MICROSOFT SENTINEL AND DEFENDER ATP INTEGRATIONS ADMIN GUIDE (DOCKER VERSION)

This integration brings Mandiant Advantage Threat Intelligence (MATI) to Microsoft Sentinel and Defender ATP, highlighting indicators of compromise (IOCs) in your network to let you identify and explore those threats that matter most.

Benefits of Docker

The Azure integration method in this document uses a Mandiant-developed Docker image instead of the Microsoft Logic App to manage the ingestion of Threat Intel data. This approach provides a more stable integration with better reporting capabilities for logs and errors. The Docker-based integration uses a simple "one-click" deployment approach similar to the Logic App version, but the deployment method has been updated to make it more robust.

> Migrating to the Docker-based integration does not result in the loss of existing data stored in your Microsoft Graph. For best results, we recommend disabling the Azure Logic App before completing the steps in this document to install the new integration.

Requirements

You need to have the following available and configured:

- Mandiant API Key and Mandiant API Secret
- Administrator access to Microsoft Entra ID (formerly known as Microsoft Azure AD)

Generate a Mandiant API key

> To obtain a **Service API Key** (which is tied to an organization rather than an individual user) for use with third-party security technologies such as a SIEM, contact **Support (https://www.mandiant.com/support)**.

To obtain an API Key ID and Secret for an individual user account, perform the following:

1. Navigate to the Mandiant Threat Intelligence web console.
2. Click **Account Settings**.
3. Select **API Access and Keys** from the navigation menu.
4. Click **Get Key ID and Secret** .
5. Copy and store the displayed values in a secure location.

Register your application

Complete the following steps to register your application with the Microsoft identity platform.

1. **Register your client application with Microsoft Entra ID**
2. **Add a secret to the registered application**
3. **Optional: Configure API permissions for threat indicator access**

Register your client application with Microsoft Entra ID

1. Sign in to the Microsoft Entra admin center as at least a Cloud Application Administrator.
2. Browse to **Identity > Applications > App registrations** and select **New registration**.
3. Enter a display **Name** for the application.
4. Select **Accounts in this organizational directory only** as the sign-in audience.
5. Don't enter anything for **Redirect URI**.
6. Select **Register** to complete the initial app registration.
7. Note the Client Id value; this value is needed when setting up the integration.

> Check the role permissions as outlined in **Assign a role to the application (https://learn.microsoft.com/en-us/azure/sentinel/connect-threat-intelligence-upload-api#assign-a-role-to-the-application)**.

Add a secret to the registered application

1. In the Microsoft Entra admin center, in App registrations, select the application you just created.
2. Select **Certificates & secrets > Client secrets > New client secret** .
3. Add a description for your client secret.
4. Select an expiration for the secret or specify a custom lifetime.
5. Select **Add**.
6. Note the value of the secret; this value is needed when setting up the integration.

> This secret value is never displayed again after you leave this page.

Optional: Configure API permissions for threat indicator access

1. Navigate to **API Permissions**.
2. Click **Add a permission** and select **Microsoft Graph**.
3. Select **Application permissions** and click the **ThreatIndicators.ReadWrite.OwnedBy** API Permission.
4. Click **Add permission**.
5. Select **Grant admin consent** to the Enterprise Application record for your subscription.
6. Click **Confirm**.

Deploy the Docker container instance

Complete the following workflow to deploy the Docker container instance.

1. Click the following button to be redirected to the Custom deployment template for this deployment.

Deploy to Azure
(https://portal.azure.com/#create/Microsoft.Template/uri/https%3A%2F%2Fwww%2Egstatic%2Ecom%2Fcloud%2Dmandiant%2Deng%2Dintegrations%2Fthreat%5Fintel%

2. Complete the **Project Details** form using the following:
    a. **Subscription**: Your Azure Subscription name.
    b. **Resource Group**: Collection of resources for your subscription.
    c. **Region**: Your Azure Region.
    d. **MATI Key**: Your credentials from the Mandiant API Key and Secret workflow.
    e. **MATI Secret**: Your credentials from the Mandiant API Key and Secret workflow.
    f. **Azure Workspace Id**: You can find your workspace ID in Azure by navigating to your Log Analytics workspace.
    g. **Azure Client Id**: Your credentials from the Azure App Registration workflow.
    h. **Azure Client Secret**: Your credentials from the Azure App Registration workflow.
    i. **Azure Tenant Id**: Your credentials from the Azure App Registration workflow.
    j. **Use Upload Indicators Api** : Recommended setting is **True** to use the Threat Intelligence Upload Indicators API connector.
3. Click **Review + Create**.

Configuration parameters

The following table lists the API parameters, whether they are mandatory or optional, their default values if applicable, and descriptions.

