

Anomali Enrichments SDK

Enrichments SDK Guide

Release: 2.0

March 31, 2020

ANOMALI®

Copyright

Copyright © 2020 Anomali, Inc. All rights reserved.

Anomali is a registered trademark, ThreatStream is a registered servicemark, and Optic, Integrator, STAXX, and Anomali Enterprise 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
Twitter	@anomali

Documentation Updates

Date	Release	Description
3/31/2020	2.0	Updated for the 2.0 release.
1/24/2020	1.6	Updated Providing Documentation for Your Enrichment .
5/29/2019	1.6	Updated for the 1.6 release.
4/17/2019	1.5	Updated for the 1.5 release.
4/3/2019	1.3	Updated for the 1.3 release.
2/8/2019	1.2	Updated for the 1.2 release.

CONTENTS

About This Release	4
Chapter 1: Introduction	5
Chapter 2: Developing Context-Based Enrichments	10
Chapter 3: Developing Pivot-Based Enrichments	24
Chapter 4: Testing Your Python Script	30
Chapter 5: Creating Enrichment Bundles	33
Chapter 6: Testing ThreatStream Cloud Enrichment Bundles	41
Chapter 7: Testing and Managing ThreatStream OnPrem and AirGap Enrichment Bundles	44
Chapter 8: Submitting ThreatStream Cloud Enrichments for Certification	50
Chapter 9: Updating Enrichment Bundles	52
Chapter 10: Troubleshooting Your Enrichment	54
Appendix A: Sample Documentation	58

About This Release

What's New in 2.0

This release includes the following enhancements:

- **Composite Objects:** Display multiple Text Widgets in a single line or create multiple lines within a Table Widget cell. See ["CompositeItem Objects" on page 19](#) for more information.
- **Multi-Transform Enrichments:** When multiple transforms are available for a single observable type, transforms are assigned sub-tabs within the enrichment on observable details page. See ["Multi-Transform Context Based Enrichments " on page 37](#) for more information.
- **Credential Rank:** Specify the order in which credentials appear on the ThreatStream user interface. See ["credentials" on page 36](#) for more information.
- **Table Column Width:** Set the width of table widget columns in context based enrichments. See ["TableWidget Objects" on page 14](#) for more information.

Chapter 1: Introduction

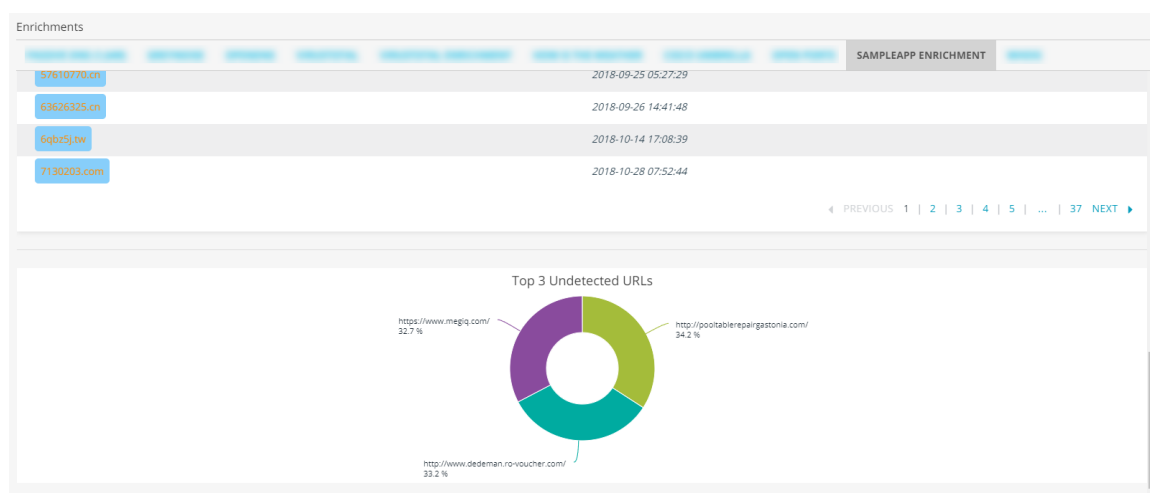
The Anomali Enrichments Software Development Kit (SDK) includes python libraries and sample code that can be used to develop enrichments for ThreatStream Cloud, ThreatStream OnPrem, or ThreatStream AirGap. Once developed and activated, data enrichments from sources outside ThreatStream can be leveraged from observable details pages or the Explore pivoting tool.

On ThreatStream Cloud, enrichments can be developed for use by your organization only or the entire Anomali Community. Enrichments developed for ThreatStream OnPrem are installed locally and for use only by your organization.

There are two types of enrichments you can develop using the Anomali Enrichments SDK: context-based enrichments and pivot-based enrichments.

Context-Based Enrichments

Context-based enrichments enable analysts to step through entire workflows on observable details pages, thus eliminating the need to jump between product screens. Up to 50 observables from the enrichment source can be displayed. The Anomali Enrichments Library enables you to customize how data is displayed on observables details pages. The following is an example of a context-based enrichment:



See ["Developing Context-Based Enrichments"](#) on page 10 for more information.

Pivot-Based Enrichments

Pivot-based enrichments expand the breadth of data that analysts can use to build out graphical relationships during threat research on the Explore pivoting tool. Further, organizations that have enabled the latest Investigations user interface can leverage pivot-based enrichments on the pivoting tool within investigations. To enable the development of pivot-based enrichments, the Anomali Enrichments SDK includes the Anomali Transform Library.



See ["Developing Pivot-Based Enrichments" on page 24](#) for more information.

Adding enrichments to ThreatStream using the Enrichments SDK includes developing an enrichment bundle that adheres to the requirements in this guide and submitting it to Anomali for certification.

Developing Enrichments for ThreatStream Cloud

Adding enrichments to ThreatStream Cloud using the Enrichments SDK includes developing an enrichment bundle that adheres to the requirements in this guide and submitting it to Anomali for certification.

To create enrichments for use on ThreatStream Cloud:

1. Develop data enrichment scripts that Anomali will use to retrieve and display data from the external source. See ["Developing Pivot-Based Enrichments" on page 24](#) and ["Developing Context-Based Enrichments" on page 10](#).

2. Test your python scripts. See ["Testing Your Python Script" on page 30](#).
3. Create required enrichment metadata. See ["Creating Enrichment Metadata Files" on page 33](#).
4. Bundle your python script and enrichment metadata as a tarball. See ["Creating the Enrichment TGZ Bundle" on page 39](#).
5. Test your completed bundle on a ThreatStream staging server. See ["Testing ThreatStream Cloud Enrichment Bundles" on page 41](#).
6. Write customer facing documentation for your enrichment. See ["Providing Documentation for Your Enrichment" on page 50](#).
7. Submit the enrichment to Anomali. See ["Submitting ThreatStream Cloud Enrichments for Certification " on page 50](#).

Developing Enrichments for ThreatStream OnPrem

Adding enrichments to your ThreatStream OnPrem appliance involves developing enrichment scripts, testing them locally, and installing the bundle on your appliance. ThreatStream OnPrem enrichments can retrieve data from both internal and external data sources.

The Anomali Enrichments SDK is compatible with ThreatStream OnPrem v4.0 only.

To create enrichments for use on ThreatStream OnPrem:

1. Develop data enrichment scripts that Anomali will use to retrieve and display data from the internal or external data source. See ["Developing Pivot-Based Enrichments" on page 24](#) and ["Developing Context-Based Enrichments" on page 10](#).
2. Test your python scripts. See ["Testing Your Python Script" on page 30](#).
3. Create required enrichment metadata. See ["Creating Enrichment Metadata Files" on page 33](#).
4. Bundle your python script and enrichment metadata as a tarball. See ["Creating the Enrichment TGZ Bundle" on page 39](#).

5. Test your enrichment. See ["Testing Enrichments on ThreatStream OnPrem "](#) on page 44.
6. Upload and activate your finalized enrichment on ThreatStream OnPrem. See ["Uploading and Activating Enrichments on ThreatStream OnPrem and AirGap"](#) on page 46.

Developing Enrichments for ThreatStream AirGap

Adding enrichments to your ThreatStream AirGap appliance involves developing enrichment scripts, testing them locally, and installing the bundle on your appliance. ThreatStream AirGap enrichments can retrieve data from both internal and external data sources.

The Anomali Enrichments SDK is compatible with ThreatStream AirGap v4.0 only.

To create enrichments for use on ThreatStream AirGap:

1. Develop data enrichment scripts that Anomali will use to retrieve and display data from the internal or external data source. See ["Developing Pivot-Based Enrichments"](#) on page 24 and ["Developing Context-Based Enrichments"](#) on page 10.
2. Test your python scripts. See ["Testing Your Python Script"](#) on page 30.
3. Create required enrichment metadata. See ["Creating Enrichment Metadata Files"](#) on page 33.
4. Bundle your python script and enrichment metadata as a tarball. See ["Creating the Enrichment TGZ Bundle"](#) on page 39.
5. Test your enrichment. See ["Testing Enrichments on ThreatStream AirGap"](#) on page 45.
6. Upload and activate your finalized enrichment on ThreatStream AirGap. See ["Uploading and Activating Enrichments on ThreatStream OnPrem and AirGap"](#) on page 46.

Prerequisites

Before continuing, ensure that the following prerequisites are met:

- The python platform is on v2.7.x.
- The python requests library is on v2.8.1.
- The xmljson python library is on v0.1.9.

The Enrichments SDK uses the following non-standard python libraries:

- requests
- dateutil

Therefore, you must run the following commands before locally testing enrichments:

- `pip install requests`
- `pip install python-dateutil`

Note: No other python packages should be installed on your local or svlpartner instance. All source code must be included in the source directory in a non-nested structure.

Chapter 2: Developing Context-Based Enrichments

In order to create enrichments that display enrichment data in widgets on observable details pages in ThreatStream, you must create a python script that utilizes the Anomali Enrichment Library. The python script must contain an enrichment object, which retrieves data from the enrichment source, and widget objects, which determine how enrichment data is displayed to users on observable details pages.

