Mandiant

ASM SERVICENOW INTEGRATION

ServiceNow is an automated cloud workflow solution. Using the Mandiant Advantage Attack Surface Management (MA-ASM) integration, you can create enterprise workflow applications to track MA-ASM Issues. This way, you can synchronize issue management between ServiceNow and MA-ASM; reflecting status changes and remediation progress in both products.

This integration provides interaction with ServiceNow Vulnerability Response only. The integration collects Issues from MA-ASM and maps them to the ServiceNow data model. This lets you work with Issues detected in MA-ASM and follow your workflow using the ServiceNow interface.

> This integration is bidirectional. Updates made in ServiceNow are seen in MA-ASM just as updates made to Issues in MA-ASM are visible in ServiceNow.

Integration configuration

Get and install the **Mandiant Advantage Attack Surface Management** Integration from the **ServiceNow Store**. Then, follow these steps in ServiceNow:

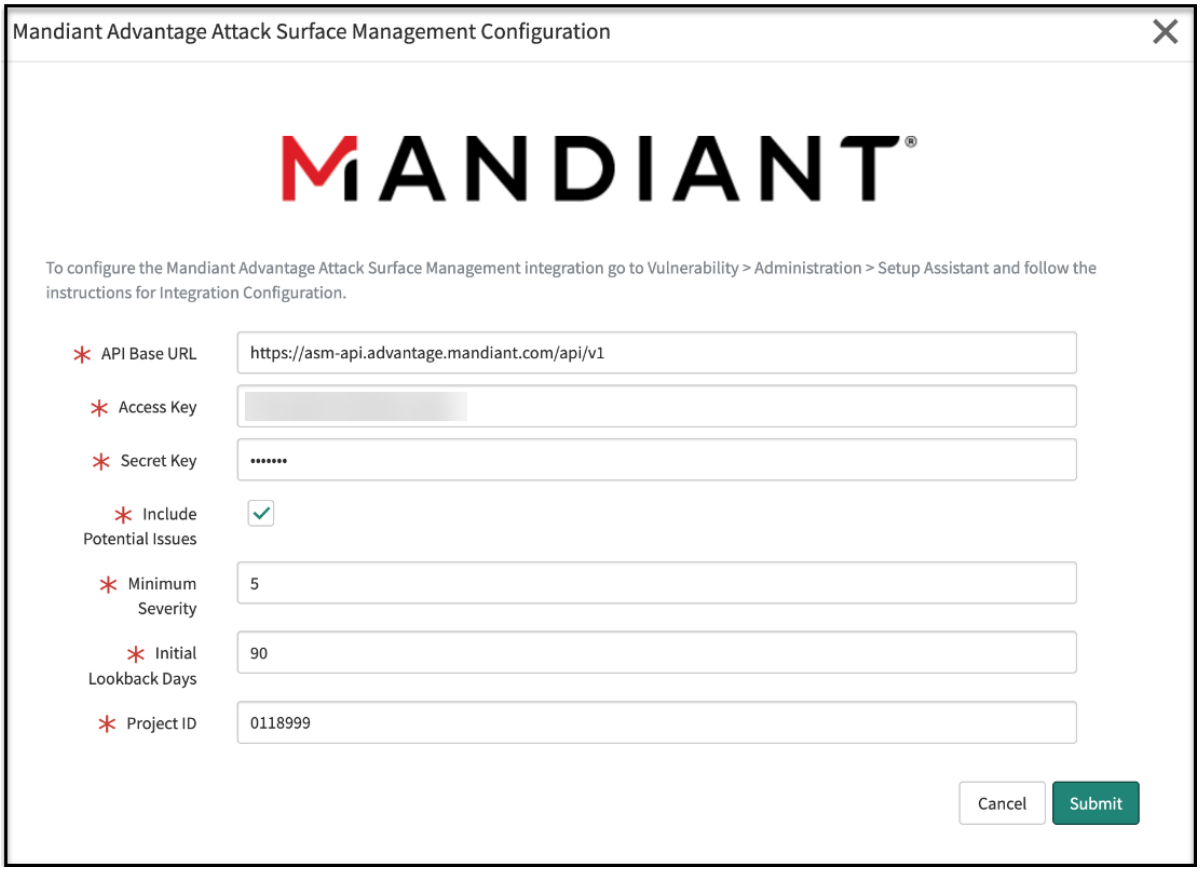
1. Navigate to **Security Operations > Integrations > Integration Configurations**.
2. Click **Configure** for the **Mandiant Advantage Attack Surface Management** integration**.**
3. Enter the integration parameters:
   - **API Base URL** defaults to `https://asm-api.advantage.mandiant.com/api/v1`.
   - MA-ASM **Access Key** and **Secret Key** are available in **API Keys** section of MA-ASM **Account Settings**.
   - (Optional) Select to **Include Potential Issues** if you'd like to include unconfirmed Issues.
   - Enter a value to define the **Minimum Severity** of Issues to import:
     - 1 = Critical
     - 2 = High
     - 3 = Medium (suggested)
     - 4 = Low
     - 5 = Informational
   - Enter a numeric value for the **Initial Lookback Days** setting. The default is 90.

