

**TC Group-IB TI application (v1.2)
for
ThreatConnect TIP**

Content

Overview	3
Installation	4
Configuration	6
Step 1. Add new Job	6
Step 2. Collections configuration	8
Usage	10
Data filtering	13
Troubleshooting	16
Common errors	16
Download logs	16
Common errors solution	17
ThreatConnect server can't reach Group-IB Threat Intelligence portal.	17
ThreatConnect token expired or wasn't created.	18
Group-IB token expired or wasn't created.	18
Group-IB account settings are not properly configured.	19
Group-IB account collections access do not match to collections, chosen in the application.	20
Client blocks incoming data from Group-IB portal	20

TC Group-IB TI v1.2 application for ThreatConnect TIP

Overview

The integration allows receiving feeds from the **Group-IB Threat Intelligence** and transforming them into the **ThreatConnect Groups** and **Indicators objects**. These objects use extra **Attribute Types**, which should be uploaded via **attributes.json** file manually at **Gear** → **Org Settings** → **Attribute Types** or will be uploaded automatically if your system allows to see listed **ThreatConnect market** apps.

Current application type - **Job App**. The **ThreatConnect Platform** provides the ability for customers to schedule applications as jobs, specifically known as **Job Apps**, that can be run at configured intervals.

URLs & IP-addresses for access list

For correct API workflow, each client must add the following addresses to their internal security access list:

1. URLs

- tap.group-ib.com/api (for API access)
- tap.group-ib.com (for web-portal access)
- sso.group-ib.com (required for interface access)
- servicedesk.group-ib.com (required for interface access)
- matrix.group-ib.com (required for interface access)
- vulnerability.group-ib.com (required for interface access)

2. IP-addresses

- 162.55.218.201
- 162.55.215.75
- 162.55.211.31
- 88.99.105.142
- 94.130.70.148
- 88.99.167.51
- 148.251.221.108

Installation

The installation process assumes that you have access to the [Group-IB TI](#) portal integrations section where you can find the **ThreatConnect** tab with download link or at least you are able to see the public [ThreatConnect GitHub](#) repository. There you need to download the application TCX archive and install it in the ThreatConnect system. The **ThreatConnect API token** is also required for further configuration steps.

NOTE: Application upload via the **ThreatConnect API token** is also available.

1. Download the appropriate version of the integration at [Group-IB TI Help Center](#) → **Integrations** → **Custom and native integrations** → find **ThreatConnect** in the tab and download integration.
2. Open **ThreatConnect** web interface and login as administrator.
3. Click the **Gear** icon in the upper right corner of the window → **Org Settings**. In the **Membership** window click **Create API User**.

Group-IB - Organization Settings

Membership | Communities/Sources | Groups | Invitations | Variables | Metrics | Settings | Email | Apps | Styling

Create API User | Create TAXII User | Create Read Only User

1 more API user can be created.

1 more TAXII user can be created.

Account	Name	Organization Role	Status	Last Login	Password Expires	User Group	Options
604140	API	Organization Administrator	OK				
		Organization Administrator	OK	02-19-2024 10:23 GMT	24 days		

4. Go to **Gear** → **Org Settings** → **Apps** tab → **Install App**.
5. Browse application TCX file (*TC_GroupIB_TI_*.tcx*) and click **Install**.
6. Extract TCX file (*TC_GroupIB_TI_*.tcx*). The TCX extension is the same as the ZIP archive. And find **attributes.json** file in the app folder. This file is required for implementing the next step.

7. Go to **Gear** → **Org Settings** → **Attribute Types** and click **Upload**. Select **attributes.json** file and click **Save**. New attributes will be added to the list.

Group-IB - Organization Config

Attribute Types | Attribute Validation Rules | Attribute Preferences | Indicator Exclusions | Potential Associations Exclusions | Security Labels | Deprecation Rules

☐ Include System Types + NEW UPLOAD Attribute Type

Name	Description	Max Length	Types	Error Message	Options
GIB Account	User account ID	200 characters	Address Campaign Report Threat Url	Max length is 200 symbols.	
GIB Card CVV	Card CVV code	200 characters	Report	Max length is 200 symbols.	
GIB Card Number	Card number	200 characters	Report	Max length is 200 symbols.	
GIB Card System	Card system	200 characters	Report	Max length is 200 symbols.	
GIB IM Chat Description	IM Chat Description	5K	Report	Max length is 5000 symbols.	
GIB IM Chat ID	IM Chat ID	200 characters	Report	Max length is 200 symbols.	
GIB IM Chat Message	IM Chat Message	5K	Report	Max length is 5000 symbols.	
GIB IM Chat Name	IM Chat Name	5K	Report	Max length is 5000 symbols.	

