



# ThreatConnect® Release Notes

Software Version 7.7

September 18, 2024



ThreatConnect® is a registered trademark, and CAL™ is a trademark, of ThreatConnect, Inc.

OpenSearch® is a registered trademark of Amazon Web Services.

Docker® is a registered trademark of Docker, Inc.

MITRE ATT&CK® and ATT&CK® are registered trademarks of The MITRE Corporation.

Java® is a registered trademark of Oracle Corporation.

Postgres® is a registered trademark of PostgreSQL Community Association of Canada.

Quad9® is a registered trademark of Quad9 Foundation.

Redis® is a registered trademark of Redis Ltd.

SAP HANA® is a registered trademark of SAP SE.



# Table of Contents

---

<b>New Features and Functionality</b>	<b>6</b>
Enhanced Search Version 2	6
Enhanced Match Insights	6
“Matched On” Filtering Option	8
Actionable Context Menu	9
Options for Indicators	10
Options for Groups	10
Options for Cases	11
Options for Tags	11
Options for Victims	11
Reporting: Customize Group and Case Templates	12
Configuring Custom Placeholder Blocks in a Report Template	12
Details	13
Attributes	14
Group and Indicator Associations	15
Victim Assets Associations	17
Creating a Report From a Customized Template	18
Unified View: Indicator Details Drawer	19
Intelligence Requirements Filters	22
Date Added and Last Modified Filters for IR Results	22
Basic Browse Screen Filters for Intelligence Requirements	24
Threat Graph: Add Associations	26
<b>Improvements</b>	<b>26</b>
Threat Intelligence	27
Browse and Details	27
Reporting	28
Search	28
Threat Graph	29
MITRE ATT&CK	30
User Administration	30
System Settings	30
UI/UX	31
API & Under the Hood	31



<b>Bug Fixes</b>	<b>32</b>
Search	32
Threat Intelligence	32
Threat Graph	32
Owner Administration	32
API & Under the Hood	32
<b>Dependencies &amp; Library Changes</b>	<b>33</b>
<b>Maintenance Releases Changelog</b>	<b>34</b>
2025-01-14 7.7.3-M0114R [Latest]	34
Bug Fixes	34
2024-12-17 7.7.3-M1217R	34
Bug Fixes	34
2024-12-12 7.7.3	34
Improvements	34
Bug Fixes	34
2024-11-14 7.7.2	35
Improvements	35
Bug Fixes	35
2024-10-25 7.7.1-M1025R	36
Bug Fixes	36
2024-10-16 7.7.1	36
Improvements	36
Bug Fixes	36
2024-09-26 7.7.0-M0926R	37
Bug Fixes	37
<b>CAL Updates</b>	<b>38</b>
2024-10-02 CAL 3.9 [Latest]	38
NEW! Polarity ThreatConnect CAL Integration	38
What's New?	38
Supported Indicator Types:	38
CAL Indicator Analytics	38
CAL Indicator Enrichments	39
Feature Update: CAL Safelist	39
Feature Update: NAICS Industry Classification in the CAL Automated Threat Library Source	39
Feature Update: ATL Source - Google Threat Analysis Group	40



Improvements

40



# New Features and Functionality

## Enhanced Search Version 2

ThreatConnect 7.7 brings thoughtful improvements to the Enhanced Search functionality we introduced in ThreatConnect 7.6, providing you with a more intuitive and powerful tool for navigating your security data. This update refines your user experience by offering detailed match insights, a new filtering option, and the ability to take action on your search results directly from the **Search** screen. With these improvements, you can efficiently understand and operationalize your search results.

### Enhanced Match Insights

In ThreatConnect 7.7, the Search feature not only detects the presence of keywords in the intelligence in your owners, but also lets you know when the keywords were found in multiple places within a piece of intelligence and highlights all the specific locations within each object where the keywords were found.

Just as in ThreatConnect 7.6, when you perform a keyword search, the **Matched On** column in the results table displays the data type on which the query matched, such as the object's Name/Summary, an Attribute, or a Tag, giving you a clear understanding of how the object matched the search term. ThreatConnect 7.7 adds **Multiple Properties** to the possible values in the **Matched On** column so that you can easily identify objects that matched the search term in multiple places.



Search BETA

Q APT30  Exact Match Any object type   1 - 50 of 89

Matched On	Type	Name/Summary	Owner	ThreatAssess	Date Added	Last Modified
<a href="#">Name/Summary</a>	Tag Tag	APT30	Mandiant Threat Intel Source			...
<a href="#">Name/Summary</a>	Intrusion Set Group	APT30	Mandiant Threat Intel Source		2021-11-05 13:08:36 GMT	2021-11-12 11:26:48 GMT
<b>Multiple Properties</b>	Intrusion Set Group	APT30	MITRE ATT&CK Source		2022-05-10 12:11:26 GMT	2022-05-10 12:11:26 GMT
<a href="#">Name/Summary</a>	Adversary Group	APT30	ISIGHT - FireEye ISIGHT Cyber ... Source		2021-09-28 16:20:54 GMT	2021-09-28 16:20:54 GMT
<b>Multiple Properties</b>	Intrusion Set Group	APT30	ACME Organization		2022-04-21 14:16:06 GMT	2022-04-21 14:16:06 GMT
<a href="#">Name/Summary</a>	Intrusion Set Group	APT30	Mandiant Advantage Threat Int... Source		2022-11-04 20:34:58 GMT	2022-11-04 20:34:58 GMT
<a href="#">Name/Summary</a>	Tag Tag	APT30	Mandiant Advantage Threat Int... Source			...
<b>Multiple Properties</b>	Report Group	16-00005408: APT30 Threat Group Profile	Mandiant Advantage Threat Int... Source		2022-11-04 20:34:58 GMT	2022-11-04 20:34:58 GMT

1 - 50 of 89   50

The **Matched On** column displays **Multiple Properties** when a keyword matches in more than one place

If you need more information on where a search term has matched within an object, you can click the link in the **Matched On** column or the icon next to it to display a **Result Details** drawer highlighting each area that contains the match. This feature provides a comprehensive view of each of your search results, enhancing your understanding of the context surrounding the search term's occurrence.



### Result Details ✕

Intrusion Set Group | [APT30](#) ↗

---

Name/Summary	Type	Owner
<a href="#">APT30</a>	🔗 Intrusion Set	MITRE ATT&CK

**Attribute Type**    Description

Security Labels    🔒 No security labels

Value

[\[ APT30 \]](#)(<https://attack.mitre.org/groups/G0013>) is a threat group suspected to be associated with the Chinese government. While [\[ Naikon \]](#)(<https://attack.mitre.org/groups/G0019>) shares some characteristics with [\[ APT30 \]](#) (<https://attack.mitre.org/groups/G0013>), the two groups do not appear to be exact matches.(Citation: FireEye [APT30](#) ) (Citation: Baumgartner Golovkin Naikon 2015)

---

**Attribute Type**    External References

Security Labels    🔒 No security labels

Value

[apt30](https://www2.fireeye.com/rs/fireeye/images/rpt-<a href=).pdf">https://www2.fireeye.com/rs/fireeye/images/rpt-[apt30](#).pdf

---

**Attribute Type**    Source

Security Labels    🔒 No security labels

Value

####Entry URL \*<https://attack.mitre.org/groups/G0013>\* ####Citation \*mitre-attack\* \*[APT30](#)\* \*FireEye [APT30](#)\* \*Baumgartner Golovkin Naikon 2015\* \*<https://attack.mitre.org/groups/G0013>\* \*[APT30](#)]

The **Result Details** drawer highlights the areas in an object that matched your search term

