ThreatQuotient

Zscaler Action Bundle

Version 1.1.0

September 16, 2024

ThreatQuotient
20130 Lakeview Center Plaza Suite 400
Ashburn, VA 20147

ThreatQ Supported

Support
Email: support@threatq.com
Web: support.threatq.com
Phone: 703.574.9893

Contents

Warning and Disclaimer

ThreatQuotient, Inc. provides this document “as is”, without representation or warranty of any kind, express or implied, including without limitation any warranty concerning the accuracy, adequacy, or completeness of such information contained herein. ThreatQuotient, Inc. does not assume responsibility for the use or inability to use the software product as a result of providing this information.

Support

This integration is designated as **ThreatQ Supported**.

Support Email: support@threatq.com
Support Web: https://support.threatq.com
Support Phone: 703.574.9893

Integrations/apps/add-ons designated as **ThreatQ Supported** are fully supported by ThreatQuotient's Customer Support team.

ThreatQuotient strives to ensure all ThreatQ Supported integrations will work with the current version of ThreatQuotient software at the time of initial publishing. This applies for both Hosted instance and Non-Hosted instance customers.

> ⚠ ThreatQuotient does not provide support or maintenance for integrations, apps, or add-ons published by any party other than ThreatQuotient, including third-party developers.

Integration Details

ThreatQuotient provides the following details for this integration:

Current Integration Version	1.1.0
Compatible with ThreatQ Versions	>= 6.1.0
ThreatQ TQO License Required	Yes
Support Tier	ThreatQ Supported

Introduction

The Zscaler Action Bundle integration provides ThreatQ users with the ability to export FQDNs, URLs, and IP Addresses in a ThreatQ data collection to a Zscaler URL Category. Users can also enrich selected indicators with information from Zscaler as well as clear URLs.

The integration provides the following actions:

- **Zscaler - Export URLs** - adds the indicators in a data collection to a predefined Zscaler URL Category.
- **Zscaler - Clear URL Category** - clears a category of URLs in Zscaler.
- **Zscaler - Get URL Categories** - enriches FQDNs and URLs with information from Zscaler.

The actions are compatible with the following indicator types:

- FQDN
- IP Address
- URL

This action is intended for use with ThreatQ TDR Orchestrator (TQO). An active TQO license is required for this feature.

Prerequisites

The following is required in order to install and use the action.

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing at least one of the following indicator types:
  - FQDN
  - IP Address
  - URL
- Zscaler Username.
- Zscaler Password.
- ZScaler API Key.

> See the following link for additional information about the Zscaler API key: https://help.zscaler.com/zia/managing-cloud-service-api-key.

Installation

Perform the following steps to install the integration:

> The same steps can be used to upgrade the integration to a new version.

1. Log into https://marketplace.threatq.com/.
2. Locate and download the action zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the action zip file using one of the following methods:
    - Drag and drop the zip file into the dialog box
    - Select **Click to Browse** to locate the zip file on your local machine

> ThreatQ will inform you if the action already exists on the platform and will require user confirmation before proceeding. ThreatQ will also inform you if the new version of the action contains changes to the user configuration. The new user configurations will overwrite the existing ones for the action and will require user confirmation before proceeding.

You will still need to configure the action.

Configuration

> ThreatQuotient does not issue API keys for third-party vendors. Contact the specific vendor to obtain API keys and other integration-related credentials.

To configure the integration:

