Threat Intelligence Director

The topics in this chapter describe how to configure and use TID in the Firepower System.

• Threat Intelligence Director Overview, on page 1
• Requirements and Prerequisites for Threat Intelligence Director, on page 4
• How To Set Up Threat Intelligence Director, on page 6
• Analyze TID Incident and Observation Data, on page 14
• View and Change Threat Intelligence Director Configurations, on page 26
• Troubleshoot Threat Intelligence Director, on page 40
• History for Threat Intelligence Director, on page 42

Threat Intelligence Director Overview

The Threat Intelligence Director operationalizes threat intelligence data, helping you aggregate intelligence data, configure defensive actions, and analyze threats in your environment. This feature is intended to supplement other Firepower functionality, offering an additional line of defense against threats.

When configured on your hosting platform, TID ingests data from threat intelligence sources and publishes the data to all configured managed devices (elements.) For more information about the hosting platforms and elements supported in this release, see Platform, Element, and License Requirements, on page 4.

Sources contain indicators, which contain observables. An indicator conveys all of the characteristics associated with a threat, and individual observables represent individual characteristics (e.g. a SHA-256 value) associated with the threat. Simple indicators contain a single observable, and complex indicators contain two or more observables.

Observables and the AND/OR operators between them form an indicator's pattern, as illustrated in the following examples.
After the observables are published to the elements, the elements monitor traffic and report observations to the Firepower Management Center when the system identifies observables in traffic.

The Firepower Management Center collects observations from all elements, evaluates the observations against TID indicators, and generates or updates incidents associated with the observable's parent indicator(s).

An incident is fully realized when an indicator's pattern is fulfilled. An incident is partially realized if traffic matches one or more observables in the indicator but not the entire pattern. For more information, see Observation and Incident Generation, on page 14.

The following diagram shows data flow in a sample Firepower System configuration.

When a TID incident is fully or partially realized, the system takes the configured action (monitor, block, partially block, or no action). For details, see Factors That Affect the Action Taken, on page 21.
TID and Security Intelligence

As part of your access control policy, Security Intelligence uses reputation intelligence to quickly block connections to or from IP addresses, URLs, and domains. Security Intelligence uniquely provides access to industry-leading threat intelligence from Cisco Talos Intelligence Group (Talos). For more information on Security Intelligence, see About Security Intelligence.

TID enhances the system's ability to block connections based on security intelligence from third-party sources as follows:

- **TID supports additional traffic filtering criteria**—Security Intelligence allows you to filter traffic based on IP address, URL, and (if DNS policy is enabled) domain name. TID also supports filtering by these criteria and adds support for filtering on SHA-256 hash values.

- **TID supports additional intelligence ingestion methods**—With both Security Intelligence and TID, you can import threat intelligence into the system by either manually uploading flat files or configuring the system to retrieve flat files from a third-party host. TID provides increased flexibility in managing those flat files. In addition, TID can retrieve and ingest intelligence provided in Structured Threat Information eXpression (STIX™) format.

- **TID provides granular control of filtering actions**—With Security Intelligence, you can specify filtering criteria by network, URL, or DNS object. Security Intelligence objects, especially list and feeds, can contain multiple IP addresses, URLs, or DNS domain names, but you can only block or not block based on entire objects, not based on individual components of an object. With TID, you can configure filtering actions for individual criteria (that is, simple indicators or individual observables).

- **TID configuration changes do not require redeployment**—After you modify Security Intelligence settings in the access control policy, you must redeploy the changed configuration to managed devices. With TID, after initial deployment of the access control policy to the managed devices, you can configure sources, indicators, and observables without redeploying, and the system automatically publishes new TID data to the elements.

For information about what the system does when either Security Intelligence or TID could handle a particular incident, see TID-Firepower Management Center Action Prioritization, on page 22.

Performance Impact of Threat Intelligence Director

**Firepower Management Center**

In some cases, you may notice the following:

- The system may experience minor performance issues while ingesting particularly large STIX sources, and ingestion may take longer than expected to finish.

- The system may take up to 15 minutes to publish new or modified TID data down to elements.

**Managed Device**

There is no exceptional performance impact. TID impacts performance identically to the Firepower Management Center Security Intelligence feature.
Threat Intelligence Director and High Availability Configurations

If you host TID on the active Firepower Management Center in a high availability configuration, the system does not synchronize TID configurations and TID data to the standby Firepower Management Center. We recommend performing regular backups of TID data on your active Firepower Management Center so that you can restore the data after failover.

For details, see About Backing Up and Restoring TID Data, on page 13.

Requirements and Prerequisites for Threat Intelligence Director

Model Support
Any

Supported Domains
Any

User Roles
Admin
Threat Intelligence Director (TID) User

Additional Requirements
The following topics explain additional requirements for using Threat Intelligence Director.