8. Make sure you have the correct credentials for the app to connect **Group-IB TI API** (TI Username and TI API token). Check the Group-IB [Starting Guide](#) for more info.

9. After installation successfully completes you will see the “**Group-IB Threat Intelligence (vx.x.x)**” app at **Gear** → **Org Settings** → **Apps** tab → **Add Job** menu → **Run Program** dropdown.

Add Job

1 Program | 2 Parameters | 3 Schedule | 4 Output

Job Name *

Run Program

Accenture DeepSight (2.0.3)

FS-ISAC Import (1.0.4)

Group-IB Threat Intelligence (vx.x.x)

Group-IB Threat Intelligence (vx.x.x)

HTTP Feed Scraper (1.0.12)

IBM QRadar (3.0.0)

My Profile
Org Settings
Org Config
Help
Logout

Metrics | Settings | Email | **Apps** | Styling

Clear

Start Time	Last Execution	Next Execution	Active	
02-16-2024 08:47 GMT	Completed	Off	<input type="checkbox"/>	
02-16-2024 11:20 GMT	Completed	Off	<input type="checkbox"/>	
02-16-2024 09:52 GMT	Completed	Off	<input type="checkbox"/>	

10. Create a new Job for the app in the **Add job** window (you'll find instructions below).

Configuration

The configuration process includes several steps. The first step is to create a **Job App** based on the integration app. The second step concerns configuring collections. Each collection is a set of data that contains different information for each type of attack. You can find a more detailed description at our [Group-IB TI Portal](#).

Before you begin

To ensure that **TC Group-IB TI** application is installed without errors, check that you use only the supported versions of **ThreatConnect Platform** software.

General information

The **TC GroupIB TI** application is based on requests to the **Group-IB TI Portal API**, gathering data and uploading it to the **ThreatConnect Platform**. Requests gather information from different collections, which are listed in **Job App** configuration steps. Each collection has **Initial date** and **Sequence update number** parameters.

Step 1. Add new Job

1. Go to **Gear** → **Org Settings** → **Apps tab** → **Add Job** menu → **Run Program** dropdown. Enter the Job name and select the app **Group-IB Threat Intelligence (vx.x.x)**. Click **Next**.

Start Time	Last Execution	Next Execution	Active
02-16-2024 08:47 GMT	Completed	Off	<input type="checkbox"/>
02-16-2024 11:20 GMT	Completed	Off	<input type="checkbox"/>
02-16-2024 09:52 GMT	Completed	Off	<input type="checkbox"/>
02-16-2024 13:21 GMT	Completed	Off	<input type="checkbox"/>
02-16-2024 13:58 GMT	Completed	Off	<input type="checkbox"/>
02-16-2024 08:20 GMT	Completed	Off	<input type="checkbox"/>

2. Fill in **ThreatConnect API User**, **ThreatConnect Owner** and **Group-IB** credentials (**Group-IB Login**, **Group-IB API Key**) in the Parameters tab.

3. Enable required collections and set the **Initial date** of data collection. Click **Next**.

Add Job

1 Program 2 Parameters 3 Schedule 4 Output

Api User * Pavel API

ThreatConnect Owner * Group-IB

Logging Level * Info

GIB API URL * <https://tap.group-ib.com/api/v2/>

GIB Login * p.reshetnikov@group-ib.com

GIB API Key *

☒ Nation-State :: Reports

Initial date 2024-02-12

Sequence update number None

☒ Nation-State :: Actors

Initial date 2024-02-12

Sequence update number None

Start Time	Last Execution	Next Execution	Active	
02-16-2024 08:47 GMT	Completed	Off	<input type="checkbox"/>	
02-16-2024 11:20 GMT	Completed	Off	<input type="checkbox"/>	
02-16-2024 09:52 GMT	Completed	Off	<input type="checkbox"/>	
02-16-2024 13:21 GMT	Completed	Off	<input type="checkbox"/>	
02-16-2024 13:58 GMT	Completed	Off	<input type="checkbox"/>	
02-16-2024 08:20 GMT	Completed	Off	<input type="checkbox"/>	
02-15-2024 12:20 GMT	Completed	Off	<input type="checkbox"/>	
02-16-2024 12:30 GMT	Completed	Off	<input type="checkbox"/>	

4. Configure the Schedule tab with the daily option and click **Next**.
5. Configure the Output tab and click **Save**.
6. **Activate** created Job to set scheduled run in the background or run it once to check.