## “Matched On” Filtering Option

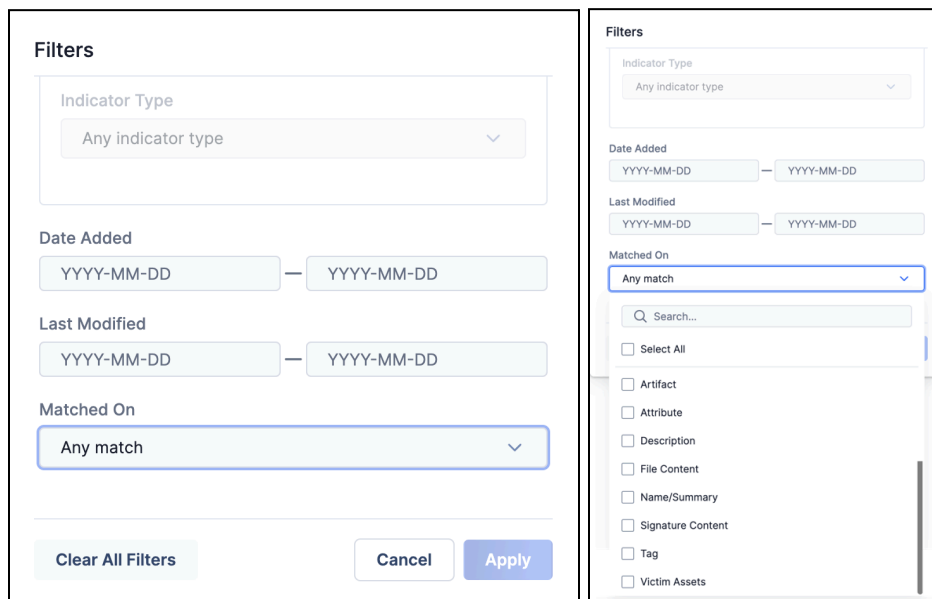
The ability to filter search results has been expanded significantly in this release. You can now filter your search results by selecting specific field types from the **Matched On** filter. For instance, if you select **Artifacts** from the filter, the results table will exclusively display entries for which the search term has matched the names of Artifacts associated with Workflow Cases in your Organization.

To use the filter, open the **Filters** ⌵ menu at the upper right of the **Search** screen, scroll to the bottom, click the **Matched On** dropdown, and choose the field(s) to which you want to






narrow your search results. Once you have made your selections, click **Apply** to update the results table.



*Filter search results to specific fields in the **Matched On** column*

This new filtering option empowers you to drill down into your data with greater precision, making it easier to find exactly what you need.

## Actionable Context Menu

Finally, we have introduced a quick-access context menu that enables you to perform relevant actions on objects directly from the search results table. Each object type has a slightly different context menu, which you can open by clicking **Options**  at the end of a result's row.



**Search** BETA

Q APT30  Exact Match Any object type  1 - 50 of 89

Matched On	Type	Name/Summary	Owner	ThreatAssess	Date Added	Last Modified
Name/Summary	Tag Tag	APT30	Mandiant Threat Intel Source			...
Name/Summary	Intrusion Set Group	APT30	Mandiant Threat Intel Source		2021-11-05 13:08:36 GMT	2021-11-12 11:26:48 GMT ...
Multiple Properties	Intrusion Set Group	APT30	MITRE ATT&CK Source		2022 12:11	Create Custom Report > View Details
Name/Summary	Adversary Group	APT30	iSIGHT - FireEye iSIGHT Cyber ... Source		2021-16:20	View Match Details
Multiple Properties	Intrusion Set Group	APT30	ACME Organization		2022 14:16	Visual Analysis > Delete...
Name/Summary	Intrusion Set Group	APT30	Mandiant Advantage Threat Int... Source		2022 20:34:58 GMT	20:34:58 GMT ...

1 - 50 of 89 50

Perform actions and view more details on a search result directly from the new context menu

## Options for Indicators

- **Add to Exclusion List:** Organization Administrators can add the Indicator to their [Organization-level Indicator Exclusion List](#).
- **Change Status to Inactive** or **Change Status to Active:** If your user account has the requisite permissions in the Indicator's owner, you can change the [status of the Indicator](#).
- **Explore in Graph:** Visualize, explore, and analyze the Indicator's associations in [Threat Graph](#).
- **View Details:** View the Indicator's [Details drawer](#).
- **View Match Details:** View the fields in the Indicator object on which your search term matched.
- **Delete:** If your user account has the requisite permissions in the Indicator's owner, you can delete the Indicator from the owner.

## Options for Groups

- **Create Custom Report:** Create a report for the Group [from scratch](#) or [from a Group report template](#).
- **View Details:** View the Group's [Details drawer](#).
- **View Match Details:** View the fields in the Group object on which your search term matched.
- **Visual Analysis:** Select from the following options:



- **Explore in Graph:** Visualize, explore, and analyze the Group's associations in [Threat Graph](#).
- **Visualize ATT&CK:** Open the [ATT&CK Visualizer](#) with the Group added as an analysis layer within a new ATT&CK® view.
- **Delete:** If your user account has the requisite permissions in the Group's owner, you can delete the Group from the owner.

## Options for Cases

- **Create Custom Report:** Create a report for the Case [from scratch](#) or [from a Case report template](#).
- **Explore in Graph:** Visualize, explore, and analyze the Case's associations in [Threat Graph](#).
- **View Details:** View the Case's [Details drawer](#).
- **View Match Details:** View the fields in the Case object on which your search term matched.
- **Delete:** If your user account has the requisite permissions in your Organization, you can delete the Case from the Organization.

## Options for Tags

- **Explore in Graph:** Visualize, explore, and analyze the Tag's associations in [Threat Graph](#).
- **View Details:** View the Tag's [Details drawer](#).
- **View Match Details:** View the fields in the Tag object on which your search term matched.
- **Delete:** If your user account has the requisite permissions in the Tag's owner, you can delete the Tag from the owner.

## Options for Victims

- **View Details:** View the Victim's [Details drawer](#).
- **View Match Details:** View the fields in the Victim object on which your search term matched.
- **Delete:** If your user account has the requisite permissions in the Victim's owner, you can delete the Victim from the owner.



# Reporting: Customize Group and Case Templates

ThreatConnect 7.7 introduces custom placeholder blocks, which provide the ability to preset Group and Case report templates with selected details, Attributes of selected Attribute Types, and advanced filters for Group, Indicator, and (for Group report templates only) Victim Asset associations. This new feature empowers you to efficiently generate detailed and customized reports that meet your organization's specific needs.

## Configuring Custom Placeholder Blocks in a Report Template

Custom placeholder blocks are available in the following **Group Data Placeholder** and **Case Data Placeholder** sections when creating a Group or Case report template in the **Template Editor**:

- **Details**
- **Attributes**
- **Group Associations**
- **Indicator Associations**
- **Victim Assets Association** (Group report templates only)

When [creating](#) or editing a Group or Case report template, click **+ Add Section** at the upper right to open the **Add Section** drawer. Then click **+** for one of the sections in the foregoing list. You will be provided with two options: **Placeholder Block** and **Custom Placeholder Block**.