Platform, Element, and License Requirements

Hosting Platforms
You can host TID on physical and virtual Firepower Management Centers:

• running Version 6.2.2 or later of the Firepower System.
• configured with a minimum of 15 GB of memory.
• configured with REST API access enabled. See Enabling REST API Access.

Elements
You can use any Firepower Management Center-managed device as a TID element if the device is running Version 6.2.2 or later of the Firepower System.

Licensing
If you want to configure file policies for SHA-256 observable publishing, the Firepower System requires a Malware license (Classic or Smart).

For more information, see Configure Policies to Support TID, on page 7 and About Firepower Licenses.
Source Requirements

Source Type Requirements:

**STIX**

Files must be STIX Version 1.0, 1.1, 1.1.1, or 1.2 and adhere to the guidelines in the STIX documentation: [http://stixproject.github.io/documentation/suggested-practices/](http://stixproject.github.io/documentation/suggested-practices/).

STIX files can include complex indicators.

**Flat File**

Files must be ASCII text files with one observable value per line.

Flat files include only simple indicators (one observable per indicator.)

Flat files can be up to 500 MB.

TID does **not** support:

- Delimiter characters separating observable values (e.g. `observable`, is invalid).
- Enclosing characters around observable values (e.g. "observable" is invalid).

Each file should contain only one type of content:

- **SHA-256** — SHA-256 hash values.
- **Domain** — domain names as defined in RFC 1035.
- **URL** — URLs as defined in RFC 1738.

---

**Note**

TID normalizes any URLs that contain port, protocol, or authentication information, and uses the normalized version when detecting indicators. For example, TID normalizes any of the following URLs:

- `http://example.com/index.htm`
- `http://example.com:8080/index.htm`
- `example.com:8080/index.htm`
- `example.com/index.htm`

as:

- `example.com/index.htm`

Or, for example, TID normalizes the following URL:

- `http://abc@example.com:8080/index.htm`

as

- `abc@example.com/index.htm/`

- **IPv4** — IPv4 addresses as defined in RFC 791.

TID does not accept CIDR blocks.
**IPv6**— IPv6 addresses as defined in RFC 4291.

TID does not accept prefix lengths.

### How To Set Up Threat Intelligence Director

**Note**
If you encounter an issue during TID configuration or operation, see Troubleshoot Threat Intelligence Director, on page 40.

**Procedure**

**Step 1**  
Ensure that your installation meets the requirements for running TID.  
See Platform, Element, and License Requirements, on page 4

**Step 2**  
For each managed device, configure the policies required to support TID and deploy those policies to the devices.  
See Configure Policies to Support TID, on page 7.  
You can configure elements before or after you ingest intelligence data sources.

**Step 3**  
Configure the intelligence sources that you want TID to ingest.  
See Source Requirements, on page 5 and the topics under Options for Ingesting Data Sources, on page 8.

**Step 4**  
Publish data to the elements if you have not yet done so. See Pause or Publish TID Data at the Source, Indicator, or Observable Level, on page 37.

**What to do next**

- Include TID in your regularly scheduled backups. See About Backing Up and Restoring TID Data, on page 13.
  
  If your Firepower Management Center deployment is a high availability configuration, see also Threat Intelligence Director and High Availability Configurations.

- (Optional) Grant administrative access to TID functionality as desired. See User Roles with TID Access, on page 13 and Firepower System User Management.

- As needed during operation, fine-tune your configuration. For example, add observables that produce false-positive incidents to the Do Not Block list. See View and Change Threat Intelligence Director Configurations, on page 26.
Configure Policies to Support TID

You must configure access control policies to publish TID data from the Firepower Management Center to your managed devices (elements). In addition, we recommend that you configure your access control policies to maximize observation and Firepower Management Center event generation.

For each managed device that you want to support TID, perform the steps below to configure the associated access control policy.

Elements that are configured to use TID after data has been published will automatically receive all currently-published observables.

Procedure

**Step 1** Verify that the **Enable Threat Intelligence Director** check box is checked in **Advanced Settings** of the access control policy. This option is enabled by default.

For more information, see **Access Control Policy Advanced Settings**.

**Step 2** Add rules that allow (rather than trust) connections to the access control policy if they are not already present. TID requires that the access control policy specify at least one rule.

Because TID depends on inspection, ensure that you allow traffic, rather than trust it, because the purpose of trusting traffic is to bypass inspection. For more information, see **Creating a Basic Access Control Policy**.

**Step 3** If you choose **Intrusion Prevention** as the default action for the access control policy and you want to decrypt traffic for TID detection, associate an SSL policy with the access control policy; see **Associating Other Policies with Access Control**.

