5 - None). To the right, there are fields for 'Primary CWE' and 'Category name'. Below these, a red box highlights the 'First detection date' field, which contains the value '2024-11-18'. Under the heading 'Vulnerability Details', there are sections for 'Threat' and 'Mitigation description'. A sub-section titled '[SN Utils] Versions (0)' is shown. Below it, a table titled 'CWEs (1)' lists one entry: 'CWE-ID' (CWE-400), 'Name' (CWE-400), and 'Class' (CWE). The table also includes columns for 'OWASP Top 10 Position' and 'SANS Top 25 Position'.

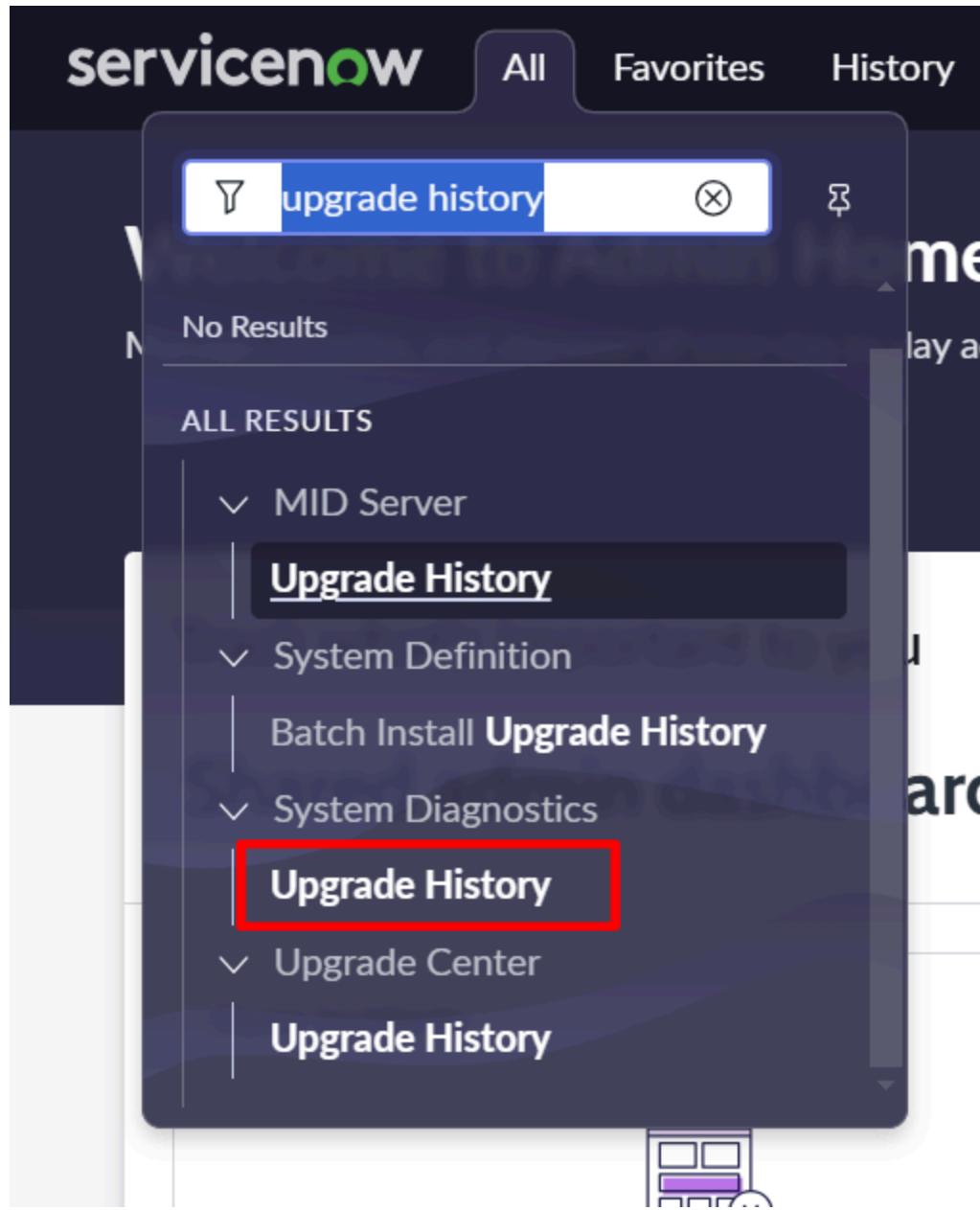
- Note: If the user has created a dashboard, assignment rule, etc., on the "last opened" field, then going forward, the user needs to use the "First detection" date of the Third-Party Entry table to get the same results.

5.2. Two false options in Vulnerability filtering (Perform the steps below to remove duplicate options)

Note: This will only apply if a user sees multiple false values on the vulnerability filtering page. Refer to the screenshot below for more details.

