ThreatQuotient

VMware Carbon Black EDR Action Bundle

Version 1.2.0

March 18, 2025

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 **3**
Support **4**
Integration Details **5**
Introduction **6**
Prerequisites **7**
Installation **8**
Configuration **9**
Process Enrichment 9
Export Indicators 11
Override Reputation 13
Manage XDR Network Data Collection 15
Actions **18**
VMware Carbon Black EDR - Process Enrichment 19
Request to Start a Search Job 19
Request to Get Search Job Results 19
VMware Carbon Black EDR - Export Indicators 22
Request to Search for Report 22
Request to Create/Update a New Report 23
VMware Carbon Black EDR - Override Reputation 25
Request to Create/Update the Reputation for an Indicator of Type SHA-256 25
Request to Create/Update Filename/File Path Reputation 26
Request to Search for Existing Reputation 26
Request to Delete Existing Reputation 27
VMware Carbon Black EDR - Manage XDR Network Data Collection 28
Request to Get the Existing IP Addresses in the XDR Network Data Collection 28
Request to Upload Indicators to XDR Network Data Collection 29
Enriched Data **30**
VMware Carbon Black EDR - Process Enrichment 30
Known Issues / Limitations **31**
Change Log **32**

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	1.2.0
Compatible with ThreatQ Versions	>= 5.12.1
ThreatQ TQO License Required	Yes
Third-Party Deployment Method	Online
Support Tier	ThreatQ Supported

Introduction

VMware Carbon Black EDR is an incident response and threat hunting solution designed for Security Operations Center teams with offline environment requirements. VMware Carbon Black EDR continuously records and stores endpoint activity data so security professionals can hunt threats in real time and visualize the complete attack kill chain, using the VMware Carbon Black Cloud's aggregated threat intelligence.

The VMware Carbon Black EDR Action Bundle installs the following actions:

- **VMware Carbon Black EDR - Process Enrichment** - submits indicators to VMware Carbon Black EDR to be enriched with related threat intelligence.
- **VMware Carbon Black EDR - Export Indicators** - exports indicators to the VMware Carbon Black EDR platform.
- **VMware Carbon Black EDR - Override Reputation** - overrides the reputation for banned applications using a SHA-256 hash or path to a known IT tool application.
- **VMware Carbon Black EDR - Manage XDR Network Data Collection** - adds approved IP addresses to XDR Network Data Collection at the organization level.

The actions are compatible with following indicator types:

- CIDR Block (Mange XDR Network Data Collection action)
- MD5 (Process Enrichment and Export Indicators actions)
- SHA-256 (Override Reputation action)
- Filename (Override Reputation action)
- File Path (Override Reputation action)
- IP Address (Mange XDR Network Data Collection action)
- IPv6 Address (Mange XDR Network Data Collection action)

The File Hash Enrichment action returns the following enriched system objects:

- Indicators
- Exploit Target
  - Exploit Target Attributes
- Events
  - Event Attributes

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

Prerequisites

- An active ThreatQ TDR Orchestrator (TQO) license.
- A data collection containing the following indicator types:
  - CIDR Block (Mange XDR Network Data Collection action)
  - MD5 (Process Enrichment and Export Indicators actions)
  - SHA-256 (Override Reputation action)
  - Filename (Override Reputation action)
  - File Path (Override Reputation action)
  - IP Address (Mange XDR Network Data Collection action)
  - IPv6 Address (Mange XDR Network Data Collection action)
- Required Permissions:

  > These permissions should be done prior to creating a VMware Carbon Black EDR API ID and Secret Key.

  - **VMware Carbon Black EDR - Process Enrichment** - requires the `org.search.events` permission. You need to create a `Custom Access Level` including each category: `Search > Events > org.search.events`, allow permission to `CREATE, READ`. See the following for more information: https://developer.carbonblack.com/reference/carbon-black-cloud/platform/latest/platform-search-api-processes
  - **VMware Carbon Black EDR - Export Indicators** - requires the `org.watchlists` permission. You need to create a `Custom Access Level` including each category: `org.watchlists`, allow permission to `CREATE, READ, UPDATE, DELETE`. See the following for more information: https://developer.carbonblack.com/reference/carbon-black-cloud/cb-threathunter/latest/watchlist-api
  - **VMware Carbon Black EDR - Override Reputation** - requires the `org.reputation` permission. You need to create a `Custom Access Level` including each category: `Application > Reputation > org.reputations`, allow permission to `CREATE, READ, DELETE`. See the following for more information: https://developer.carbonblack.com/reference/carbon-black-cloud/platform/latest/reputation-override-api/#configure-reputation-override
  - **VMware Carbon Black EDR - Manage XDR Network Data Collection** - requires the `org.policies` permission. You need to create a `Custom Access Level` including each category: `Policies > Policies > org.policies`, allow permission to `CREATE, READ, UPDATE, DELETE`. See the following for more information: https://developer.carbonblack.com/reference/carbon-black-cloud/platform/latest/policy-service
    All the permissions mentioned above can be added to the same Custom Access Level used to generate the API Key
- A VMware Carbon Black Organization Key.
- A VMWare Carbon Black EDR API ID.
- A VMWare Carbon Black EDR API Secret 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 bundle zip file.
3. Navigate to the integrations management page on your ThreatQ instance.
4. Click on the **Add New Integration** button.
5. Upload the 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
6. Select the individual actions to install, when prompted, and then click **Install**.