**Step 4** If you want **SHA-256** observables to generate observations and Firepower Management Center events:

a) Create a file policy containing one or more **Malware Cloud Lookup** or **Block Malware** file rules.

   For more information, see **Configure File Policies**.

b) Associate this file policy with one or more rules in the access control policy.

**Step 5** If you want **IPv4**, **IPv6**, **URL**, or **Domain Name** observations to generate connection and security intelligence events, enable connection and security intelligence logging in the access control policy:

a) In access control rules where you invoked a file policy, enable **Log at End of Connection** and **File Events: Log Files**, if not already enabled.

   For more information, see **Logging Connections with Access Control Rules**.

b) Verify that default logging (**DNS Policy**, **Networks**, and **URLs**) is enabled in your Security Intelligence settings.

   For more information, see **Logging Connections with Security Intelligence**.

**Step 6** Deploy configuration changes; see **Deploy Configuration Changes**.

What to do next

Complete remaining items in **How To Set Up Threat Intelligence Director, on page 6**
Options for Ingesting Data Sources

Choose a configuration option based on the data type and delivery mechanism you want to use.

For more information about these data types, see Source Requirements, on page 5.

**Table 1: Options for Ingesting Data Sources**

<table>
<thead>
<tr>
<th>Data Type</th>
<th>Ingestion Options</th>
</tr>
</thead>
</table>
| STIX      | • Ingest STIX feeds from a TAXII server:  
           | See Fetch TAXII Feeds to Use as Sources, on page 8  
           | • Download STIX data from a URL:  
           | See Fetch Sources from a URL, on page 9  
           | • Upload a STIX file:  
           | See Upload a Local File to Use as a Source, on page 10  |
| Flat file | • Download data from a URL:  
           | See Fetch Sources from a URL, on page 9  
           | • Upload a flat file:  
           | See Upload a Local File to Use as a Source, on page 10  |

Fetch TAXII Feeds to Use as Sources

If you encounter an issue during TID configuration or operation, see Troubleshoot Threat Intelligence Director, on page 40

**Procedure**

1. **Step 1** Make sure your source meets the requirements in Source Requirements, on page 5
2. **Step 2** Choose Intelligence > Sources.
3. **Step 3** Click Add (➕).
4. **Step 4** Choose TAXII as the Delivery method for the source.
5. **Step 5** Enter information.
   - If the host server requires an encrypted connection, configure the SSL Settings as described in Configure TLS/SSL Settings for a TID Source, on page 12.
   - You cannot change the Action selection for TAXII sources.

   *Block* is not an Action option for TAXII sources, as STIX data can contain complex indicators, which the system cannot block. Devices (elements) store and take action based on single observables; they cannot take action based on multiple observables.
However, after ingestion, you can block individual observables and simple indicators obtained from the source. For more information, see Edit TID Actions at the Source, Indicator, or Observable Level, on page 35.

• It may take some time for the list of feeds to load.

• The Update Every interval specifies the frequency that TID retrieves updates from the TAXII source. Set an update frequency that makes sense for how often the data source is updated. For example, if the source is updated 3 times per day, set your update interval to 1440/3 or 480 minutes to regularly capture the latest data.

• After the number of days you specify for TTL, TID deletes:
  • all of the source's indicators that are not included in subsequent source updates.
  • all observables not referenced by a surviving indicator.

Step 6 If you want to immediately begin publishing to elements, confirm that the Publish Slider (●) is enabled. When this option is enabled, the system automatically publishes the initial source data and any subsequent changes.

For details, see Pause or Publish TID Data at the Source, Indicator, or Observable Level, on page 37.

Step 7 Click Save.

What to do next

• TAXII feeds can contain a lot of data, it may take some time for the system to ingest all of the data. To view ingestion status, refresh the Sources page.

• If you see an error for this source, hover over status for details.

• If you are doing initial TID configuration, return to How To Set Up Threat Intelligence Director, on page 6.

Fetch Sources from a URL

Configure a URL source if you want TID to fetch files from a host.

If you encounter an issue during TID configuration or operation, see Troubleshoot Threat Intelligence Director, on page 40

Procedure

Step 1 Make sure your source meets the requirements in Source Requirements, on page 5

Step 2 Choose Intelligence > Sources.

Step 3 Click Add (✚).

Step 4 Choose URL as the Delivery method for the source.

Step 5 Complete the form.
• If you are ingesting a flat file, choose a **Type** that describes the data contained within the source.

• If the host server requires an encrypted connection, configure the **SSL Settings** as described in **Configure TLS/SSL Settings for a TID Source**, on page 12.

• For Name: To simplify sorting and handling of incidents based on TID indicators, use a consistent naming scheme across sources. For example, `<source>-<type>`.