     > This setting only applies to the first run of the scheduled import job. Subsequent runs are performed on an incremental basis as defined in the **Vulnerable Item Import** page of ServiceNow.

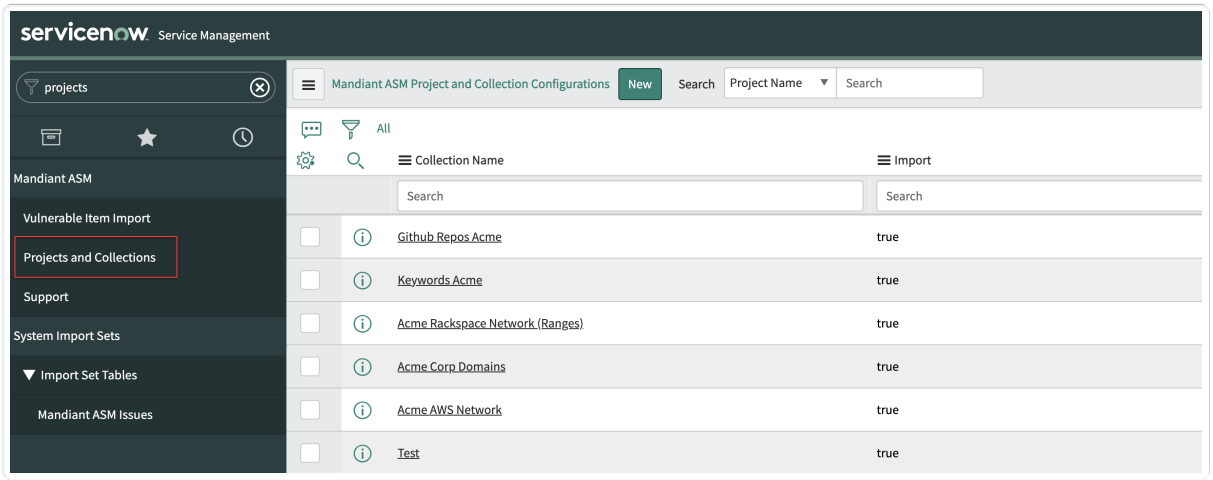
   - Enter a string value representing the **Project ID** that you want to access.

     > To identify a `project_id`, run the following curl command:
     >
     > ```
     > curl --location --request GET 'https:\
     > //{{baseUrl}}/api/v1/projects' \
     > --header 'INTRIGUE_ACCESS_KEY: {{intrigue_access_key}}' \
     > --header 'INTRIGUE_SECRET_KEY: {{intrigue_secret_key}}'
     > ```
     >
     > For more information, see **Attack Surface Management API**.