   > 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.

7. The action(s) will be added to the integrations page. You will still need to configure the action(s).

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:

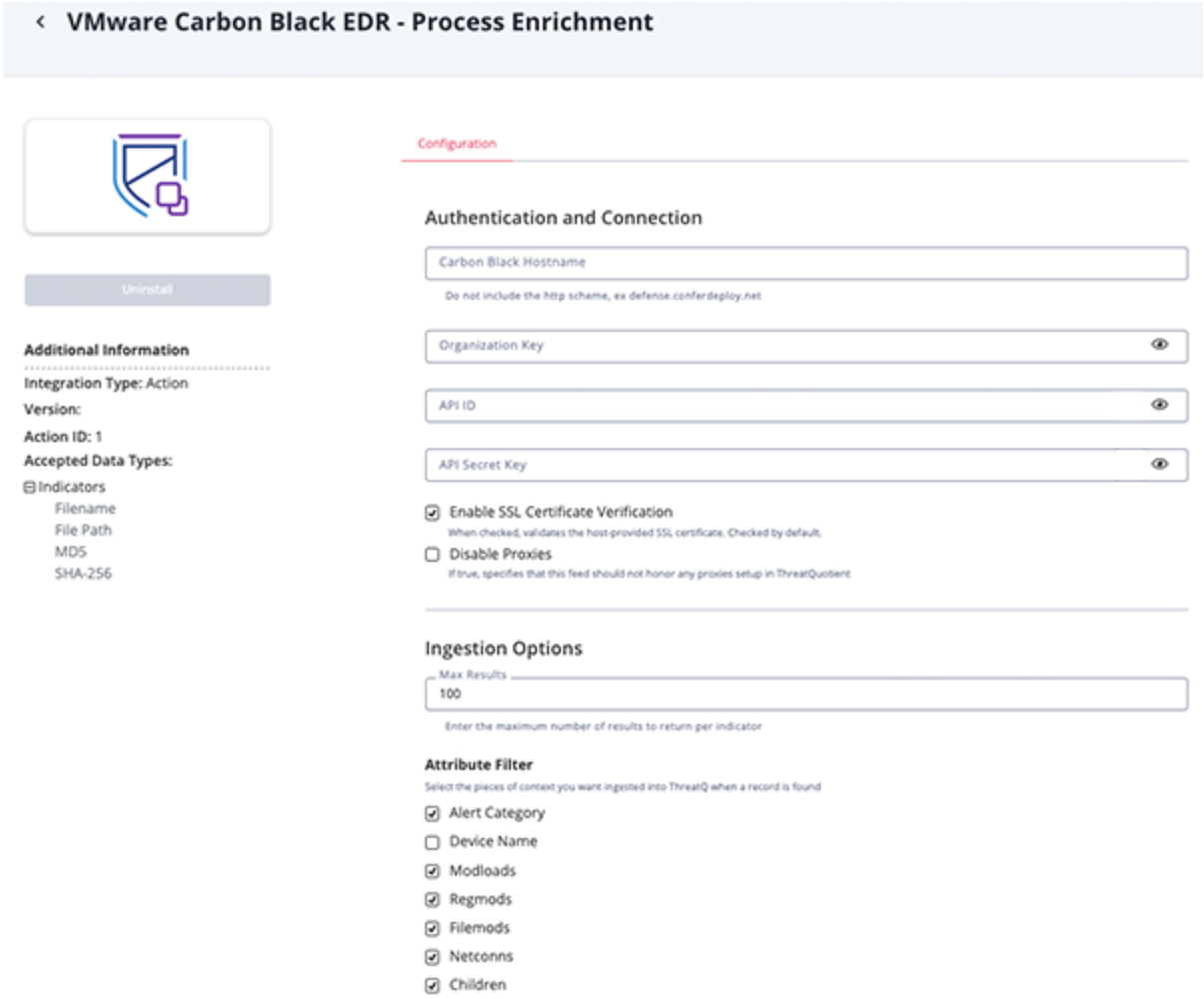
1. Navigate to your integrations management page in ThreatQ.
2. Select the **Actions** option from the *Category* dropdown (optional).
3. Click on the action entry to open its details page.
4. Enter the following parameters under the **Configuration** tab:

> 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.

Process Enrichment

PARAMETER	DESCRIPTION
Carbon Black Hostname	Your VMWare Carbon Black EDR hostname.
Organization key	Your Organization key which can be found in the API Access section of Account Settings on your EDR instance.
API ID	Your API ID which can be found in the API Access section of Account Settings on your EDR instance.
API Secret Key	Your API Secret which can be found in the API Access section of Account Settings on your EDR instance.
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.