  Including the source name simplifies returning to the source for further information or feedback.

  Be sure to enter the name consistently. For example, for a source with IPv4 addresses, you might always use IPV4 (not IPv4 or ipv4 or IP_v4 or IP_V4 or ip-v4 or IP-v4, IP-V4, etc.)

• If you are ingesting a STIX file, **Block** is not an **Action** option, as STIX data can contain complex indicators, which the system cannot block. Devices (elements) store and take action based on single observables; they cannot take action based on multiple observables.

  However, after ingestion, you can block individual observables and simple indicators obtained from the source. For more information, see **Edit TID Actions at the Source, Indicator, or Observable Level**, on page 35.

• Set an update frequency that makes sense for how often the data source is updated. For example, if the source is updated 3 times per day, set your update interval to 1440/3 or 480 minutes to regularly capture the latest data.

• After the number of days you specify for the **TTL** interval, TID deletes:
  • all of the source's indicators that are not included in subsequent source updates.
  • all observables not referenced by a surviving indicator.

**Step 6**  
If you want to immediately begin publishing to elements, confirm that the **Publish Slider** (○) is enabled.

When this option is enabled, the system automatically publishes the initial source data and any subsequent changes.

For details, see **Pause or Publish TID Data at the Source, Indicator, or Observable Level**, on page 37.

**Step 7**  
Click **Save**.

---

**What to do next**

• To view ingestion status, refresh the Sources page. If you see an error, hover over status for details.

• If you are doing initial TID configuration, return to **How To Set Up Threat Intelligence Director**, on page 6.

---

**Upload a Local File to Use as a Source**

Use this procedure for a one-time manual upload of a local file.

When ingesting a STIX file, TID creates a simple or complex indicator from the contents of the STIX file.

When ingesting a flat file, TID creates a simple indicator for each observable value in the file.
If you encounter an issue during TID configuration or operation, see Troubleshoot Threat Intelligence Director, on page 40

Procedure

Step 1  Make sure your file meets the requirements in Source Requirements, on page 5
Step 2  Choose Intelligence > Sources.
Step 3  Click Add (†).
Step 4  Choose Upload as the Delivery method for the source.
Step 5  Complete the form.
  • If you are uploading a flat file, choose a Type that describes the data contained within the source.
  • For Name: To simplify sorting and handling of incidents based on TID indicators, use a consistent naming scheme across sources. For example, <source>-<type>.
     Including the source name simplifies returning to the source for further information or feedback.
     Be sure to enter the name consistently. For example, for a source with IPv4 addresses, you might always use IPV4 (not IPv4 or ipv4 or IP_v4 or IP_V4 or ip-v4 or IP-v4, IP-V4, etc.)
  • If you are uploading a STIX file, Block is not an Action option, because STIX data can contain complex indicators. Devices (elements) store and take action based on single observables; they cannot take action based on multiple observables.
     However, you can block a simple indicator at the indicator or observable level. For more information, see Edit TID Actions at the Source, Indicator, or Observable Level, on page 35.
  • After the number of days you specify for the TTL interval, TID deletes:
    • all of the source's indicators that are not included in a subsequent upload.
    • all observables not referenced by a surviving indicator.
Step 6  If you want to immediately begin publishing to elements, confirm that the Publish Slider (○) is enabled.
     If you do not publish the source at ingestion, you cannot publish all source indicators at once later; instead, you must publish each observable individually. See Pause or Publish TID Data at the Source, Indicator, or Observable Level, on page 37.
Step 7  Click Save.

What to do next
  • To view ingestion status, refresh the Sources page. If you see an error, hover over status for details.
  • If you are doing initial TID configuration, return to How To Set Up Threat Intelligence Director, on page 6.
Handling of Duplicate Indicators

If a single indicator is included in multiple sources:

- Indicators from flat file sources – Each instance of the indicator generates an incident, so one encounter with a particular threat may generate multiple incidents.
- Indicators from STIX sources – If indicators from different STIX sources share the same ID, only one incident will be generated for that indicator, regardless of the number of sources that include it.

To avoid future duplicate incidents, pause publishing of all but one of the duplicated indicators. See Pause or Publish TID Data at the Source, Indicator, or Observable Level, on page 37.

Configure TLS/SSL Settings for a TID Source

Configure SSL Settings if the host server requires an encrypted connection.

Before you begin

- Begin configuring a TAXII or URL source, as described in Fetch TAXII Feeds to Use as Sources, on page 8 or Fetch Sources from a URL, on page 9.

Procedure

Step 1 In the Edit Source dialog, expand the SSL Settings section.

Step 2 If your server certificate is self-signed:

a) Enable Self-Signed Certificate.

b) Choose a SSL Hostname Verification method.