4. Click **Submit**.

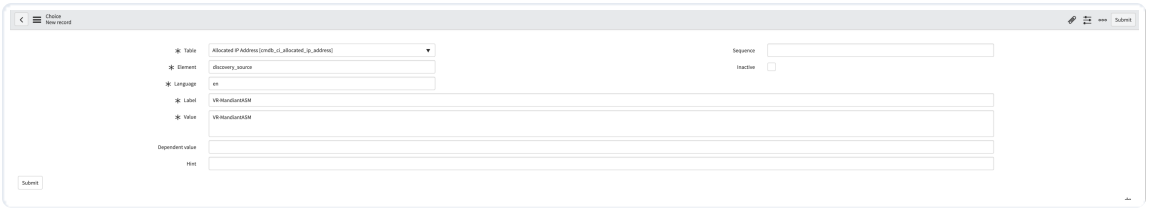


5. Navigate to **Mandiant ASM > Projects and Collections** and select the Collections to be imported.

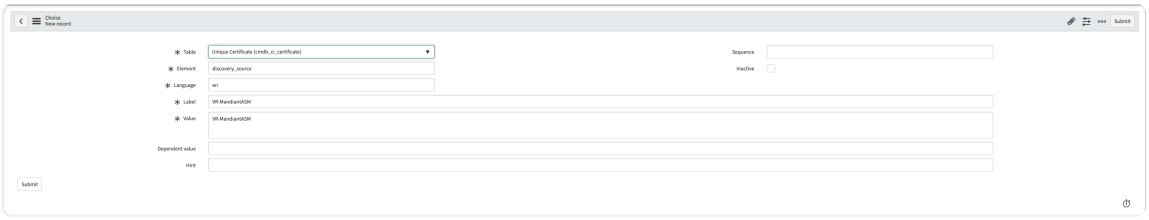


Collections must all be from the same Project.

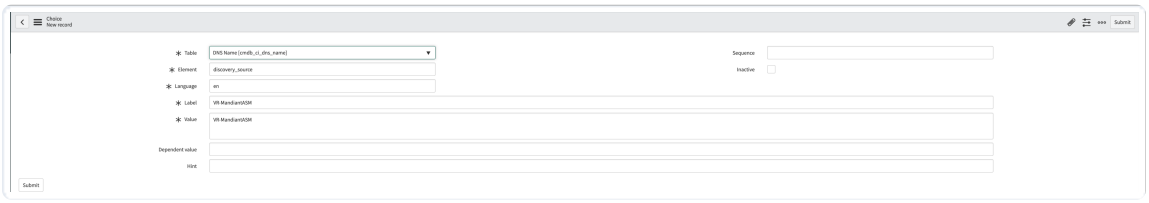
6. Ensure you are in the *CMDB CI Class Models* application. Search for `sys_choice.list` in the Search field. Add three new Choices as follows:
   a. **Table**: `Allocated IP Address [cmdb_ci_allocated_ip_address]`
      Element: `discovery_source`
      Label: `VR-MandiantASM`
      Value: `VR-MandiantASM`



