



Azure Sentinel Integration

Setup and Testing Guide

Release: 1.1

November 30, 2020

ANOMALI[®]

Copyright Notice

© 2020 Anomali, Incorporated. All rights reserved.

Anomali is a registered trademark, ThreatStream is a registered servicemark, and Optic, Integrator, STAXX, Anomali Enterprise, Anomali Match, and Anomali Lens are trademarks of Anomali, Inc.

All other brands, products, and company names used herein may be trademarks of their respective owners.

Support

Support Portal	https://support.anomali.com
Email	support@anomali.com
Phone	+1 844-4-THREATS (847328)
Twitter	@anomali

Documentation Updates

Date	Description
11/30/2020	Update for v1.1
7/2/2020	Documentation update
2/13/2020	Initial release for the Azure Sentinel Integration v1.0.0

CONTENTS

- Release Notes for Azure Sentinel Integration 1.1 4
 - What's New in This Release 4
 - Fixed Issues 5
- Introduction 7
- Setting up a New Azure Sentinel Destination 8
 - Optional Metadata in JSON Format Fields11
 - Redact JSON Key Values16
- Testing the Connection17

Release Notes for Azure Sentinel Integration 1.1

This document covers the following topics:

["What's New in This Release" below](#)

["Fixed Issues" on the next page](#)

["Release Notes for Azure Sentinel Integration 1.1" above](#)

What's New in This Release

Azure Sentinel Integration 1.1 is the next release for the Azure Sentinel integration extension. This release includes the following features and enhancements:

- **Proxy Support:** You can now specify a proxy to use with Sentinel (see ["Proxy Support" on page 12](#) for details).
- **User Agent:** A user agent has been defined (Anomali-AzureSentinelExtension/1.1.0), which is used by ThreatStream Integrator when making REST API requests to Sentinel. This agent aids tracking and auditing on Sentinel.
- **Python 3:** The integration has been moved to Python 3 as support for Python 2 is ending.
- **iType Mapping:** The mapping of iTypes from ThreatStream to fields in Sentinel has been improved (see ["Customized iType Mapping" on page 14](#) for details).
- **Sentinel Fields:** By default, two additional fields are now populated in Sentinel:

Field	Description
description	Indicates the intelligence feed from which the observable was received. The default value is: Indicator from ThreatStream

Field	Description
additionalInformation	<p>Displays the value of these fields in JSON format:</p> <ul style="list-style-type: none">■ itype—the type of observable, for example, <code>mal_ip</code>■ value_type—the type of observable value, for example, <code>ip</code>.■ source—the original source of the observable, for example, <code>analyst</code>. <p>For example, <code>{"itype": "mal_ip", "value_type": "ip", "source": "analyst"}</code></p> <div>Note: Refer to Appendix D in the <i>Anomali ThreatStream Integrator Installation & Administration Guide</i> for a full list of iTypes.</div>

Note: The default settings can be changed ("[Customized Sentinel Fields](#)" on [page 13](#) for details).

Fixed Issues

The following issues were fixed in this release.

Issue Number	Description
INTS-9984	<p>ThreatStream IP address was wrongly mapped in Sentinel.</p> <p>FIX: This issue has been fixed in this version.</p>

Issue Number	Description
INTS-9878	<p data-bbox="394 342 1378 415">No log rotation was provided. This meant that the log file continued to grow causing potential issues with disk space.</p> <p data-bbox="394 432 1284 506">FIX: This issue has been fixed in this version with these default settings:</p> <ul data-bbox="394 541 1378 800" style="list-style-type: none"><li data-bbox="394 541 643 573">• level : DEBUG<li data-bbox="394 611 1378 684">• backup_count : 10—the total number of backups a log file can have before the earliest is overwritten<li data-bbox="394 722 1378 800">• file_max_bytes : 10485760—the largest size, in bytes, that an individual file can reach (10MB) <div data-bbox="394 831 1369 953"><p data-bbox="410 852 1227 926">Note: The default settings can be changed ("Log Rotation Settings" on page 15 for details).</p></div>