< Add Details ×

Placeholder Block ⓘ  Custom Placeholder Block ⓘ

---

Section Preview

Placeholder  
Group Data - Details

---

Keep panel open after adding

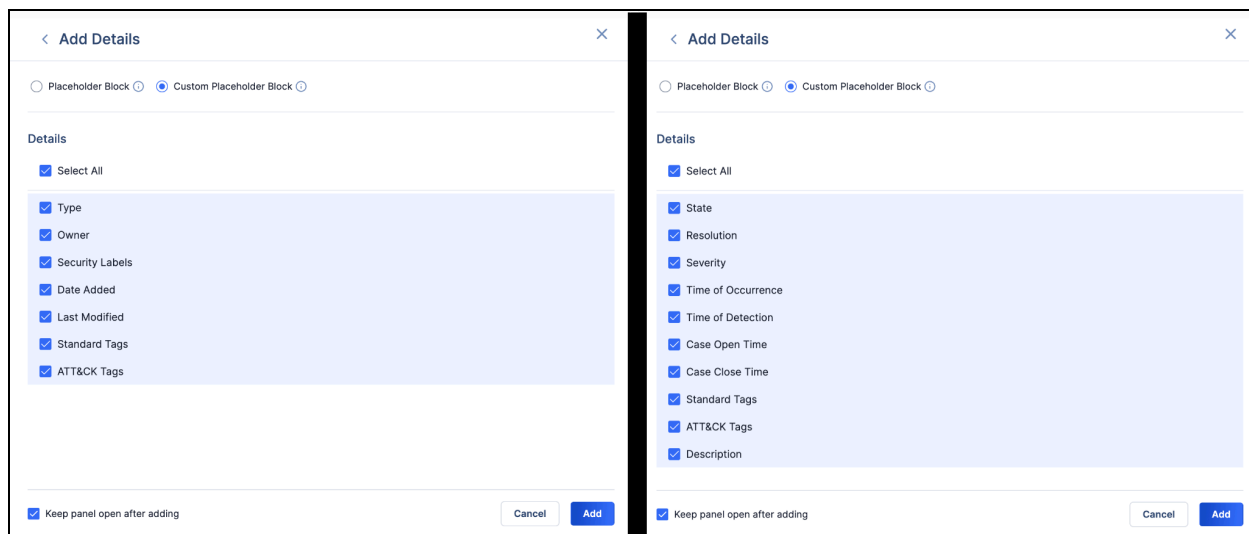
*Add a placeholder block or custom placeholder block to a report template*

Select **Custom Placeholder Block**, and then configure the placeholder block to include only the information that you want a report using the template to display, as described next for each type of section.

## Details

For Group and Case report templates, the **Details** custom placeholder block lets you choose the **Details** data fields to include in a report.

**Tip:** Use the placeholder block when you want to include all **Details** fields for a Group or Case in reports built from the report template. Use the custom placeholder block when you want to display only a subset of **Details** fields for a Group or Case in reports built from the report template.



Choose the **Details** fields to add to a Group (left) or Case (right) custom placeholder block

By default, all **Details** fields are selected. Deselect the fields you don't want, keep the selections for the fields you do want, and click **Add**. A **Custom Placeholder** section for **Details** will be added to the report template. When a user creates a report from the template, a **Details** section displaying only the fields you selected will be included in the report.

## Attributes

For Group and Case report templates, the **Attributes** custom placeholder block lets you choose the Attribute Types you want to include in a report. Each Attribute the Group or Case has of each selected Attribute Type will be displayed in its own section in the report.

**Tip:** Use the placeholder block when you want a user creating a report from the template to select specific Attributes to include in the report. Use the custom placeholder block when you want to display all Attributes of a specific set of Attribute Types for a Group or Case in reports built from the report template.



*Choose the Attribute Types for which to create a custom placeholder block (shown for Group, but almost identical for Case)*

Select the Attribute Types you want to include, and click **Add**. A **Custom Placeholder** section for each Attribute Type will be added to the report template. When a user creates a report from the template, a section for each Attribute the Group or Case has for each selected Attribute Type will be included in the report, without further configuration required from the user.

## Group and Indicator Associations

For Group and Case report templates, the **Group Associations** and **Indicator Associations** custom placeholder blocks let you add filters to display only associated Groups and Indicators, respectively, of the selected types, owners, dates added, and last modified dates, ensuring that reports created from the template include only the most relevant Group and Indicator associations. You can adjust the **Table Settings** to specify which columns to include in the associations table and the maximum number of associations to show. You can



also specify which column the associations table should be sorted by and the sort order (ascending or descending).

**Tip:** Use the placeholder block when you want to display a table containing all associated Groups or Indicators, with all available table columns, for a Group or Case in reports built from the report template. Use the custom placeholder block when you want to filter the associated Groups or Indicators displayed for a Group or Case and to customize the display settings for the associations table in reports built from the report template.

*Configure the filters and table settings for a Group Associations table in a custom placeholder block (identical for Indicator Associations)*

Make your selections, and click **Add**. A **Custom Placeholder** section for Group or Indicator associations will be added to the report template. When a user creates a report from the template, a table displaying the Group's or Case's associated Groups or Indicators, configured to the specifications in the report template, will be included in the report.





## Victim Assets Associations

For Group report templates only, the **Victim Assets Associations** custom placeholder block lets you select the types of associated Victim Assets to display, ensuring that reports created from the template include only the most relevant Victim Asset associations. You can adjust the **Table Settings** to specify which columns to include in the associations table and the maximum number of associations to show. You can also specify which column the associations table should be sorted by and the sort order (ascending or descending).

**Tip:** Use the placeholder block when you want to display a table containing all associated Victim Assets, with all available table columns, for a Group in reports built from the report template. Use the custom placeholder block when you want to filter the associated Victim Assets displayed for a Group and to customize the display settings for the associations table in reports built from the report template.

< Add Victim Assets Associations

Placeholder Block  Custom Placeholder Block

**Filters**

Type  
Choose

**Table Settings**

Table Columns: 4 items selected  
Table Cutoff: 20

Sort By  
Type  
 Ascending  Descending

Keep panel open after adding

Cancel Add

*Configure the filters and table settings for a Victim Assets Associations table in a custom placeholder block (Group report templates only)*

Make your selections, and click **Add**. A **Custom Placeholder** section for Victim Asset associations will be added to the report template. When a user creates a report from the



template, a table displaying the Group's associated Victim Assets, configured to the specifications in the report template, will be included in the report.

## Creating a Report From a Customized Template

After you have saved a Group or Report report template with custom placeholder blocks, you and other users can utilize it to [generate reports for a Group or Case](#), respectively. The custom placeholder blocks in the report will display only the information you have selected and will not require any further configuration. After generating the report, review the contents to ensure they meet your needs. You can edit any section, including those created from custom placeholder blocks, to modify its content, enabling further customization. This flexible approach allows you to create comprehensive and tailored reports efficiently.



## Unified View: Indicator Details Drawer

Over the past several releases, we've added functionality intended to make it easier to find and understand context around Indicators. In ThreatConnect 7.7, we are taking this work a step further and introducing a **Unified View** option on the Indicator **Details** drawer available in various areas of ThreatConnect, including the **Browse** screen and Threat Graph. This new option displays a version of the Indicator **Details** drawer showing information from all of the Indicator's owners to which you have access, enabling you to view critical contextual information without having to visit each version of the Indicator in each of its different owners.

The **Unified View** option is available in the **Owners** dropdown at the top left of the Indicator **Details** drawer. Please keep in mind that this option is available only for Indicators and is a beta feature in this version of ThreatConnect.

**Note:** Your System Administrator must turn on the **multiSourceViewEnabled** system setting for the **Unified View** option to be available on your ThreatConnect instance.