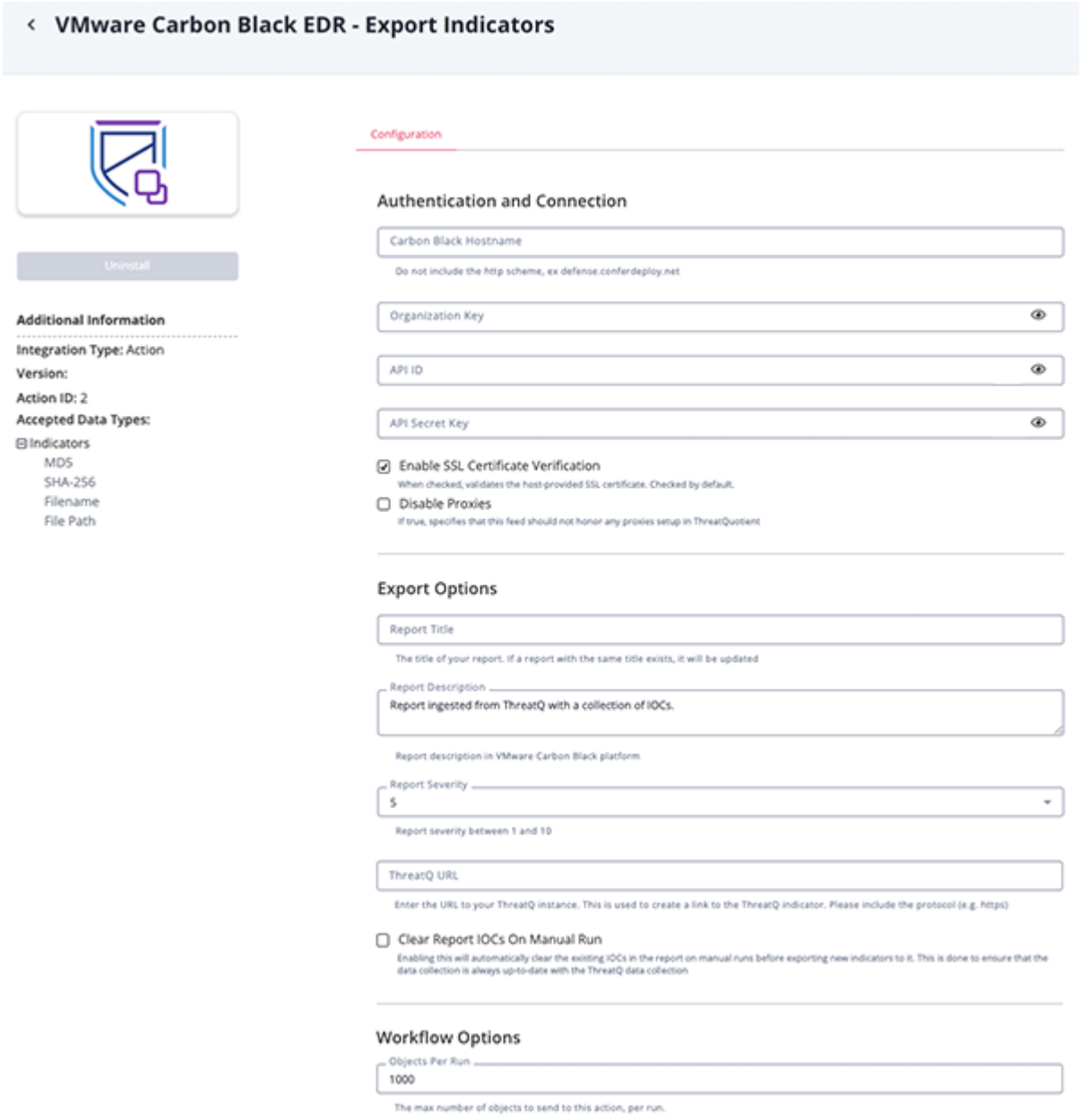
PARAMETER	DESCRIPTION
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Max Results	Enter the maximum number of results to return per indicator.
Attribute Filter	Select the pieces of context to ingest into ThreatQ when a record is found. Options include: ◦ Alert Category *(default)* ◦ Device Name *(default)* ◦ Modloads *(default)* ◦ Regmods *(default)* ◦ Filemods *(default)* ◦ Netconns *(default)* ◦ Children *(default)* ◦ Cross Process *(default)*
Related Objects Filter	Select the related objects to ingest into ThreatQ when a record is found. Options include: ◦ MD5 *(default)* ◦ SHA-256 *(default)* ◦ File Path *(default)* ◦ Username *(default)*
Objects Per Run	The max number of objects per run.



Export Indicators

PARAMETER	DESCRIPTION
Carbon Black Hostname	Your VMWare Carbon Black EDR hostname.
Organization key	Your Organization key which can be found in the API Access section of Account Settings on your EDR instance.
API ID	Your API ID which can be found in the API Access section of Account Settings on your EDR instance.

