MICROSOFT DEFENDER ADVANCED THREAT PROTECTION (ATP)

This document applies to Classic/Legacy Integrations. You may continue to use these integration configurations. While no active development is happening for these integrations, we continue to provide Classic/Legacy Integrations in the product. You do not have to move to MSI Integrations. If your support engineer or TSC recommends or you choose to move to MSI Integrations, you can take advantage of the latest features and functionality. For more information, see the MSI Integration documentation in the **Integrations Overview** (https://docs.mandiant.com/home/msv-integrations-overview).

This integration is remote capable.

Update Defender ATP

1. Identify or create credentials to access integration with read access, at minimum.
2. Identify the following values in the Azure Web portal:

   Refer to the **Microsoft documentation** (https://docs.microsoft.com/en-us/microsoft-365/security/defender-endpoint/exposed-apis-create-app-webapp?view=o365-worldwide) for instructions on creating an app to get this information.

   - Client ID
   - Client Secret
   - Authorization URL
   - Tenant ID

API Calls

The following API calls are used by the Validation Platform.

Purpose	Call
Get alerts for the Actor	/api/alerts
Get authorization token	Authorization URL provided by Defender ATP

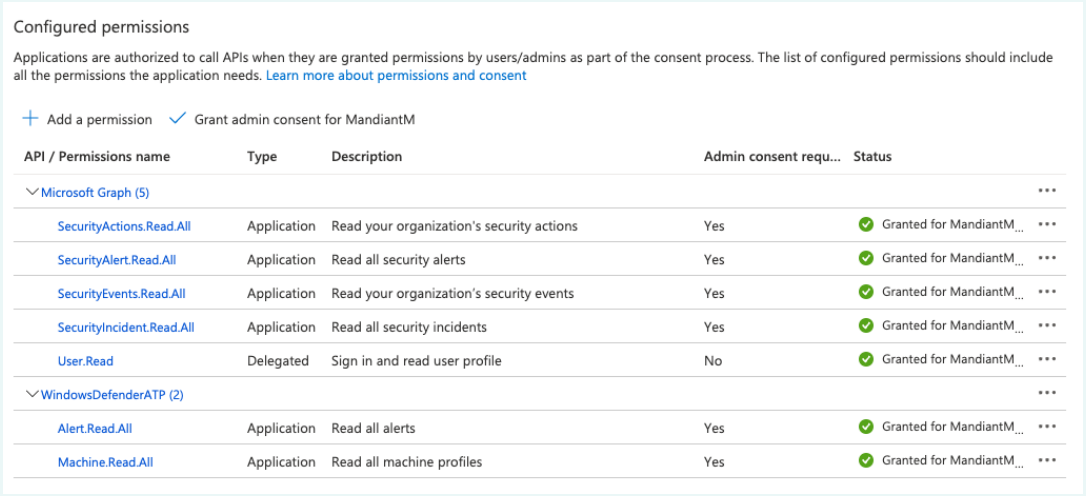
Update the Validation Platform

Prerequisites

Information to gather before you start:

- Identify the host, or geographic region, of your Defender ATP instance (US, UK, or EU).
- Identify the Port used for Defender ATP communication (this defaults to 443).
- Identify the Client ID unique to your application.
- Identify the Client Secret unique to your application.
- Identify the Authorization URL unique to your application.
- Identify the Tenant ID unique to your application.

Microsoft SIEM API is being replaced with Microsoft Graph for accessing Defender events. If your system employs Microsoft Graph, the settings shown here will need to be configured before you can successfully integrate with Microsoft Defender ATP.



Configured permissions

Applications are authorized to call APIs when they are granted permissions by users/admins as part of the consent process. The list of configured permissions should include all the permissions the application needs. Learn more about permissions and consent

+ Add a permission ✓ Grant admin consent for MandiantM

API / Permissions name	Type	Description	Admin consent requ...	Status
Microsoft Graph (5)				
SecurityActions.Read.All	Application	Read your organization's security actions	Yes	Granted for MandiantM...
SecurityAlert.Read.All	Application	Read all security alerts	Yes	Granted for MandiantM...
SecurityEvents.Read.All	Application	Read your organization's security events	Yes	Granted for MandiantM...
SecurityIncident.Read.All	Application	Read all security incidents	Yes	Granted for MandiantM...
User.Read	Delegated	Sign in and read user profile	No	Granted for MandiantM...
WindowsDefenderATP (2)				
Alert.Read.All	Application	Read all alerts	Yes	Granted for MandiantM...
Machine.Read.All	Application	Read all machine profiles	Yes	Granted for MandiantM...

TO ADD THE DEFENDER ATP INTEGRATION

1. Go to **Settings** > **Integrations**.
2. Click **Add Integration** > **Defender ATP**.

   You can add this as either a Local or Remote Integration.

3. Enter information for the **Host**, **Port**, and **Protocol**.

   - If using an alternate hostname, that needs to be defined on Windows Actors for MS Defender ATP to make a hostname-based match.
   - The host is auto-populated with the required info for the current API version but can be changed to one of the options listed that follow the **Host** text box.

4. Enter information for the **Client ID** and **Client Secret**.
5. (Optional) Update the **API Version**. This is set to the current supported API by default.
6. Update the **Auth URL**.

   This is set correctly for MS Defender for Endpoint API. Update this if you are not using the MS Defender for Endpoint API.

7. Add the **Tenant ID**.

   This is necessary if you're using the MS Defender for Endpoint API.

8. Add the **Resource**.

   This is necessary if you are using the Legacy SIEM API.

9. Expand **Advanced options** and update the information if necessary.
10. Click **Submit**.

Set up Proxy Assignment

If all outbound connections go through a proxy, you may want to set up a proxy definition and assignment for your integration. For information on setting up your proxy rules, see **Proxy Rules (https://docs.mandiant.com/home/msv-proxy-rules)**.

Verify connectivity

TO VERIFY CONNECTIVITY TO DEFENDER ATP

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.