Introduction

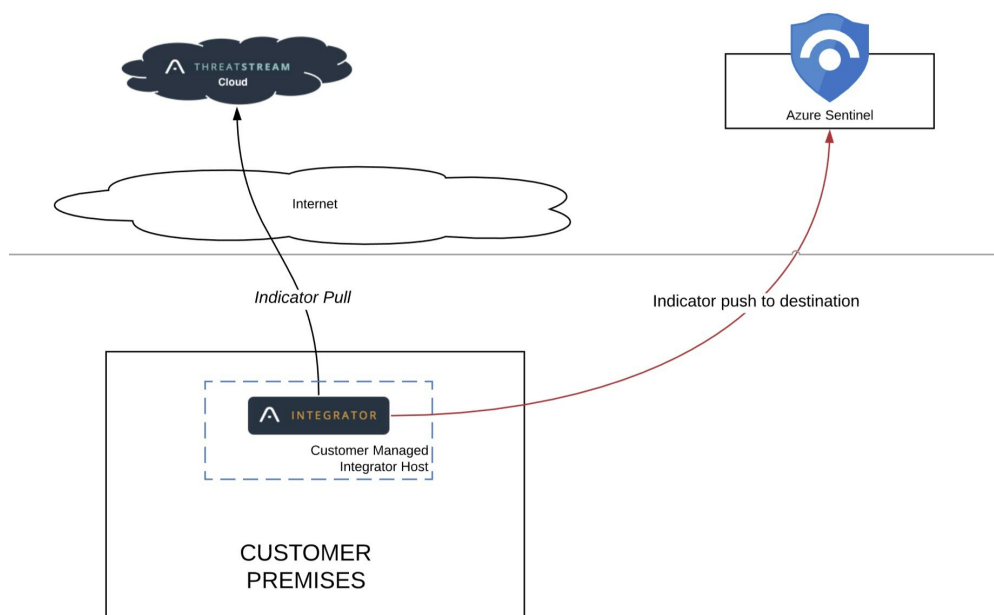
This guide provides details on how to set up and test the integration between Anomali ThreatStream and Microsoft Azure Sentinel.

Azure Sentinel is a cloud-native security information and event manager (SIEM) platform that analyzes large volumes of data across an enterprise. Anomali Threatstream aggregates observables from multiple sources which can be pulled down by ThreatStream Integrator and pushed to your Azure Sentinel instance. Sentinel Analytics matches these observables against your events to produce security alerts and incidents, and Sentinel Workbooks allow you to visualize this threat intelligence in various ways.

Note:

Contact Anomali Customer Support if there are any problems installing/running the integration.

Contact Microsoft if you have any queries regarding utilization of data once it is pushed to Microsoft Azure Sentinel.



Setting up a New Azure Sentinel Destination

Note: You must have a version of ThreatStream Integrator installed that supports SDK (v6.6 or later) before you can set up the Azure Sentinel destination. Anomali recommends updating to the latest version of Integrator where possible.

To install the Azure Sentinel integration extension:

1. Unzip and place the Azure Sentinel Integration folder in the location where you want to install the Azure Sentinel Integration, for example:

Linux:

```
/home/user/azure-sentinel/
```

Windows:

```
c:\home\user\azure
```

Note: To support configuration of multiple Azure Sentinel destinations to the same Azure Sentinel instance, copy the `azure_sentinel` binary from the folder specified to a separate, unique path for each destination. This will ensure each destination logs to its own dedicated log file.

2. Register the extension with Microsoft and save the **client/application ID**, **tenant ID**, and **client/application secret** needed to configure the extension.

See <https://docs.microsoft.com/en-us/azure/sentinel/connect-threat-intelligence> for details.


3. Create a new SDK destination in Integrator—refer to the iThreatStream Integrator documentation for details.

4. Configure the new destination fields as follows:

Setting	Description
Name	Provide a meaningful name for the new destination.
Destination Filter	Apply any filtering you may require to be applied to the IOC data, for example, confidence >90.
SDK Executable Command	<p>Provide the fully qualified path to azure sentinel installation file (including filename), for example:</p> <p>Linux:/</p> <p><code>/home/user/azure-sentinel/azure-sentinel</code></p> <p>Windows:</p> <p><code>C:\home\user\azure\azure-sentinel.exe</code></p>

Setting	Description
Metadata in JSON Format	<p>Supply these keys (obtained in Step 2) in JSON format:</p> <p>"client_id" "tenant_id" "app_secret" "target_product"</p> <p>The keys should be entered as a comma separated list, for example:</p> <pre>{ "client_id": "12345678-aaa-bbb-ccc-0z0z0z", "tenant_id": "87654321-aaa-bbb-ccc-z0z0z0z0", "app_secret": "I-am-a_VERY-s3cr3t-KeY", "target_product": "Azure Sentinel" }</pre> <p>By default, the value of these keys is displayed. To redact the value of any of the Sentinel fields, see "Redact JSON Key Values" on page 16 for details.</p> <div><p>Note: These are mandatory fields. See "Optional Metadata in JSON Format Fields" on the next page for optional fields.</p></div>
Integrator API Version	Select version: 1.0 from the drop-down list.