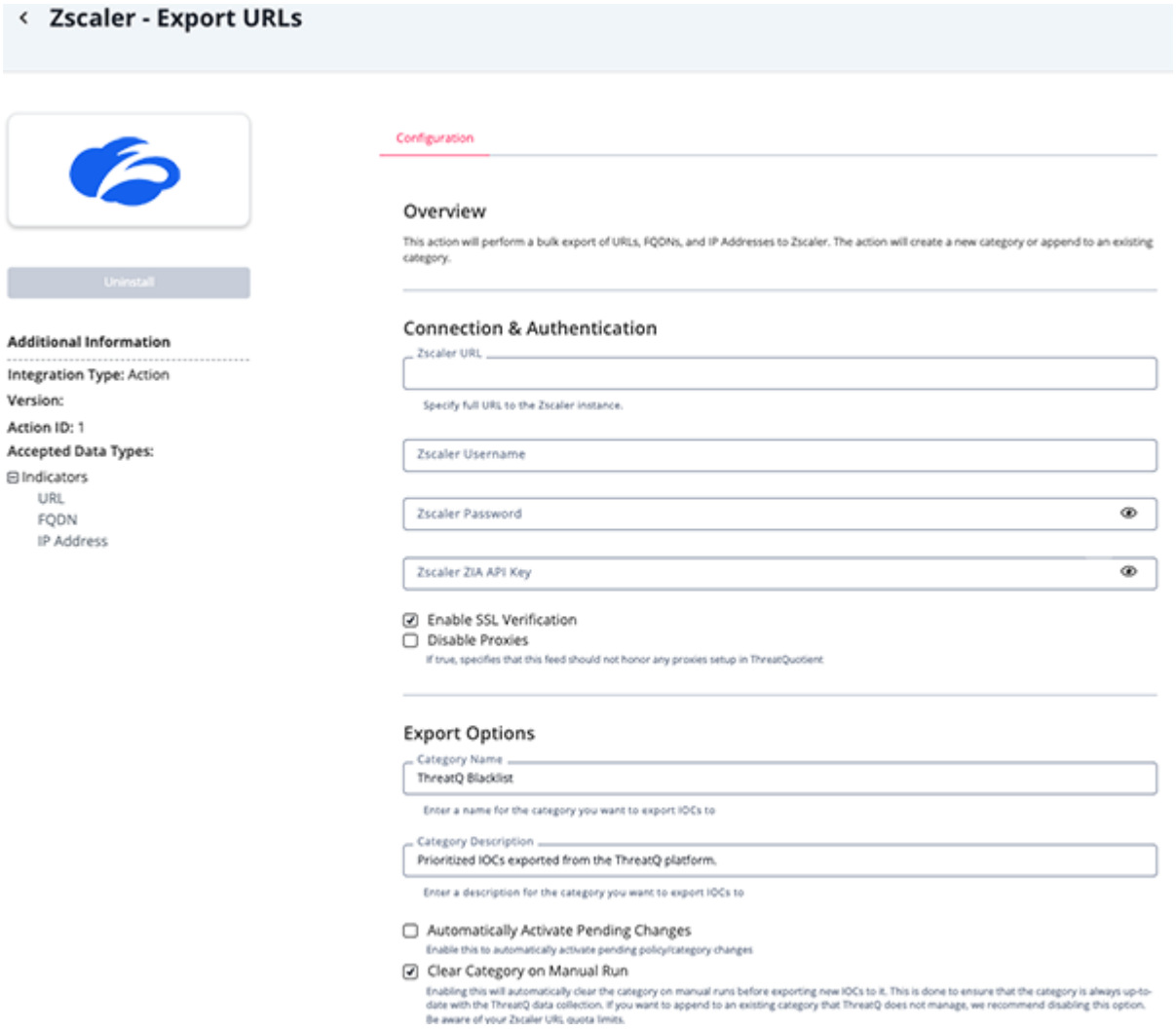
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> The configurations set on this page will be used as the default settings when inserting this action into a new workflow. Updating the configurations on this page will not update any instances of this action that have already been deployed to a workflow. In that scenario, you must update the action's configurations within the workflow itself.

Export URLs Parameters

PARAMETER	DESCRIPTION
Zscaler URL	Enter the full URL of your Zscaler instance.
Zscaler Username	Enter your Zscaler Cloud (ZIA) username to authenticate.
Zscaler Password	Enter your Zscaler Cloud (ZIA) password to authenticate.
Zscaler ZIA API Key	Enter the API key provided in Zscaler. This can be found under Administration -> Cloud Service API Security in in your Zscaler instance. Additional information can be found at https://help.zscaler.com/zia/managing-cloud-service-api-key.
Enable SSL Verification	Enable or Disable Host SSL certificate verification.

PARAMETER	DESCRIPTION
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Category Name	Enter a name for the category to export IOCs to when using the action.
Category Description	Enter a description for the category to export IOCs to when using the action.
Automatically Activate Pending Changes	Enable this parameter to automatically activate pending policy/ category changes after uploading the indicators.
Clear Category on Manual Run	Enable this option to clear the category before exporting new IOCs when performing manual runs .
Objects Per Run	Enter the max number of objects to send to this action per run.

