

ASM CORTEX XSOAR INTEGRATION

Cortex XSOAR from Palo Alto Networks is a security orchestration, automation, and response (SOAR) platform that unifies case management, automation, real-time collaboration, and threat intel management to serve security teams across the incident lifecycle.

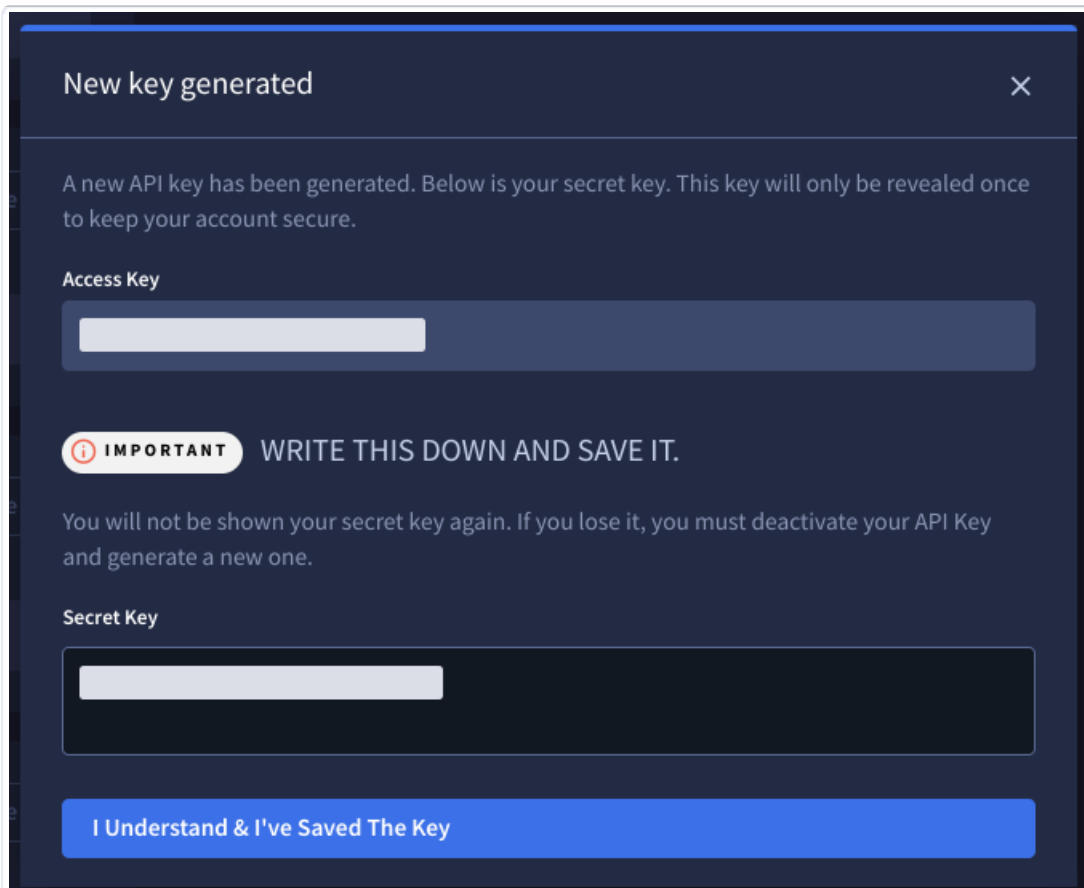
This Cortex XSOAR integration lets you import Mandiant Advantage Attack Surface Management (MA-ASM) Issues into XSOAR as Incidents. The process for configuring this integration is outlined in the following sections.

Generate API credentials in the MA-ASM platform

1. In MA-ASM, navigate to **Projects and Settings > Account Settings**.
2. Click **API Keys** to bring up a list of any keys that exist.
3. Click **Generate New Key** and make a note of the **Access Key** and **Secret Key** that are shown. These keys are used when configuring access to a Collection in XSOAR.



This is the **ONLY** time that you have access to this information. If these keys are lost, you must remove this set and generate a new pair.