Step 2. Collections configuration

All listed collections can be enabled and run as one separate Job or can be configured as one Job for each collection. This option is available as API requests 1-second limit applies only to one collection, but can run in separate thread.

The screenshot displays the ThreatConnect 'Add Job' interface. On the left, a sidebar shows the configuration steps: 1. Program, 2. Parameters (active), 3. Schedule, and 4. Output. Under 'Parameters', several collections are listed with checkboxes and input fields for 'Initial date' and 'Sequence update number':

- ☒ Nation-State :: Reports
 - Initial date: 2024-02-12
 - Sequence update number: None
- ☒ Nation-State :: Actors
 - Initial date: 2024-02-12
 - Sequence update number: None
- ☒ Attacks :: DDoS
 - Initial date: 2024-02-12
 - Sequence update number: None
- ☒ Attacks :: Deface
 - Initial date: 2024-02-12
 - Sequence update number: None
- ☐ Attacks :: Phishing
 - Initial date: 2024-02-12
 - Sequence update number: None
- ☐ Attacks :: Phishing Kit
 - Initial date:

At the bottom of the sidebar are buttons: CANCEL, PREVIOUS, and NEXT.

On the right, a table lists existing jobs with columns: Start Time, Last Execution, Next Execution, and Active. Each row includes a toggle switch and action icons (refresh, edit, delete).

Start Time	Last Execution	Next Execution	Active
02-16-2024 08:47 GMT	Completed	Off	<input checked="" type="checkbox"/>
02-16-2024 11:20 GMT	Completed	Off	<input checked="" type="checkbox"/>
02-16-2024 09:52 GMT	Completed	Off	<input checked="" type="checkbox"/>
02-16-2024 13:21 GMT	Completed	Off	<input checked="" type="checkbox"/>
02-16-2024 13:58 GMT	Completed	Off	<input checked="" type="checkbox"/>
02-16-2024 08:20 GMT	Completed	Off	<input checked="" type="checkbox"/>
02-15-2024 12:20 GMT	Completed	Off	<input checked="" type="checkbox"/>
02-16-2024 12:30 GMT	Completed	Off	<input checked="" type="checkbox"/>
02-16-2024 10:47 GMT	Failed	Off	<input checked="" type="checkbox"/>
02-16-2024 10:26 GMT	Completed	Off	<input checked="" type="checkbox"/>
02-16-2024 13:30 GMT	Completed	Off	<input checked="" type="checkbox"/>
02-19-2024 11:20 GMT	Completed	Off	<input checked="" type="checkbox"/>

Here in the example on the screenshot how you can mark collections you need, to get data from **Threat Intelligence**. Gathered data will be transferred to the **ThreatConnect Groups** and **Indicators objects** and uploaded to the system. Mark the required collection using the checkbox. After finishing the configuration process, click "Next" and finish a Job creation.

- **Initial date** – the “starting point” of the collection data download process. When the download process starts this date will be ignored and iteration over collection data will be based on “Sequence update number”. So if you need to change this date and get a fresh download process you need to set “Sequence update number” to “None”.
- **Sequence update number** – Each row in our database has its own unique sequence update number. So, we can get all the events one by one, using the iteration. This number helps to fix the “end point” of data for the last day. And continue iteration on the next day with new data.

NOTE: Please, be careful with the choice of data storage in TIP, as some collections can grow up quickly (especially Attacks :: DDOS, Compromised :: Bank Cards / Masked Cards and Suspicious IP group collections).

NOTE: The “Sequence update number” accepts values “None”, “0” or microseconds (“17083410361167”). One of these values is required. An empty “Sequence update number” field will raise an error.

Initial date value is primarily informative for you, because after a while you can see which date you set earlier. After completing the configuration process and clicking “Save”, the data pull process starts.

It gets the last “Sequence update number” on the date you selected and starts downloading data in limited portions.

Each time portion is gathered by the application - a new “Sequence update number” is stored and used for the next portion. When the download process stops the last “Sequence update number” will be used the next day, not **Initial date** value. In other words, if you need to change **Initial date** value, follow these steps:

- Set a new Initial date.
- Set Sequence update number to “None”
- Save changes.
- Run the Job.

NOTE: Collection IOC :: Common – is specially created to get only IoC and has no extra attribution. Contains information from the following collections: [APT :: Threat, APT :: Threat Actor, HI :: Threat, HI :: Threat Actor, Malware :: C2]. It is possible to find correlations between collections but this is not the case. The main idea of IOC :: Common collection is to use it for firewall rules.