Understanding the Anomali Enrichment Library

This section contains information on creating enrichment objects using the Anomali Enrichment Library. The library—`anomalienrichment.py`—is available for reference and testing purposes in the Enrichments SDK package.

Method	Description	Return
<code>anomali_enrichment.parseArguments()</code>	Parses input arguments for the transform script.	None
<code>anomali_enrichment.getTransformName()</code>	Gets the name of the executed transform.	Transform Name (string)
<code>anomali_enrichment.getEntityValue()</code>	Gets the value of the entity on which the transform was executed.	Entity Value (String)
<code>anomali_enrichment.getFieldValue (String fieldName)</code>	Gets the value of additional field for the entity on which the transform was executed.	Field Value (String)
<code>anomali_enrichment.getCredentialValue (String credentialName)</code>	Gets required credential values for the data enrichment source.	Credential Value (String)

Method	Description	Return
<code>anomali_enrichment.addEntity(String entityType, String entityValue)</code>	Adds the entity to the transform object.	Entity Object
<code>anomali_enrichment.addMessage(String messageType, String messageText)</code>	Adds a type of message that will be displayed in the JSON output for debugging purposes. Possible values could include: "DEBUG", "INFO", "WARNING", "ERROR", "CRITICAL"). See "Creating Enrichment Bundles" on page 33 for information on viewing these messages.	None
<code>anomali_enrichment.addException(String exceptionString)</code>	Adds the text of the message that will be displayed on the ThreatStream user interface in case of errors.	None
<code>anomali_enrichment.returnOutput()</code>	Returns the result of the transform in JSON format.	Transform Result (JSON formatted String)

Widget Objects

This section contains information on the widgets provided by the Anomali Enrichment Library. Your enrichment can contain multiple widgets.

TextWidget Objects

TextWidget objects display data as formatted plain text. The following is an example of a TextWidget Object:

```
IP Enrichment for 104.27.158.93
```

TextWidget objects must be specified in python scripts as follows:

```
text_widget = TextWidget(ItemInWidget item, Boolean lineBreakEnding)
```

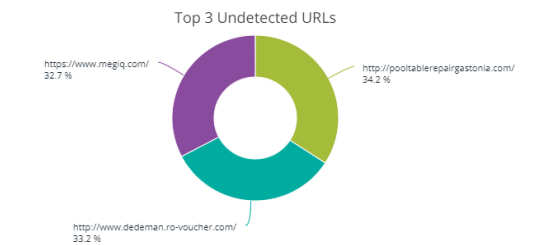
Method	Description	Return
<code>text_widget.setItem</code> (ItemInWidget item)	Sets the ItemInWidget object.	None
<code>text_widget.setLineBreakEnding</code> (Boolean lineBreakEnding)	Sets the boolean flag to indicate whether there is a line break following the text. Note: If the last widget in your script is a TextWidget, you must set this method to <code>true</code> .	None

See **6** under "Creating Your Context-Based Enrichment Script" on page 20 for a TextWidget example.

ChartWidget Objects

ChartWidget objects enable you to display data in a formatted chart.

The following is an example of a ChartWidget:



JSON strings developed with the Highcharts v6.2 library can be added to the enrichment. The Anomali Enrichments SDK supports any combination of the following Highcharts chart types:

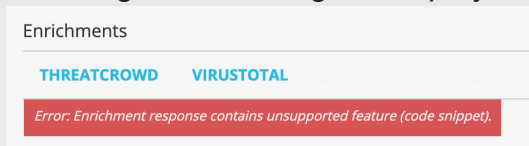
- area
- areaspline
- bar
- boxplot
- column
- columnrange
- errorbar

- gauge
- heatmap
- line
- pie
- spline
- waterfall
- xrange

Only the chart types listed above are supported. To read more about supported Highcharts chart types, see <https://www.highcharts.com/docs/chart-and-series-types/chart-types>

Notes:

- 3D chart options are not supported.
- Callback functions and properties such as allowHTML or useHTML are not supported. In these cases, enrichment responses are not rendered and the following error message is displayed:



Bundles containing such code snippets will be rejected during code review.

ChartWidget objects must be specified in python scripts as follows:

```
chart_widget = ChartWidget(String chartName, String highchartsJson)
```

Method	Description	Return
chart_widget.setChartName(String chartName)	Sets the name for the chart.	None

Method	Description	Return
<code>chart_widget.setHighchartsJson(String highchartsJson)</code>	<p>Sets the JSON string to be rendered by Highcharts in UI.</p> <p>The string you reference must be included in your python script. See 4 and 10 in "Creating Your Context-Based Enrichment Script" on page 20 for an example.</p>	None

TableWidget Objects

TableWidget objects enable you to display data in a formatted table. When you add a TableWidget to an enrichment, the ThreatStream user interface automatically enables the sorting of data within columns.

The following is an example of a TableWidget:

25 ▾ 1 - 25 of 918 items

Hostname	Last Resolved
06903609.cn	2019-01-16 20:20:04
12fanclub.mil	2018-12-20 17:07:04
1387it.com	2018-04-19 10:04:53
1742919.top	2016-11-17 00:00:00
2000k6.tw	2018-11-20 23:54:06
2grktgnet.mil	2018-09-23 23:28:28
33115286.cn	2018-09-26 12:35:18
33d3d6.ga	2018-11-19 19:52:10
38mm.xyz	2019-01-24 13:23:15
3sootsport.com	2018-09-30 16:10:07
3tc.cloud	2019-02-09 22:12:04

TableWidget objects must be specified in python scripts as follows:

```
table_widget = TableWidget(String tableName, StringList columnHeadings,
StringList columnTypes)
```

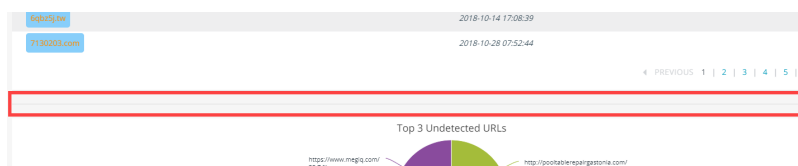
Method	Description	Return
<code>table_widget.setTableName(String tableName)</code>	Sets the name for the table.	None
<code>table_widget.setColumnHeadings(StringList columnHeadings)</code>	Sets the table column headings as a list of strings.	None

Method	Description	Return
<code>table_widget.setColumnTypes</code> (<code>StringList columnTypes</code>)	(Optional) Sets the table column types as a list of strings(itemTypes). Note: If you do not specify a column type, each item in the table must be given an itemType.	None
<code>table_widget.setColumnWidths</code> (<code>StringList columnWidths</code>)	Sets table column widths as a list of strings. For example: <code>columnWidths=['20%', '80%']</code> In the above example, column one is given a width of 20% and column two is given a width of 80%. If no width is specified, columns are rendered with equal width.	None
<code>table_widget.addRowOfItems</code> (<code>ItemInWidgetList listOfItems</code>)	Adds a row into the table as a list of <code>ItemInWidget</code> objects.	None

See **7** under "[Creating Your Context-Based Enrichment Script](#)" on page 20 for a `TableWidget` example.

HorizontalRuleWidget Objects

`HorizontalRuleWidget` objects enable you to add lines between widgets in your enrichment. The following is an example of a `HorizontalRuleWidget`:



`HorizontalRuleWidget` objects must be specified in python scripts as follows:

```
horizontalrule_widget = HorizontalRuleWidget()
```

See **8** under "[Creating Your Context-Based Enrichment Script](#)" on page 20 for a `HorizontalRuleWidget` example.

ItemInWidget Objects

ItemInWidget objects are used to format content within widgets, such as table cells, or text of any kind.

ItemInWidget objects must be specified in python scripts as follows:

```
item_in_widget = ItemInWidget(String itemType, String itemValue, String  
itemLabel, String backgroundColor, String textColor, String fontSize,  
String fontStyleWeight)
```


Method	Description	Return
<code>item_in_widget.setType</code> (String itemType)	<p>Sets the type for the item. Available types include:</p> <ul style="list-style-type: none"> • String = "String" • Integer = "Integer" • Float = "Float" • Date = "Date" • DateTime = "DateTime" • Link = "Link" • Domain = "Domain" • IPv4 = "IPv4" • Hash = "Hash" • Email = "Email" • URL = "URL" • Phrase = "Phrase" • AS = "AS" • NSRecord = "NSRecord" <p>Note: Use the Link type for any URL you want to make clickable. All other types render the item as text. The following is an example of a valid link:</p> <pre>anomaly_enrichment.addWidget(TextWidget(ItemInWidget(ItemTypes.Link, "https://www.example.com" % search_string, "Click here"), False))</pre>	None