The screenshot shows the 'Vulnerability Filtering' screen. At the top, there is a note about Snyk SAST Vulnerabilities Import supports: Organizations, Lowest Severity, Projects, Branch, Target Name, Environment, Lifecycle, Source, Tags, Ignored, Status. It also includes a note about selecting filters for OR conditions. Below this, there are several dropdown menus for filtering vulnerabilities. Some dropdowns have 'All' selected, while others like 'Lowest Severity' and 'Ignored' show other options like 'Low' and 'True'. On the right side, there are additional filter categories: Branch, Languages, Exploit Maturity, Target Name, Environment, Lifecycle, Source, Tags, and Fixable.

- Navigate to System Diagnostic > Upgrade History.



- Search with To=x_snyk2_snyk_vr_in and Sorted in descending order with the field Upgrade started.

From	To	Upgrade started	Upgrade finished	Changes skipped	Changes applied	Changes processed
n/a	x_snyk2_snyk_vr_in	2024-12-11 01:16:13	2024-12-11 01:16:51	22	576	598
n/a	x_snyk2_snyk_vr_in	2024-12-11 00:32:23	2024-12-11 00:32:44	34	361	395
n/a	x_snyk2_snyk_vr_in	2024-12-10 23:31:04	2024-12-10 23:31:30	20	211	231
n/a	x_snyk2_snyk_vr_in	2024-12-10 23:12:24	2024-12-10 23:12:45	22	576	598
n/a	x_snyk2_snyk_vr_in	2024-12-10 21:52:12	2024-12-10 21:52:46	33	391	424
n/a	x_snyk2_snyk_vr_in	2024-12-10 21:37:40	2024-12-10 21:38:01	22	576	598
n/a	x_snyk2_snyk_vr_in	2024-12-10 20:58:59	2024-12-10 20:59:21	561	37	598

- Open the first record.
- Review the Skipped Changes to Review with a Disposition as Skipped Manual Merge.

Application scope: Rapid7 InsightCloudSec CC Integration
Update set: mayur dhamecha [Rapid7 InsightCloudSec CC Integration]

Upgrade History Details

Changes skipped	20
Changes applied	211
Changes processed	231
Copies to review	0
Auto resolved	0

• Changes skipped - The total number of records that were different from the previous upgrade and the upgrade component was not applied. To learn more, see [Skipped Changes to Review](#).
 • Changes applied - The total number of changes that were applied as a part of this upgrade.
 • Changes processed - The total number of records that were processed as a part of this upgrade.
 • Copies to review - The total number of copied records to review whose base record has been upgraded.
 • Claim outcomes to review - The total number of records impacted by claims as part of this upgrade. To learn more, see [Claim Outcomes to Review](#).
 • Auto resolved - The number of records automatically resolved by upgrade plans or skipped record rules

[SN Utils] | Versions (0)

Skipped Changes to Review (20) | Skipped Changes Reviewed | Copies to Review | Copies Reviewed | Customizations Unchanged (7) | Changes Applied (211) | Upgrade Details (644) | Claim Outcomes to Review

File name	Disposition	Claim Status	Priority	Resolution	Comment	Target name	Plugin	Type	Table	Reason
sys_choice_x_snyk2_snyk_vr_in_vulnerabil...	Skipped Manual Merge	● Priority 5	Not Reviewed	Vulnerability Filtering Environment	x_snyk2_snyk_vr_in	Choice list	sys_choice			
sys_choice_x_snyk2_snyk_vr_in_vulnerabil...	Skipped Manual Merge	● Priority 5	Not Reviewed	Vulnerability Exploit Maturity	x_snyk2_snyk_vr_in	Choice list	sys_choice			

- Open every record and do the following.
- Click on Resolve Conflicts

The Resolve Conflicts page displays a side-by-side comparison of the base system record and the corresponding customized record. Use the built-in diff editor to resolve conflicts in multi-line text fields.

- Click on Revert to Base System.

```

Base System
1 [<?xml version="1.0" encoding="UTF-8"?><record_update>
2   <sys_choice action="INSERT_OR_UPDATE" field="languages" table="x_snyk2_snyk_vr_in_vulnerability_filtering_languages">
3     <sys_choice_set action="INSERT_OR_UPDATE">
4       <element>languages</element>
5       <name>x_snyk2_snyk_vr_in_vulnerability_filtering</name>
6       <sys_class_name>sys_choice_sets</sys_class_name>
7       <sys_created_by>janviba.jhalac</sys_created_by>
8       <sys_created_on>2022-07-12 07:07:24</sys_created_on>
9       <sys_id>408e00ef97cbc1021f734771153afbg</sys_id>
10      <sys_mod_count>0</sys_mod_count>
11      <sys_name>languages</sys_name>
12      <sys_package display_value="Snyk Vulnerability Integration" source="x_snyk2_snyk_vr_in_vulnerability_filtering_l">
13        <sys_policy/>
14        <sys_scope display_value="Snyk Vulnerability Integration">72ac3c4487d81</sys_scope>
15        <sys_update_name>sys_choice_x_snyk2_snyk_vr_in_vulnerability_filtering_l</sys_update_name>
16        <sys_updated_by>janviba.jhalac</sys_updated_by>
17        <sys_updated_on>2022-07-12 07:07:24</sys_updated_on>
18      </sys_choice_set>
19      <sys_choice action="INSERT_OR_UPDATE">
20        <dependent_value/>
21        <element>languages</element>
22        <hint/>
23        <inactive>false</inactive>
24        <label>javascript</label>
25        <language>en</language>
26        <name>x_snyk2_snyk_vr_in_vulnerability_filtering</name>
27        <sequence>1</sequence>
28      </sys_choice>