191.101.104.37

Address Indicator | Organization: PM Demo Inc | Active | Status set locally

Unified View  
All Owners

Organization: PM Demo Inc

ThreatAssess & CAL | Source: ThreatConnect Intelligence

CAL 182

281  
0 MEDIUM 1000

ThreatAssess Impact Factors

- Recent False Positive Reported
- Impacted by Recent Observations

Security Labels | No security labels

Confidence Rating | 0 - Unassessed

Threat Rating | Unknown

Date Added | 2024-04-23 12:03:37 GMT

Last Modified | 2024-08-09 14:06:23 GMT

Description | None specified

Source | None specified

CAL™ Classifiers

- DNSHosts.Excessive.Current
- DNSHosts.Malicious.Historical
- DNSHosts.MultipleResolutions
- Rel.URLs.MultipleQueries

Collapse All | Expand All

Tags Across Owners | BETA

GeoLocation Data

Use the **Owners** dropdown to change to the unified view for an Indicator

After you select **Unified View**, the Indicator **Details** drawer will show information about the Indicator from all the owners you have access to in which the Indicator exists. The available data include the earliest date added, which shows when the Indicator was first added to any of the owners, and the most recent “last modified” date, which shows when the Indicator was last modified in any of the owners. In addition, the drawer will display a few select cards: the **Tags Across Owners** card introduced in ThreatConnect 7.6; **Owners & Feeds** (which shows the Indicator’s Threat Rating and Confidence rating in all its owners to which you have access); **Observations, False Positives, & Impressions**; and **Investigation Links**.



www.eloples.com

Host Indicator | Unified View BETA

ThreatAssess & CAL

CAL 173

413  
MEDIUM

0 1000

**ThreatAssess Impact Factors**

- Recent False Positive Reported
- Impacted by Recent Observations

Date Added: 2024-07-18 20:10:07 GMT  
Earliest Source: CAL Automated Threat Library

Last Modified: 2024-08-08 15:01:19 GMT  
Most Recent Source: CAL Automated Threat Library

CAL™ Classifiers

DNSRes.NoResolution

Collapse All Expand All

- Tags Across Owners BETA
- Owners & Feeds
- Observations, False Positives, & Impressions
- Investigation Links

Unified view of an Indicator's **Details** drawer shows its earliest date added and most recent "last modified" date



# Intelligence Requirements Filters

We continue to make incremental improvements and enhancements to our Intelligence Requirement (IR) feature. In this version of ThreatConnect, we introduce additional filtering options on IR results and basic **Browse** screen filters for IRs. IRs look at all available information in an instance, and sometimes that investigation brings historical data to the surface. The new filter options for IR results will help you focus your processing and analysis efforts on items that are most recent. With these new options, you can filter your IR results list by date added and “last modified” date so you can focus on just the things that are in a specific timeframe of interest.

## Date Added and Last Modified Filters for IR Results



On an IR’s **Details** screen, the results table on the **Keyword Tracking & Results** card now displays a new **Date Added** column by default, and you can use the column selector to add a **Last Modified** column as well. These columns are both sortable, allowing you to order your IR results by the date when they were first added or last modified in their owner.

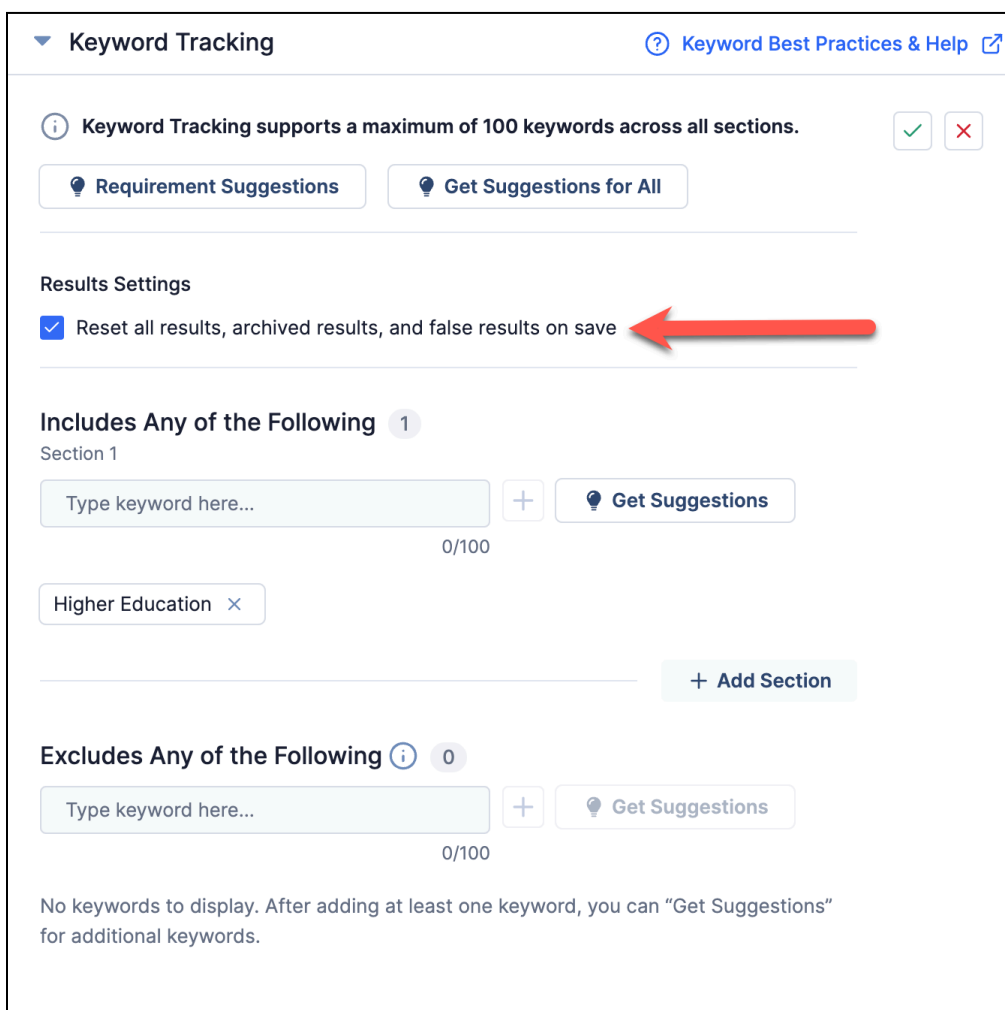
The screenshot displays the 'Results' section of the ThreatConnect interface. At the top, it shows 'Results 241' and a 'Retrieve Results' button. Below this, there are radio buttons for 'Local' (selected) and 'Global'. A search bar is present with a search icon and a filter icon. The main area is a table of IR results. The table has columns for Name, Type, Owner, Date Added, and Matched. A column selector menu is open over the table, showing options to 'Select All', 'Name', 'Type', 'Owner', 'DateAdded', 'LastModified', and 'Matched'. The 'Date Added' and 'Matched' columns are currently selected. The table contains several rows of results, including 'Cybersecurity Pioneer s: Lessons from Virgi...', 'Where Are States Using AI? Survey Says Cy...', 'Book Review: 'Why Cybersecurity Fails in Am...', and 'Amazon Names New Cohort of Government, ...'. Each row shows the title, type (Report Group), owner (CAL Automated Threat Library Source), date added, and matched date.