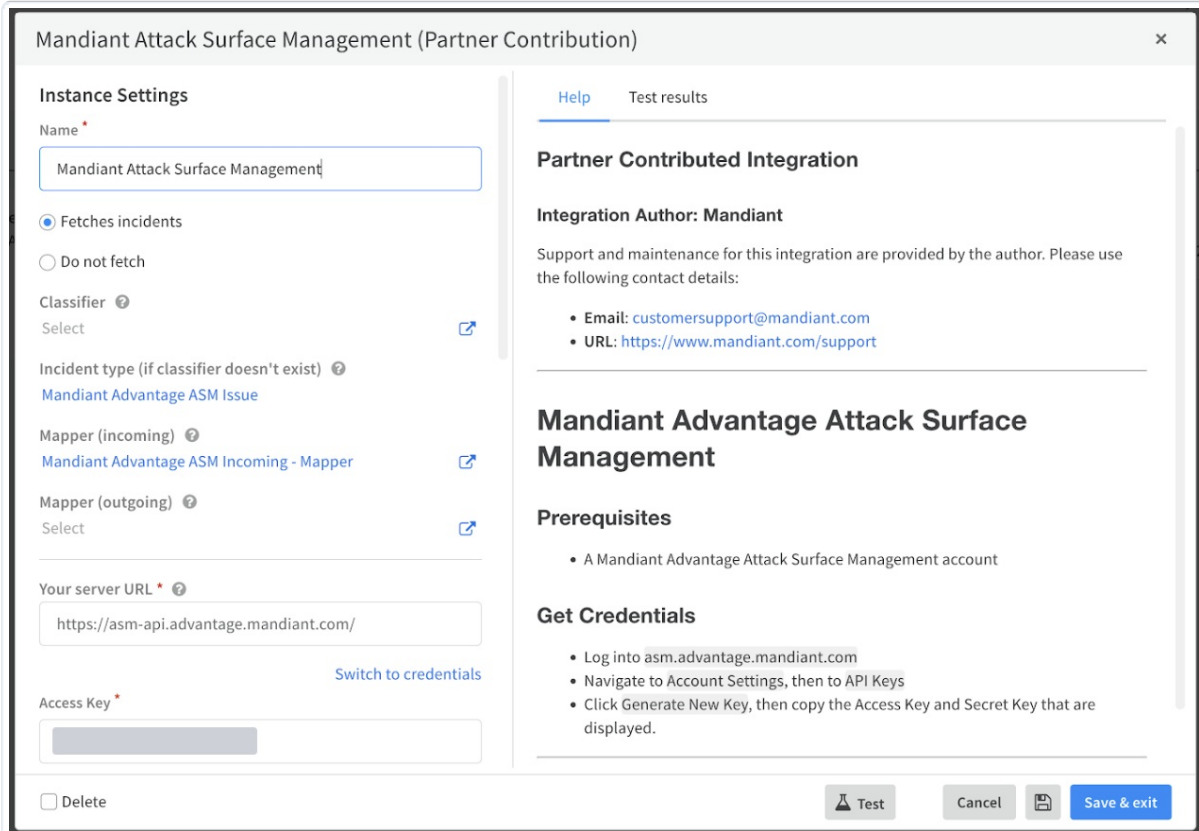


4. Click **I understand & saved the key**.

Add the MA-ASM Integration to your Cortex XSOAR Configuration

1. Access the **Cortex XSOAR Marketplace** (<https://cortex.marketplace.pan.dev/marketplace/>) and search for the Mandiant Advantage Attack Surface Management integration.
2. Download and install the Mandiant Attack Surface Management integration pack.

3. Within your Cortex XSOAR instance, navigate to **Settings > Integrations**.
4. Search for the Mandiant Advantage Attack Surface Management integration, and click **Add Instance** to configure a new instance of the integration.
5. Enter **Name**, select **Fetches incidents**, and enter `https://asm-api.advantage.mandiant.com/` as **Your server URL**.



The screenshot shows the configuration interface for the Mandiant Advantage Attack Surface Management integration. The window title is "Mandiant Attack Surface Management (Partner Contribution)".

Instance Settings

- Name:** Mandiant Attack Surface Management
- Fetches incidents:** Fetches incidents, Do not fetch
- Classifier:** Select (with a help icon)
- Incident type (if classifier doesn't exist):** Mandiant Advantage ASM Issue
- Mapper (incoming):** Mandiant Advantage ASM Incoming - Mapper
- Mapper (outgoing):** Select
- Your server URL:** `https://asm-api.advantage.mandiant.com/` (with a help icon)
- Access Key:** [Redacted]

[Switch to credentials](#)

Delete

Partner Contributed Integration

Integration Author: Mandiant

Support and maintenance for this integration are provided by the author. Please use the following contact details:

- **Email:** `customersupport@mandiant.com`
- **URL:** `https://www.mandiant.com/support`

Mandiant Advantage Attack Surface Management

Prerequisites

- A Mandiant Advantage Attack Surface Management account

Get Credentials

- Log into `asm.advantage.mandiant.com`
- Navigate to Account Settings, then to API Keys
- Click Generate New Key, then copy the Access Key and Secret Key that are displayed.

