Mandiant

ASM CORTEX XSOAR INTEGRATION

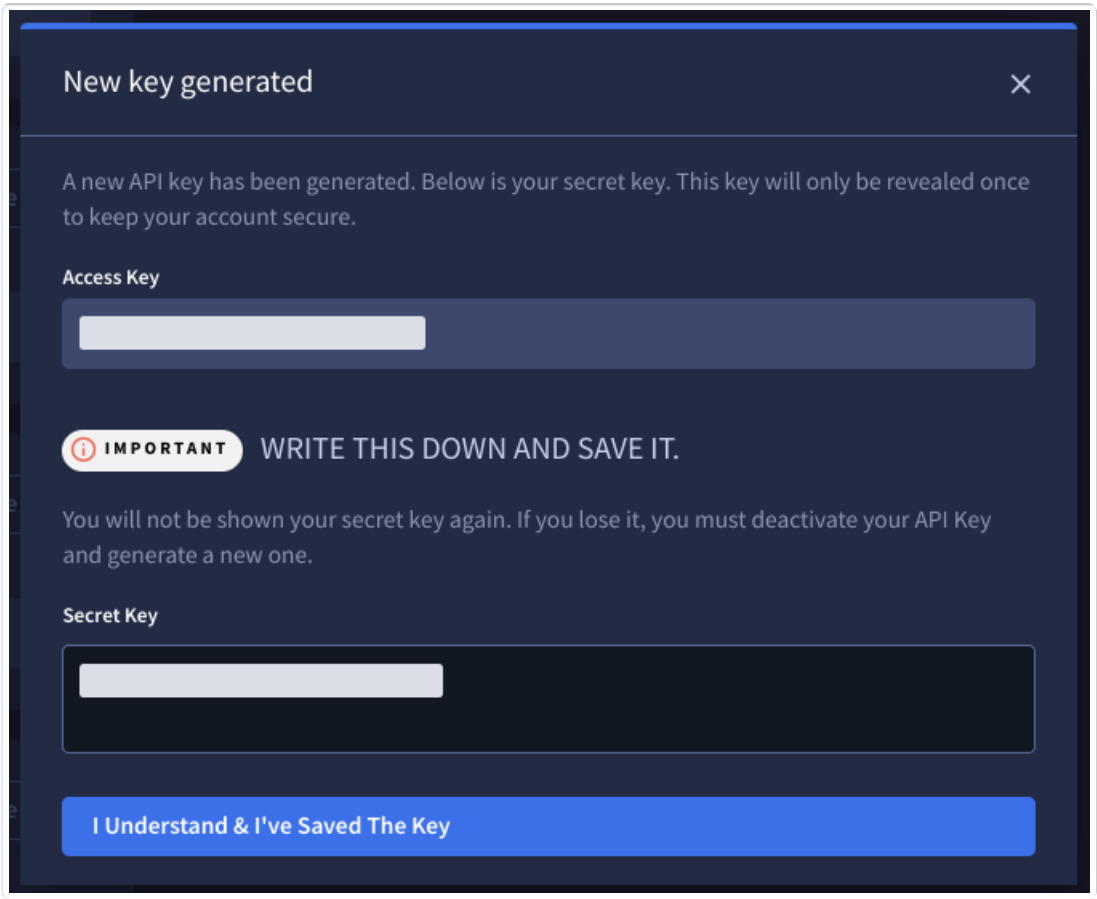
Cortex XSOAR from Palo Alto Networks is a security orchestration, automation, and response (SOAR) platform that unifies case management, automation, real-time collaboration, and threat intel management to serve security teams across the incident lifecycle.

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.