Name	Type	Owner	Date Added	Matched
Cybersecurity Pioneer s: Lessons from Virgi...	Report Group	CAL Automated Threat Library Source	2024-08-18	2024-08-18
Where Are States Using AI? Survey Says Cy...	Report Group	CAL Automated Threat Library Source	2024-08-17	2024-08-17
Book Review: 'Why Cybersecurity Fails in Am...	Report Group	CAL Automated Threat Library Source	2024-08-11	2024-08-11
Amazon Names New Cohort of Government, ...	Report Group	CAL Automated Threat Library Source		2024-07-26

*View and sort by IR results by date added and “last modified” date*



It is important to note that IRs created in your Organization prior to your ThreatConnect instance's update to 7.7 will not immediately have data populated into the **Date Added** and **Last Modified** columns of their results table. In order to populate these columns for legacy results (i.e., results matched prior to the instance's update to 7.7), expand the **Keyword Tracking** section of the **Keyword Tracking & Results** card, click  at the upper right to edit the card, select the **Reset all results, archived results, and false results on save** checkbox, and then click  at the upper right to save the changes. This will reset the IR's results and populate the two date fields for all legacy results. If you do not want to reset an IR's results, all results generated after the update to 7.7 will have the date fields populated, but the legacy results will not have data in those fields.



**Keyword Tracking** [Keyword Best Practices & Help](#)

**Keyword Tracking supports a maximum of 100 keywords across all sections.**

**Requirement Suggestions** **Get Suggestions for All**

**Results Settings**

**Reset all results, archived results, and false results on save**

**Includes Any of the Following** 1

Section 1

Type keyword here... 0/100 **Get Suggestions**

Higher Education

**+ Add Section**

**Excludes Any of the Following** 0

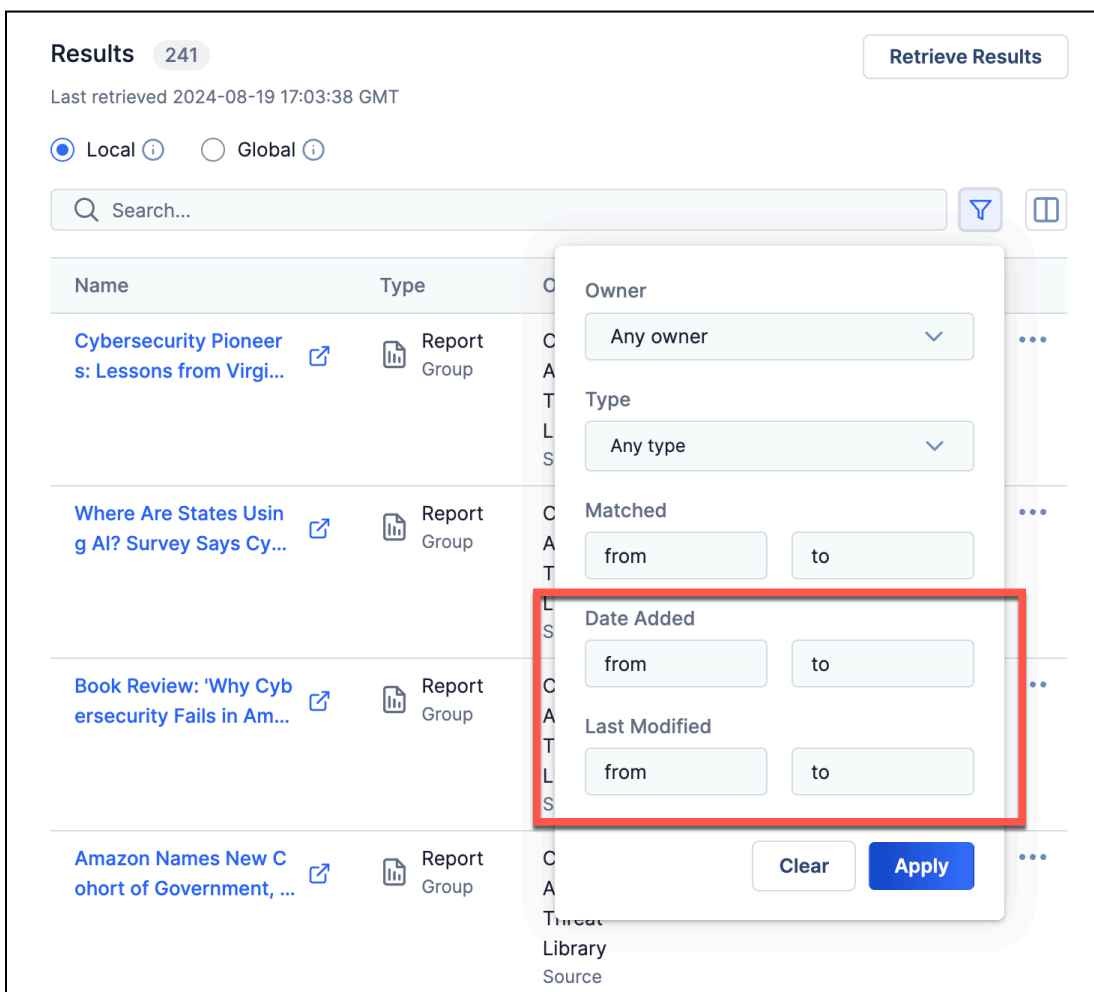
Type keyword here... 0/100 **Get Suggestions**

No keywords to display. After adding at least one keyword, you can "Get Suggestions" for additional keywords.

*Reset your IR's results to populate the **Date Added** and **Last Modified** columns for legacy results*




The filters for **Date Added** and **Last Modified** can be accessed via **Filters**  menu at the upper right of the results table.





*Date Added and Last Modified ranges are now in the Filters dropdown*

## Basic Browse Screen Filters for Intelligence Requirements

While ThreatConnect has historically supported IR filtering by ThreatConnect Query Language (TQL), IRs did not have basic filters available on the **Browse** screen. As of ThreatConnect 7.7, you can now filter IRs in the **Browse** screen UI by subtype, category, date added, and “last modified” date. These options are available in the new **Filters**  menu at the upper right of the table.





Exact Match  

	Category ↑↓			
Requirement (IR)	Category1			
Requirement (IR)				05-
Information (RFI)	CISO Priorities			
Requirement (IR)				07-
Requirement (IR)				10-
Requirement (PIR)				
Information (RFI)			2023-08-30	2023-08-30
			2023-	2023-