Setting	Description
Timeout in Seconds	<p>Default value: 600</p> <p>The time duration after which the destination is considered unresponsive.</p> <div><p>Note: However, Anomali recommends that you allow approximately 15 seconds per 100 observables that are sent to Azure Sentinel. Selecting a timeout that is not long enough to send all the observables will cause Integrator to timeout and declare that the transfer was unsuccessful..</p></div>
Indicator Update Mode	<p>Anomali recommends you select the Only Changed option for this integration.</p> <p>Options:</p> <ul style="list-style-type: none">■ Only Changed— only push the observables changed between the last push and the current one■ Full Snapshot—push all observables in the Integrator database, every time intelligence is updated on the destination

5. Select the **Override schedule and sync now** option from the Settings menu (the  icon in the top right-hand corner of the screen), or wait for the next sync to occur.

The new destination widget should update with the number of observables pushed to the destination.

6. Check the Azure Sentinel portal to ensure that the observables were successfully pushed to the destination (see ["Testing the Connection" on page 17](#) for details).

Optional Metadata in JSON Format Fields

A number of optional fields can be added. This is done by adding the relevant configuration information as described in the following sections.

Proxy Support

To specify a proxy with the Sentinel integration, add the following JSON object to the comma separated list in the ["Introduction"](#) field:

```
"proxy":  
{  
  "type": "http",  
  "host": "10.10.10.10",  
  "port" : 8080,  
  "username": "test",  
  "password": "pass@123"  
}
```

where:

Setting	Description
Type	Default: HTTP The proxy type. Note: Only standard HTTP is supported.
Host	IP address or hostname of the proxy server.
Port	Port on which proxy server listens for connections
Username	User name to be used to connect to the proxy server.
Password	Password for the specified username.

Note: If you are connecting to an unauthenticated proxy, do not include a username or password in the configuration.

When the proxy information is included with the mandatory fields, the entry in the ["Introduction"](#) field appears as follows:

```
{"client_id": "12345678-aaa-bbb-ccc-0z0z0z", "tenant_id":  
"87654321-aaa-bbb-ccc-z0z0z0z0", "app_secret": "I-am-a_VERY-  
s3cr3t-KeY", "target_product": "Azure Sentinel", "proxy{"typehostport" : 8080,  
"username" : "test", "password" : "pass@123" }}
```

Proxy Certificate

By default, Sentinel users `verify_ssl_certificate=true` when making https requests. If the proxy used decrypts the traffic, a failure occurs if the relevant

certificate is not installed in a local trusted certificate authority.

To avoid this potential problem, you can add the following JSON object to the comma separated list in the ["Introduction"](#) field:

```
"verify_ssl_cert" : false
```

Customized Sentinel Fields

By default, the Sentinel fields (**description** and **additionalInformation**) display the following information:

Field	Description
description	Indicates the intelligence feed from which the observable was received. The default value is: Indicator from ThreatStream
additionalInformation	<p>This displays the value of these fields in JSON format:</p> <ul style="list-style-type: none">• itype—the type of observable, for example, <code>mal_ip</code>• value_type—the type of observable value, for example, <code>ip</code>.• source—the original source of the observable, for example, <code>analyst</code>. <p>For example, <code>{"itype": "mal_ip", "value_type": "ip", "source": "analyst"}</code></p> <div>Note: Refer to Appendix D in the <i>Anomali ThreatStream Integrator Installation & Administration Guide</i> for a full list of iTypes.</div>

You can change the mapping of these two fields to suit your specific needs by adding a JSON object to the comma separated list in the ["Introduction"](#) field. How the information displays is dependent on the number of elements mapped to the fields. For a single element mapping, the information is displayed as a value; for multiple element mappings, the information is displayed as JSON. The following examples show both scenarios.