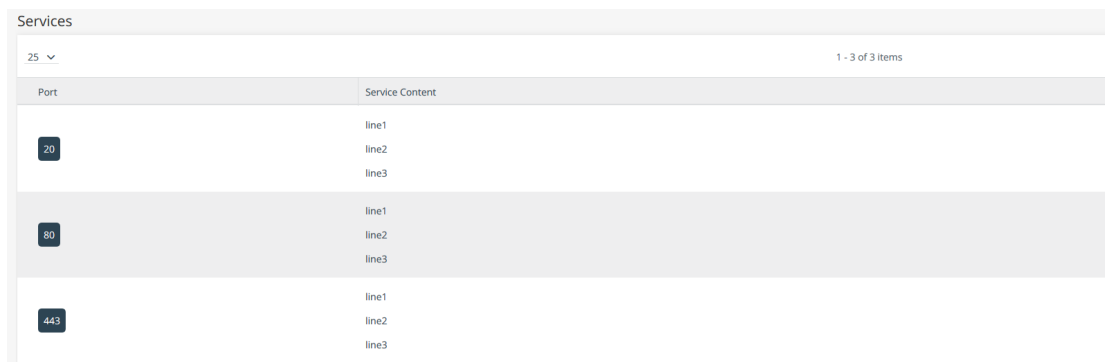
Method	Description	Return
<code>item_in_widget.setValue (String itemValue)</code>	Sets the value for the item.	None
<code>item_in_widget.setLabel (String itemLabel)</code>	Sets the label for the item.	None
<code>item_in_ widget.setBackgroundColor (String backgroundColor)</code>	<p>(Optional) Sets the background color for the item.</p> <p>If you do not specify a value, ThreatStream uses a default color.</p> <p>Tip: You can use any of the 140 standard color names supported by HTML, such as <code>SteelBlue</code>. You can also specify a hexadecimal value, such as <code>#4682B4</code>.</p>	None
<code>item_in_ widget.setTextColor (String textColor)</code>	<p>(Optional) Sets the text color for the item.</p> <p>If you do not specify a value, ThreatStream uses a default color.</p> <p>Tip: You can use any of the 140 standard color names supported by HTML, such as <code>SteelBlue</code>. You can also specify a hexadecimal value, such as <code>#4682B4</code>.</p>	None
<code>item_in_ widget.setFontSize(String fontSize)</code>	<p>(Optional) Sets the font size for the item.</p> <p>If you do not specify a value, ThreatStream uses a default font size.</p> <p>Tip: Valid values include <code>xx-small</code>, <code>x-small</code>, <code>small</code>, <code>medium</code>, <code>large</code>, <code>x-large</code>, and <code>xx-large</code>. You can also specify a pixel size, such as <code>16px</code>.</p>	None

Method	Description	Return
<code>item_in_widget.setFontStyleWeight(String fontStyleWeight)</code>	(Optional) Sets the font style and weight for the item. If you do not specify a value, ThreatStream uses a default font style. Tip: Valid values include <code>normal</code> , <code>italic</code> , <code>bold</code> , and <code>italic-bold</code> .	None

CompositeItem Objects

CompositeItem Objects enable you to display multiple Text Widgets in a single line or create multiple lines within a Table Widget cell.

The following is an example of a CompositeItem within a Table Widget:



Services	
25 ▾	1 - 3 of 3 items
Port	Service Content
20	line1 line2 line3
80	line1 line2 line3
443	line1 line2 line3

The following is an example of a CompositeItem within a Text Widget:



CompositeItem Objects must be specified in python scripts as follows:

```
composite_item = CompositeItem(Boolean onSeparateLines)
```

Method	Description	Return
<code>composite_item.addItemInWidget(ItemInWidget itemInWidget)</code>	Adds an ItemInWidget object to the CompositeItem object.	ItemInWidget Object

Method	Description	Return
<code>composite_item.setOnSeparateLines</code> (Boolean <code>onSeparateLines</code>)	Sets the boolean flag to indicate whether objects are displayed on separate lines.	None

See [10](#) and [11](#) under "[Creating Your Context-Based Enrichment Script](#)" below for `CompositeItem` examples.

Creating Your Context-Based Enrichment Script

Depending on the data source and its specific requirements, the content of enrichment python scripts will vary. The example described below is a truncated version of the example context-based enrichment script—`vt_anomali_enrichment.py`—included in the Anomali Enrichments SDK package. The script includes three enrichments and provides a high level illustration of what is required for enrichments to function on observable details pages.

```
import os
import sys
import copy
import json
import requests

from AnomaliEnrichment import AnomaliEnrichment, TextWidget, ChartWidget, TableWidget, HorizontalRuleWidget, \
    ItemInWidget, ItemTypes, CompositeItem

api_base = "https://www.virustotal.com/vtapi/v2/"
api_key = None

piechart_template_dict = {
    "chart": {
        "height": 300,
        "margin": 0,
        "marginTop": -20,
        "plotBackgroundColor": None,
        "plotBorderWidth": None,
        "backgroundColor": "#fff"
    },
    "credits": {
        "enabled": False
    },
    "title": {
        "text": "Pie Chart Example"
    },
    "tooltip": {
        "headerFormat": "<span style='font-size: 10px'>{point.key}</span><br/>",
        "pointFormat": "<b>{point.y}</b> {point.percentage:.1f}%</b>"
    },
    "plotOptions": {
        "pie": {
            "allowPointSelect": True,
            "animation": True,
            "cursor": "pointer",
            "innerSize": 100,
            "dataLabels": {
                "enabled": True,
                "format": "{point.prettyName}<br>{point.percentage:.2f} %",
                "style": {
                    "width": "200px"
                }
            },
            "point": {
                "events": {}
            },
            "size": "45%",
            "center": ["50%", "60%"]
        }
    },
    "series": [
        {
            "type": "pie",
            "name": "",
            "data": []
        }
    ]
}
```

- 1 Imports the system level libraries needed to execute your script.
- 2 Imports the Anomali Enrichment Library.
- 3 Specifies the API of the external data source and any necessary credentials.
- 4 Highcharts JSON template to be referenced by the chart widget.

```
def enrichDomainTabOne(anomali_enrichment, search_string):
    try:
        response = requests.get(api_base + 'domain/report?apikey=' + api_key + '&domain=' + search_string)
        response_json = response.json()
        resp_code = int(response_json['response_code'])
        if resp_code == 1:
            anomali_enrichment.addWidget(TextWidget(ItemInWidget(ItemTypes.String,
                                                                "Domain Enrichment for %s" % search_string,
                                                                "Domain Enrichment for %s" % search_string,
                                                                "SteelBlue", "White", "large", "bold"), True))
            anomali_enrichment.addWidget(TextWidget(ItemInWidget(ItemTypes.Link,
                                                                "https://www.virustotal.com/#/domain/%s" % search_string,
                                                                "View"), False))
            anomali_enrichment.addWidget(TextWidget(ItemInWidget(ItemTypes.String,
                                                                "comparison"), True))

            if 'resolutions' in response_json:
                table_widget = TableWidget("Resolutions", ["IP Address", "Last Resolved", "Reference"])
                for resolution in response_json['resolutions']:
                    table_widget.addRowOfItems([ItemInWidget(ItemTypes.IPv4,
                                                                resolution['ip_address'],
                                                                resolution['ip_address']),
                                                ItemInWidget(ItemTypes.DateTime,
                                                                resolution['last_resolved'],
                                                                resolution['last_resolved']),
                                                ItemInWidget(ItemTypes.Link,
                                                                "https://www.virustotal.com/#/ip-address/%s" % resolution['ip_address'],
                                                                "detail"))])
                anomali_enrichment.addWidget(table_widget)

            # Create HorizontalRuleWidget
            anomali_enrichment.addWidget(HorizontalRuleWidget())
```

- 5 Enrichment 1: Retrieves data from the external source.
- 6 Enrichment 1: Adds a text widget to the enrichment. See ["TextWidget Objects"](#) on page 11 for an example of this widget.
- 7 Enrichment 1: Adds a table widget to the enrichment. See ["TableWidget Objects"](#) on page 14 for an example of this widget.
- 8 Enrichment 1: Adds a horizontal rule widget to the enrichment. See ["HorizontalRuleWidget Objects"](#) on page 15 for an example of this widget.

```
def create_chart_widget(template_dict, data):
    graph_dict = copy.deepcopy(template_dict)
    # fill in the data
    graph_dict['series'][0]['data'] = data
    graph_json = json.dumps(graph_dict)
    pie_chart_widget = ChartWidget("Requester Distribution", graph_json)
    return pie_chart_widget

data = [{'y': 0.8, 'prettyName': 'u'US', 'name': 'u'US'},
        {'y': 0.1, 'prettyName': 'u'DE', 'name': 'u'DE'},
        {'y': 0.1, 'prettyName': 'u'IN', 'name': 'u'IN'}]
# Create Pie ChartWidget
chart_widget = create_chart_widget(piechart_template_dict, data)
anomali_enrichment.addWidget(chart_widget)

# Create composite_item for TextWidget
# always declare a new CompositeItem before using it
text_composite_item = CompositeItem(onSeparateLines=False)
port_list = [20, 80, 443]
for port in port_list:
    text_composite_item.addItemInWidget(ItemInWidget(ItemTypes.String, str(port), textColor='ffffff',
                                                        backgroundColor='#2D4453', fontSize='medium'))
port_text_widget = TextWidget(text_composite_item, True)
anomali_enrichment.addWidget(port_text_widget)

# Create composite_item for TableWidget
services_table_widget = TableWidget(tableName='Services', columnHeadings=['Port', 'Service Content'],
                                     columnTypes=[ItemTypes.Integer, ItemTypes.String],
                                     columnWidths=[200, 800])

# In real world, get data from the API response
services_data = [{'port': 20, 'lines': ['line1', 'line2', 'line3']},
                 {'port': 80, 'lines': ['line1', 'line2', 'line3']},
                 {'port': 443, 'lines': ['line1', 'line2', 'line3']}]
for service_data in services_data:
    port = ServiceData['port']
    # always declare a new CompositeItem before using it
    table_composite_item = CompositeItem(onSeparateLines=True)
    for line in service_data['lines']:
        table_composite_item.addItemInWidget(ItemInWidget(ItemTypes.String, line))
    services_table_widget.addRowOfItems([ItemInWidget(ItemTypes.String, port,
                                                        textColor='ffffff', backgroundColor='#2D4453',
                                                        table_composite_item)])
    anomali_enrichment.addWidget(services_table_widget)

except:
    anomali_enrichment.addException('enrichDomain Unknown Error: %sType: %sValue: %s' %
                                    (os.linesep, sys.exc_info()[0], os.linesep, sys.exc_info()[1]))
    return anomali_enrichment
```

9 Enrichment 1: Adds a chart widget to the enrichment. The code in this section gathers and injects data into the chart template defined in **4**. See ["ChartWidget Objects" on page 12](#) for an example of this widget.

10 Enrichment 1: Adds a text widget that contains composite item objects. See ["Compositeltem Objects" on page 19](#) for an example of this object.