```

```

Customized
1 [<?xml version="1.0" encoding="UTF-8"?><sys_choice action="INSERT_OR_UPDATE" field="languages">
2   <sys_choice_set action="INSERT_OR_UPDATE">
3     <element>languages</element>
4     <name>x_snyk2_snyk_vr_in_vulnerability_filtering</name>
5     <sys_class_name>sys_choice_sets</sys_class_name>
6     <sys_created_by>kashyap.mistry</sys_created_by>
7     <sys_created_on>2024-12-11 09:16:08</sys_created_on>
8     <sys_id>4b58c2d787961e107d5210ed3fb35ba</sys_id>
9     <sys_mod_count>0</sys_mod_count>
10    <sys_name>languages</sys_name>
11    <sys_package display_value="Snyk Security for Application Vulnerability Response Integration">Snyk Security for Application Vulnerability Response Integration</sys_package>
12    <sys_policy/>
13    <sys_scope display_value="Snyk Security for Application Vulnerability Response Integration">Snyk Security for Application Vulnerability Response Integration</sys_scope>
14    <sys_update_name>sys_choice_x_snyk2_snyk_vr_in_vulnerability_filtering_languages</sys_update_name>
15    <sys_updated_by>kashyap.mistry</sys_updated_by>
16    <sys_updated_on>2024-12-11 09:16:08</sys_updated_on>
17  </sys_choice_set>
18  <sys_choice action="INSERT_OR_UPDATE">
19    <dependent_value/>
20    <element>languages</element>
21    <hint/>
22    <inactive>false</inactive>
23    <label>javascript</label>
24    <language>en</language>
25    <name>x_snyk2_snyk_vr_in_vulnerability_filtering</name>
26    <sequence>1</sequence>
27    <synonyms/>
28  </sys_choice>

```

The Resolve Conflicts page displays a side-by-side comparison of the base system record and the corresponding customized record. Use the built-in diff editor to resolve conflicts in multi-line text fields.

- Do the same for the remaining record.
- Alternatively, the user can run the script below in "script - background" (Global Scope) to remove duplicate choices.

```

ar choiceGr = new GlideRecord("sys_choice");
choiceGr.addEncodedQuery("name=x_snyk2_snyk_vr_in_vulnerability_filtering
^element=fixable^ORelement=ignored^ORelement=isfixed^ORelement=is_fix
d^ORelement=is_patchable^ORelement=is_upgradable^ORelement=patched^
ORelement=is_pinnable^value!SEMPY");
choiceGr.query();
choiceGr.deleteMultiple();

choiceGr = new GlideRecord("sys_choice");
choiceGr.addEncodedQuery("name=x_snyk2_snyk_vr_in_fixable_filters^eleme
nt=is_fixable_upstream^ORelement=is_fixable_manually^ORelement=is_fixabl
e_snyk^value!SEMPY");
choiceGr.query();
choiceGr.deleteMultiple();

```

6. Upgrade Behaviour (From 3.1.0)

6.1. Changed mapping of Source exploitability in AVIT

- In previous versions, the source exploitability field wasn't mapped for the AVITs fetched using Integration - Snyk SCA & IaC Vulnerabilities Import (All Region - Rest API).
- To see the "Source exploitability" in ServiceNow, navigate to Application Vulnerable Items.
- Open any SCA AVIT that is fetched from REST integration.