Usage

All downloaded feeds from **Group-IB Threat Intelligence** are stored **Groups** and **Indicators**. To get access to this information you should click the **Browse** tab on the top panel → select **Indicators** or **Groups**. Data table with additional information will be opened.

Type	Summary	Tags	Owner	Threat Rating	ThreatAssess	Obs	F/P	Added	Modified
Address	119.91.194.71	1	Group-IB	5				2024...	2024-0...
Address	123.60.168.69	1	Group-IB	5	281			2024...	2024-0...
Address	192.121.87.187	1	Group-IB	5				2024...	2024-0...
Address	213.183.56.95	1	Group-IB	5				2024...	2024-0...
Address	45.138.157.90	1	Group-IB	5				2024...	2024-0...
Address	45.142.212.34	1	Group-IB	5	503			2024...	2024-0...
Address	45.144.311.00	1	Group-IB	5				2024...	2024-0...
Address	45.150.64.111	1	Group-IB	5				2024...	2024-0...
Address	51.255.19.177	1	Group-IB	5				2024...	2024-0...
Host	03o7yt10888.buzz	1	Group-IB	5				2024...	2024-0...

Select any row in the data table to expand the overview tab.

In the **Overview** tab you will see the following data:

- Security label
- First seen
- Date added
- Last modified
- Description
- Attributes
- etc.

ThreatConnect

Dashboard Workflow Posts Graph ATT&CK Reporting Playbooks Browse Spaces Create Import

Browse / APT29 - New indicators have been found

Revert to Legacy View + Create Custom Report Visual Analysis

APT29 - New indicators have been found Campaign Group | Organization: Group-IB

Follow Item Notification Priority

Intel Rating: 0

Overview Associations 2 Activity

Overview Collapse All Expand All

Details

Security Labels No security labels Date Added 2024-02-19 11:20:42 GMT by Pavel API

First Seen None specified Last Modified 2024-02-19 11:20:42 GMT

Description

This report is published automatically.

During daily monitoring of malicious infrastructure by the Group-IB Threat Intelligence detected the following indicators:

hosts (1)files (3)

The disclosed indicators with medium/medium-high confidence belong to the APT29. The indicators have already been used or will be used in future attacks.

Source description:

Open threats - information obtained from public sources.

Detected network indicators:

In the **Associations** tab you'll find all the data, related to the chosen indicator. It includes the following blocks:

- TQL Queries
- Groups
- Indicators
- etc.

ThreatConnect

Dashboard Workflow Posts Graph ATT&CK Reporting Playbooks Browse Spaces Create Import

Browse / Lazarus - New indicators have been found

Revert to Legacy View + Create Custom Report Visual Analysis

Lazarus - New indicators have been found Campaign Group | Organization: Group-IB

Follow Item Notification Priority

Intel Rating: 0

Overview Associations 21 Activity

Associations Collapse All Expand All

TQL Queries

Name Type Status

No queries to display.

Groups 1

Search group name/summary ...