11 Enrichment 1: Adds a table widget that contains composite item objects. See ["Compositeltem Objects" on page 19](#) for an example of this object.

11 Enrichment 1: Specifies the exception—what should be done in cases where no data is returned.

```
def enrichDomainTabTwo(anomali_enrichment, search_string):  
    (... omitted for brevity ...)  
  
def enrichIP(anomali_enrichment, search_string):  
    (... omitted for brevity ...)  
  
functions = {  
    'enrichDomainTabOne': enrichDomainTabOne,  
    'enrichDomainTabTwo': enrichDomainTabTwo,  
    'enrichIP': enrichIP  
}  
  
if __name__ == '__main__':  
    anomali_enrichment = AnomaliEnrichment()  
    anomali_enrichment.parseArguments()  
    transform_name = anomali_enrichment.getTransformName()  
    entity_value = anomali_enrichment.getEntityValue()  
    api_key = anomali_enrichment.getCredentialValue('api_key')  
  
    functions[transform_name](anomali_enrichment, entity_value)  
    anomali_enrichment.returnOutput()
```

13 Enrichment 2: Omitted for brevity. To view this enrichment code, see the example script in the Anomali Enrichments SDK package.

14 Enrichment 3: Omitted for brevity. To view this enrichment code, see the example script in the Anomali Enrichments SDK package.

15 Specifies the list of enrichments supported by the script.

16 Initializes the Anomali Enrichment SDK object and input parameters.

17 Retrieves the credentials for your data enrichment source from STDIN using Anomali Enrichment SDK object.

18 Returns data enrichment output to STDOUT in Anomali Enrichment format.

Chapter 3: Developing Pivot-Based Enrichments

In order to create data enrichments that can be leveraged on the standalone Explore pivoting tool and the pivoting tool on the Investigations user interface within ThreatStream, you must create transforms that utilize the Anomali Transform Library. ThreatStream will use these transforms to dynamically enrich threat intelligence with data from the external enrichment source.

Note: Anomali Enrichments SDK also supports Maltego transforms for purposes of backwards compatibility. This guide does not include information on creating ThreatStream enrichments that leverage Maltego Transforms.

Understanding the Anomali Transform Library

Transforms must be constructed using the Anomali Transform Library. The library—`anomalitransform.py`—is available for reference and testing purposes in the Enrichments SDK package.

Transform Objects

This section contains information on creating transform objects using the Anomali Transform Library.

Method	Description	Return
<code>at.parseArguments()</code>	Parses input arguments for the transform script.	None
<code>at.getTransformName()</code>	Gets the name of the executed transform.	Transform Name (string)
<code>at.getEntityValue()</code>	Gets the value of the entity on which the transform was executed.	Entity Value (String)

Method	Description	Return
<code>at.getFieldValue(String fieldName)</code>	Gets the value of additional field for the entity on which the transform was executed.	Field Value (String)
<code>at.getCredentialValue(String credentialName)</code>	Gets required credential values for the data enrichment source.	Credential Value (String)
<code>at.addEntity(String entityType, String entityValue)</code>	Adds the entity to the transform object.	Entity Object
<code>at.addMessage(String messageType, String messageText)</code>	Adds a type of message that will be displayed in the JSON output for debugging purposes. Possible values could include: "DEBUG", "INFO", "WARNING", "ERROR", "CRITICAL"). See "Creating Enrichment Bundles" on page 33 for information on viewing these messages.	None
<code>at.addException(String exceptionString)</code>	Adds the text of the message that will be displayed on the ThreatStream user interface in case of errors.	None
<code>at.returnOutput()</code>	Returns the result of the transform in JSON format.	Transform Result (JSON formatted String)

Entity Objects

This section contains information on specifying entity objects using the Anomali Transform Library.

The following methods must be used when specifying entity objects:

Method	Description	Return
<code>ae.setType(String entityType)</code>	<p>Sets the type for the entity. Available types include:</p> <ul style="list-style-type: none">Domains Example: <code>EntityTypes.Domain = "anomaly.Domain"</code>IP addresses Example: <code>EntityTypes.IPv4 = "anomaly.IPv4Address"</code>Hashes Example: <code>EntityTypes.Hash = "anomaly.Hash"</code>Email addresses Example: <code>EntityTypes.EmailAddresses = "anomaly.EmailAddress"</code>URLs Example: <code>EntityTypes.URL = "anomaly.URL"</code>Phrases Example: <code>EntityTypes.Phrase = "anomaly.Phrase"</code>Autonomous system numbers	None

Method	Description	Return
	<p>Example: <code>EntityTypes.AS = "anomali.AS"</code></p> <ul style="list-style-type: none">DNS name server records <p>Example: <code>EntityTypes.NSRecord = "anomali.NSRecord"</code></p>	
<code>ae.setValue(String entityValue)</code>	Set the value for the entity.	Transform Name (string)
<code>ae.addAdditionalField(String fieldName, String displayName, String fieldValue)</code>	Add an additional field to the entity.	Entity Value (String)

Creating Your Pivot-Based Enrichment Script

Depending on the data source and its specific requirements, the content of enrichment python scripts will vary. The example described below is identical to the example pivot-based script—`vt_anomali_transform.py`— provided by the Anomali Enrichments SDK package. The example below provides a high level illustration of what is required for pivoting enrichments to function.

```
import os
import sys
import requests

from AnomaliTransform import AnomaliTransform
from AnomaliTransform import EntityTypes

api_base = "https://www.virustotal.com/vtapi/v2/"
api_key = None

def domainToIP(at, search_string):
    try:
        response = requests.get(api_base + 'domain/report?apikey=' + api_key + '&domain=' + search_string)
        response_json = response.json()
        resp_code = int(response_json['response_code'])
        if resp_code == 1:
            if 'resolutions' in response_json:
                for resolutions in response_json['resolutions']:
                    ae = at.addEntity(EntityTypes.IPv4, '%s' % resolutions['ip_address'])
                    ae.addAdditionalField('last_resolved', 'Last Resolved', '%s' % resolutions['last_resolved'])
            else:
                ae = at.addEntity(EntityTypes.IPv4, '%s' % search_string)
        except:
            at.addException('domainToIP Unknown Error:%sType: %s%sValue:%s' %
                           (os.linesep, sys.exc_info()[0], os.linesep, sys.exc_info()[1]))
        return at

functions = {
    'domainToIP': domainToIP,
}

if __name__ == '__main__':
    at = AnomaliTransform()
    at.parseArguments()
    transform_name = at.getTransformName()
    entity_value = at.getEntityValue()
    api_key = at.getCredentialValue('api_key')
    functions[transform_name](at, entity_value)
    at.returnOutput()
```

- 1 Imports the system level libraries needed to execute your script.
- 2 Imports the Anomali Transform Library.
- 3 Specifies the API of the external data source and any necessary credentials.
- 4 Section of the transform that retrieves data from the external source.
- 5 Section of the transform that formats the data for consumption by Anomali.
- 6 Specifies the exception—what should be done in cases where no data is returned.
- 7 Specifies the list of transforms supported by the script.
- 8 Initializes the Anomali Transform SDK object and input parameters.
- 9 Retrieves the credentials for your data enrichment source from STDIN using Anomali Transform SDK object.
- 10 Returns data enrichment output to STDOUT in Anomali Transform format.

Chapter 4: Testing Your Python Script

When development on a python script is complete, you can use the instructions in this section to test it on your local machine.

To test your script locally:

1. Create a virtual environment:

```
virtualenv venv
```

2. Activate the virtual environment:

```
source venv/bin/activate
```

3. Install the requests library.

```
(venv) pip install requests
```

4. Use your preferred method to copy the script you want to test and the `anomalienrichment.py` (for context-based enrichments) or `theanomalitransform.py` (for pivot-based enrichments) file to the same directory.

5. Execute a transform or enrichment contained in the script:

```
(venv) python <script_name>.py <transform_or_enrichment_name>  
anomali.com  
--credentials "{\"api_key\":\"<api_key_value>\"}"
```

For example, to test a transform in a pivot-based script, you would run:

```
(venv) python vt_anomali_transform.py domainToIP anomali.com --  
credentials "{\"api_key\":\"REDACTED\"}"
```

To test an enrichment in a context-based script, you would run:

```
(venv) python vt_anomali_enrichment.py enrichDomain anomali.com --  
credentials "{\"api_key\":\"REDACTED\"}"
```