Application Vulnerable Item
AVIT0388933 View: Snyk

Number: AVIT0388933
Scan type: SCA
Risk rating: 5 - None
Risk score: 0
Recommendation:
Category name: package_vulnerability
Vulnerability: CVE-2019-9193
Discovered Applications: mayurdhamecha-crest/k8s-goof/Dockerfile
Package: postgresql-9.6/libpq5
Application module:
Source exploitability: Proof of Concept
Description:
Location:
Summary:
Vulnerability score (v3):

State: Open
Assignment group:
Assigned to:
First found: 2024-11-20
Last found:
Last opened: 2025-08-11
Snyk Organization:
IsFixed:

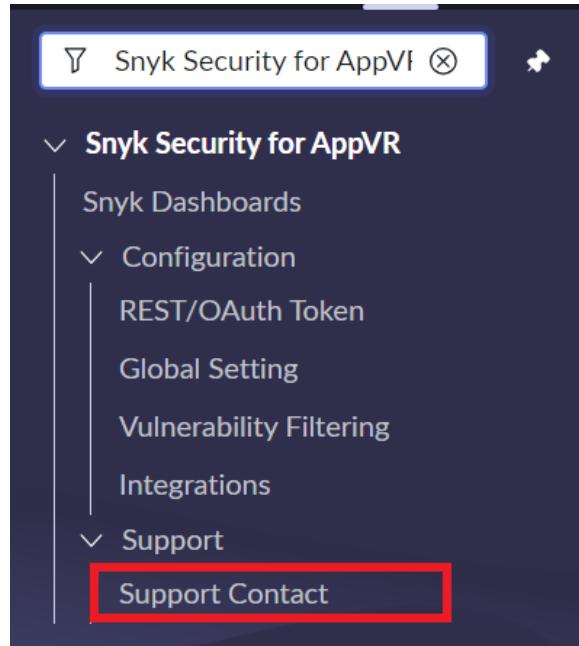
Findings **notes**

- The Source exploitability field is now mapped to the CVSSv4 value. If CVSSv4 is not available for that vulnerability, the CVSSv3 value will be used instead.
- Note: To map this field for existing records, clear the Start Time of the integration Snyk SCA & IaC Vulnerabilities Import (All Regions – REST API) and execute the integration again.

7. Support, Troubleshooting, and Known Behaviors

7.1. Support

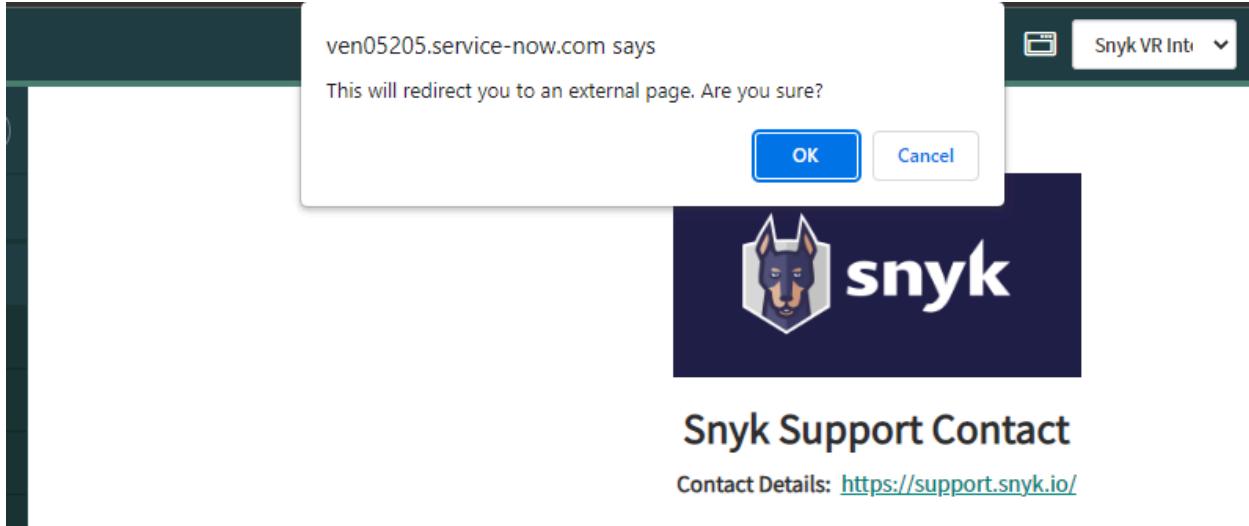
- Navigate to "Snyk Security for AppVR."
- For any issues related to the application, navigate to "Snyk Security for AppVR," and under it look for "Support" and select "Support Contact" from the dropdown menu.



- Support Contact opens with the Snyk support URL.
-



- Click on the contact detail links, which opens a pop-up with the message "You will be redirected to an external website. Are you sure?" Click on "OK" to open the link.



7.2. Troubleshooting

7.2.1. Unable to generate the token

- Navigate to Fix script under system definition from the navigation module.
- Search "Update Credentials" in the name.
- Open the record and click on "Execute Now."