   - Strict—TID requires the source URL to match the hostname provided in the server certificate.
   
   For example, if subdomain1.subdomain2.cisco.com is your source URL and *.cisco.com is the hostname provided in the server certificate:

   - Strict hostname verification fails.

   - Browser Compatible hostname verification succeeds.

   - Allow All hostname verification ignores the hostname values completely.

   c) For Server Certificate:
• If you have access to the PEM-encoded self-signed server certificate, open the certificate in a text editor and copy the entire block of text, including the `BEGIN CERTIFICATE` and `END CERTIFICATE` lines. Enter this entire string into the field.

• If you do not have access to the self-signed server certificate, leave the field blank. After you save the source, TID retrieves the certificate from the server.

Step 3

If your server requires a user certificate:

a) Enter a **User Certificate**:

   Open the PEM-encoded certificate in a text editor and copy the entire block of text, including the `BEGIN CERTIFICATE` and `END CERTIFICATE` lines. Enter this entire string into the field.

b) Enter a **User Private Key**:

   Open the private key file in a text editor and copy the entire block of text, including the `BEGIN RSA PRIVATE KEY` and `END RSA PRIVATE KEY` lines. Enter this entire string into the field.

What to do next

• Take note of the certificate's expiration date. You may want to set a calendar reminder to enter a new server certificate after the current certificate expires.

• Continue configuring the source:

  • Fetch TAXII Feeds to Use as Sources, on page 8
  • Fetch Sources from a URL, on page 9

**User Roles with TID Access**

You can use Firepower Management Center user accounts to access the TID menus and pages:

• Accounts with the **Admin** or **Threat Intelligence Director User** user role.

• Accounts with a custom user role containing the **Intelligence** permission.

In addition, you can use Firepower Management Center user accounts with the **Admin**, **Access Admin**, or **Network Admin** user role to enable or disable TID in your access control policies.

For more information about user accounts, see **Firepower System User Management**.

**About Backing Up and Restoring TID Data**

You can use the Firepower Management Center to back up and restore all of the data needed for TID: Element data, security intelligence events, connection events, TID configurations, and TID data. For more information, see **Backup and Restore**.
If you host TID on the active Firepower Management Center in a high availability configuration, the system does not synchronize TID configurations and TID data to the standby Firepower Management Center. We recommend performing regular backups of TID data on your active Firepower Management Center so that you can restore the data after failover.

### Table 2: TID-Related Backup and Restore File Contents

<table>
<thead>
<tr>
<th>TID-Related File Contents</th>
<th>Backup Selection</th>
<th>Restore Selection</th>
</tr>
</thead>
<tbody>
<tr>
<td>Element data</td>
<td>Back Up Configuration</td>
<td>Restore Configuration Data</td>
</tr>
<tr>
<td>Firepower Management Center event data</td>
<td>Back Up Events</td>
<td>Restore Event Data</td>
</tr>
<tr>
<td>TID configurations and TID data</td>
<td>Back Up Threat Intelligence Director</td>
<td>Restore Threat Intelligence Director Data</td>
</tr>
</tbody>
</table>

### Analyze TID Incident and Observation Data

To analyze incident and observation data generated by TID elements, use the Incidents table and Incident Details page.

### Observation and Incident Generation

TID generates an incident when the first observable for an indicator is seen in traffic. Simple indicators are fully realized after a single observation. Complex indicators are partially realized until one or more additional observations fulfill their pattern. Complex indicators need not necessarily be fulfilled during a single transaction; each observable can be fulfilled separately over time, by different transactions.

**Note**

When evaluating an indicator's pattern, TID ignores unsupported and invalid objects and observables on the Do Not Block list.

After an incident is fully realized, subsequent observations trigger new incidents.
If TID ingested the observables from the example above and the observables were seen in order, incident generation would proceed as follows:

1. When the system identifies Observable A in traffic, TID:
   - Generates a fully-realized incident for Indicator 1.
   - Generates partially-realized incidents for Indicator 2 and Indicator 3.

2. When the system identifies Observable B in traffic, TID:
   - Updates the incident to fully-realized for Indicator 2, since the pattern was fulfilled.
   - Updates the incident to partially-realized for Indicator 3.

3. When the system identifies Observable C in traffic, TID:
   - Updates the incident to fully-realized for Indicator 3, since the pattern was fulfilled.

4. When the system identifies Observable A for a second time, TID:
   - Generates a new fully-realized incident for Indicator 1.
   - Generates new partially-realized incidents for Indicator 2 and Indicator 3.

If a particular indicator exists in multiple sources, you may see duplicate incidents. For more information, see *Troubleshoot Threat Intelligence Director*, on page 40.