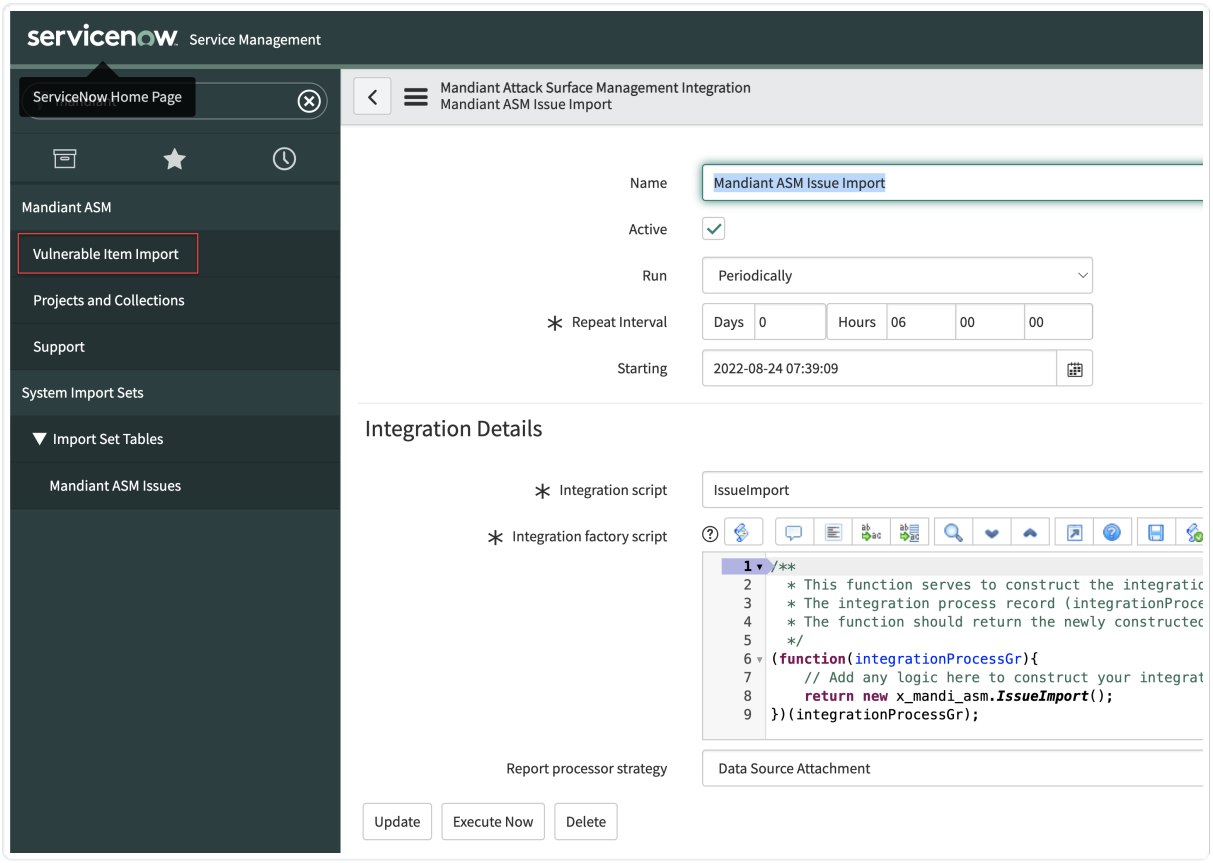
b. **Table**: `Unique Certificate [cmdb_ci_certificate]`
Element: `discovery_source`
Label: `VR-MandiantASM`
Value: `VR-MandiantASM`



c. **Table**: `DNS Name [cmdb_ci_dns_name]`
Element: `discovery_source`
Label: `VR-MandiantASM`
Value: `VR-MandiantASM`



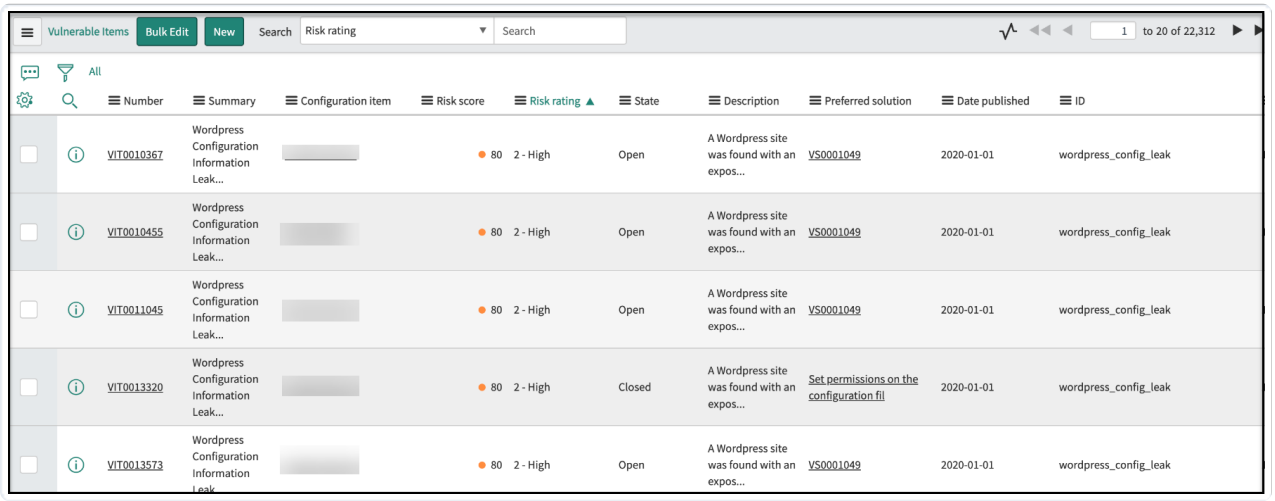
7. Navigate to **Mandiant ASM > Vulnerable Item Import** and define the schedule you want to use. The default is six hours.