The screenshot shows the ServiceNow System Definition - Fix Scripts interface. A fix script named "Update Credentials" is selected. The "Run Fix Script" button is highlighted in yellow. The script code is as follows:

```

1. try{
2. gs.info("Executing migration script to update snyk credentials.");
3. var authentityGr = new GlideRecord("auth_entity");
4. if(authentityGr.get(gs.getProperty("x_snyk2_snyk_vr_in.authentity$sysId"))){
5. authentityGr.client_id = gs.getProperty("x_snyk2_snyk_vr_in.clientId");
6. authentityGr.client_secret = gs.getProperty("x_snyk2_snyk_vr_in.clientSecret");
7. authentityGr.client_secret = authentityGr.client_secret.getDecryptedValue();
8. if(!authentityGr.update()){
9. gs.error("Error while updating the Credentials!");
10 }
11 gs.info("Successfully completed script for update snyk credentials.");
12 }catch(e){
13 gs.error("Exception in fix script: " + e);
14 }

```

- Now, try to generate the token again. It should be generated successfully.
- If you still face an error in token generation, follow the steps below.
- Navigate to Application Registry under System OAuth.
- Right-click on the header of the table column and open Configure > Table.

The screenshot shows the ServiceNow Application Registry interface. On the left, there's a sidebar with 'Security Operations' sections like Utilities, SecOps Application Registry, System Applications, Application Restricted Caller Ac..., System OAuth, and Application Registry. The 'Application Registry' section is highlighted. In the main area, a list of applications is shown with columns for Name, Type, Active status, and Search. A context menu is open over the 'ServiceNow Request' application, with 'Configure' selected. The menu also includes options like Sort (a to z), Sort (z to a), Ungroup, Group By Name, Bar Chart, Pie Chart, Launch Interactive Analysis, Import, Export, Update Selected, Update All, Data Management, Create Application Files, Import XML, Show XML, and Dictionary.

- Check the "Can Update" checkbox under application access. Mark it true and save the record.
- Run the "Update Credentials" fix script again.
- Generate the token. It should be generated successfully.

The screenshot shows the 'Application Access' configuration page for the 'ServiceNow Request' application. At the top, it says 'Table Application Registries' and 'You are editing a record in the Global application (cancel)'. Below that is a note: 'A table is a collection of records in the database. Each record corresponds to a row in a table, and each field on a record corresponds to a column on that table. Applications use tables and records to manage data and processes. [More Info](#)'. The configuration form has fields for Label ('Application Registries'), Name ('oauth_entity'), Application ('Global'), and Extends table ('Application File'). Under the 'Application Access' tab, there are sections for 'Accessible from' (set to 'All application scopes'), 'Can read' (checked), 'Can create' (unchecked), 'Can update' (checked, highlighted with a yellow box), 'Can delete' (unchecked), 'Allow access to this table via web services' (checked), and 'Allow configuration' (unchecked). At the bottom are 'Update' and 'Delete All Records' buttons, and a 'Related Links' section with links to Design Form, Layout Form, Layout List, and Show Form.

7.2.2. Unable to install "Snyk VR Integration" from the ServiceNow Store

- Verify you have the role of system administrator (admin).
- Navigate to "System Definition" and select "All" from the dropdown menu in your instance.
- Verify whether the following application has been installed or not. If not, then first [install this application](#).

7.2.3. Unable to create a new user

- Review the following link and execute the steps.

https://www.servicenow.com/docs/bundle/washingtondc-customer-service-management/page/administer/users-and-groups/task/t_CreateAUser.html

7.2.4. Unable to install/activate the plugin in ServiceNow Instance

- Review the following link and execute the steps.

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

7.2.5. The user deletes the Application Registry default record

- Uninstall the application and reinstall the application.

7.2.6. The user deletes the REST Message default record

- Uninstall the application and reinstall the application.

7.2.7. The user deletes any of the Integrations records

- Uninstall the application and reinstall the application.

7.2.8. Unable to search Lifecycle & Environment from AVIT

- Navigate to Application Vulnerable items.
- Click on the Show/Hide Filter icon from the top.

Number	Summary	Discovered Applications	Risk score	Risk rating	State	Remediation target	Remediation status
AVIT0149579	Apache Log4j2 2.0-beta9 through 2.15.0 (empty) (...)	mnichols-snyk/java-goof:todoist-goof/to...	100	1 - Critical	Open	(empty)	No Target
AVIT0151133	Apache Log4j2 2.0-beta9 through 2.15.0 (empty) (...)	mnichols-snyk/java-goof:log4shell-goof/l...	100	1 - Critical	Open	(empty)	No Target
AVIT0151917	Apache Log4j2 2.0-beta9 through 2.15.0 (empty) (...)	mnichols-snyk/java-goof:log4shell-goof/l...	100	1 - Critical	Open	(empty)	No Target

- Click on the dropdown and select Show Related Fields.

Number	Summary	Discovered Applications	Risk score	Risk rating	State	Remediation target	Remediation status
AVIT0149579	Apache Log4j2 2.0-beta9 through 2.15.0 (empty) (...)	mnichols-snyk/java-goof:todoist-goof/to...	100	1 - Critical	Open	(empty)	No Target
AVIT0151133	Apache Log4j2 2.0-beta9 through 2.15.0 (empty) (...)	mnichols-snyk/java-goof:log4shell-goof/l...	100	1 - Critical	Open	(empty)	No Target
AVIT0151917	Apache Log4j2 2.0-beta9 through 2.15.0 (empty) (...)	mnichols-snyk/java-goof:log4shell-goof/l...	100	1 - Critical	Open	(empty)	No Target

- Again, open the dropdown and select the Discovered Application > Discovered Application fields.