Note that incidents are generated only by actual traffic. If there is an observable for URL B, and a user visits URL A which displays a link to URL B, no incident occurs unless the user clicks the URL B link.
View and Manage Incidents

The Incidents page displays summary information for TID incidents; see Incident Summary Information, on page 17.

Before you begin

• Configure the feature as described in How To Set Up Threat Intelligence Director, on page 6.
• Understand observation and incident generation, as described in Observation and Incident Generation, on page 14.

Procedure

Step 1
Select Intelligence > Incidents.

Step 2
View your incidents:

• Click Filter ( ) to add one or more filters. The default filter is 6 hours. For more information, see Filter TID Data in Table Views, on page 33.

• To view the date and time an incident was last updated by TID, hover the cursor over the value in the Last Updated column.

• To view more information about the indicator associated with the incident, click the text in the Indicator Name column; see View and Manage Indicators, on page 29.

Step 3
View additional details by clicking a value in the Incident ID column.

For an explanation of the details you see, see Incident Details, on page 17.

• To view indicator details, click an indicator value (for example, an IP address or SHA-256 value) under the Indicator heading in the lower section of the window.

• To view observation details, click the arrow to the left of an observation immediately under the Observations heading.

• To view this incident on the Security Intelligence Events page, click the Events link in the observation details section.

Step 4
(Optional) Enter descriptive information on the incident details page:

Tip: To maximize consistency and usefulness of the options below, plan ahead and document your naming conventions, category choices, and confidence level criteria.

• Enter any value you like in the following fields: Name, Description, and Category.

• Click a rating level for Confidence.

• Indicate the status of your investigation into the incident by choosing a value from the drop-down list in the Status field.
Incident Summary Information

The Incidents page displays summary information for all TID incidents.

Table 3: Incident Summary Information

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last Updated</td>
<td>The number of days since either the system or a user last updated the incident. To view the date and time of the update, hover the cursor over the value in this column.</td>
</tr>
</tbody>
</table>
| Incident ID | The unique identifier for the incident. This ID has the following format: <type>-<date>-<number>  
  • <type>—The type of indicator or observable involved in the incident. For simple indicators, this value indicates the observable type: IP (IPv4 or IPv6), URL (URL), DOM (domain), or SHA (SHA-256). For complex indicators, this value is COM.  
  • <date>—The date (yyyymmd) on which the incident was created.  
  • <number>—The daily incident number, that is, a number specifying where the incident occurs in the daily sequence of incidents. Note that this sequence starts at 0. For example, DOM-20170828-10 is the 11th incident created on that day.  
  Next to the identifier, the system displays an icon that indicates whether the incident is Partially Realized or Fully Realized. For more information, see Observation and Incident Generation, on page 14. |
| Indicator Name| The name of the indicator involved in the incident. To view additional information about the indicator, click the value in this column; see View and Manage Indicators, on page 29. |
| Type | The type of indicator involved in the incident.  
  • Indicators that contain a single observable display the data type (URL, SHA-256, etc.)  
  • Indicators that contain two or more observables display as Complex. |
| Action Taken | The action taken by the system in relation to the incident. For more information, see Incident Details, on page 17. |
| Status | The status of your investigation into the incident. For more information, see Incident Details, on page 17. |
| Delete (🗑️) | Clicking this icon permanently deletes the incident. |

Incident Details

The Incident Details window displays information about a single TID incident. This window is divided into two sections:

• Incident Details: Basic Information, on page 18
• Incident Details: Indicator and Observations, on page 19
Incident Details: Basic Information

The upper section of the Incident Details window provides the information described below.

### Table 4: Basic Incident Information Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
</table>
| **Partially-Realized IncidentID** or **Fully-Realized IncidentID** | An icon indicating the incident's status (partially-realized or fully-realized), as well as the unique identifier for the incident.  
**Note** When determining an incident's status, TID ignores unsupported and invalid observables and observables on the Do Not Block list. |
| **Opened**                     | The date and time the incident was last updated.                                                                                                                                                    |
| **Name**                       | A custom, optional incident name that you enter manually.  
**Tip:** If there is information from the source in the Description field (in the bottom part of the window), use information from that field to name the incident. |
| **Description**                | A custom, optional incident description that you enter manually.  
**Tip:** If there is information from the source in the Description field (in the bottom part of the window), use information from that field to describe the incident. |
| **Observations**               | The number of observations within the incident.                                                                                                                                                       |
| **Confidence**                 | An optional rating that you can manually select to indicate the relative importance of the incident.                                                                                                 |
| **Action Taken**               | The action taken by the system: **Monitored**, **Blocked**, or **Partially Blocked**.  
**Partially Blocked** indicates that the incident contained both **Monitored** and **Blocked** observations.  
**Note** The **Action Taken** indicates the action taken by the system, not necessarily the action selected in TID. For more information, see [TID-Firepower Management Center Action Prioritization](#), on page 22. |
| **Category**                   | A custom, optional tag or keyword that you manually add to the incident.                                                                                                                                |
| **Status**                     | A value indicating the current stage of your analysis of the incident. All incidents are **New** until you change the **Status** for the first time.  
This field is optional. Depending on the needs of your organization, consider using the status values as follows:  
• **New**—The incident requires investigation, but you have not started investigating.  
• **Open**—You are currently investigating the incident.  
• **Closed**—You investigated the incident and took action.  
• **Rejected**—You investigated the incident and determined there was no action to take. |
| **Delete (払い下げ)**          | Clicking this icon permanently deletes this incident.                                                                                                                                                    |
Incident Details: Indicator and Observations