Type Name/Summary Tags Last Modified Date Added

Threat Lazarus 1 2024-02-19 2024-02-19

Indicators 20

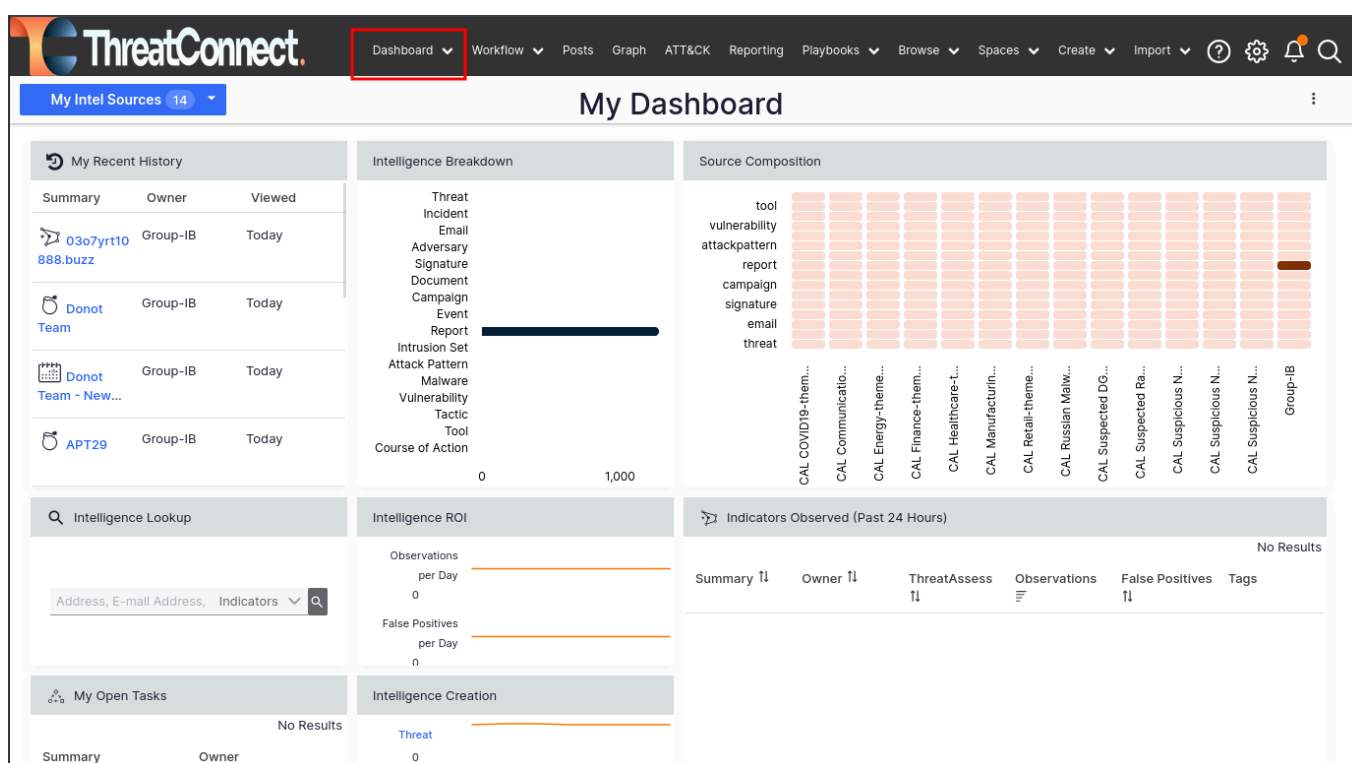
Search indicator name/summary ...

Type Name/Summary Threat Rating Tags Last Modified Date Added

Host akamaitechcloudservices.com 1 2024-02-19 2024-02-19

Total data information can be found at the **Dashboard** tab on the top panel. Here you can see widgets with plots and diagrams about each event. The following widgets are available:

- My Recent History
- Intelligence Breakdown
- Source Composition
- Intelligence Lookup
- Intelligence ROI
- Indicators Observed (Past 24 Hours)
- My Open Tasks
- Intelligence Creation



You can customize your dashboard and different widgets for your needs.

Data filtering

All data received from a particular collection is marked with special tags. The table below displays the mapping of **Group-IB collections** into **Groups** and **Indicators** presented in **ThreatConnect Platform**.

Collection	TC data type	Tag
Nation-State :: Reports	Campaign	APT/Threat
	Threat	APT/Threat Actor
	File	APT/Threat
	URL	APT/Threat
	Address	APT/Threat
	Host	APT/Threat
Nation-State :: Actors	Threat	APT/Threat Actor
Attacks :: DDoS	Incident	Attacks/DDOS
	Address	Attacks/DDOS, CNC, DDOS
Attacks :: Deface	Report	Attacks/Deface
Attacks :: Phishing	Incident	Attacks/Phishing
	URL	Attacks/Phishing
Attacks :: Phishing Kit	Incident	Attacks/Phishing Kit
	URL	Attacks/Phishing Kit
	E-mail	Attacks/Phishing Kit
Compromised Data :: Shops	Report	Compromised Data/Shop
	URL	Compromised Data/Shop
	Address	Compromised Data/Shop
Compromised Data :: Accounts	Report	Compromised Data/Account
	URL	Compromised Data/Account, CNC
	Address	Compromised Data/Account, CNC
Compromised Data :: Bank Cards	Report	Compromised Data/Bank Card
Compromised Data :: Masked Cards	Report	Compromised Data/Masked Card
IM :: Discord	Report	Compromised Data/Discord
IM :: Telegram	Report	Compromised Data/Telegram
Compromised Data :: IMEI	Report	Compromised Data/IMEI