The screenshot shows a ServiceNow application window titled "Application Vulnerable Items View: Snyk". The top navigation bar includes "Run", "Save...", "AND", "OR", "Add Sort", and a search icon. Below the navigation is a search bar with dropdown operators ("-- oper --" and "-- value --") and buttons for "AND", "OR", and "X". A dropdown menu is open, showing various filter options such as "Discovered Applications", "Discovered Applications fields", "Domain", "Domain => Group fields", "Evidence", "Extension count", "First found", and "Has Vulnerable Methods". The main table displays two rows of data:

	Discovered Applications	Risk score	Risk rating	State	Remediation target	Remediation status
AVIT0151133	Apache Log4j2 2.0-beta9 through 2.15.0 (empty)	● 100	1 - Critical	Open	(empty)	No Target
AVIT0151917	Apache Log4j2 2.0-beta9 through 2.15.0 mnichols-snyk/java-goof:log4shell-goof/l...	● 100	1 - Critical	Open	(empty)	No Target

At the bottom, there is a navigation bar with arrows and a page number indicator "1 to 100 of 3,578".

- Now again, open the dropdown and select the Description.

This screenshot shows the same "Application Vulnerable Items View: Snyk" window. The dropdown menu is now focused on the "Discovered Applications.Description" option. The main table displays the same two rows of data as the previous screenshot. The navigation bar at the bottom is identical.

7.2.9. Unable to see CVE & CWE in the Third-party records

- Open Application Vulnerability Response> Libraries> Third-Party, Open the third-party record.
- Click on Additional Action > Configure> Related Lists. The form will open. Add the CVE & CWE to the selected list and click save.

7.2.10. Organizations were not found, or you do not have permission to access them

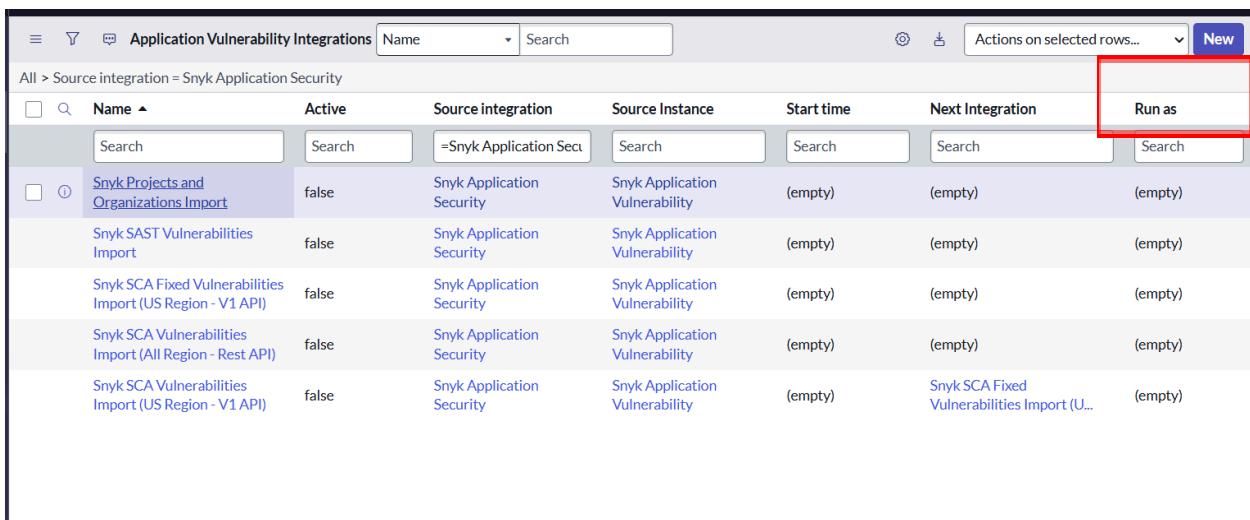
- Snyk Apps can only be authorized for a single org or all orgs in a group. If you attempt to authorize for multiple orgs (without using All Orgs), the authorization will only be for the last Org authorized.

7.2.11. Invalid Redirect URL error message while authorizing Snyk Application

- The user must ensure that the instance redirect URL (i.e., https://YOUR-INSTANCE.service-now.com/oauth_redirect.do) is provided to the Snyk team through email (servicenow@snyk.io).

7.2.12. Able to generate the token, but integration is failing.

- The integration run fails if a value is assigned in the **Run as** field in the integration configuration. Make sure that you keep it empty for all the integrations.