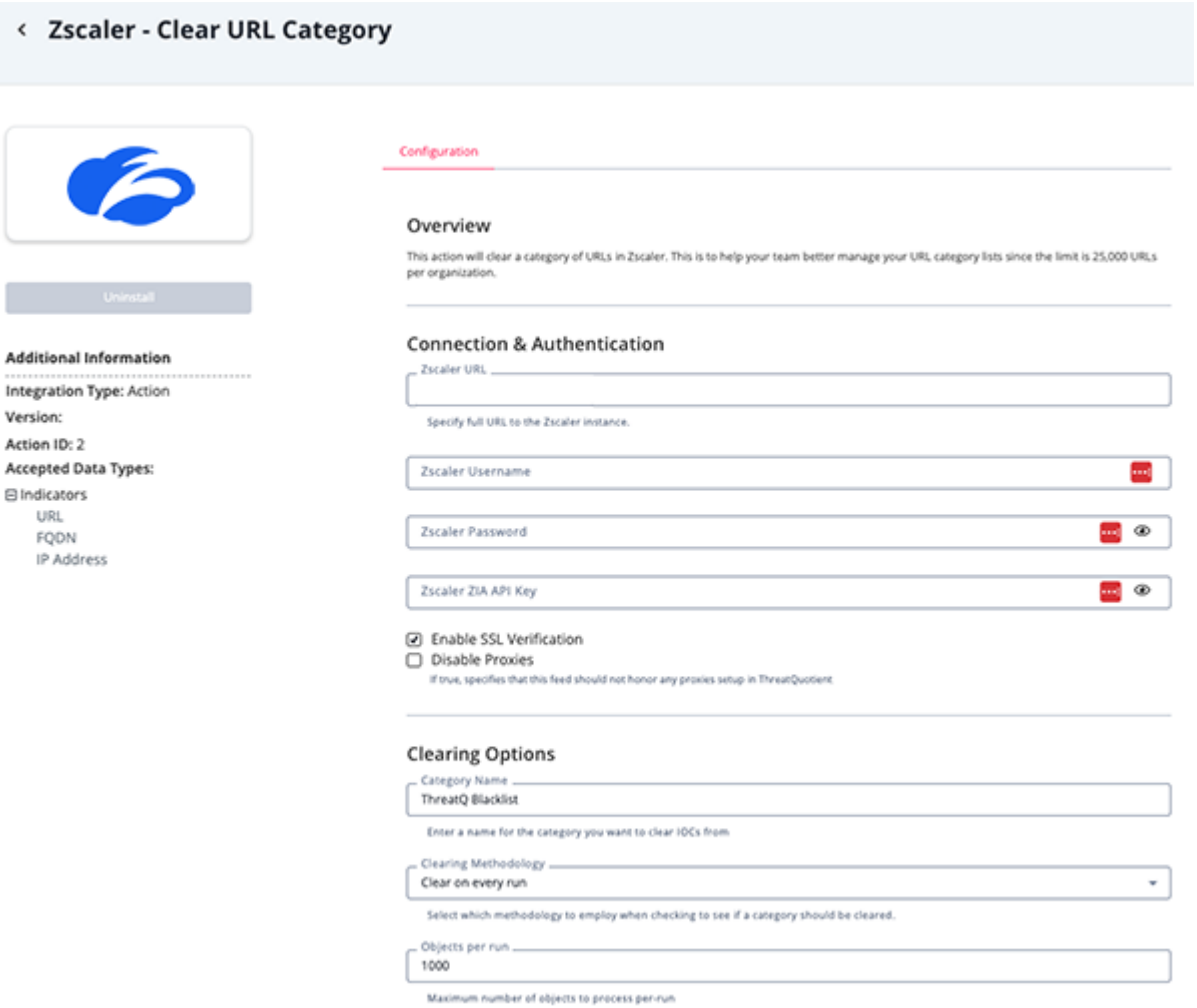


Clear URL Category Parameters

PARAMETER	DESCRIPTION
Zscaler URL	Enter the full URL of your Zscaler instance.
Zscaler Username	Enter your Zscaler Cloud (ZIA) username to authenticate.
Zscaler Password	Enter your Zscaler Cloud (ZIA) password to authenticate.
Zscaler ZIA API Key	Enter the API key provided in Zscaler. This can be found under Administration -> Cloud Service API Security in in your Zscaler