The lower section of the Incident Details window provides an in-depth view of the indicator and observation information. This information is organized as Indicator fields, the indicator pattern, and Observations fields.

Indicator Section

When you first view indicator details, this section displays only the indicator name.

Click the indicator name to view the indicator on the Indicators page.

Click the down arrow next to the indicator name to view more indicator details without leaving the incident.

Detail fields include:

Table 5: Indicator Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Description</td>
<td>The indicator description provided by the source.</td>
</tr>
<tr>
<td>Source</td>
<td>The source that contained the indicator. Click this link to access full source details.</td>
</tr>
<tr>
<td>Expires</td>
<td>The date and time the incident will expire, based on the source's TTL value.</td>
</tr>
<tr>
<td>Action</td>
<td>The action associated with the indicator. For more information, see Edit TID Actions at the Source, Indicator, or Observable Level, on page 35.</td>
</tr>
<tr>
<td>Publish</td>
<td>The publish setting for the indicator. For more information, see Pause or Publish TID Data at the Source, Indicator, or Observable Level, on page 37.</td>
</tr>
<tr>
<td>Download STIX</td>
<td>If the source type is STIX, click this button to download the STIX file.</td>
</tr>
</tbody>
</table>

Indicator Pattern

The indicator pattern is a graphical representation of the observables and operators that comprise the indicator. Operators link the observables within the indicator. AND relationships are indicated with the AND operator. OR relationships are indicated with the OR operator or by a close grouping of several observables.

If an observable in the pattern has already been seen, the observable box is white. If an observable has not already been seen, the observable box is grey.

In the indicator pattern:

- Click the Whitelist button to add the observable to the Do Not Block list. This icon is present in both white and grey observable boxes. For more information, see About Adding TID Observables to the Do Not Block List, on page 38.

- If you hover the cursor over a white observable box, the system highlights the related observation in the Observations section.

- If you click a white observable box, the system highlights the related observation in the Observations section, scrolls that observation into view (if multiple observations are present), and expands that observation's detailed display.

- If you hover the cursor over or click a grey observable box in the indicator pattern, there is no change in the Observations section. Because the observable is unseen, there are no observation details to display yet.
Observations Section

By default, the Observations section displays summary information, which includes:

- The type of observable that triggered the observation (for example, Domain)
- The data that comprises the observable
- Whether the observation is the first observation or a subsequent observation (for example, 1st or 3rd)

Note

If a single observable has been seen three or more times, TID displays the first and last observation details. The details for intermediary observations are not available.

- The date and time of the observation
- The action configured for the observable

If you hover the cursor over an observation in the Observations section, the system highlights the related observable in the indicator pattern.

If you click an observation in the Observations section, the system highlights the related observable(s) in the indicator pattern and scrolls the first related observable into view (if multiple observables are present). Clicking an observation also expands the details of the observation in the Observations section.

Observation details include the following fields:

Table 6: Observation Detail Fields

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>SOURCE</td>
<td>The source IP address and port for the traffic that triggered the observation.</td>
</tr>
<tr>
<td>DESTINATION</td>
<td>The destination IP address and port for the traffic that triggered the observation.</td>
</tr>
<tr>
<td>ADDITIONAL INFORMATION</td>
<td>DNS and authentication information related to the traffic that triggered the observation.</td>
</tr>
<tr>
<td>Events</td>
<td>This clickable link displays if the observation generated connection, security intelligence, file, or malware events. Click the link to view the events in the Firepower Management Center event table; see About Connection Events.</td>
</tr>
</tbody>
</table>

View Events for a TID Observation

For more information about the Firepower Management Center events that TID observations generate, see TID Observations in Firepower Management Center Events, on page 21.
The system action logged for TID-related events can vary, depending on the interaction of TID and other Firepower Management Center features. For more information about action prioritization, see TID-Firepower Management Center Action Prioritization, on page 22.