Collection	TC data type	Tag
	URL	Compromised Data/IMEI, CNC
	Address	Compromised Data/IMEI, CNC
Compromised Data :: Mules	Report	Compromised Data/Mules
	URL	Compromised Data/Mules, CNC
	Address	Compromised Data/Mules, CNC
Open Threats	Campaign	HI/Open Threats
	File	HI/Open Threats
	URL	HI/Open Threats
	Address	HI/Open Threats
	Host	HI/Open Threats
	E-mail	HI/Open Threats
Cybercriminals :: Reports	Campaign	HI/Threat
	Threat	HI/Threat Actor
	File	HI/Threat
	URL	HI/Threat
	Address	HI/Threat
	Host	HI/Threat
Cybercriminals :: Actors	Threat	HI/Threat Actor
IOC :: Common	Report	IoC/Common
	File	IoC/Common
	URL	IoC/Common
	Address	IoC/Common
Malware :: C2		
	URL	Malware/CNC, CNC
	Address	Malware/CNC, CNC
	Host	Malware/CNC, CNC
Malware :: Configs	Incident	Malware Config
	File	Malware, Malware Config
Malware :: Report	Report	Malware Report
Malware :: Signature	Signature	Suricata, Signature
Malware :: Yara rule	Signature	YARA, Signature



Collection	TC data type	Tag
Compromised Data :: Git Leaks	Incident	OSI/Git Leak
Compromised Data :: Public Leak	Incident	OSI/Public Leak
OSI :: Vulnerability	Incident	OSI/Vulnerability
Suspicious IP :: Open Proxy	Address	Open Proxy
Suspicious IP :: Scanners	Address	Scanner
Suspicious IP :: Socks Proxy	Address	Socks Proxy
Suspicious IP :: Tor Node	Address	Tor Node
Suspicious IP :: VPN	Address	VPN

Troubleshooting

First of all, as you begin the troubleshooting process, we kindly ask you to familiarize yourself with the common errors that occur when using our application. If errors occur outside of common cases, we will need more details for this purpose. To get to know what happened with the application on your side we need to gather information about your system, time when the error occurred and application logs. If you encounter any problems, please, follow the instructions below.

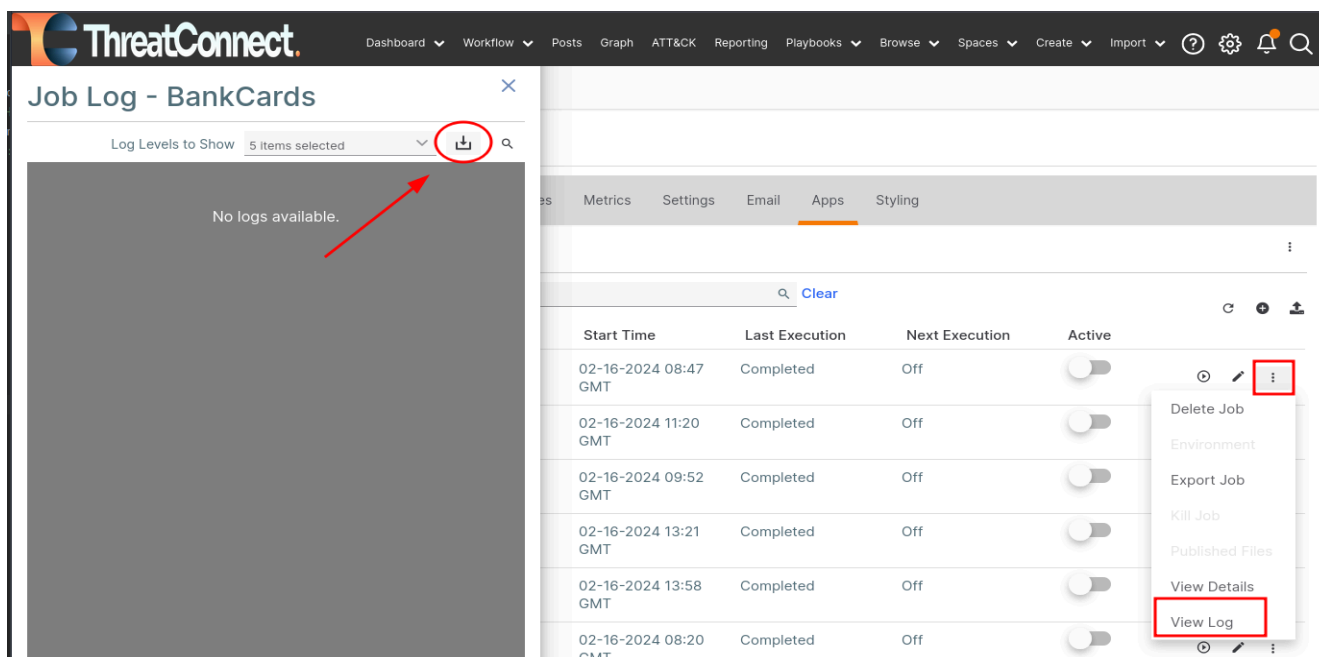
Common errors

To find detailed information about each of the common errors, please check the section **Common errors solution**.