For context-based enrichments, you will see output similar to the following:

```
"exceptions": [],
"messages": [],
"widgets": [
  {
    "widgetType": "Text",
    "item": {
      "backgroundColor": "SteelBlue",
      "fontSize": "large",
      "fontStyleWeight": "bold",
      "itemLabel": "Domain Enrichment for anomali.com",
      "itemType": "String",
      "itemValue": "Domain Enrichment for anomali.com",
      "textColor": "White"
    },
    "lineBreakEnding": true
  },
  {
    "widgetType": "Table",
    "tableName": "Resolutions",
    "columnHeadings": [
      "IP Address",
      "Last Resolved"
    ],
    "rows": [
      [
        {
          "itemLabel": "216.218.192.90",
          "itemType": "IPv4",
          "itemValue": "216.218.192.90"
        },
        {
          "itemLabel": "2019-02-07 19:05:40",
          "itemType": "DateTime",
          "itemValue": "2019-02-07 19:05:40"
        }
      ],
      [
        {
          "itemLabel": "64.62.160.174",
          "itemType": "IPv4",
          "itemValue": "64.62.160.174"
        },
        {
          "itemLabel": "2015-12-06 00:00:00",
          "itemType": "DateTime",
          "itemValue": "2015-12-06 00:00:00"
        }
      ]
    ]
  },
  {
    "widgetType": "HorizontalRule"
  },
  {
    "widgetType": "Chart",
    "chartName": "Top 3 Undetected Referrer Samples",
    "highchartsUson":
    "({\"chart\":{\"height\":300,\"margin\":0,\"marginTop\":-20,\"plotBackgroundColor\":null,\"plotBorderWidth\":null,\"background\":\"#fff\"},\"credits\":{\"enabled\":false},\"title\":{\"text\":\"Top 3 Undetected Referrer Samples\"},\"tooltip\":{\"headerFormat\":\"<span style=\\\"font-size: 10px\\\">{point.key}</span><br/>\", \"pointFormat\":\"<b>{point.y}</b>({point.percentage:.1f})</b>\", \"plotOptions\":{\"pie\":{\"allowPointSelect\":true,\"animation\":false,\"cursor\": \"pointer\"}, \"innerSize\":100,\"dataLabels\":{\"enabled\":true,\"format\":\"{point.prettyName}<br>{point.percentage:.1f}\"}, \"style\":{\"width\":\"200px\"}}, \"point\":{\"events\":{}}, \"size\":\"65%\"}}, \"series\":[{ \"type\":\"pie\", \"name\":\"\", \"data\":{\"y\":71,\"prettyName\":\"807ed3a83aeb8731502639e50726aada10433fef3eb306f92ee54d13c2a5a344\", \"name\":\"807ed3a83aeb8731502639e50726aada10433fef3eb306f92ee54d13c2a5a344\"}, { \"y\":70,\"prettyName\":\"82c989f1871d627a9a3bedda0ccf9a113c0c61491ee7a638b50955355382dd7\", \"name\":\"82c989f1871d627a9a3bedda0ccf9a113c0c61491ee7a638b50955355382dd7\"}, { \"y\":70,\"prettyName\":\"77fcd2ad32felbe4b7bdd2772faf95ab8e18404f1967ded44a9db730171691ab\", \"name\":\"77fcd2ad32felbe4b7bdd2772faf95ab8e18404f1967ded44a9db730171691ab\"}}]})"
```

For pivot-based enrichments, you will see output similar to the following:

```
{
  "entities": [
    {
      "additionalFields": [
        {
          "displayName": "Last Resolved",
          "fieldName": "last_resolved",
          "fieldValue": "2018-09-04 03:17:59"
        }
      ],
      "entityType": "anomaly.IPv4Address",
      "entityValue": "216.218.192.90"
    },
    {
      "additionalFields": [
        {
          "displayName": "Last Resolved",
          "fieldName": "last_resolved",
          "fieldValue": "2015-12-06 00:00:00"
        }
      ],
      "entityType": "anomaly.IPv4Address",
      "entityValue": "64.62.160.174"
    }
  ],
  "exceptions": [],
  "messages": []
}
```

As these example show, the output must be in valid JSON format. The output must not contain messages that result from print statements. To add messages for debugging purposes, use the `at.addMessage` method, as described in ["Testing Your Python Script" on page 30](#).

Notes:

- Enrichment transforms that take longer than 30 seconds to complete will result in a timeout on the ThreatStream UI.
- Virtual environments created for testing your script must not be included in the final enrichment bundle.

Chapter 5: Creating Enrichment Bundles

Once you have developed and tested your enrichment python scripts, you must create a bundle that contains your python scripts and other supporting files. The bundle must contain the following items:

1. Python enrichment scripts

The enrichment scripts you developed must be included in the bundle within a directory called `source`.

2. Metadata file in JSON format

Metadata files must be created using the guidelines in ["Creating Enrichment Metadata Files" below](#). The metadata file must be named `metadata.json`

3. Enrichment Icons

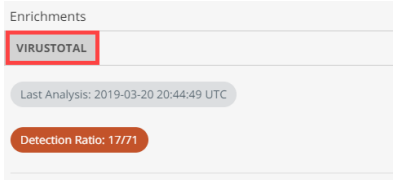
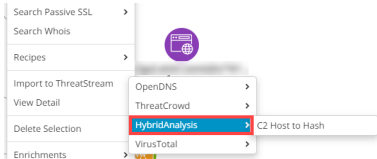
You must provide a full size icon for your enrichment, in addition to an icon thumbnail.

Creating Enrichment Metadata Files

In order to display enrichments on the ThreatStream user interface, you must create a JSON file that includes information such as enrichment names, transform names, icons, required credentials, and so on.


Items that must be specified in the metadata file include:

Metadata Item	Description
title	Name of the data enrichment source.

Metadata Item	Description
transform_set_name	<p>Name of the enrichment to be displayed on the ThreatStream user interface.</p> <p>For context-based enrichments, this sets the name of the tab in the Enrichments section on observable details pages.</p>  <p>For pivot-based enrichments, this sets the name of the menu item on the Explore pivoting tool which contains your transforms.</p>  <p>Displayed on the Explore user interface during pivoting.</p> <p>Note: You can only set one transform_set_name per bundle.</p> <p><i>For ThreatStream OnPrem and AirGap enrichments only:</i> you can use transform_set_name to distinguish enrichments undergoing testing from finalized enrichments.</p> <p>For example: sampleapp-anomali-beta</p>
description	Description of the data provided by the source. Displayed on the Enrichments tab within ThreatStream settings.
icon_display	Filename of the icon that will be displayed on the ThreatStream user interface.
icon_thumbnail	Filename of the icon thumbnail that will be displayed on the ThreatStream user interface.
sdk_type	Type of transform—you must specify anomali.

Metadata Item	Description
app_name	<p>Unique identifier used by ThreatStream to track enrichments. Must follow the format <domain_suffix>.<company_name>.<app-name></p> <p>For example: <code>com.anomali.sampleapp</code></p> <p>If updates to your enrichment are ever required, simply ensure an identical <code>app_name</code> is used and re-upload your updated bundle.</p> <p><i>For ThreatStream OnPrem and AirGap enrichments only:</i> you can use the <code>app_name</code> to distinguish enrichments undergoing testing from finalized enrichments.</p> <p>For example: <code>com.anomali.sampleapp-beta</code></p>
version	<p>Version of the enrichment. Must follow the format <major_version>.<minor_version>.<patch></p> <p>For example: <code>3.0.1</code></p> <p><i>For ThreatStream OnPrem enrichments only:</i> you can use the version number to distinguish enrichments undergoing testing from finalized enrichments.</p> <p>For example: <code>1.0.0-beta</code></p>

Metadata Item	Description
credentials	<p>Specifies credential requirements for users activating the enrichment. Items include:</p> <ul style="list-style-type: none">• <code>name</code>—name used to identify the credential in your python script.• <code>description</code>—description of the credential.• <code>label</code>—name of credential displayed to users on the ThreatStream user interface.• <code>required</code>—whether users are required to enter the credential for enrichment activation.• <code>sensitive</code>—whether the credential is case-sensitive.• <code>rank</code>—order in which credential fields appear on the user interface. <p>Example: <code>"rank": 1</code> (appears at the top of the list), <code>"rank": 2</code> (appears second in the list)</p> <div><p>Note: Each credential field must be given a ranking if specifying rank for your credential fields. Rank will not be honored if you specify rank for only a partial set of credential fields.</p></div>

Metadata Item	Description
transforms	<p>List of features supported by the data enrichment script. You must specify values for:</p> <ul style="list-style-type: none"> <code>transform_name</code>—name used to identify the transform in your python script. <code>pivoting</code>—whether the transform is leveraged on the Explore pivoting tool. <code>enrichment</code>—whether the transform is leveraged on observable details pages. <p>Note: For a given transform, you must set either <code>pivoting</code> <i>OR</i> <code>enrichment</code> to <code>true</code>. You <i>cannot</i> set both <code>pivoting</code> and <code>enrichment</code> to <code>true</code>. A single transform cannot be used on both context-based and pivot-based enrichments.</p> <p>Multi-Transform Context Based Enrichments</p> <p>If your metadata file contains multiple context-based transforms (<code>"enrichment": true</code>) for the same <code>entity_type</code>, each transform is assigned a dedicated tab in your enrichment. A maximum of 10 transforms (and thus 10 tabs) are allowed.</p> <p>Only the transform on the first tab is executed when users access your multi-transform context based enrichment, thus reducing the chance of timeouts. Transforms on subsequent tabs are not executed until users open the respective tabs.</p> <p>Tabs are ordered based on the <code>rank</code> of the transforms for each <code>entity_type</code> (indicator type) in the metadata file. Values specified for <code>transform_name</code> are used for tab labels.</p> <p>The following is an example of a multi-tab enrichment:</p>  <p>Note: Tabs must load within 30 seconds to prevent timeouts.</p>

Metadata Item	Description
	<ul style="list-style-type: none"> <code>display_name</code>—name of the transform displayed to users on the ThreatStream user interface. <code>description</code>—description of the transform. <code>author</code>—the name of your organization. <code>parameters</code>— filename of the python script which contains the transform and the name of the transform. Example: <code>sample_enrichment.py ipToDomain</code> <code>entity_type</code>—type of entity on which the transform can be activated in ThreatStream. <code>rank</code>—order in which transforms appear on the user interface for the specified <code>entity_type</code> (indicator type). Example: <code>"rank": 1</code> (appears at the top of the list), <code>"rank": 2</code> (appears second in the list) <p>Note: Each transform must be given a ranking if specifying rank for your transforms. Rank will not be honored if you specify rank for only a partial set of available transforms.</p>
<code>author</code>	(Optional) Developer of the enrichment.
<code>long_description</code>	(Optional) Detailed description of the enrichment. Not currently displayed on the ThreatStream user interface.
<code>license</code>	(Optional) License for the enrichment scripts.
<code>source_url</code>	(Optional) URL for where the enrichment scripts are hosted.