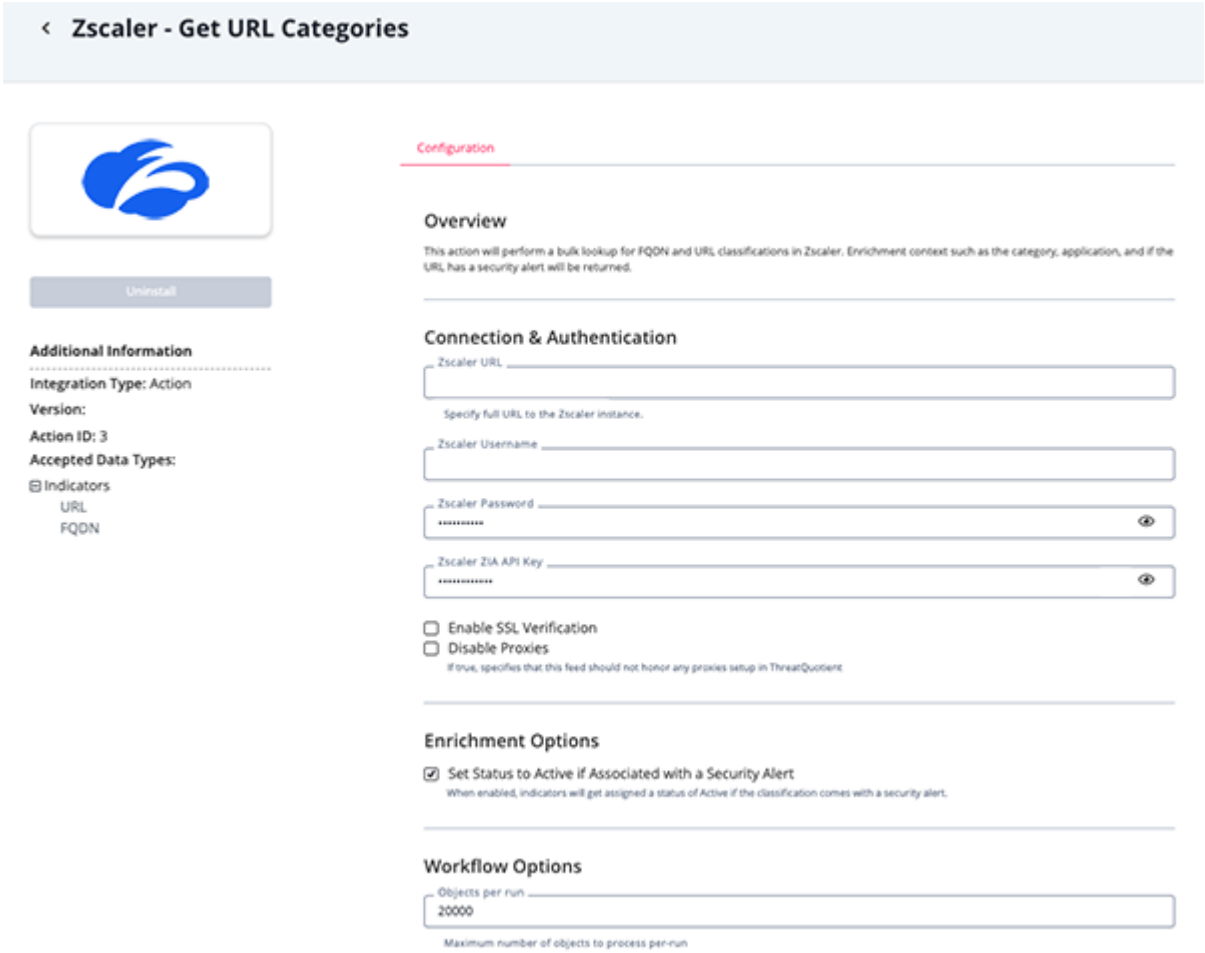
PARAMETER	DESCRIPTION
	instance. Additional information can be found at https://help.zscaler.com/zia/managing-cloud-service-api-key.
Enable SSL Verification	Enable or Disable Host SSL certificate verification.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Category Name	Enter a name for the category to export IOCs to when using the action.
Clearing Methodology	xx Options include: ◦ Clear on every run ◦ Clear if category URL count is greater than threshold ◦ Clear if remaining total URL quota is less than threshold ◦ Clear if category URL count is greater than X percent of the total URL quota
Clear Category if URL Count is Greater Than...	Enter the minimum number of URLs required to clear the category. This option is only available if you selected **Clear if category URL count is greater than threshold** as the **Clearing Methodology** above.
Clear Category if Remaining Total URL Quota is Less than...	Enter the maximum remaining URL quota required to clear the category. This option is only available if you selected **Clear if remaining total URL quota is less than threshold** as the **Clearing Methodology** above.
Clear Category if Count Exceeds X Percent of Total URL Quota	Enter the percentage of the total URL quota that the category URL count must exceed to clear the category.