Deployment Parameter	Mandatory or Optional	Default Value	Description
Region	Mandatory		The Azure region for resource deployment.
Deployment Name	Mandatory		A unique identifier for your deployment within the resource group.
Location	Mandatory	[resourceGroup().location]	Inherits the resource group location for streamlined deployment.
MATI Key	Mandatory		Your Mandiant API key.
MATI Secret	Mandatory		Your Mandiant API secret.
Azure Workspace Id	Mandatory		The unique identifier of your Azure Log Analytics workspace. This workspace serves as the repository for ingested Mandiant threat intelligence data.
Azure Client Id	Mandatory		The Application (client) ID of an Azure Active Directory application authorized to access your Log Analytics workspace. This ensures secure communication between the deployment and your workspace.
Azure Client Secret	Mandatory		The secret associated with the Azure Client Id.
Azure Tenant Id	Mandatory		The unique identifier of your Azure Active Directory tenant. This associates the deployment with your organization's Azure subscription.
Ip Indicator Expiration	Optional	7	Defines the validity period (in days) for IP address indicators after ingestion.
Fqdn Indicator Expiration	Optional	7	Defines the validity period (in days) for Fully Qualified Domain Name (FQDN) indicators after ingestion.
Url Indicator Expiration	Optional	7	Defines the validity period (in days) for URL indicators after ingestion.
Hash Indicator Expiration	Optional	90	Defines the validity period (in days) for file hash indicators after ingestion.
Initial Lookback	Optional	30	Specifies the initial historical period (in days) for retrieving indicators from Mandiant.
Minimum Confidence	Optional	80	Sets the minimum Mandiant Confidence Score (0-100) for indicators to be ingested.
Minimum Threat Score	Optional	80	Sets the minimum Mandiant Threat Score for indicators to be ingested, allowing you to filter based on the severity and potential impact of the threat.
Exclude OS Int	Optional	TRUE	Excludes Open Source Intelligence (OSINT) indicators from ingestion.
Default Action	Optional	alert	Specifies the default action (e.g., "alert," "block", "allow") to be taken by Microsoft security products when an indicator is matched.
Include Uncategorized	Optional	TRUE	Determines whether indicators without a defined category in Mandiant are ingested.

Deployment Parameter	Mandatory or Optional	Default Value	Description
Hash Type	Optional	md5	Specifies the hash algorithm (e.g., "md5," "sha1," "sha256") to be used for file hash indicators. SHA-256 is recommended for enhanced security.
Include I Pv4	Optional	TRUE	Includes IPv4 address indicators in the ingested threat intelligence data.
Include Hash	Optional	TRUE	Includes file hash indicators in the ingested threat intelligence data.
Include URL	Optional	TRUE	Includes URL indicators in the ingested threat intelligence data.
Include FQDN	Optional	TRUE	Includes FQDN indicators in the ingested threat intelligence data.
Passive Only	Optional	FALSE	Configures the integration for passive monitoring only, meaning it will not actively block or prevent threats.
Sync Schedule	Optional	4	Defines the frequency (in hours) for synchronizing with Mandiant to retrieve updates.

Release Notes

Mandiant | Azure Sentinel Integration v1.2.4 (June 25, 2025)

Key changes

- For improved security and reduced size, we've updated our Docker base image. To get these benefits, simply pull the latest copy of the Docker image. The new SHA256 is `sha256:8430dd5b9eae87e33e117834f3703662836554ae488f18f48db2248f19434adf`

New settings

- **None**

Removed settings

- **None**

Mandiant | Azure Sentinel Integration v1.2.3 (January 9, 2025)

Key changes

- Fixes an issue where the local cache would be updated even if a call to Sentinel fails, resulting in indicators included in the failed upload not being ingested into Sentinel

New settings

- **None**

Removed settings

- **None**

Mandiant | Azure Sentinel Integration v1.2.2 (January 8, 2025)

Key changes

- Added a feature to rebuild cache based on the minimum value of the indicator expiry settings. This is required to update indicators that are still valid beyond their previously defined valid until date.

New settings

- **None**

Removed settings

- **None**

Mandiant | Azure Sentinel Integration v1.2.1 (December 20, 2024)

Key changes

- **Deduplication:** This version introduces a new feature to prevent duplicate indicators from being uploaded to Sentinel. The integration now performs checks to ensure only new or changed indicators are added, preventing unnecessary clutter and improving the accuracy of your threat intelligence data.

New settings

- **Enable Deduplication:** This setting allows you to enable the deduplication feature. Set this to `True` to activate deduplication and prevent duplicate indicators in your Sentinel workspace. To use this feature, you must also populate the `azureWorkspaceName`, `azureSubscriptionId`, and `azureResourceGroupName` settings with values from your Azure tenant.

Removed settings

- **None**

Mandiant | Azure Sentinel Integration v1.2 (October 1, 2024)

Key changes

- **Exclusive use of Microsoft Azure Sentinel Upload Indicators API** : The integration now exclusively uses the Microsoft Azure Sentinel Upload Indicators API. This means support for adding indicators to Microsoft Defender for Endpoint has been removed.
- **New Indicator Expiration Settings**: You can now configure expiration settings for different indicator types based on the number of days since creation or update:
  - **IP Address**: `IP_INDICATOR_EXPIRATION` (default: 7 days)
  - **FQDN**: `FQDN_INDICATOR_EXPIRATION` (default: 7 days)
  - **URL**: `URL_INDICATOR_EXPIRATION` (default: 7 days)
  - **Hash**: `HASH_INDICATOR_EXPIRATION` (default: 90 days)

- **New Indicator Score Thresholds**: You can now set minimum thresholds for indicator ingestion:
  - **Confidence Score**: `MINIMUM_CONFIDENCE` (default: 80)
  - **Threat Score** `MINIMUM_THREAT_SCORE` (default: 80)
  - **Note**: An indicator must meet or exceed *both* thresholds to be ingested.

Removed settings

- **Use Upload Indicators API**: This setting is deprecated as the integration now uses this API exclusively.
- **Indicator Expiration**: This setting has been replaced with individual expiration settings per indicator type.
- **Target Application**: This setting is deprecated as the integration now only supports Microsoft Azure Sentinel.