Buttons: **Test**, **Cancel**, **Save & exit**

6. Enter **Access Key** and **Secret Key** from the Cortex XSOAR integration settings in the MA-ASM platform described in the preceding section.
7. Define **Maximum Issues to Fetch** and **Minimum Severity**. See the **Numeric Severity** (<https://docs.mandiant.com/home/asm-issue-severity-definitions-and-examples#numeric>) for more information.
8. Adjust additional settings to suit your environment and requirements then click **Save & exit**.

Mandiant Attack Surface Management (Partner Contribution)

Access Key *

[Help](#) Test results

Partner Contributed Integration

Integration Author: Mandiant

Support and maintenance for this integration are provided by the author. Please use the following contact details:

- Email: customersupport@mandiant.com
- URL: <https://www.mandiant.com/support>

Mandiant Advantage Attack Surface Management

Prerequisites

- A Mandiant Advantage Attack Surface Management account

Get Credentials

- Log into asm.advantage.mandiant.com
- Navigate to Account Settings, then to API Keys
- Click Generate New Key, then copy the Access Key and Secret Key that are displayed.

Secret Key *

Project ID ?

Collection IDs ?

First fetch timestamp (<number> <time unit>, e.g., 12 hours, 7 days) ?

Maximum Issues To Fetch * ?

Minimum Severity * ?

Trust any certificate (not secure)

Use system proxy settings

Delete

Test Cancel Save & exit

Included commands for XSOAR

Two commands have been included with this integration to assist you with obtaining the Project IDs and Collection IDs for the configuration.

1. `!attacksurfacemanagement-get-projects` shows a list of all the Projects associated with your API key and their corresponding IDs.

May 4, 2023 9:38 AM

`!attacksurfacemanagement-get-projects`

DBot
May 4, 2023 9:38 AM

Command: `!attacksurfacemanagement-get-projects` (AttackSurfaceManagement)

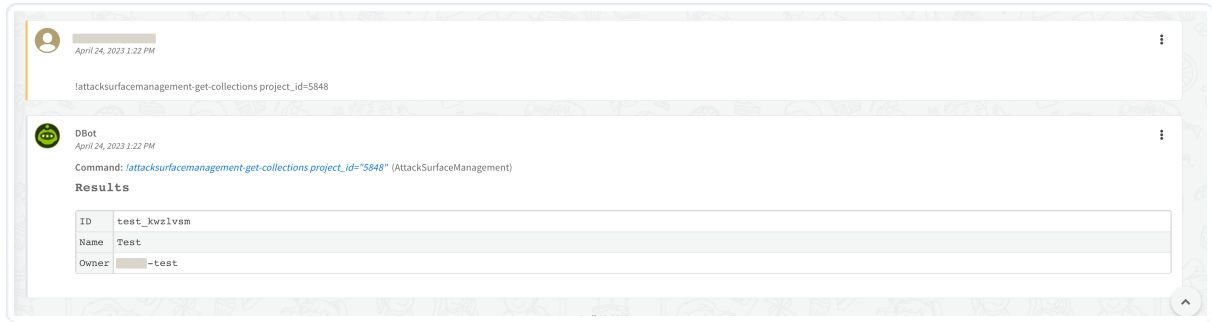
Results

ID	Name	Owner
2771	ASM Sample Project	[REDACTED]@mandiant.com
5081	Crazy Catfood	[REDACTED]@mandiant.com
5848	chris-test	[REDACTED]@mandiant.com

2. `!attacksurfacemanagement-get-collections` shows a list of all the collections within the Project configured in the instance configuration.



If a `project_id` is provided, it overrides the Project ID in the integration configuration.



April 24, 2023 1:22 PM

tattacksurfacemanagement-get-collections project_id=5848

DBot
April 24, 2023 1:22 PM

Command: `tattacksurfacemanagement-get-collections project_id="5848"` (AttackSurfaceManagement)

Results

ID	test_kwzlvsm
Name	Test
Owner	-test