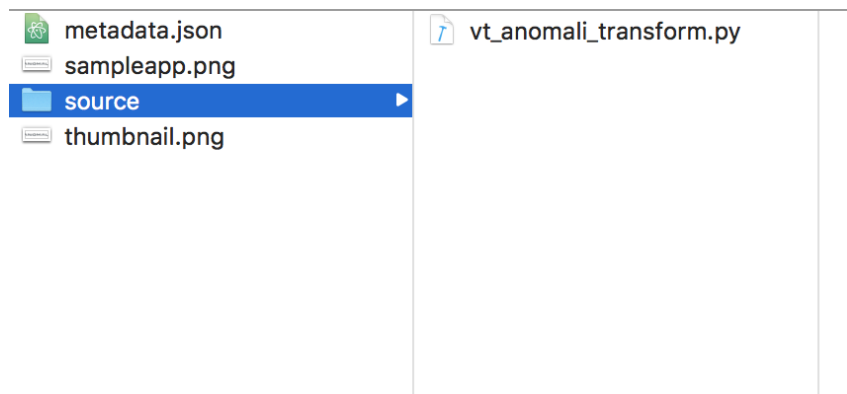
The following example illustrates a valid metadata file. An example metadata file is also included in the Enrichments SDK package provided by Anomali.

```
{
  "title": "SampleApp Enrichment",
  "transform_set_name": "SampleApp Enrichment",
  "description": "Transform set of Anomali enrichments for VirusTotal",
  "icons": {
    "icon_display": "virustotal.png",
    "icon_thumbnail": "thumbnail.png"
  },
  "sdk_type": "anomali",
  "app_name": "com.anomali.SampleApp_Enrichment",
  "version": "2.0.0",
  "credentials": [
    {
      "name": "api_key",
      "description": "API Key for Anomali Sampleapp (VirusTotal API",
      "label": "API Key",
      "required": true,
      "sensitive": true,
      "rank": 1
    },
    {
      "name": "optional_param_1",
      "description": "optional_param_1 for Anomali Sampleapp",
      "label": "Optional Param 1",
      "required": false,
      "sensitive": false,
      "rank": 2
    },
    {
      "name": "optional_param_2",
      "description": "optional_param_2 for Anomali Sampleapp",
      "label": "Optional Param 2",
      "required": false,
      "sensitive": false,
      "rank": 3
    }
  ],
  "transforms": [
    {
      "transform_name": "enrichDomainTabOne",
      "pivoting": false,
      "enrichment": true,
      "display_name": "enrichDomainTabOne",
      "description": "Find all the enrichment for the domain",
      "author": "Anomali",
      "parameters": "vt_anomali_enrichment.py enrichDomainTabOne",
      "entity_type": "anomali.Domain",
      "rank": 1
    },
    {
      "transform_name": "enrichDomainTabTwo",
      "pivoting": false,
      "enrichment": true,
      "display_name": "enrichDomainTabTwo",
      "description": "Find all the enrichment for the domain",
      "author": "Anomali",
      "parameters": "vt_anomali_enrichment.py enrichDomainTabTwo",
      "entity_type": "anomali.Domain",
      "rank": 2
    },
    {
      "transform_name": "enrichIP",
      "pivoting": false,
      "enrichment": true,
      "display_name": "enrichIP",
      "description": "Find all the enrichment for the IP",
      "author": "Anomali",
      "parameters": "vt_anomali_enrichment.py enrichIP",
      "entity_type": "anomali.IPv4Address",
      "rank": 1
    }
  ]
}
```

Creating the Enrichment TGZ Bundle

Once you have assembled the python scripts, metadata file, and icon images, use the instructions in this section to create the final TGZ bundle for the enrichment.

The following is an example of a directory that contains all required files for the Enrichment SDK bundle:



To create the enrichment bundle:

1. Create a directory at the same level as your enrichment folder:

```
mkdir bundle
```

2. Move to the directory that contains the enrichment bundle components:

```
cd <dir_name>
```

3. Bundle the enrichments components in TGZ format:

```
tar cvf ../bundle/<file_name>.tgz .
```

Note: MacOS users must use the `COPYFILE_DISABLE` flag for the bundle to be compatible with ThreatStream. As such MacOS users should use the following command:

```
COPYFILE_DISABLE=1 tar cvf ../bundle/<file_name>.tgz .
```

If you intend to use your enrichment on ThreatStream Cloud, proceed to ["Testing ThreatStream Cloud Enrichment Bundles"](#) on page 41.

If you intend to use your enrichment on ThreatStream OnPrem or AirGap, proceed to ["Testing and Managing ThreatStream OnPrem and AirGap Enrichment Bundles"](#) on page 44.

Chapter 6: Testing ThreatStream Cloud Enrichment Bundles

If you are developing your enrichment for use on ThreatStream Cloud, you must test your enrichment on a staging server before submitting it to Anomali for certification.


To gain access to a staging instance, send an email to ***enrichments.sdk@anomali.com*** that includes the following information:

- Organization name
- Email addresses of all users in need of access
- Which users should be given administrative privileges
- IP addresses from which you will access the staging server

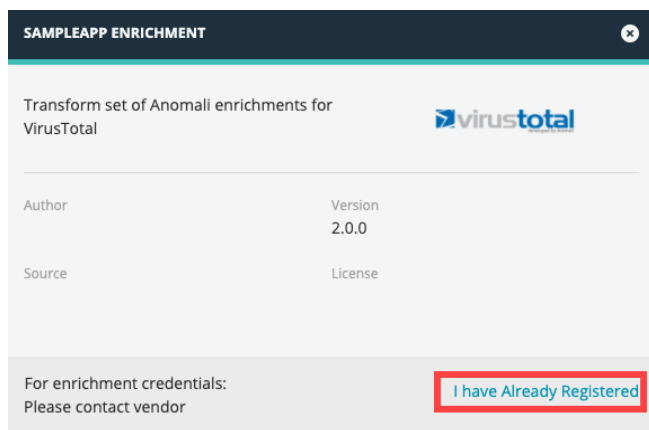
After your request is approved, Anomali will email you with further instructions on accessing the staging instance. Once you have access, you can connect to the staging instance and upload the bundle for testing.

Note: *Do not add users or change user privileges through the staging server user interface.* Send all staging server user administration requests to ***enrichments.sdk@anomali.com***.

To upload and activate your enrichment:

1. Connect to the ThreatStream staging user interface.
2. In the top navigation bar, click  and then **Integrations**.
3. Click **Upload New Enrichment** and browse for the TGZ file on your system.
4. Click **Upload & Install**. After installation, the enrichment is displayed on the Integrations screen.
5. Locate your enrichment and click **Set Up**.

6. If credentials are required, click **I have already registered** and enter the credentials for your enrichment.



SAMPLEAPP ENRICHMENT

Transform set of Anomali enrichments for VirusTotal

Author	Version 2.0.0
Source	License

For enrichment credentials:
Please contact vendor

I have Already Registered

7. Click **Activate**.

Your enrichment is now active on ThreatStream staging and ready to test.

Note: Only users with Org Admin privileges can upload and install enrichments.

Debugging Enrichments

If you added any debugging messages to your enrichment using the `at.addMessage` method, they will be displayed in the JSON output of the enrichment.

To view debugging messages:

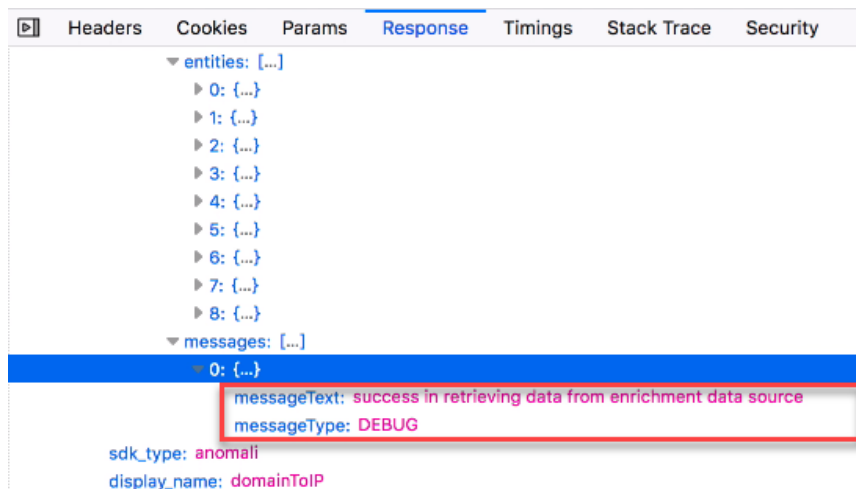
1. Open the developer console on your web browser.
2. To debug a context-based enrichment, navigate to the details page of an observable on which enrichment data is returned and open the tab for the enrichment under Enrichments.

To debug a pivot-based enrichment, navigate to **Research > Explore**, add an observable to the chart, and run the enrichment you want to debug.

3. If using Google Chrome, open the Network tab of the developer console.

If using another browser, locate a comparable resource.

4. Use the developer console search to locate a POST request that uses `https://svlpartner-optic-api.threatstream.com/api/v1/integration_package/transform/`.
5. Debugging messages are displayed in the `messages` field under `transform_result`.



Chapter 7: Testing and Managing ThreatStream OnPrem and AirGap Enrichment Bundles

Use the information in this chapter to test, upload and activate, and manage enrichment bundles developed for ThreatStream OnPrem or AirGap.

Testing Enrichments on ThreatStream OnPrem

Anomali does not provide cloud staging environments for enrichments developed for use on ThreatStream OnPrem. Therefore, ThreatStream OnPrem enrichments can be tested on existing ThreatStream OnPrem v4.0 deployments.

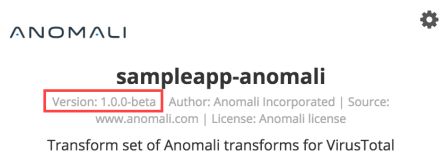
To demarcate enrichments that are currently undergoing testing from finalized enrichments, you can use the following metadata items to distinguish enrichments undergoing testing from finalized enrichments:

- `app_name`

For example: `com.anomali.sampleapp-beta`

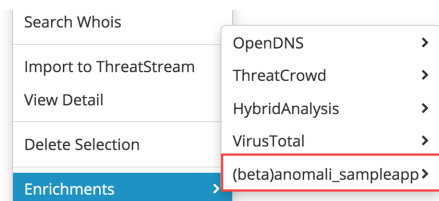
- `version` (displayed on the settings/integrations UI)

For example: `1.0.0-beta`



- `transform_set_name`

For example: (beta)anomali_sampleapp



Alternatively, if your organization leverages a secondary ThreatStream OnPrem deployment for testing purposes, you can upload and test your enrichment on this independent deployment.