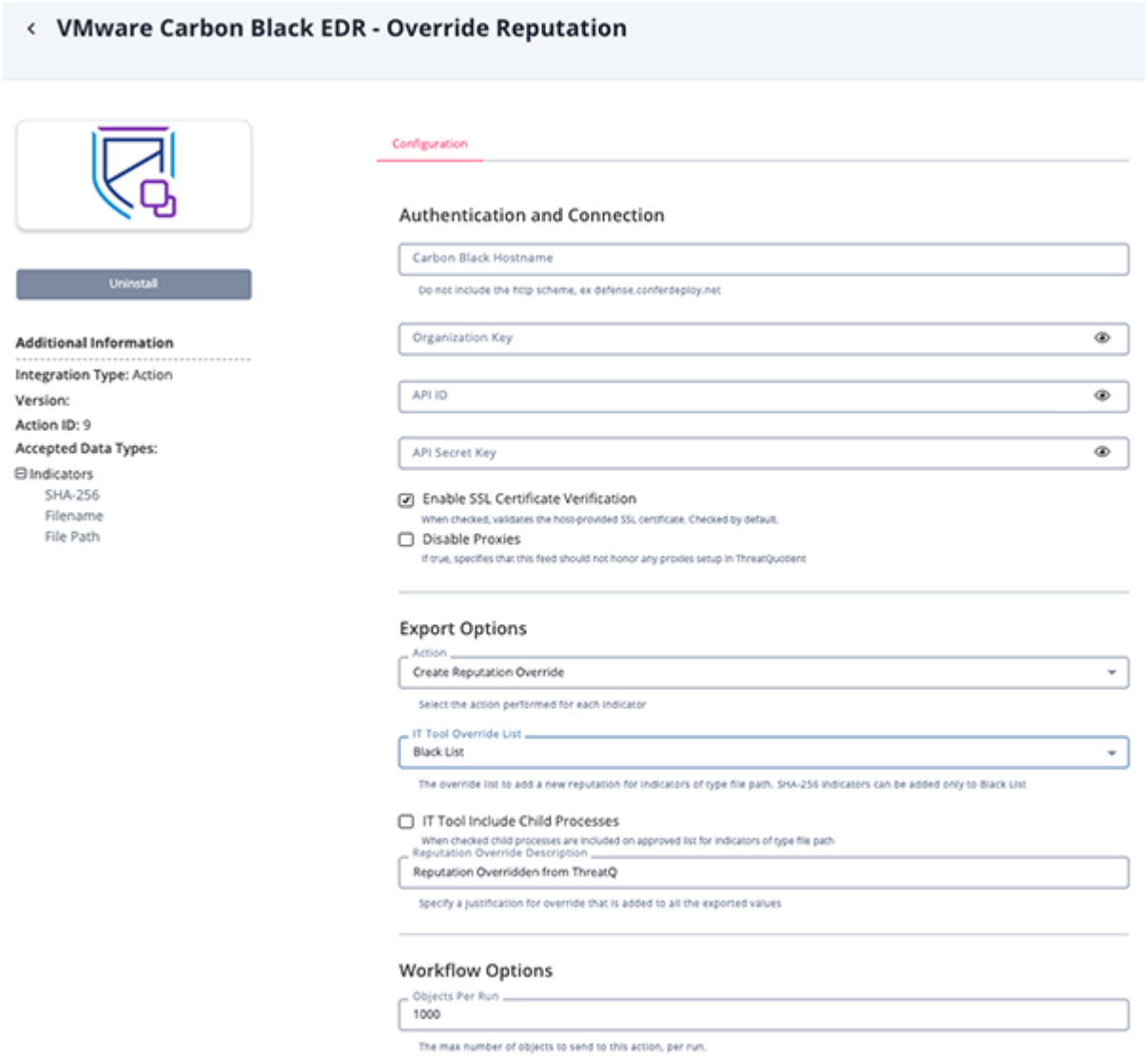
PARAMETER	DESCRIPTION
API Secret Key	Your API Secret which can be found in the API Access section of Account Settings on your EDR instance.
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Report Title	Enter a report title.
Report Description	Enter a report description.
Report Severity	Enter the report severity ranging from 1 to 10. The default selection is 5.
ThreatQ URL	Enter the URL to your ThreatQ instance. This is used to create a link to the ThreatQ indicator. Be sure to include the protocol (e.g. https).
Clear Report IOCs on Manual Run	Enable this parameter to automatically clear the existing IOCs in the report on manual runs before exporting new indicators to it. This is done to ensure that the data collection is always up-to-date with the ThreatQ data collection
Objects Per Run	The max number of objects per run. The Export Indicators action can only send 1,000 objects per run.



Override Reputation

PARAMETER	DESCRIPTION
Carbon Black Hostname	Your VMWare Carbon Black EDR hostname.