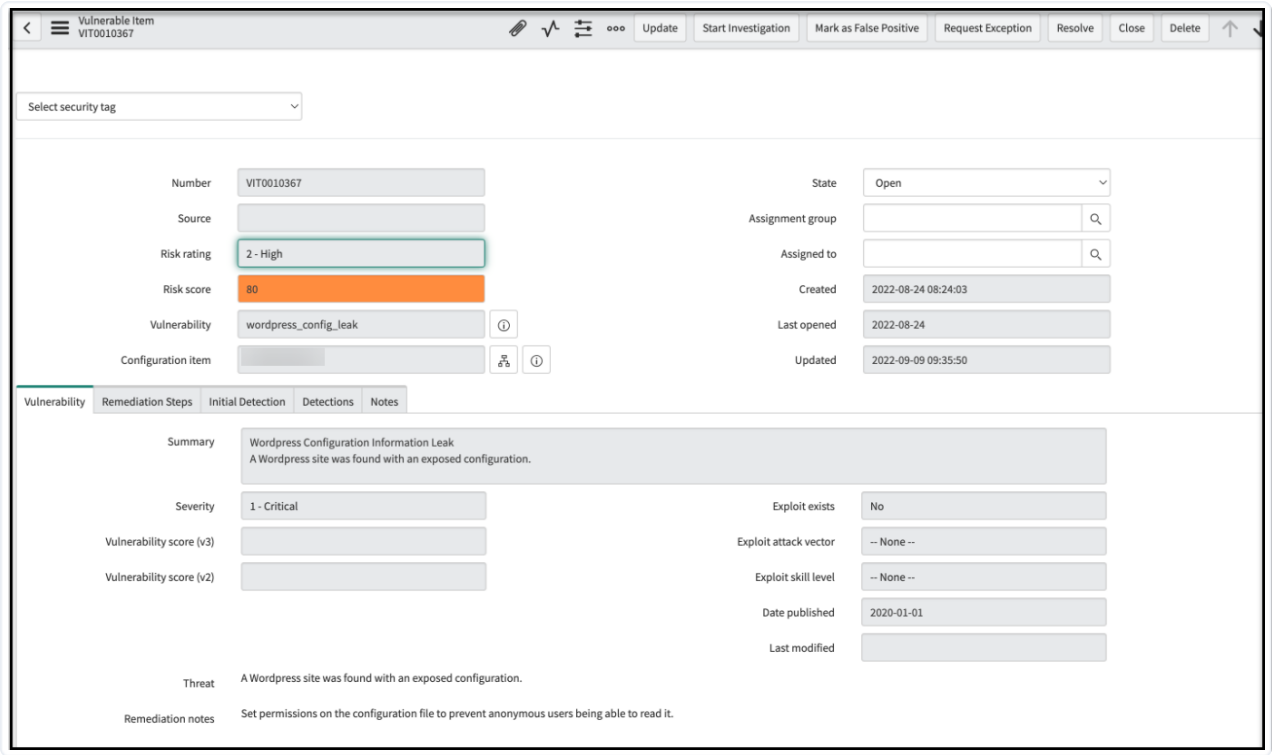
8. Click **Update**. Alternatively, click **Execute Now** if you want to run the job immediately.