Proceed to ["Uploading and Activating Enrichments on ThreatStream OnPrem and AirGap" on the next page](#) for instructions on uploading and activating your enrichment for testing.

For information on viewing debugging messages, see ["Debugging Enrichments" on page 42](#).

Testing Enrichments on ThreatStream AirGap

Enrichments developed for ThreatStream AirGap can be tested on your existing deployment by using one of two methods:

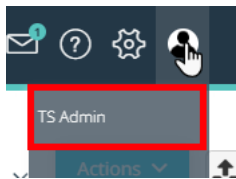
- Upload and activate enrichments as a member of your current organization on ThreatStream AirGap and use the meta data items listed in ["Testing Enrichments on ThreatStream OnPrem" on the previous page](#) to distinguish enrichments undergoing testing from finalized enrichments.
- Create a new organization on your ThreatStream AirGap deployment which is dedicated to enrichment testing and separate from your day-to-day operations. See the *Anomali ThreatStream AirGap Deployment & Administration Guide* for information on creating a new organization.

If you plan to create a dedicated organization for testing enrichments, you must enable the *Can setup enrichment bundle* setting on the Django Site Administration interface which allows the organization to upload and activate enrichments.

Note: Only users with the `is_staff` privilege can access the Django-Site Administration interface.

To enable enrichment uploads for your test organization:

1. Connect to the ThreatStream AirGap UI.
2. In the ThreatStream menu, click **TS Admin**.



3. Under Tsdb, click **User organizations**.
4. Click the ID of the new organization.
5. Under Properties, select **Can setup enrichment bundle**.

A screenshot of a 'Properties' configuration form. The form has a light blue header with the word 'Properties'. It contains several sections with labels and input fields:

- 'Default classification:' with a dropdown menu set to 'Private'.
- 'Default tag tip:' with a dropdown menu set to 'White'.
- 'Default display confidence:' with a dropdown menu set to 'confidence'.
- 'Is tfa enabled' with an unchecked checkbox.
- 'Is newnav enabled' with a checked checkbox.
- 'Can setup enrichment bundle' with a checked checkbox, which is highlighted by a red rectangular box.

6. Click **Save**.

You can now upload and activate enrichments on your dedicated ThreatStream AirGap testing organization.

Proceed to "[Uploading and Activating Enrichments on ThreatStream OnPrem and AirGap](#)" below for instructions on uploading and activating your enrichment for testing.


For information on viewing debugging messages, see "[Debugging Enrichments](#)" on page 42.

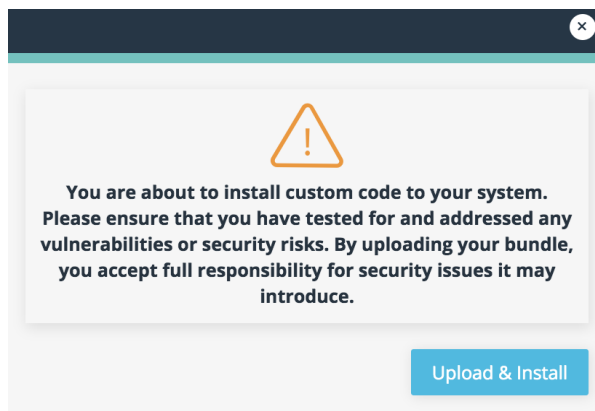
Uploading and Activating Enrichments on ThreatStream OnPrem and AirGap

If your enrichment was developed for use on your ThreatStream OnPrem or AirGap appliance, certification from Anomali is not necessary. Use the steps in this section to upload and activate your enrichment directly on your appliance. These steps can

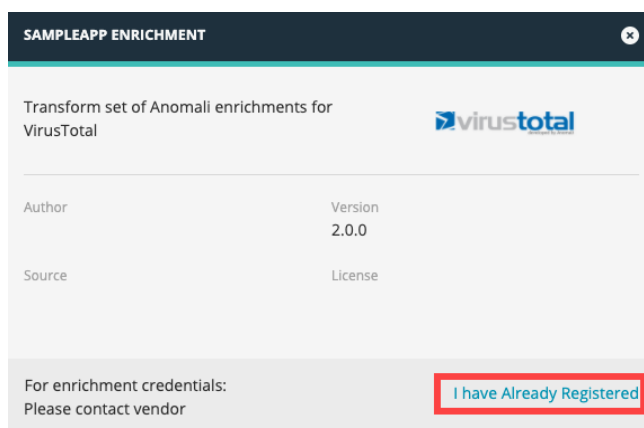
be used for uploading enrichments currently undergoing testing or finalized enrichments.

To upload and activate your enrichment on ThreatStream OnPrem or AirGap:

1. Connect to your ThreatStream OnPrem or AirGap user interface.
2. In the top navigation bar, click  and then **Integrations**.
3. Click **Upload New Enrichment** and browse for the TGZ file on your system. You will see the following warning message:



4. Click **Upload & Install**. After installation, the enrichment is displayed on the Integrations screen.
5. Locate your enrichment and click **Set Up**.
6. If credentials are required, click **I have already registered** and enter the credentials for your enrichment.



7. Click **Save**.

Your enrichment is now activated and ready for testing or general use.


If updates are ever required, simply follow the above steps to re-upload your enrichment. ThreatStream upgrades existing enrichments based on the value specified for `app_name` in enrichment metadata files.

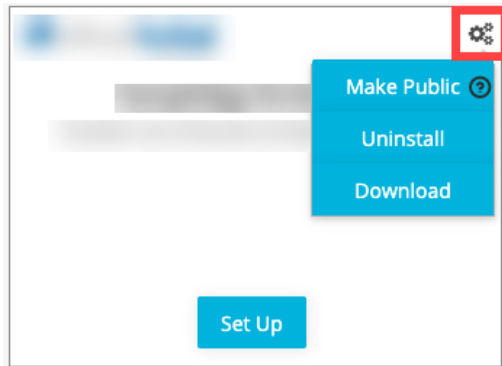
Making Enrichments Public Between Organizations on ThreatStream AirGap Deployments

By default, enrichments developed for ThreatStream AirGap are private and visible only to the organization which uploaded and installed the bundle. For cases in which ThreatStream AirGap deployments include multiple organizations, administrative users can make enrichments publicly available on the deployment—that is, visible to all organizations configured on the ThreatStream AirGap appliance.

When enrichments are made public, all organizations on the deployment have the ability to activate them from the Integrations tab within settings on ThreatStream AirGap. Enrichments are not automatically activated for all organizations when made public. Credentials for activating enrichments cannot be shared across organizations.

To make enrichments publicly available between organizations on ThreatStream AirGap:

1. Connect to your ThreatStream AirGap user interface.
2. In the top navigation bar, click  and then **Integrations**.
3. Locate your enrichment and click the settings icon in the top right corner of the tile.



4. Click **Make Public**.

5. Click **Yes**.

The enrichment is now visible to all organizations on your ThreatStream AirGap deployment.

Chapter 8: Submitting ThreatStream Cloud Enrichments for Certification

Once you have tested your enrichment intended for use on ThreatStream Cloud you can submit it to Anomali for certification.

Prerequisites

Before submitting your enrichment you will need:

- Final enrichment bundle in TGZ format
See ["Creating Enrichment Bundles" on page 33](#) for more information.
- Documentation for your enrichment
See ["Providing Documentation for Your Enrichment" below](#) for more information.

Providing Documentation for Your Enrichment

As part of the enrichment development process, you must provide documentation that instructs users on activating and using your enrichment. Documentation must include the following:

- Supported observables types
- Screenshots of the enrichment on the Explore pivoting tool and observable details pages
- A full list of transformations
- Activation instructions
- Links to more information on your organization and the enrichment
- (If updating your enrichment) A change-log describing updates to your enrichment in the latest release

See ["Sample Documentation " on page 58](#) for an example.

Enrichment Submission Process

After the above prerequisites are met, follow the process below to submit your enrichment.

1. Compress your TGZ enrichment bundle and documentation into a single ZIP file.
2. Email the ZIP file to ***enrichments.sdk@anomali.com***. Include the following in the email:
 - Visibility setting for the enrichment—whether it should be private to your organization or available to the Anomali community.
 - Credentials needed to activate the enrichment. These are needed for Anomali to activate and certify your enrichment.
 - Credentials and any other information relevant to accessing the portal from which your data originates. As part of certification, Anomali must check data returned by the enrichment against data from the source.
 - Version number of Anomali Enrichments SDK you used to develop the enrichment.
3. Anomali performs code review and sanity checks on the enrichment. You will be notified if further changes are required. If no further changes are required, Anomali certifies your enrichment.
4. Anomali installs the enrichment on ThreatStream production, making it available to your organization only or the Anomali community.

Chapter 9: Updating Enrichment Bundles

The Anomali Enrichments SDK enables in-place updates of enrichment bundles. You can use the guidelines in this section to make necessary changes to your enrichment and upload it, thus replacing the previous version. When enrichments are updated in adherence with these guidelines, all subscriptions remain active and do not require user intervention.

Updates can involve changes to source python scripts, enrichment icons, or any of the following metadata items:

- `title`
- `transform_set_name`
- `description`
- `icon_display`
- `icon_thumbnail`
- `version`
- `transforms`
- `author`
- `long_description`
- `license`
- `source_url`

Note: Updates to credentials are not supported for in-place upgrades. If credential updates are required, such as adding a new credential field or changing the order of fields on the ThreatStream user interface, you must update your enrichment through a fresh installation of the updated bundle.