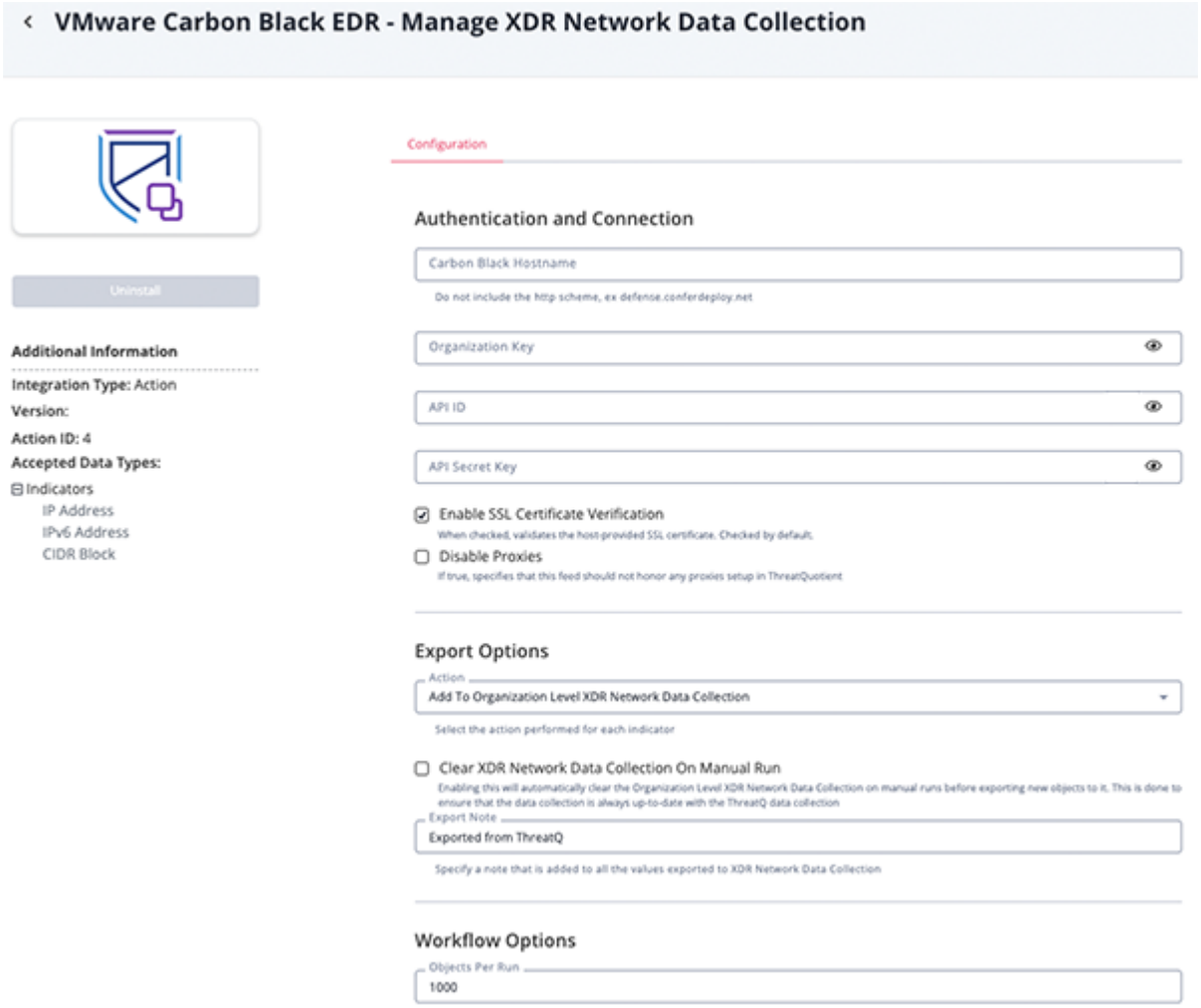
PARAMETER	DESCRIPTION
Organization key	Your Organization key which can be found in the API Access section of Account Settings on your EDR instance.
API ID	Your API ID which can be found in the API Access section of Account Settings on your EDR instance.
API Secret Key	Your API Secret which can be found in the API Access section of Account Settings on your EDR instance.
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Action	Select the action to perform for each indicator. Options include: ◦ Create Reputation Override *(default)* ◦ Delete Reputation Override
IT Tool Override List	Select the list to add a new reputation for File Path type indicators. Options include: ◦ Black List *(default)* ◦ White List SHA-256 type indicators can only be added to Black List.
IT Tool Include Child Processes	Enable this parameter child to include child processes on approved list for File Path type indicators.
Reputation Override Description	Enter a justification for that override that will be added to all the exported values.
Objects Per Run	The max number of objects per run.



Manage XDR Network Data Collection

PARAMETER	DESCRIPTION
Carbon Black Hostname	Your VMWare Carbon Black EDR hostname.
Organization key	Your Organization key which can be found in the API Access section of Account Settings on your EDR instance.

PARAMETER	DESCRIPTION
API ID	Your API ID which can be found in the API Access section of Account Settings on your EDR instance.
API Secret Key	Your API Secret which can be found in the API Access section of Account Settings on your EDR instance.
Enable SSL Certificate Verification	Enable this for the action to validate the host-provided SSL certificate.
Disable Proxies	Enable this option if the action should not honor proxies set in the ThreatQ UI.
Action	Select the action to perform for each indicator. Options include: ◦ Add To Organization Level XDR Network Data Collection *(default)* ◦ Remove From Organization Level XDR Network Data Collection
Clear XDR Network Data Collection on Manual Run	Enable this parameter to automatically clear the Organization Level XDR Network Data Collection on manual runs before exporting new objects to it. This is done to ensure that the data collection is always up-to-date with the ThreatQ data collection.  This parameter is only accessible if you have selected `Add To Organization Level XDR Network Data Collection` for the **Action** parameter.
Export Note	Specify a note that is added to all the values exported to XDR Network Data Collection.
Objects Per Run	The max number of objects per run.