Application Vulnerability Integrations							Name	Search			Actions on selected rows...	New
All > Source integration = Snyk Application Security	<input type="checkbox"/>	<input type="checkbox"/>	Name	Active	Source integration	Source Instance	Start time	Next Integration	Run as			
	<input type="checkbox"/>	<input type="checkbox"/>	Search	Search	=Snyk Application Secu	Search	Search	Search	Search	Search		
	<input type="checkbox"/>	Snyk Projects and Organizations Import	false	Snyk Application Security	Snyk Application Vulnerability	(empty)	(empty)	(empty)				
	<input type="checkbox"/>	Snyk SAST Vulnerabilities Import	false	Snyk Application Security	Snyk Application Vulnerability	(empty)	(empty)	(empty)				
	<input type="checkbox"/>	Snyk SCA Fixed Vulnerabilities Import (US Region - V1 API)	false	Snyk Application Security	Snyk Application Vulnerability	(empty)	(empty)	(empty)				
	<input type="checkbox"/>	Snyk SCA Vulnerabilities Import (All Region - Rest API)	false	Snyk Application Security	Snyk Application Vulnerability	(empty)	(empty)	(empty)				
	<input type="checkbox"/>	Snyk SCA Vulnerabilities Import (US Region - V1 API)	false	Snyk Application Security	Snyk Application Vulnerability	(empty)	Snyk SCA Fixed Vulnerabilities Import (U...	(empty)				

7.2.13. Getting Reconcile-related errors while running integration.

- This error occurs when multiple VR integrations are running on the same instance.
- Follow the steps below if you get this error while running Snyk integrations.

Vulnerability Integration Run
VINTRUN0007378

Number	VINTRUN0007378	State	Complete
Integration	Snyk Projects and Organizations	Substate	Failed
Start datetime	05.04.2024 04:28:59	Import source	Snyk
End datetime	05.04.2024 04:28:59		

Notes

Create a new integration run when the Reconcile unmatched discovered items job is complete.

Parameters

Fatal error message

- Navigate to `sn_sec_cmn_background_job.list`
- Make sure all the listed job states are complete. If any job is not in a "complete" state and the job is important, wait for [the background job to finish](#). If a background job is unimportant, mark it complete using the script below.
- If you can change the state of the job from the UI, then you can mark the job as completed. Otherwise, run the script below in scripts - Background while in the Global scope. You can copy the sys_id of job by right-clicking on the record.


```
var gr = new GlideRecord("sn_sec_cmn_background_job");
if (gr.get("<sys_id of background job>")){
    gr.state = "complete";
    gr.update();
}
```
- Run the Snyk integration again.

7.2.14. [Unable to ignore an issue from ServiceNow to Snyk. Getting 403 Error in Outbound HTTP Calls.](#)

- Open the Snyk platform at the organization level. Go to Settings.

Ignores

Control how ignore policies are applied to projects within this organization.

Ability to ignore an issue, or edit the ignore settings on an issue through the Snyk app or API

Admin users only
 All users in any environment

Ability to ignore issues through the CLI or .snyk file

- In General settings, You must select "All users in any environment" to successfully ignore the issue.
- To restrict the ability of developers to ignore issues in Snyk without ignoring them in ServiceNow, a custom group role must be created in the Snyk UI at the Group level that

does not allow members of that group to ignore items. Then, developers who should not be allowed to add an ignore in Snyk must be added to that group. See this documentation from Snyk on how to create the custom roles:

<https://docs.snyk.io/snyk-admin/manage-permissions-and-roles/user-role-management>.

7.3. Known Behaviors

- 7.3.1. **Vulnerability Integration fails when one integration is running and the second integration is executed.**
 - Snyk uses the ServiceNow default OAuth2 mechanism to manage tokens. The OAuth credentials table is only accessible by the token owner, a user with the "maint" role, or a system admin.
 - Because of the limitations of the read ACL, the Snyk integration run fails when run as the user VR.system while a job with that user is still running.
 - The vulnerability response scheduler runs the integration as a VR.system user when one job is already running and the second executes.
 - To avoid this case, don't manually execute a Snyk import job when one run is already in process. If you want to run an integration job, then cancel the running integration run and retry.
- 7.3.2. **The Snyk application vulnerable item is in the open state even if the Snyk issue is fixed in the Snyk platform.**
 - If the first ingestion of the Snyk issue does not contain CVEs, but the second ingestion of the same Snyk issue does, two AVITs are made for that issue.
 - AVIT that refers to the third-party vulnerability
 - AVIT that refers to the particular CVE
 - If the Snyk issue is fixed on the Snyk side, only the AVIT that refers to the CVE will be closed, while the other AVIT will remain open.
 - To avoid this case, follow the steps below to close AVIT manually.
 - Navigate to the Application Vulnerable Item "Application Vulnerability Response." Under it, click "Vulnerable Items" and then select "All."
 - Filter as "Source" "is" "Snyk," and then click on "Run" to view all the issues that are fetched from the Snyk.
 - Click the AVIT record that you want to close manually.
 - Click on the "Close" UI action.