### Filters

**Subtype**  
Any subtype

**Category**  
1 Selected

**Date Added**  
2024-01-01 — YYYY-MM-DD

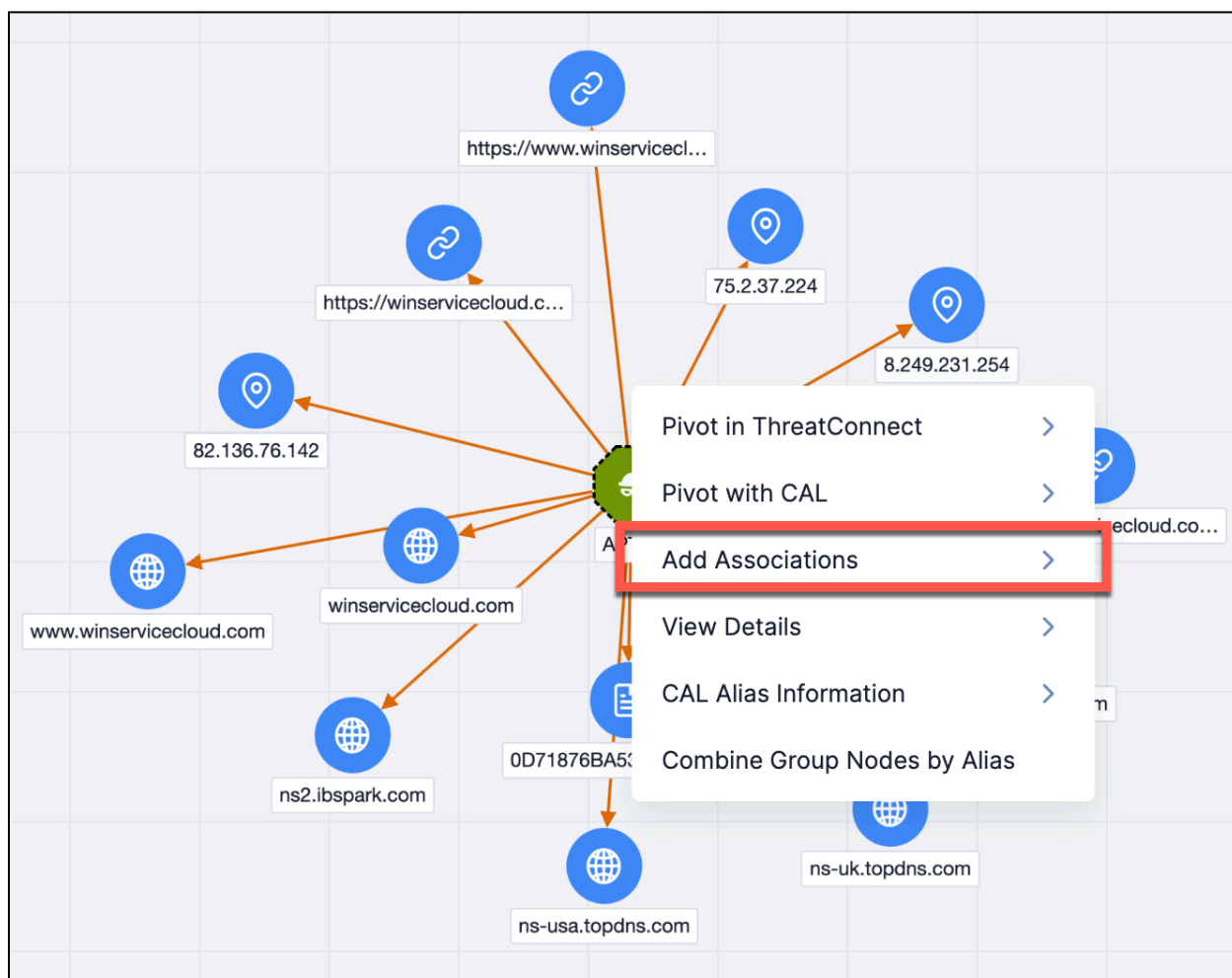
**Last Modified**  
YYYY-MM-DD — YYYY-MM-DD

The **Browse** screen now provides options to filter IRs



## Threat Graph: Add Associations

We've received countless pieces of feedback around the Threat Graph feature since its release a few years ago. In ThreatConnect 7.7, we are pleased to share that, in response to your feedback, we have introduced the ability to add associations directly in the graph. We know many analysts prefer to work in link analysis tools like the ThreatConnect Threat Graph. With this update, you will now be able to build out your work without having to leave the graph. In this version of ThreatConnect, you can add Indicator-to-Group associations, Group-to-Indicator associations, and Group-to-Group associations without leaving the graph. You can also add multiple associations at once, and those associations are reflected not only in Threat Graph, but also on the **Associations** tab of the object's **Details** screen and on the **Associations** card on the object's legacy **Details** screen. We hope this update helps you streamline your research and analysis going forward.



*Add associations to an object directly from Threat Graph*



# Improvements

## Threat Intelligence

- When an Indicator's status is updated by a user or through certain system processes, its **Last Modified** date, as well as the **Last Modified** date of all copies of that Indicator in all owners on the ThreatConnect instance if the **indicatorStatusLock** system setting is turned off, will be updated. This change will be noted on the **Activity** tab of the **Details** screen for each copy of the Indicator, except when the Indicator's status is changed via the v2 Batch API.
- The [TQL Auto Associate feature](#) is now available for IRs, enabling you to assign up to two TQL queries to an IR—one for Groups and one for Indicators. You may access this feature on the **TQL Queries** card on the **Associations** tab of an IR's **Details** screen.

## Browse and Details

- Organization Administrators can now set default custom views for the **Custom View** tab on the **Details** screen—one for Groups and one for Indicators. This is a great option when you want to take the guesswork away from your users and provide them with a view that is ideal for your Organization's needs. When a default custom view has been set, users in the Organization have the option to select it or use a custom view of their own. To set a custom view for your Organization, navigate to the new **Default Custom Views** tab of the **Organization Config** screen and import a **.tccv** file for Indicators or Groups into the corresponding section. You can also delete a custom view from this screen. Alternatively, you can build the view you want on the **Custom View** tab of an object's **Details** screen and then select **Set View as Org Default** from the ... menu on the **Manage View** drawer to set that view as the Organization's custom default view for the object type (Group or Indicator). Once a default custom view has been set for Groups or Indicators, users in the Organization can select the **Enable org default view** checkbox in the **Manage View** drawer from the **Custom View** tab of an object's **Details** screen if they want to use the Organization's default view.
- The **Tags** filter on the **Browse** screen has been updated to a more intuitive and user-friendly design. In addition, you can now search by ATT&CK technique ID when doing a **Basic** search, as well as filter by the date the Tag was last used. When doing an **Advanced** search, there is now a tooltip to the left of the search bar that lets you



know whether your TQL query is valid and provides more information on the errors found in invalid queries.

- Following on the update of the Indicator **Details** drawer in ThreatConnect 7.6, we have updated the Group **Details** drawer in ThreatConnect 7.7. The new format gives you an efficient way to get easy-to-read context on a Group while working in areas of the platform such as Browse, Threat Graph, and Search. As with the Indicator **Details** drawer, the Group **Details** drawer includes cards for features such as UserAction Playbooks, Attributes, associations, and Notes. The updated Group **Details** drawer is available for all Group types except Email, Signature, and Task.
- The new Indicator and Group **Details** drawer now has a pop-out icon next to the object's name that lets you open the object's **Details** screen in a new browser tab.

## Reporting

- When adding a **Group Data** section to a report, you can now select a different Group in the section's configuration instead of having to go back to the **Add Group Data** menu to swap the Group.
- When adding a **Case Data** section for **Details** or **Attributes** to a report, you can now select a different Case in the section's configuration instead of having to go back to the **Add Case Data** menu to swap the Case.
- The format of Attributes in ThreatConnect's reporting feature has been adjusted to provide a more useful and efficient display. The Attribute's **Value** is now on top, followed by **Security Labels** and **Attribute Source** on the next line. The **Date Added** and **Last Modified** fields have been removed.

## Search

- The default view for the ThreatConnect search engine is now set to whichever view you most recently used. If you click **Try Search Beta** from the legacy **Search** drawer, then the new **Search** screen will be your default view the next time you click the magnifying glass at the upper right of the top navigation bar. If you click **Revert to Legacy Search** from the **Search** screen, then the legacy **Search** drawer will be your default view.
- You can now sort the results table on the new **Search** screen by the **Name/Summary** column. Note that the names of some Report Groups in the **CAL Automated Threat Library Source** currently have a space at the beginning of their Name/Summary,



which will cause them to appear to be out of order (i.e., at the top of the list or at the bottom of the list) when the **Name/Summary** column is sorted.

- You can now sort the results table on the new **Search** screen by the **ThreatAssess** column, enabling you to bubble results with the highest or lowest ThreatAssess score to the top of the table.
- On the new **Search** screen, all **Exact Match** searches in your recent search history will be enclosed in double quotes so you can easily identify that you were searching for an exact phrase. If you re-run one of these searches, it does not matter whether you select the **Exact Match** checkbox or not, as the system will no longer surround the search term with an extra set of quotes.
- In addition to **[.]**, **[:]**, and **[@]**, the **Search** screen now recognizes the following defanged character sequences: **[dot]**, **h..p://**, **h..ps://**, and **f.p://**.