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

Actions

The bundle provides the following actions:

ACTION	DESCRIPTION	OBJECT TYPE	OBJECT SUBTYPE
VMware Carbon Black EDR - Process Enrichment	Submits indicators to VMware Carbon Black EDR to be enriched with related threat intelligence	Indicator	MD5
VMware Carbon Black EDR - Export Indicators	Exports indicators to VMware Carbon Black EDR platform.	Indicator	MD5
VMware Carbon Black EDR - Override Reputation	Override the reputation for banned applications using a SHA-256 hash or path to a known IT tool application.	Indicator	SHA-256, File Path, Filename
VMware Carbon Black EDR - Manage XDR Network Data Collection	Adds approved IP addresses to XDR Network Data Collection at the organization level.	Indicator	IP Address, IPv6 Address, CIDR Block

VMware Carbon Black EDR - Process Enrichment

The Process Enrichment action enriches the selected collection of indicators.

Request to Start a Search Job

`POST https://defense.conferdeploy.net/api/investigate/v2/orgs/{{org_key}}/processes/search_jobs`

Sample Request Body:

```
{
  "query": "svchost.exe"
}
```

Sample Response:

```
{
    "job_id": "5c692179-1bc1-4131-a99d-fa8a084b426e-rmq"
}
```

Request to Get Search Job Results

`GET https://defense.conferdeploy.net/api/investigate/v2/orgs/{{org_key}}/processes/search_jobs/{{job_id}}/results`


```
{
  "results": [
    {
      "backend_timestamp": "2025-03-11T13:37:33.459Z",
      "childproc_count": 0,
      "crossproc_count": 13,
      "device_group_id": 0,
      "device_id": 7444880,
      "device_name": "rtest\\cb-rc-01",
      "device_policy_id": 80947,
      "device_timestamp": "2025-03-11T13:36:34.286Z",
      "enriched": true,
      "enriched_event_type": [
        "NETWORK"
      ],
      "filemod_count": 12025,
      "ingress_time": 1741700182373,
      "legacy": true,
      "modload_count": 40,
      "netconn_count": 55773,
      "org_id": "7DESJ9GN",
      "parent_guid": "7DESJ9GN-00719990-000002e8-00000000-1da983f288cac88",
      "parent_pid": 744,
```

```
      "process_guid": "7DESJ9GN-00719990-00001cb8-00000000-1db408a351377de",
      "process_hash": [
        "145dcf6706eeea5b066885ee17964c09",
        "f13de58416730d210dab465b242e9c949fb0a0245eef45b07c381f0c6c8a43c3"
      ],
      "process_name": "c:\\windows\\system32\\svchost.exe",
      "process_pid": [
        7352
      ],
      "process_username": [
        "NT AUTHORITY\\NETWORK SERVICE"
      ],
      "regmod_count": 610,
      "scriptload_count": 0
    }
  ]
}
```


ThreatQuotient provides the following default mapping for this action:

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
results[].device_name	Indicator.Attribute	Device Name	.results[].ingress_time	rtest\cb-rc-01	User-configurable.
.results[].alert_category	Indicator.Attribute	Alert Category	.results[].ingress_time	N/A	User-configurable.
.results[].childproc_count	Indicator.Attribute	Children	.results[].ingress_time	0	User-configurable. Updatable.
.results[].crossproc_count	Indicator.Attribute	Cross Process	.results[].ingress_time	13	User-configurable. Updatable.
.results[].filemod_count	Indicator.Attribute	Filemods	.results[].ingress_time	12025	User-configurable. Updatable.
.results[].modload_count	Indicator.Attribute	Modloads	.results[].ingress_time	40	User-configurable. Updatable.
.results[].netconn_count	Indicator.Attribute	Netconns	.results[].ingress_time	55773	User-configurable. Updatable.
.results[].regmod_count	Indicator.Attribute	Regmods	.results[].ingress_time	610	User-configurable. Updatable.
.results[].process_name	Related.Indicator	File Path	.results[].ingress_time	c:\windows\system32\svchost.exe	User-configurable.
.results[].process_hash	Related.Indicator	MD5/SHA-256	.results[].ingress_time	145dcf6706eeea5b066885ee17964c09	User-configurable.

FEED DATA PATH	THREATQ ENTITY	THREATQ OBJECT TYPE OR ATTRIBUTE KEY	PUBLISHED DATE	EXAMPLES	NOTES
.results[].process_username	Related.Indicator	Username	.results[].ingress_time	NT AUTHORITY\NETWORK SERVICE	User-configurable.

VMware Carbon Black EDR - Export Indicators

The Export Indicators action exports a collection of indicators. It first searches for a report with the given name on the VMware Carbon Black platform. If a report is found, it then updates the report's information and IOCs with the collection. If no report is found, it will create a new report with the information provided and the threat collection.