PARAMETER	DESCRIPTION
	This option is only available if you selected **Clear if category URL count is greater than X percent of the total URL quota** as the **Clearing Methodology** above.
Automatically Activate Pending Changes	Enable this parameter to automatically activate pending policy/ category changes after uploading the indicators.
Objects Per Run	Enter the max number of objects to send to this action per run.



Get URL Categories Parameters

PARAMETER	DESCRIPTION
Zscaler URL	Enter the full URL of your Zscaler instance.
Zscaler Username	Enter your Zscaler Cloud (ZIA) username to authenticate.
Zscaler Password	Enter your Zscaler Cloud (ZIA) password to authenticate.
Zscaler ZIA API Key	Enter the API key provided in Zscaler. This can be found under Administration -> Cloud Service API Security in in your Zscaler instance. Additional information can be found at https://help.zscaler.com/zia/managing-cloud-service-api-key.
Enable SSL Verification	Enable or Disable Host SSL certificate verification.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Set Status to Active if Associated with a Security Alert	When enabled, indicators will get assigned a status of Active if the classification comes with a security alert.
Objects Per Run	Enter the max number of objects to send to this action per run.



5. Review any additional settings, make any changes if needed, and click on **Save**.

Actions

The following action is available:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
Zscaler - URL Category Export Indicators	Adds indicators to a predefined Zscaler URL Category.	Indicator	IP Address, URL, FQDN
Zscaler - Clear URL Category	Clears a category of URLs in Zscaler	Indicators	IP Address, URL, FQDN
Zscaler - Get URL Categories	Enriches Indicators with information from Zscaler	Indicators	URL, FQDN

Zscaler - Export URLs

The Zscaler - Export URLs action uploads the indicators from the selected collection to a predefined Zscaler URL Category. The name of the predefined category must be specified in the action configuration (**Category Name** parameter). The category will be deleted if it already exists, together with all the associated URLs and IP Addresses. The URLs are upload without the HTTP schema.

`POST "{{ZSCALER_URL}}/api/v1/urlCategories"`

Sample Body:

```
{
  "configuredName": "ThreatQ Blacklist",
  "superCategory": "SECURITY",
  "customCategory": true,
  "description": "Prioritized IOCs exported from the ThreatQ platform.",
  "urls": [
    "217.60.9.178",
    "253.106.205.92.host.secureserver.net/konto-creedientials",
    "vetfashion.xyz/css/10/admin/index.php"
  ]
}
```

Sample Response:

```
{
  "configuredName": "ThreatQ Blacklist",
  "customCategory": true,
  "customIpRangesCount": 0,
  "customUrlsCount": 3,
  "dbCategorizedUrls": [],
  "description": "Prioritized IOCs exported from the ThreatQ platform.",
  "editable": true,
  "id": "CUSTOM_04",
  "ipRangesRetainingParentCategoryCount": 0,
  "keywords": [],
  "keywordsRetainingParentCategory": [],
  "superCategory": "SECURITY",
  "type": "URL_CATEGORY",
  "urls": [
    "217.60.9.178",
    "vetfashion.xyz/css/10/admin/index.php",
    "253.106.205.92.host.secureserver.net/konto-creedientials"
  ],
  "urlsRetainingParentCategoryCount": 0,
  "val": 131
}
```

Zscaler - Clear URL Category

The Zscaler Clear URL Category action will clear a category of URLs in Zscaler. This is to help your team better manage your URL category lists since the limit is 25,000 URLs per organization.