## Threat Graph

- A number of design and functionality improvements were made to the Threat Graph feature, including the following:
  - **Graph Objects drawer:** The **Details** table, which displays information about the objects shown in Threat Graph, has been renamed as the **Graph Objects** drawer and it is more intuitive to open, view, and use. You can easily open it by clicking the **View Table** button at the upper right of the **Threat Graph** screen. New features in the redesigned table are pagination, a column selector, separate columns for object type and name, and an options menu in each row for actions such as adding an object to an owner, running a Playbook on the object, and removing the object from the Threat Graph.
  - **Legend:** The icon to open the legend has been moved to the new toolbar at the top left of the Threat Graph. The legend's UI has been updated to match the look and feel of other areas of ThreatConnect. The objects in the legend are now grouped by object type, and there is a search bar, as well as a **Select All** option, at the top.
  - **Layout controls:** The layout controls have been moved to a toolbar at the top left of the Threat Graph, and **Scroll to zoom** is now a toggle on that strip instead of an option under a gear-wheel icon. The **Options** ... menu has moved to the top right of the Threat Graph, and the **Save** option that was previously in that menu is now a separate **Save Graph** button at the top right.
  - **Screen Header:** The name of the Threat Graph you are viewing and a link to the main **Graph** screen (the screen that displays all saved Threat Graphs in



your Organization) are now displayed in the upper left corner of a Threat Graph.

- **Nodes:**
  - Objects that exist in multiple owners now have a dashed border around their node instead of a solid black border.
  - All Group nodes are now the same color, with the Group type differentiated by the icon in the node. Similarly, all Indicator nodes are now the same color, with the Indicator type differentiated by the icon in the node.
  - The arrows that connect nodes have been simplified for a cleaner look and feel.

## MITRE ATT&CK

- The ThreatConnect ATT&CK Visualizer and ATT&CK Tags have been updated to include MITRE ATT&CK® 15.1 data. These updates will be automatically deployed for all ThreatConnect instances, including those that do not have CAL™ turned on.

## User Administration

- Support was added for API tokens with configurable expiration times. The expiration time is defined when creating or editing an API user, with the default and upper limit defined in the **apiUserDefaultTokenExpiration** and **apiUserMaxTokenExpiration** system settings, respectively.
- Accounts Administrators can now create user accounts with a System role of API User in On-Premises and Dedicated Cloud ThreatConnect instances.

## System Settings

- The following new system settings were added:
  - **apiUserDefaultTokenExpiration:** This setting determines the default lifetime, in days, for an API user account token.
  - **apiUserMaxTokenExpiration:** This setting specifies the maximum lifetime, in days, that can be configured for an API user account token.



## UI/UX

- The following changes were made to the ThreatConnect UI to provide a more consistent and comfortable user experience:
  - The tabbed navigation bar for the following screens has been updated to match that of the **System Settings** screen: **Account Settings, Community Config, Community Info, Source Config, Source Info, Org Config, Org Settings, and My Profile.**
  - As part of our efforts to refine the ThreatConnect UI to be more visually friendly and consistent, we have changed the color of many of the clickable buttons in the UI from orange to blue.
  - In the **Dashboard** dropdown on the top navigation bar, the options for importing and creating a dashboard were redesigned.

## API & Under the Hood

- The **threatconnect/app/log** folder is now a Docker® mount, which means the logs will now be local to the host machine. In addition, the **threatconnect-docker.zip** files have been upgraded.
- You can now configure the maximum allocation of memory for your Redis® and OpenSearch® Docker containers.



## Bug Fixes

### Search

- An issue causing extra text to be added to owner hyperlinks in legacy **Search** drawer results was fixed.

### Threat Intelligence

- When copying a Group from one owner to another, ATT&CK Tags on associated Indicators were being copied as standard Tags, creating duplicate Tags on target Indicators that already had those ATT&CK Tags applied to them before the copy operation. In addition, if the Indicators with duplicate Tags were included in a subsequent copy operation, an error would occur. This issue was resolved, and the duplicate standard Tags are automatically removed when an instance is updated to version 7.7 of ThreatConnect.
- **#totalhash** is no longer supported as an Investigation Link.

### Threat Graph

- The **Last Seen** column was removed from the table in the **Graph Objects** drawer (formerly known as the **Details** table) in Threat Graph.

### Owner Administration

- An issue preventing Organizations containing Tags with cross-owner associations from being deleted was fixed.

### API & Under the Hood

- Efficiency improvements were made for ThreatAssess.





# Dependencies & Library Changes

- ThreatConnect is now running Redis 7.2.4.
- ThreatConnect is now running Java® 17.



# Maintenance Releases Changelog

2025-01-14 7.7.3-M0114R [Latest]

## Bug Fixes

- The cache size limitation for Organizations has been removed.

2024-12-17 7.7.3-M1217R

## Bug Fixes

- Fixed an issue causing non-inherited card owner selections on shared dashboards to be reset for all users when a user with a Community role of Banned in one or more of the Communities and Sources selected on the card opens the dashboard.

2024-12-12 7.7.3

## Improvements

- When deleting a user on the **Membership** tab of the **Organization Settings** screen, Organization Administrators are now provided with dropdowns to assign the user's "Run As" Playbooks (i.e., Playbooks assigned to execute under the user's account) to an active user and to assign the user's Jobs to an API user.

## Bug Fixes

- Service directories are now deleted from local storage after their corresponding Services have been deleted.



2024-11-14 7.7.2

## Improvements

- Local storage was expanded to include additional settings.

## Bug Fixes

- Users with a certain custom owner role configuration were unable to select their Organization when adding additional details to a new Indicator association. This issue was corrected.
- An issue preventing custom associations from being made was fixed.
- Deletion of a Group from its new **Details** screen was not being logged on **Activity** tabs for System, Organization, and user activities. This issue was corrected.
- An issue causing no results to be returned for Intelligence Requirements with more than 25 keywords was fixed.
- An issue preventing the creation of an Attribute of a custom Attribute Type that is defined in multiple owners under the same name was fixed.
- Improvements to data sorting on the **Browse** screen and in results returned by the v3 API were made to ensure consistency of results across pagination.
- An issue causing some system settings to reset upon container re-creation or restart was fixed.
- A security improvement was implemented to mask command-line arguments from the OpenSearch reindex app.
- **DB\_SUPER\_USER** is now the user account that initializes Postgres® and administers the ThreatConnect database.
- A script was added for creating a database user who has fewer privileges than **DB\_SUPER\_USER** to run ThreatConnect.
- The default values for **REDIS\_ARGS** and **OPENSEARCH\_JAVA\_OPTS** were updated in **.env.sample**.



## 2024-10-25 7.7.1-M1025R

### Bug Fixes




- An issue preventing the default Description Attribute from being displayed on the **Details** screen for Groups with large numbers of Attributes was fixed.
- An issue causing out-of-memory errors to occur was fixed.

## 2024-10-16 7.7.1

### Improvements

- In order to reduce the memory used by Redis, the API App Service payload is now deleted from Redis after the API response has completed.