Request to Search for Report

`GET https://{{user_fields.hostname}}/threathunter/feedsearch/v1/orgs/{{user_fields.org_key}}/search`

Query Parameters:

```
{
  "query": "title:\"ThreatQ_Report\""
}
```

Sample Response:

```
{
  "took": 12,
  "timed_out": false,
  "hits": {
    "total": 1,
    "max_score": null,
    "hits": [
      {
        "_index": "report_index-2018.11.17-1",
        "_type": "_doc",
        "_id": "M4nggaRoWmJnsKwoHs7w",
        "_score": null,
        "_source": {
          "severity": 8,
          "access": "private",
          "iocs": [
            {
              "field": "process_name",
              "values": [
                "root.exe"
              ],
              "link": "https://my.threatq.online/indicators/130/details",
              "match_type": "equality",
              "id": "threatq_130"
            }
          ],
          "link": null,
          "description": "Test",
          "title": "ThreatQ_Report",
```

```
          "tags": null,
          "source_label": "Custom",
          "id": "M4nggaRoWmJnsKwoHs7w",
          "timestamp": 1741786964,
          "feed": {
            "feed_category": null,
            "feed_summary": null,
            "feed_id": null,
            "feed_name": null,
            "feed_provider_url": null
          },
          "telemetry": {
            "global_hit_rate_1d": 0,
            "global_hit_rate_1w": 0
          }
        },
        "sort": [
          "M4nggaRoWmJnsKwoHs7w"
        ]
      }
    ]
  },
  "facets": {}
}
```


Request to Create/Update a New Report

`POST https://{{user_fields.hostname}}/threathunter/watchlistmgr/v3/orgs/{{user_fields.org_key}}/reports`

`PUT https://{{user_fields.hostname}}/threathunter/watchlistmgr/v3/orgs/{{user_fields.org_key}}/reports/{{report_id}}`

Request Body:


```
{
  "title": "ThreatQ_Report",
  "severity": 8,
  "description": "Test",
  "timestamp": 1741787157,
  "iocs_v2": [
    {
      "field": "process_name",
      "id": "threatq_130",
      "link": "https://crinela.sandbox.threatq.online/indicators/130/details",
      "match_type": "equality",
      "values": [
        "root.exe"
      ]
    }
```

```
  ]
}
```

VMware Carbon Black EDR - Override Reputation

The Override Reputation action creates a new reputation override for indicators of type SHA-256, Filename and File Path.

The indicators of type File Path and Filename must contain valid paths to applications. Filename is included because sometimes it is populated with valid paths. If an indicator already has a reputation override, then its properties are updated.

The action is also able to delete a reputation override if it already exists.

> The API allows adding SHA-256 only to Black List. File paths can be added to Black List or White List.

Request to Create/Update the Reputation for an Indicator of Type SHA-256

```
POST https://{{user_fields.hostname}}/appservices/v6/orgs/
{{user_fields.org_key}}/reputations/overrides
```

Sample Request Body:

```
{
  "override_list": "BLACK_LIST",
  "override_type": "SHA256",
  "sha256_hash":
"4b322cd349f647ab5f84766cb2f2176bac77f0b8d64c2a59b91a6d30c4072315"
}
```

Sample Response:

```
{
  "id": "5391cdcff5d811efaf2eb11d241b9f6d",
  "created_by": "NG4IXXXXXX",
  "create_time": "2025-02-28T13:31:33.558Z",
  "override_list": "BLACK_LIST",
  "override_type": "SHA256",
  "description": "ThreatQ integration",
  "source": "APP",
  "source_ref": null,
  "sha256_hash":
"4b322cd349f647ab5f84766cb2f2176bac77f0b8d64c2a59b91a6d30c4072315",
  "filename": null
}
```

Request to Create/Update Filename/File Path Reputation

The following details a request to create or update the reputation of a Filename or File Path type indicator.

```
POST https://{{user_fields.hostname}}/appservices/v6/orgs/
{{user_fields.org_key}}/reputations/overrides
```

Sample Request Body:

```
{
  "override_list": "WHITE_LIST",
  "override_type": "IT_TOOL",
  "path": "/var/logtemo",
  "include_child_processes": false
}
```

Sample Response:

```
{
    "id": "35b9a9aef5cf11efb9b96f9c5168538a",
    "created_by": "NG4IXXXXXX",
    "create_time": "2025-02-28T12:26:18.017Z",
    "override_list": "WHITE_LIST",
    "override_type": "IT_TOOL",
    "description": "Threatq integration",
    "source": "APP",
    "source_ref": null,
    "path": "/var/logtemo",
    "include_child_processes": false
}
```

Request to Search for Existing Reputation

The following details a request to search for an existing reputation.

```
POST https://{{user_fields.hostname}}/appservices/v6/orgs/
{{user_fields.org_key}}/reputations/overrides/_search
```

Sample Request Body:

```
{
  "query": "4b322cd349f647ab5f84766cb2f2176bac77f0b8d64c2a59b91a6d30c4072315"
}
```

Sample Response:

```
{
  "results": [
    {
      "id": "5391cdcff5d811efaf2eb11d241b9f6d",
      "created_by": "NG4IXXXXXX",
      "create_time": "2025-02-28T13:31:33.558Z",
```

```
      "override_list": "BLACK_LIST",
      "override_type": "SHA256",
      "description": "ThreatQ integration",
      "source": "APP",
      "source_ref": null,
      "sha256_hash":
"4b322cd349f647ab5f84766cb2f2176bac77f0b8d64c2a59b91a6d30c4072315",
      "filename": null
    }
  ]
}
```

Request to Delete Existing Reputation

The following endpoint is used to delete an existing reputation.

```
DELETE https://{{user_fields.hostname}}/appservices/v6/orgs/
{{user_fields.org_key}}/reputations/overrides/{reputation_id}
```

VMware Carbon Black EDR - Manage XDR Network Data Collection

The Manage XDR Network Data Collection action adds or removes a collection of indicators to/from VMWare Carbon Black XDR Network Data Collection at organization level. On manual runs if the option Clear XDR Network Data Collection On Manual Run is enabled then the existing IP addresses from XDR Network Data Collection are removed before adding the ones from the ThreatQ Collection.