Single element - JSON object and sample field contents

```
"field_mappings": {  
  "additionalInformation": ["itype"],  
  "description": ["source"]  
}
```

Field	Sample Content
description	mal_ip
additionalInformation	analyst

Multiple elements - JSON object and sample field contents

```
"field_mappings": {  
  "additionalInformation": ["itype", "source"],  
  "description": ["source", "value_type"]  
}
```

Field	Sample Content
description	{"itype": "mal_ip", "source": "analyst"}
additionalInformation	{"source": "analyst", "value_type": "ip"}

Customized iType Mapping

The mapping of iTypes from ThreatStream to fields in Sentinel has been improved with the following defaults:

```
"threat_type_mappings": {  
  "Botnet": "^bot_.*",  
  "C2": "^c2_.*",  
  "CryptoMining": "^crypto_.*",  
  "MaliciousUrl": "^mal_url$",  
  "Malware": "^mal_[^url].*",  
  "Phishing": "^phish_.*",  
  "Proxy": "(proxy|i2p|p2p|tor|anon|vpn)_.*",  
  "PUA": "^adware_.*"  
}
```

To amend the iType mappings, copy these default settings from the PDF, edit as required, and add to the comma separated list in the ["Introduction"](#) field.

Note: The iType mappings have been optimized from the previous version and may differ from those you already have. You can edit these settings as required if you want to retain the old mappings.

Log Rotation Settings

To keep log files manageable, log rotation is used to restrict the volume of the log data. This is done by limiting the amount of data stored, the number of log files used, and the size of the log files. When the stored data reaches the specified limit, the files 'rotate', and the oldest file is cleared and re-used.

These fields are used to specify the settings.

Field	Description
Level	<p>Default: DEBUG</p> <p>The level of detail to be included in the log. Four levels are available, specified using the following values:</p> <p>10 for DEBUG 20 for INFO 30 for WARNING 40 for ERROR</p> <p>For example, to set the level to error use:</p> <pre>"level": 40</pre> <p>Note: The levels are listed in decreasing levels of detail (verbosity).</p>
backup_count	<p>Default: 10</p> <p>The total number of backups a log file can have before they start being overwritten.</p>
file_max_bytes	<p>Default: 10485760</p> <p>The largest size, in bytes, that an individual file can reach (10MB).</p>

To change the default log rotation settings, add the following to the comma separated list in the ["Introduction"](#) field:

```
"log": {"level": <required logging level>, "backup_count":  
<number of backup files>, "file_max_bytes": <size of each file>}
```

When the updated log rotation settings are included with the mandatory fields, the entry in the "Introduction" field will appear as follows:

```
{"client_id": "12345678-aaa-bbb-ccc-0z0z0z", "tenant_id":  
"87654321-aaa-bbb-ccc-z0z0z0z0", "app_secret": "I-am-a_VERY-  
s3cr3t-KeY", "target_product": "Azure Sentinel", "log": {"level":  
20, "backup_count": 10, "file_max_bytes": 100000}}
```

Redact JSON Key Values

By default, values entered for keys specified in the "Introduction" field are displayed.

To hide the value of these keys:

1. Open the `integrator.conf` file.
2. Scroll to the SDK Destination section and locate the `redacted_metadata_fields` parameter for the required destination (each configured destination is uniquely identified by its Destination ID).
3. Specify the keys whose value you want to hide. This is done by entering the keys as a comma separated list, for example:

```
redacted_metadata_fields = "client_id,tenant_id,app_secret"
```

4. Save the configuration file.
5. Specify the keys in the "Introduction" field as a comma separated list, for example:

```
{"client_id": "12345678-aaa-bbb-ccc-0z0z0z", "tenant_id":  
"87654321-aaa-bbb-ccc-z0z0z0z0", "app_secret": "I-am-a_VERY-  
s3cr3t-KeY", "target_product": "Azure Sentinel"}
```

Note: The key values are displayed as you enter them, however, they are redacted after the destination has been saved in the next step.

6. Save the changes made and close the destination. When you return to the destination, the specified keys are displayed in the "Introduction" field as follows:

```
{client_id: *****,tenant_id: *****, app_secret:
*****}
```

Testing the Connection

To test the connection to the Azure Sentinel Integration:

1. Log onto portal.azure.com.
2. Go to services and select **Azure Sentinel**.
3. Select a valid workspace from the list.
4. Select **Logs** under the **General** heading.
5. Within the **SecurityInsights**, locate the **ThreatIntelligenceIndicator** table log group and run this query:

```
ThreatIntelligenceIndicator
| where TimeGenerated < now()
| order by TimeGenerated desc
```

If the connection was successfully established, you should see the observables you pushed into Sentinel.