Requirements

In order to update enrichments in-place, you *must* adhere to these requirements:

- `app_name` values must be identical to the values of previously installed enrichments
- `version` must be updated to reflect the latest version

Example: 1.0.0 to 1.1.0 or 1.0.0 to 2.0.0

After making necessary changes to your bundle and ensuring that the above requirements are met, you can test your enrichment in the environment appropriate to your deployment. When testing is complete, ThreatStream Cloud users can submit updated enrichment to Anomali using the guidelines in ["Submitting ThreatStream Cloud Enrichments for Certification " on page 50](#) ThreatStream OnPrem and AirGap users can upload and install updates using the instructions in ["Uploading and Activating Enrichments on ThreatStream OnPrem and AirGap" on page 46](#).

Chapter 10: Troubleshooting Your Enrichment

If your enrichment does not work as expected, consult the information in this section to troubleshoot the issue before sending an email to Anomali support. This section also provides instructions on gathering relevant information that must be included in support emails.

To troubleshoot your enrichment:

1. Ensure your script does not contain exceptions.

Use the instructions in ["Testing Your Python Script" on page 30](#) to execute the script on your local machine. Inspect the output of the script and verify that the "exceptions" field is empty.

The following is an example of valid output that does not contain exceptions:

```
python abc_enrichment.py enrichIP 145.239.87.21 --credentials {"api_key\":"y3*****T8r\"}
{"widgets":[{"chartName":"Geo-map","widgetType":"Chart","highchartsJson":{"series\":[{"borderColor\":"#A0A0A0\","nullColor\":"rgba(200, 200, 200, 0.3)\","name\":"Basemap\","showInLegend\":"*****"itemType":"String","itemValue":"A honeypot probability score ranging from 0 (not a honeypot) to 1.0 (is a honeypot)"}, {"widgetType":"Text","lineBreakEnding":true}], "exceptions":[], "messages":[]}]
Process finished with exit code 0
```

2. Ensure your enrichment is activated.

Verify that the correct credentials were used to activate your enrichment.

3. Ensure all transforms perform as expected.

Verify that the issue is not caused by issues with the python script.

Sending Enrichment SDK Support Emails to Anomali

If your issue was not solved by following the troubleshooting steps above, send an email to enrichsdksupport@anomali.com that contains the information detailed in this section. The required information differs based on the ThreatStream form factor for which you developed the enrichment.

For ThreatStream Cloud enrichments, support emails must contain the following information:

- **ThreatStream User:** Email address associated with the account on the ThreatStream staging instance used for testing.
- **ThreatStream Organization:** Name of the organization registered on the ThreatStream staging instance.

Example: *anomali.com*

- **Enrichment Bundle Name:** Name of the enrichment displayed on the Integrations screen within settings.
- **Enrichment Version:** Version number specified in the metadata file.

Example: *1.0.1*

- **Enrichment Bundle:** Attach your enrichment bundle in .tar format to the email.
- **Credentials:** Credentials that Anomali can use to activate your enrichment. The credentials you include can be temporary. However, you must ensure that the credentials you include give Anomali full access to the services offered by the enrichment.
- **Input entity type and value:** Type of observable on which the enrichment runs and an example observable value for which it should exhibit expected behavior.

Example: *IP, 136.56.103.201*

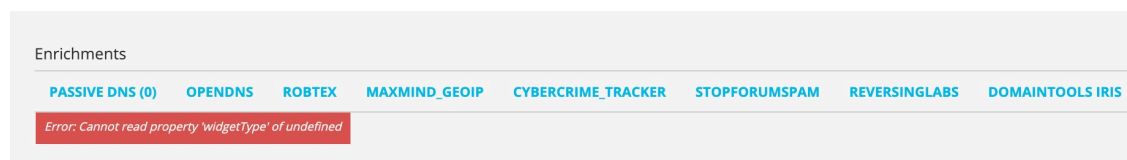
- **Backend Response:** Include the full text of the error message in addition to screenshots of the error as displayed on the user interface and the backend. Use the developer tools on your browser and locate the response for the following endpoint:

`https://svlpartner-optic-api.threatstream.com/api/v1/integration_package/transform/`

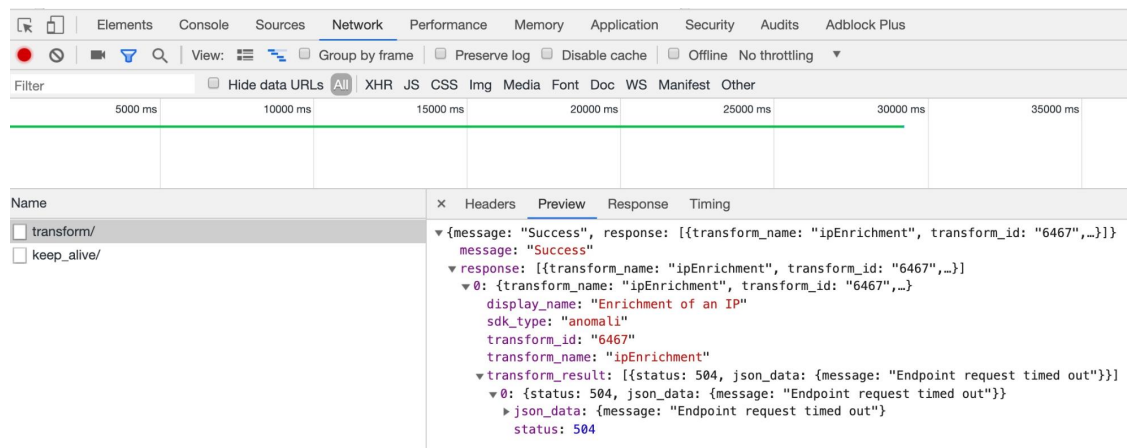
Example error text:

```
{"message": "Success", "response": [{"transform_name": "ipEnrichment",  
  "transform_id": "1111", "transform_result": [{"status": 504, "json_data":  
    {"message": "Endpoint request timed out"}}], "sdk_type": "anomali", "display_  
  name": "Enrichment of an IP"}]}
```

Example UI screenshot:



Example backend screenshot:



- **Expected Behavior:** Screenshot that depicts a rendering of the expected behavior on your portal.
- **Portal Credentials:** (Optional) Credentials for accessing the portal that provides enrichment data.
- **Client Details:** Browser, browser version, OS, and OS version on which the issue was experienced.

For ThreatStream OnPrem or ThreatStream AirGap enrichments, the above details are optional. However, Anomali recommends including the backend response and screenshots of the issue to expedite troubleshooting. Additionally, ThreatStream

OnPrem and AirGap enrichment support emails must contain the following information:

- **Appliance Type:** Whether you are using ThreatStream OnPrem or ThreatStream AirGap.
- **Appliance Version:** Version of ThreatStream OnPrem or ThreatStream AirGap you are currently running.
- **Client Details:** Browser, browser version, OS, and OS version on which the issue was experienced.

If you cannot provide the details requested to adequately describe the issue, email enrichsdksupport@anomali.com for further support.

Appendix A: Sample Documentation

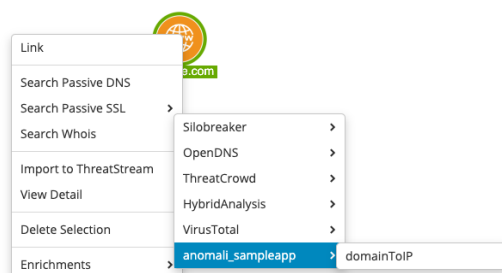
This appendix contains documentation for the Anomali Sample App, which is included in the Anomali Enrichments SDK bundle. You can use it as a template to guide documentation creation for your enrichment.

Enriching Data with the Anomali Sample App

What's New in Anomali Sample APP v2:

- Added a Domain to Email address transformation.
- General bug fixes.

When activated, the Anomali Sample App enrichment can provide data enrichments from Virus Total for domains, email, addresses, and IP addresses. You can leverage Anomali Sample App data on the Explore pivoting tool after activation.



The Anomali Sample App also displays enrichment data is available on observable details pages. For example, the following displays the hostnames to which an IP address resolves.



The screenshot shows the 'Enrichments' section of the Anomali interface. A header bar contains navigation links and a 'SAMPLEAPP ENRICHMENT' button. Below this, a blue pill-shaped button displays 'IP Enrichment for 104.27.158.93'. The main content area is titled 'Resolutions' and shows a list of 25 items (1 - 25 of 924 items). The table has two columns: 'Hostname' and 'Last Resolved'. Each row contains a hostname in a blue pill and a timestamp. A settings gear icon is visible in the top right of the table.

Hostname	Last Resolved
06903609.cn	2019-01-16 20:20:04
12fandub.mt	2018-12-20 17:07:04
13870.com	2018-04-19 10:04:53
1742919.sop	2016-11-17 00:00:00
2000k6.tw	2018-11-20 23:54:06
2grktgnet.mt	2018-09-23 23:28:28
33115286.cn	2018-09-26 12:35:18
33d3d6.ga	2018-11-19 19:52:10

To read more about Anomali, see www.anomali.com

The Anomali Sample App enables the following data transformations:


- **domaintoIP**: returns IP addresses that resolve to the domain.
- **IPtodomain**: returns domains that resolve to the IP address.
- **domaintoEmail**: returns email addresses associated with the domain.

To activate the Anomali Sample App enrichment:

1. Log in to the ThreatStream user interface.
2. In the top navigation bar, click the settings icon and then **Integrations**.
3. Click **Set Up** in the sampleapp-anomali box.
4. Click **I have already registered** and enter your Virus Total API Key.

SAMPLEAPP ENRICHMENT

Transform set of Anomali enrichments for VirusTotal



Author	Version
	2.0.0
Source	License

For enrichment credentials:
Please contact vendor

I have Already Registered

Note: If you do not have a Virus Total API Key see the following URL for more information: <https://support.virustotal.com/hc/en-us/articles/115002088769-Please-give-me-an-API-key>

5. Click **Activate**.

If errors occur, contact support@anomali.com for assistance.

The Anomali Sample App enrichment is now active.