There is no default mapping for this action because no data is ingested. The following sections detail how the requests are made.

Request to Get the Existing IP Addresses in the XDR Network Data Collection

```
GET https://{{user_fields.hostname}}/policyservice/v1/orgs/
{{user_fields.org_key}}/rule_configs/data_collection
```

Sample Response:

```
{
  "results": [
    {
      "id": "cc075469-8d1e-4056-84b6-0e6f437c4010",
      "name": "XDR",
      "description": "Turns on XDR network data collection at the sensor",
      "inherited_from": "",
      "category": "data_collection",
      "parameters": {
        "ids_approved_list": [
          {
            "ip_address": "1.1.1.2",
            "note": "Exported from ThreatQ"
          },
          {
            "ip_address": "2001:db8:3333:4444:5555:6666:7777:8888"
          },
          {
            "ip_address": "5.15.134.0/24"
          }
        ]
      }
    }
  ]
}
```

For user configuration **Action** set to `Add To Organization Level XDR Network Data Collection` the values from `.results[].parameters.ids_approved_list[] for results[].name` equals `XDR` are concatenated with the IP addresses from the input ThreatQ collection and uploaded to VMWare Carbon Black.

For user configuration **Action** set to `Remove From Organization Level XDR Network Data Collection` the values from `.results[].parameters.ids_approved_list[] for results[].name` equals `XDR` that are not present in input ThreatQ collection are uploaded back to VMWare Carbon Black.

Request to Upload Indicators to XDR Network Data Collection

`PUT https://{{user_fields.hostname}}/policyservice/v1/orgs/{{user_fields.org_key}}/rule_configs/data_collection`

Request Body:

```
[
  {
    "id": "cc075469-8d1e-4056-84b6-0e6f437c4010",
    "parameters": {
      "ids_approved_list": [
        {
          "ip_address": "1.1.1.3",
          "note": "Exported from ThreatQ"
        }
      ]
    }
  }
]
```

Sample Response:

```
{
  "successful": [
    {
      "id": "cc075469-8d1e-4056-84b6-0e6f437c4010",
      "name": "XDR",
      "description": "Turns on XDR network data collection at the sensor",
      "inherited_from": "",
      "category": "data_collection"
    }
  ],
  "failed": []
}
```

Enriched Data

Object counts and action runtime are supplied as generalities only - objects returned by a provider can differ based on credential configurations and action runtime may vary based on system resources and load.

VMware Carbon Black EDR - Process Enrichment

METRIC	RESULT
Run Time	1 minute
Exploit Target	7
Exploit Target Attributes	15
Events	189
Event Attributes	1,344
Indicators	1

Known Issues / Limitations

- The VMWare Carbon Black Report can contain a maxim of 1000 indicators..

Change Log

- **Version 1.2.0**
  - Renamed the **VMware Carbon Black EDR - File Hash Enrichment** action to **VMware Carbon Black EDR - Process Enrichment**.
  - Added the following new configuration parameters to the **VMware Carbon Black EDR - Process Enrichment** action:
    - **Max Results** - enter the maximum number of results to return per indicator.
    - **Attribute Filter** - select the pieces of context you want ingested into ThreatQ when a record is found.
    - **Related Object Filter** - select the related objects you want ingested into ThreatQ when a record is found.
  - Improved how indicators are exported by the **VMware Carbon Black EDR - Export Indicators** action.
  - Added the following new configuration parameters to the **VMware Carbon Black EDR - Export Indicators** action:
    - **ThreatQ URL** - Enter the URL to your ThreatQ instance. This is used to create a link to the ThreatQ indicator.
    - **Clear Report IOCs on Manual Run** - Enabling this parameter will automatically clear the existing IOCs in the report on manual runs before exporting new indicators to it.
  - Added a new action:
    - **VMware Carbon Black EDR - Manage XDR Network Data Collection** - adds approved IP addresses to XDR Network Data Collection at the organization level.
- **Version 1.1.0**
  - Added the following configuration parameters to all actions:
    - **Enable SSL Certificate Verification** - enable or disable verification of the server's SSL certificate.
    - **Disable Proxies** - determine if the action should honor proxy settings set in the ThreatQ UI.
  - Added a new action:
    - **VMware Carbon Black EDR - Override Reputation** - override the reputation for banned applications using a SHA-256 hash or path to a known IT tool application.
- **Version 1.0.0 rev-a**
  - Guide Update - updated introduction chapter.
- **Version 1.0.0**
  - Initial release