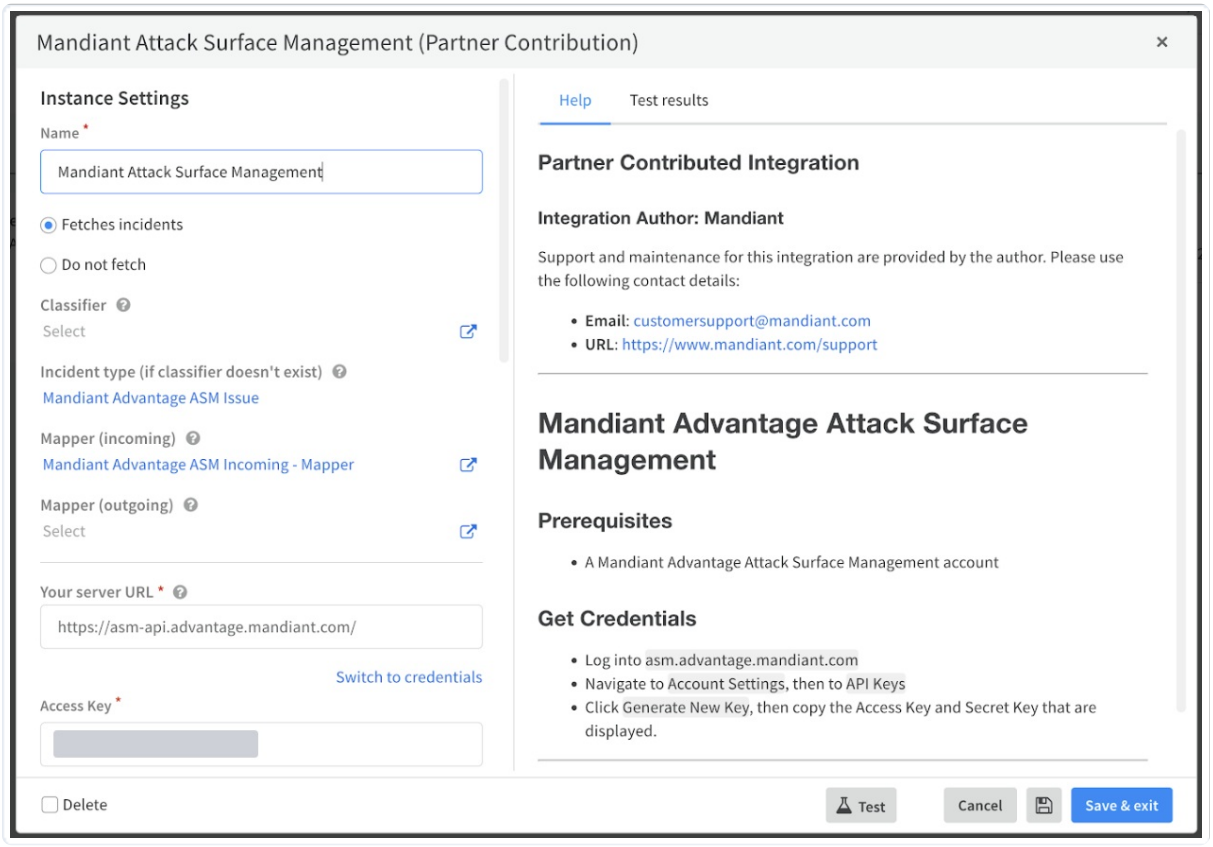


4. Click **I understand & saved the key** .

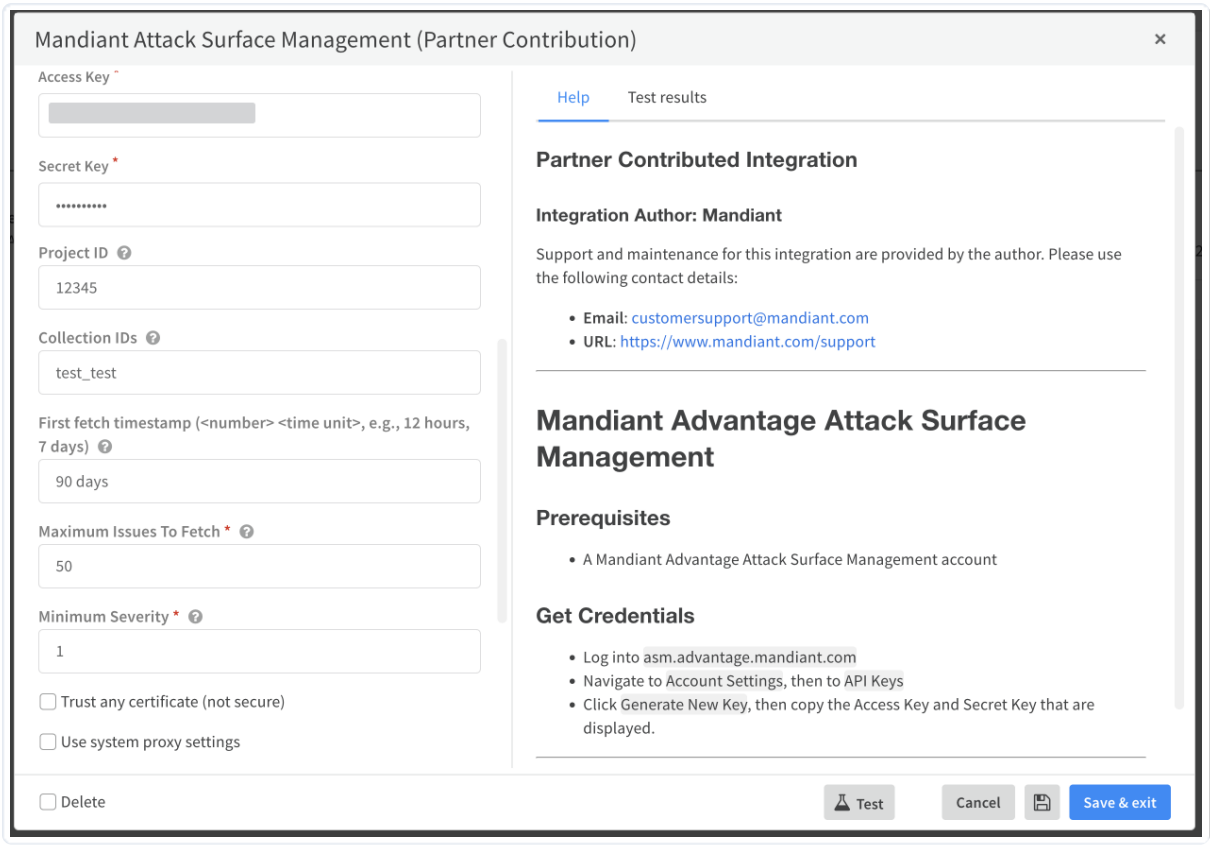
Add the MA-ASM Integration to your Cortex XSOAR Configuration

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**.



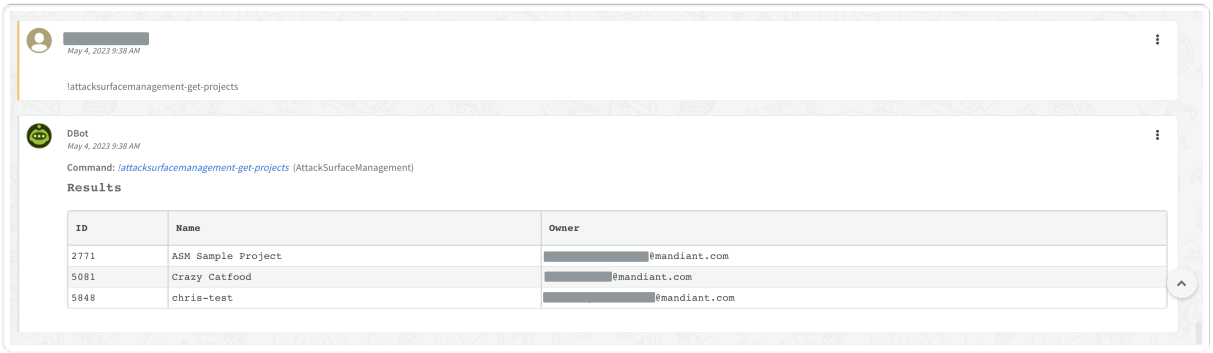
6. Enter **Access Key** and **Secret Key** from the Cortex XSOAR integration settings in the MA-ASM platform described in the preceding section.
7. Define **Maximum Issues to Fetch** and **Minimum Severity**. See the **Numeric Severity (https://docs.mandiant.com/home/asm-issue-severity-definitions-and-examples#numeric)**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



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.



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.