The screenshot shows the 'Application Vulnerable Item' record view in ServiceNow. The record ID is AVIT0004760 [Snyk view]. The 'Close' button in the top right corner is highlighted with a red box. The form contains various fields: Number (AVIT0004760), Scan type (SCA), Risk rating (1 - Critical), Risk score (100), Category name (vuln), Assignment group (App-Sec Manager), Assigned to (empty), First found (2022-10-19), Last found (empty). Other fields include Vulnerability (npm:marked:20170815-1), Application release (JanvibaJhala/snyk-goof;package.json), Package (marked), Application module (empty), Location (empty), and Summary (empty). Below the main form, there are tabs for Findings, HTTP Request/Response, and notes. Under the Findings tab, Source AVIT ID is npm:marked:20170815-1, Source severity is medium, Source mitigation status is empty, and Source remediation status is empty.

7.3.3. The state of existing AVIT will not update from "Deferred" to Open when Triaging in ServiceNow is selected.

- An AVIT already fetched with Triaging in ServiceNow as false in vulnerability filtering will have a "Deferred" state if ignore is true. When Triaging in ServiceNow is selected, and integration is executed again, the existing AVIT state won't be updated to Open, as ServiceNow doesn't allow changing the state automatically if it is deferred.
- If you want to change the state from "Deferred" to "Open," you must do so manually. ServiceNow doesn't override the "Deferred" state to "Open."

7.3.4. Recently Ignored issues on the Snyk side could take ~5 hours to reflect in SCA V1 API.

- When the user ignores the issue from ServiceNow or manually ignores the SCA or IaC issue, it could take up to ~5 hours to reflect in GET v1 API.

7.3.5. Additional comments and state updates on the Snyk side may take up to ~9 hours in the US region. Typical performance is right away.

- When a user marks an AVIT as "Mark as False positive" or "Request Exception," then the "Additional comment" added by the user and the state of the issue will be updated to the Snyk platform after 9 hours ([Ref](#)).
- While changing the state of vulnerability from ServiceNow to Snyk, wait at least 9 hours to compare the state on Snyk with ServiceNow.

7.3.6. Users must be added to the approver group for performing "Mark as False positive" and "Request Exception."

- When the user marks an AVIT as "Mark as False Positive" or "Request Exception," the AVIT state will be set to "In Review," and the request must be approved.

- For users to approve the request of "Mark as False Positive," they must be in the "False Positive Approver" group.
- Users must be in the Application Exception Approver-Level 1 group to approve the request of "Request Exception."
- If users are not added to the group, the Request will be automatically rejected, as per ServiceNow VR default behavior.
- To avoid this case, ensure users are added to the approver group for performing "Mark as False positive" and "Request Exception."

7.3.7. Users must initiate the Reapply calculator's UI action inside the VR scope.

- If the user wants to change or reapply the Snyk calculator, ensure this is done in the Vulnerability Response scope.

7.3.8. Unable to "Mark as False positive" or "Request Exception" for IaC issues.

- If the user has set the REST mechanism for fetching the IaC issues in Global Settings and fetched IaC issues from integration, the integration cannot set an ignore on the Snyk platform.
- Release 3.0.0 version does not support the "Mark as false positive" or "Request exception" for IaC issues fetched from REST integration.

7.3.9. Use of "Move Project" V1 Snyk API can lead to unexpected results in SN Integration.

- Using the Snyk V1 "Move Projects" API to move a project will result in unexpected results, including the likelihood that the AVITs associated with the project will become orphaned in ServiceNow. The recommended process is to delete the target in Snyk and re-import the project into the new Org.

7.3.10. OAuth Process

- Snyk now allows customers to have a "Tenant" with multiple Groups. Customers may only select orgs from a single group during the OAuth process. A single integration will not import data across multiple groups due to the permission boundaries of the OAuth tokens.

The OAuth token process can only grant authorization to a SINGLE Org or all Orgs. Selecting multiple Orgs is currently unavailable and will be included in a future release.



Snyk for ServiceNow AppVR is requesting access permissions

- Read and Write** access to: Edit organization information and settings, Edit project information, Activate and deactivate projects, Create new project ignores, Configure project ignores
- Read** access to: View organization information and settings, View reports in your organization, View project information and settings, View project dependencies, vulnerabilities, and other information obtained by scanning projects, View project ignore information

Give Snyk for ServiceNow AppVR access to the following:

- Partner NFR

A group is a parent that can contain one or multiple organizations. [View Docs](#)

Give Snyk for ServiceNow AppVR access to the following organizations

- All Organizations
 Select Organizations

NFR - Shared

Cancel

Grant app access

END OF DOCUMENT...