Mandiant

MICROSOFT DEFENDER FOR ENDPOINT INTEGRATION WITH SECURITY VALIDATION

This integration collects events generated by Microsoft Defender for Endpoint to test the efficacy and configuration of the security control using Security Validation jobs.

API Calls

API	Usage
`login.microsoftonline.com`	Authentication workflow
`/api/machines/{id}/alerts`	Get alerts
`/api/machines`	Query for devices in Microsoft Defender for Endpoint
`/api/machineactions`	Query for machine actions in Microsoft Defender for Endpoint

Supported Versions

Defender for Endpoint Plan 2

Before You Begin

To configure this integration, you need:

- The hostname of your Microsoft Defender for Endpoint instance
- Tenant ID
- Client ID
- Client Secret

Get Tenant ID

1. Log in to the Microsoft Azure management portal with a user that has permission to Azure Active Directory.
2. Select **Azure Active Directory** from the hamburger menu. The **Overview** page loads.
3. While viewing the **Overview** page, copy the value of the **Tenant ID** and paste it to a safe location for use in the integration configuration.

Create an Azure Active Directory Application

1. While in the Azure Active Directory management portal, click **App Registrations** from the menu.
2. Click **New Registration**
3. Enter a **Name** for the application. For example, Mandiant Advantage Defender for Endpoint Integration.
4. Select the **Supported Account Types** option that best suits your needs.
5. Click **Register**. The application is created.
6. Copy the value of the **Application (client) ID** and paste it to a safe location for use in the integration configuration.
7. Click **Add a certificate or secret**.
8. Click **New client secret**.
9. Enter a **Description** for the client secret.
10. Set an expiry date for the client secret using the **Expires** drop-down option.
11. Click **Add**.
12. Copy the **Value** of the client secret and paste it to a safe location for use in the integration configuration. **NOTE:** this value cannot be viewed again once you close this page.

Define API Permissions

1. While in the newly created application configuration in the Azure Portal, click **API Permissions** from the menu.

2. Click **Add a permission**.
3. Click the **APIs my organization uses** tab.
4. Click **WindowsDefenderATP**.
5. Select the **Alert.Read.All** and **Machine.Read.All** permissions.
6. Click **Add permissions**.

Configure Security Validation

1. Go to **Settings** > **Integrations**.
2. From the Integrations table, click **Add Integration > Microsoft Defender for Endpoint**.

   You can add this as either a Direct or Remote Integration.
3. Enter a meaningful **Integration Name**.
4. Optional: From the **Proxy** drop-down, choose a proxy profile if one is available. If one isn't available and all outbound connections go through a proxy, first, set up a **Proxy Rule** (https://docs.mandiant.com/home/msv-proxy-rules).
5. Optional: Change the **HttpProtocols** value to determine what protocol is used for requests (**Https** or **Http**).
6. Enter the **API Endpoint FQDN** value for the Microsoft Defender for Endpoint instance. The default is **api.securitycenter.window.com**.
7. Enter a **Port** value. The default is **443.**
8. Enter the **Client Id** and **Client Secret** values that you generated.
9. Enter the **Tenant ID** for your Microsoft Defender for Endpoint instance.
10. Optional: Change the **Authorization URL**, if needed. The default is **https://login.microsoftonline.com/**.
11. Optional: Check **Verify Ssl** if you want this verification done for requests to an upstream server.
12. Optional: Change the **Timeout** value if you want a different frequency of requests to an upstream server. The default is **30** (seconds).
13. Optional: Modify the **Field Map** values, as necessary.

    - Each field map box can hold a JSON-formatted comma-separated list of columns returned by the API to be considered for each field when translating into the normalized event object format. Example: description could be configured to be 'msg_s' or 'SyslogMessage' in some environments. The field map tries both if set to: ['msg_s','SyslogMessage'] and whichever matches first is the column that is used.
    - When configuring an integration in Security Validation, you can assign additional host values in the Field Map settings. If none of the assigned fields return a valid host name, Network Actions may miss matched events from the third-party technology. Additional hosts values helps ensure the likelihood of a match between the two environments.

14. Optional: Expand **Advanced options** and update the information as necessary.
    a. Update **Query Time** and **Delay Time**.

       The **Query time** is the amount of time (minutes) before and after the query runs that the platform looks for events, while the **Delay time** is the amount of time (minutes) that the platform waits to run the first query after a Job Action starts. For example, you configure your integration with the following values: **Query time** = 5, **Query interval** = 30 seconds, and **Delay time** = 0. When a Job Actions starts at 12:00:00, the first time the query runs, the platform looks for events from 11:55:00 to 12:00:00. Then 30 seconds later, it looks for events from 11:55:30 to 12:00:30. This interval continues, with the last query looking from 12:00:00 to 12:05:00. If you instead configured the **Delay time** to equal 10, it would run the same query, but it wouldn't start that query until 12:10:00.

> If your monitors are set to run more frequently than the query time, this configuration impacts the pass/fail results for AEDA monitors.

b. Update **Query Interval** (seconds).
c. Configure correlation queries:
    i. Select **Correlation Query Enabled** and fill in the **Correlation Query**.
    ii. Modify the **Correlation Query Interval**, if necessary (minutes).
d. Select **Discover network devices automatically**, the default and recommended option.

> If unselected, reported events won't include product information for any matching network security technology.

e. Select **Save Suspicious Events**.
f. Modify the **Event Time Adjustment** (seconds). The default is **0**.
g. Modify the **Limit** value if you need to prevent a flood of results. This value is set to **10000** by default. This limit applies to both events and alerts individually, so if you set it to **10**, you can still see a maximum of 10 events and 10 alerts.

15. Click **Save**.

Verify connectivity

1. Go to **Settings > Integrations**.
2. From the Direct Integrations table, click ⋮ **> Test** to verify that:
    - The Director can communicate with the integration host on the port and protocol specified.
    - The integration credentials are valid and working.

For more information on setting up queries, see **Manage Integrations** (https://docs.mandiant.com/home/msv-managing-integrations).