`GET "{{ZSCALER_URL}}/api/v1/urlCategories/lite"`

Sample Response:


```
[
  {
    "configuredName": "ThreatQ Blacklist",
    "customCategory": true,
    "customIpRangesCount": 0,
    "customUrlsCount": 0,
    "dbCategorizedUrls": [],
    "description": "Prioritized IOCs exported from the ThreatQ platform.",
    "editable": true,
    "id": "CUSTOM_06",
    "ipRangesRetainingParentCategoryCount": 0,
    "type": "URL_CATEGORY",
    "urls": [],
    "urlsRetainingParentCategoryCount": 0,
    "val": 133
  },
  {
    "configuredName": "ThreatQ Crypto Blacklist",
    "customCategory": true,
    "customIpRangesCount": 0,
    "customUrlsCount": 0,
    "dbCategorizedUrls": [],
    "description": "Prioritized IOCs exported from the ThreatQ platform.",
    "editable": true,
    "id": "CUSTOM_07",
    "ipRangesRetainingParentCategoryCount": 0,
    "type": "URL_CATEGORY",
    "urls": [],
    "urlsRetainingParentCategoryCount": 0,
    "val": 141
  }
]
```


The IDs of the URL Categories that should be deleted are selected from the API Response according to Clearing Methodology configuration.

The .id is used to call the DELETE Endpoint: `DELETE "{{ZSCALER_URL}}/api/v1/urlCategories/{ID}"`

Zscaler - Get URL Categories

The Zscaler - Get URL Categories action will perform a bulk lookup for FQDN and URL classifications in Zscaler. Enrichment context such as the category, application, and if the URL has a security alert will be returned.

```
POST "{{ZSCALER_URL}}/api/v1/urlLookup"
```

Sample Body:

```
[
  "speedlab.com.eg"
]
```

Sample Response:

```
[
  {
    "url": "speedlab.com.eg",
    "urlClassifications": [
      "BLOG"
    ],
    "urlClassificationsWithSecurityAlert": [
      "MALWARE_SITE"
    ]
  }
]
```

ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.application	Indicator.Attribute	Application	N/A	N/A	N/A
.urlClassifications	Indicator.Attribute	Category	N/A	BLOG	N/A
.urlClassificationsWithSecurityAlert	Indicator.Attribute	Category	N/A	MALWARE_SITE	N/A
.urlClassificationsWithSecurityAlert	Indicator.Attribute	Has Security Alert	N/A	True	`True` if `urlClassificationsWithSecurityAlert` has a value, otherwise `False`

Known Issues / Limitations

- The changes to a URL Category must be activated in the Zscaler Portal. You can either enable the **Automatically Activate Pending Changes** configuration parameter to automatically activate any pending changes or go to the Zscaler Portal to manually activate them.
- Zscaler allows for a maximum of 25,000 values across all Categories.
- Zscaler allows for a maximum of 64 predefined categories.
- Zscaler does not accept URLs longer than 1024 characters. Anything longer than this limit is truncated.
- The endpoint used by `Zscaler - Get URL Categories` may somethings return a `412 Unexpected Error`. If this happens, the search will fail.

Change Log

- **Version 1.1.0**
  - Added two new actions:
    - Zscaler - Clear URL Category
    - ZScaler - Export URL Categories
  - Renamed the **Zscaler URL Category Export Indicators** action to **Zscaler - Export URLs**.
  - Resolved the following issues:
    - conflicts would occur between actions within the same workflow
    - URL categories being cleared on each action run. Scheduled (incremental) runs will append new URLs to the category. Manual (full) runs will clear the category and add all URLs from your data collection.
  - Added a new parameter to the **Zscaler - Export URLs** action: **Clear Category on Manual Run.** This will allow users to append to existing categories on manual runs.
  - Added a new known issue for the **Zscaler - Get URL Categories** action regarding a `412 Unexpected Error`.
  - Renamed the integration to Zscaler Action Bundle.
- **Version 1.0.0**
  - Initial release