### Bug Fixes

- The **Add to Exclusion List** option on an Indicator's **Details** screen, legacy **Details** screen, and **Search** screen results ... menu was adding the Indicator to its owner's exclusion list instead of the exclusion list of the home Organization of the user who selected the option. This issue was fixed.
- The **Add to Exclusion List** option on the legacy **Details** screen was not working for custom Indicators. This issue has been fixed.
- Clicking on certain hyperlinked values in dashboard cards was causing an error to occur. This issue was resolved.
- An issue causing Playbooks with a WebHook Trigger configured to have a timeout value greater than the default value of 5 minutes to return no results was fixed.
- Previously, the **Build as Component**  and **Build as Workflow**  icons at the upper right of the Playbook Designer were available even if no Playbook elements were selected. Clicking one of these icons created a new Playbook Component or Workflow Playbook that contained only the original Playbook's Trigger. Now, these icons are available only after you have used the **Select**  icon to choose the elements you want to include in the new Playbook Component or Workflow Playbook.



2024-09-26 7.7.0-M0926R

## Bug Fixes

- Additional arguments were added to the default value of the **REDIS\_ARGS** Docker environment variable to set **maxmemory-policy** and **maxmemory-samples**.



# CAL Updates

## 2024-10-02 CAL 3.9 [Latest]

### NEW! Polarity ThreatConnect CAL Integration

Now available for [Polarity](#) users at the point of decision and to aid analysts' investigations with automated intelligence, the Polarity ThreatConnect CAL integration provides access to CAL's global intelligence engine, with 267+ billion data points and visibility into 2.2+ billion Indicators worldwide!

#### What's New?

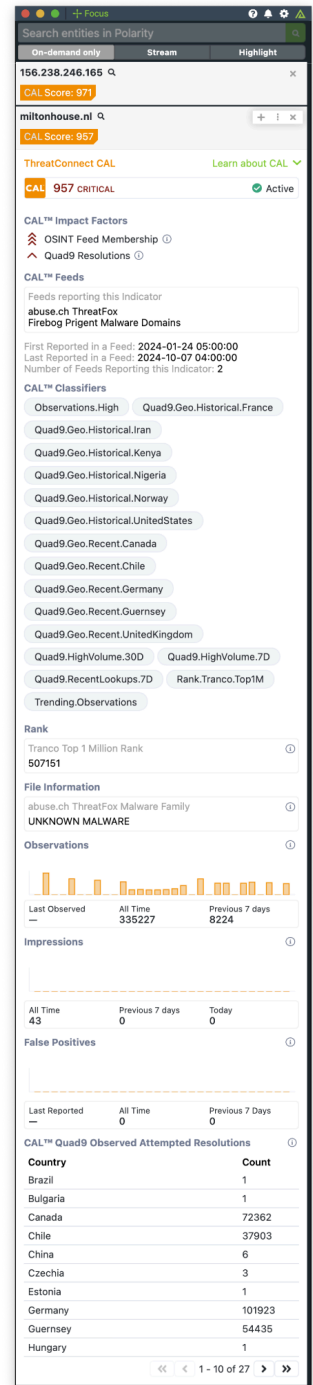
- The Polarity ThreatConnect CAL integration is now available for both ThreatConnect and Polarity customers to access the same useful CAL data in a brand-new way!
- CAL community analytics are growing to include both the ThreatConnect and Polarity user base, enabling CAL to provide more analytics about actively investigated and seen Indicators than ever before!

#### Supported Indicator Types:

- Address
- Email Address
- File
- Host
- URL

#### CAL Indicator Analytics

- [CAL reputation score](#) with 14 impact factors
- [Indicator Status](#)
- 350K+ of the following daily:
  - Community impressions based on engagement
  - Community observations in actual networks





- Community false-positive reports

## CAL Indicator Enrichments

- Indicator visibility in 52 active OSINT feeds and all historical feeds
- Additional OSINT feed enrichment information, including tags, malware families, file information, and more
- SHA1, SHA256, and MD5 file hash information
- [103 CAL Classifiers](#)
- Suspected DGA detection
- Quad9<sup>®</sup> observed and attempted resolutions
- Information from known good sources or CAL Safelist
- IP owner, region, and service

## Feature Update: CAL Safelist

In this release, we've expanded the CAL Safelist to include trusted domains such as cybersecuritynews.com, ubuntu.com, redhat.com, and others. These additions help reduce false positives by ensuring that Indicators from these sources are automatically flagged as benign, streamlining workflows across ThreatConnect and Polarity. This update enhances the accuracy of your threat intelligence, allowing you to focus on real threats, while providing contextual insights and minimizing unnecessary noise in document analysis, Indicator queries, and automated workflows.

## Feature Update: NAICS Industry Classification in the CAL Automated Threat Library Source

In this release, we've updated [CAL's North American Industry Classification System \(NAICS\) AI model](#) to reduce variability in its outputs, providing more consistent and reliable classifications. This improvement enhances the accuracy of how CAL identifies industries, ensuring that the tagging of content using [NAICS codes](#) is more precise. For users, this means a more stable and predictable classification of industry-related data, leading to better filtering and organization of

The screenshot displays the Polarity interface for a specific indicator. At the top, the search bar shows the hash: 7EB70257593DA06F682A3DDA54A9D260D4FC514F645237F5CA74B08F8DA61A6. Below this, the indicator is identified as 'ThreatConnect CAL' with a 'CAL Score: 0'. The status is 'LOW' and 'Inactive'. The page lists 'CAL™ Impact Factors' including OSINT Feed Membership and File Reputation. It also shows 'CAL™ Feeds' reporting the indicator, such as Hybrid Analysis and MalShare Daily Malware List. A section for 'CAL™ Classifiers' includes Executable.Android, Executable.Legacy, Executable.Modern, and Executable.iOS. 'External tags' include Hybrid Analysis Tags and 'text'. 'File Information' details the file name 'is-HI84G.tmp', size '2', and type 'ASCII text; with CRLF line terminators'. 'CAL™ File Hash Information' shows 'Hash Validation' as 'Incomplete' and lists 'Known MD5', 'Known SHA1', and 'Known SHA256' hashes. The 'Source of Triplet' is 'CAL Proprietary'. An 'Observations' chart shows activity over time, and 'Impressions' are listed as 32 for 'All Time', 0 for 'Previous 7 days', and 0 for 'Today'. 'False Positives' are also listed as 0 for all time periods.



intelligence. With this reduced output variability, you can trust the classifications you rely on for decision making, which ultimately improves the efficiency of your workflows, reduces the need for manual adjustments, and enhances the overall quality of intelligence insights.

## Feature Update: ATL Source - Google Threat Analysis Group

### What is changing?

In this release, the **Google Threat Analysis Group blog** content in the [CAL Automated Threat Library \(ATL\) Source](#) is accessed via a link to the original site in the body of the Report object instead of being delivered directly. This format preserves content creators' rights while maintaining access to essential information. All other ATL features, including AI-generated summaries, MITRE ATT&CK tags, NAICS tags, and other contextual information, remain unchanged.

### Why is this changing?

This update ensures compliance with copyright and data ownership requirements while continuing to provide valuable threat intelligence. This change aligns with evolving concerns regarding copyright, data ownership, and the ethical use of AI, ensuring that content creators' intellectual property is respected while maintaining the integrity of the threat intelligence provided.

### Will there be more changes?

This shift in how content is accessed is part of a broader change affecting multiple sources in the CAL ATL. You can expect similar updates for some other sources in future releases, as these changes enable us to respect data ownership without compromising the quality of intelligence. If this change impacts your workflow, please reach out to your Customer Success Manager so that we can assess future changes to this feature.

## Improvements

- Tool tips were updated to reflect that CAL community analytics include both the Polarity and ThreatConnect user bases.
- Service to the open source Haley SSH Bruteforce IPs feed was restored after downtime caused by the owner restricting access and requesting re-verification due to feed abuse.