1. **ThreatConnect** server can't reach **Group-IB Threat Intelligence** portal.
2. **ThreatConnect** token expired or wasn't created.
3. **Group-IB** token expired or wasn't created.
4. **Group-IB** account settings are not properly configured (IP addresses are not added to access list).
5. **Group-IB** account collections access do not match to collections, chosen in the application.
6. Client blocks incoming data from **Group-IB** portal (Client didn't add necessary Threat Intelligence IP addresses to his access list).

Download logs

Downloading logs is the most important thing in troubleshooting. To get logs of the app you should **expand settings of the failed Job** → select **View Log** → **press download button**.



The screenshot displays the ThreatConnect interface. The top navigation bar includes links for Dashboard, Workflow, Posts, Graph, ATT&CK, Reporting, Playbooks, Browse, Spaces, Create, Import, and a search icon. The main content area is titled 'Job Log - BankCards'. Below the title, there is a search bar and a dropdown menu for 'Log Levels to Show' with '5 items selected'. A red arrow points to a download icon (a square with a downward arrow) located in the top right corner of the log area. The log area itself is currently empty, displaying 'No logs available.' Below this, there is a table of job executions. The table has columns for Start Time, Last Execution, Next Execution, and Active. A dropdown menu is open for one of the jobs, showing options: Delete Job, Environment, Export Job, Kill Job, Published Files, View Details, and View Log. The 'View Log' option is highlighted with a red box.

Start Time	Last Execution	Next Execution	Active
02-16-2024 08:47 GMT	Completed	Off	<input type="checkbox"/>
02-16-2024 11:20 GMT	Completed	Off	<input type="checkbox"/>
02-16-2024 09:52 GMT	Completed	Off	<input type="checkbox"/>
02-16-2024 13:21 GMT	Completed	Off	<input type="checkbox"/>
02-16-2024 13:58 GMT	Completed	Off	<input type="checkbox"/>
02-16-2024 08:20 GMT	Completed	Off	<input type="checkbox"/>

Common errors solution

All necessary instructions can be found at the [Integration manual page](#).

ThreatConnect server can't reach Group-IB Threat Intelligence portal.

Execute the command below in the terminal, using your **Group-IB** username and **Group-IB** token credentials instead of LOGIN and API_KEY words.

```
curl 'https://tap.group-ib.com/api/v2/sequence_list' -u 'LOGIN:API_KEY' -H 'Accept: */*' -v
```

If your **Group-IB** and proxy credentials are correct, please attach output to [Email](#) or [Service Desk](#) ticket, we will check your **Group-IB** profile.

NOTE: If you have a proxy with authentication, add flag `--proxy` with relevant proxy configurations `--proxy '<protocol>://<user>:<password>@<IP address>:<port>'`.







If you have a proxy without authentication, add flag `--proxy` with relevant proxy configurations `--proxy '<protocol>://<IP address>:<port>'`

For example, command can look as:

```
curl --proxy https://127.0.0.1:3128 'https://tap.group-ib.com/api/v2/sequence_list' -u  
'mr.demo@group-ib.com:wYM2gZ4Tc' -H 'Accept: */*' -v
```

ThreatConnect token expired or wasn't created.

Please make sure that your ThreatConnect token is active and ready to use. For that purpose check it at **Gear** → **Org Settings** → **Membership tab**. Make sure that the API token exists and has not expired.

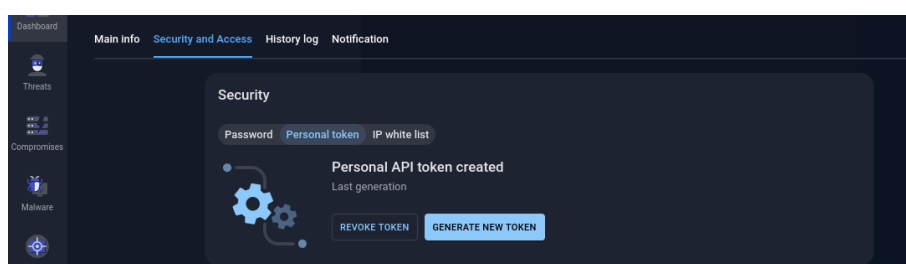
		Standard User	Password Expired		Expired
		Organization Administrator	OK	02-19-2024 14:36 GMT	23 days
		Organization Administrator	OK	12-18-2023 20:05 GMT	Expired

Group-IB token expired or wasn't created.