Vulnerable Items in ServiceNow

Once integrated, you can view **Vulnerable Items** in ServiceNow:



To display more details and perform actions on an item, select a Vulnerable Item from the list.



Troubleshooting Tips

To view application logs:

- In ServiceNow, open a failed **Project and Collections** import.
- Open the **Notes** tab.
- Review the logs.

To force an import using the original **Lookback Days** setting:

- In ServiceNow, search for the `x_mandi_asm_mandiant_attack_surface_management_integration.list` page.
- To reset the job last run date and force an update, manually clear the **Download Issues Since** field.

The next time the job runs, the original **Lookback Days** setting is used as the start date.

ASM ServiceNow Field Mapping

ASM Field	ServiceNow Table	ServiceNow Field
confidence	Vulnerable Item Detection	Confirmed
summary/status_new	Vulnerable Item Detection	Source status
id	Vulnerable Item Detection	Vulnerable Item/external_id
details/proof	Vulnerable Item Detection	Proof
name	Vulnerable Item Detection	Solution/source_id
identifiers/name	Vulnerable Item Detection	Vulnerability

ASM Field	ServiceNow Table	ServiceNow Field
details/name	Vulnerable Item Detection	Vulnerability
summary/status	Vulnerable Item Detection	Status
first_seen	Vulnerable Item Detection	First found
details/remediation	Vulnerable Item Detection	Solution summary
last_seen	Vulnerable Item Detection	Last found
display_name	Mandiant ASM Projects and Collections Configuration	Display Name
project_name	Mandiant ASM Projects and Collections Configuration	Project Name
collection_id	Mandiant ASM Projects and Collections Configuration	Collection ID
collection_name	Mandiant ASM Projects and Collections Configuration	Collection Name
project_id	Mandiant ASM Projects and Collections Configuration	Project ID
details/remediation	National Vulnerability Database Entry	Solution
details/category	National Vulnerability Database Entry	Classification
identifiers/name	National Vulnerability Database Entry	ID
details/pretty_name	National Vulnerability Database Entry	Name
details/severity	National Vulnerability Database Entry	Source Severity
details/description	National Vulnerability Database Entry	Threat
details/severity	National Vulnerability Database Entry	Normalized Severity
details/added	National Vulnerability Database Entry	Date Published
details/pretty_name	National Vulnerability Database Entry	Summary
details/description	National Vulnerability Database Entry	Summary
details/vendor	Third Party Vulnerability Entry	Vendor
details/added	Third Party Vulnerability Entry	Date Published
details/pretty_name	Third Party Vulnerability Entry	Summary
details/description	Third Party Vulnerability Entry	Summary
name	Third Party Vulnerability Entry	Preferred Solution
details/name	Third Party Vulnerability Entry	ID
details/severity	Third Party Vulnerability Entry	Source Severity
details/remediation	Third Party Vulnerability Entry	Solution

ASM Field	ServiceNow Table	ServiceNow Field
details/severity	Third Party Vulnerability Entry	Normalized Severity
details/category	Third Party Vulnerability Entry	Category
details/description	Third Party Vulnerability Entry	Threat
category	Third Party Vulnerability Entry	Classification
details/description	Third Party Vulnerability Entry	Name
details/remediation	Vulnerability Solution	Description
name	Vulnerability Solution	Source ID
description	Vulnerable Item	Description
id	Vulnerable Item	External ID
status	Vulnerable Item	Status
summary/pretty_name	Vulnerable Item	Short Description
identifiers/name	Vulnerable Item	Vulnerability
details/name	Vulnerable Item	Vulnerability
summary/status	Vulnerable Item	State