Please make sure that your **Group-IB** token is active and ready to use. For that purpose check your account settings at [Group-IB portal](#).

- Click the username in the upper-right corner and then go to the **Profile** tab.
- Go to the **Security and Access** tab → **Personal token**.
- Click **Generate token** if you don't have one or **Generate new token** if it is required.
- Click **Save** to submit changes.

Open your application **API** profile and insert a new **Group-IB** token in the form. Also make sure you have a **ThreatConnect API** token. **API** profile update form requires both of them.

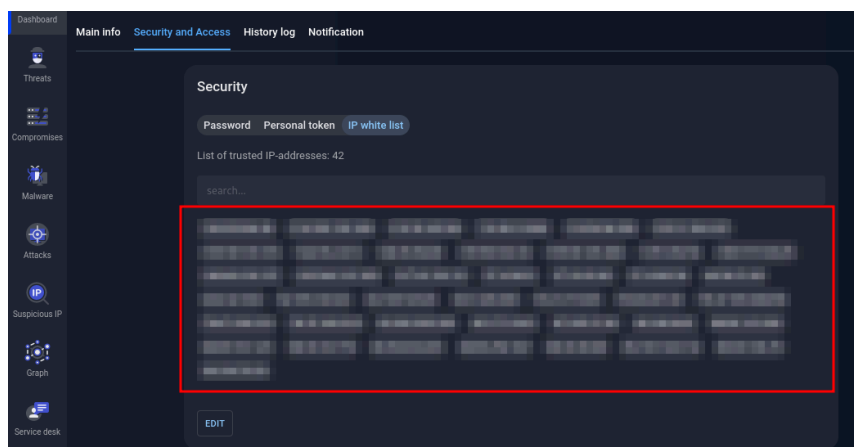


Group-IB account settings are not properly configured.

Please make sure that your **Group-IB** account settings are properly configured. For that purpose check your account settings at [Group-IB portal](#).

- Click the username in the upper-right corner and then go to the **Profile** tab.
- Go to the **Security and Access** tab → **IP white list**.

Please make sure that all your public IPs are listed in the box below. If something is missing - please, inform us via [Email](#) or [Service Desk](#) ticket. We will try to solve this issue promptly.



Group-IB account collections access do not match to collections, chosen in the application.

Please make sure that your **Group-IB** collection settings match and you didn't overselect them. For that purpose please compare the application collections settings and collections listed at your account settings at [Group-IB portal](#).

- Click the username in the upper-right corner and then go to the **Profile** tab.
- Go to the **Security and Access** tab.

Compare collections.

The left screenshot shows the 'Edit Job' page in ThreatConnect. It has a progress bar with four steps: 1. Program, 2. Parameters, 3. Schedule, and 4. Output. The 'Parameters' step is currently selected. Below the progress bar, there are several sections for configuring the job, each with an 'Initial date' and 'Sequence update number' field. The sections are: Nation-State :: Actors, Attacks :: DDoS, Attacks :: Deface, Attacks :: Phishing, and Attacks :: Phishing Kit. Each section has a checkbox to enable it and a 'None' option for the sequence update number.

The right screenshot shows the 'Security and Access' page. It has tabs for 'Main info', 'Security and Access', 'History log', and 'Notification'. The 'Security and Access' tab is selected. Under the 'Security' section, there are tabs for 'Password', 'Personal token', and 'IP white list'. The 'Personal token' tab is selected, showing a 'Personal API token created' message and a 'Last generation' timestamp. There are buttons for 'REVOKE TOKEN' and 'GENERATE NEW TOKEN'. Below this, the 'Access to' section shows a table of access permissions. The table has columns for 'Section' and 'Subsection'. The 'Compromised & Leaks' section is highlighted with a red box, showing a list of subsections: Accounts, Bank cards, Masked cards, IMEI, Mules, Public leaks, Git leaks, Breached DB, and Shops.

Client blocks incoming data from Group-IB portal

Please make sure that **URLs** and **IPs** listed in section **Overview** are added to the access list on your side.

Preventing and investigating cybercrime since 2003

intelligence@group-ib.com
integration@group-ib.com
[+65 3159-3798](tel:+6531593798)

www.group-ib.com
blog.group-ib.com