**Before you begin**

- Configure the feature as described in How To Set Up Threat Intelligence Director, on page 6.
- Confirm that you enabled event logging required for TID in your access control policy, as described in Configure Policies to Support TID, on page 7.

**Procedure**

<table>
<thead>
<tr>
<th>Step</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Step 1</td>
<td>Choose <strong>Intelligence</strong> &gt; <strong>Incidents</strong>.</td>
</tr>
<tr>
<td>Step 2</td>
<td>Click the <strong>Incident ID</strong> value for the incident.</td>
</tr>
<tr>
<td>Step 3</td>
<td>Click the observation in the <strong>Indicator</strong> section to display the observation box.</td>
</tr>
<tr>
<td>Step 4</td>
<td>Expand the observation box by clicking the arrow in the upper-left corner of the box.</td>
</tr>
<tr>
<td>Step 5</td>
<td>Click the <strong>Events</strong> link in the observation information. For more information on the Security Intelligence display, see About Connection Events.</td>
</tr>
</tbody>
</table>

**TID Observations in Firepower Management Center Events**

If you fully configure your access control policy, TID observations generate the following Firepower Management Center events:

<table>
<thead>
<tr>
<th>Observation Content</th>
<th>Connection Events Table</th>
<th>Security Intelligence Events Table</th>
<th>File Events Table</th>
<th>Malware Events Table</th>
</tr>
</thead>
<tbody>
<tr>
<td>SHA-256</td>
<td>Yes</td>
<td>No</td>
<td>Yes</td>
<td>Yes, if disposition is Malware or Custom Detection.</td>
</tr>
<tr>
<td>Domain Name, URL, or IPv4/IPv6</td>
<td>Yes</td>
<td>Yes TID-related connection events are identified with a TID-related <strong>Security Intelligence Category</strong> value.</td>
<td>No</td>
<td>No</td>
</tr>
</tbody>
</table>

**Factors That Affect the Action Taken**

Many factors determine when the system takes action and what action the system takes when it detects traffic that matches a TID observable.
• Features like Security Intelligence take action before TID does. For details, see TID-Firepower Management Center Action Prioritization, on page 22.

• Generally, the action configured for an observable (which may differ from the action configured for its parent indicator or source) is the action that will be taken.

• Because STIX sources can contain complex indicators, the Action setting for the source can be set only to Monitor. However, individual simple indicators or observables contained in a STIX feed or file can be set to Block.

• Action settings for indicators and observables can be inherited or individually configured to override inheritance. See Inheritance in TID Configurations, on page 34 and Edit TID Actions at the Source, Indicator, or Observable Level, on page 35.

• Traffic that might otherwise be actionable might be on a Do Not Block list. For details, see Add TID Observables to a Do Not Block List, on page 39.

• The configured action is taken for both partially- and fully-realized incidents.

• An incident based on a complex indicator can be partially blocked. This can occur if the indicator includes both monitored and blocked observations.

• Pausing publishing affects actions the system takes. See About Pausing Publishing, on page 36 and Pause or Publish TID Data at the Source, Indicator, or Observable Level, on page 37.

• Pausing the TID feature prevents all actions. After you resume the feature, actionable data may be different from before. For details, see Pause TID and Purge TID Data from Elements, on page 37.

**TID-Firepower Management Center Action Prioritization**

If TID observable actions conflict with Firepower Management Center policy actions, the system prioritizes actions as follows:

• Security Intelligence Do Not Block

• Security Intelligence Block

• TID Block

• Security Intelligence Monitor

• TID Monitor

Specifically:

**Table 8: TID URL Observable Action vs. Security Intelligence Action**

<table>
<thead>
<tr>
<th>Setting: Security Intelligence Action</th>
<th>Setting: TID Observable Action</th>
<th>TID Incidents Field: Action Taken</th>
<th>Security Intelligence Events Fields:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whitelist</td>
<td>Monitor or Block</td>
<td>No TID incident</td>
<td>No Security Intelligence event</td>
</tr>
<tr>
<td>Setting: Security Intelligence Action</td>
<td>Setting: TID Observable Action</td>
<td>TID Incidents Field: Action Taken</td>
<td>Security Intelligence Events Fields:</td>
</tr>
<tr>
<td>--------------------------------------</td>
<td>---------------------------------</td>
<td>---------------------------------</td>
<td>----------------------------------</td>
</tr>
<tr>
<td>Block</td>
<td>Monitor</td>
<td>Blocked</td>
<td>Action as determined by system analysis; see Security Intelligence Categories</td>
</tr>
<tr>
<td>Block</td>
<td>No TID incident</td>
<td>Block</td>
<td>Reason as determined by system analysis; see Security Intelligence Categories</td>
</tr>
<tr>
<td>Monitor</td>
<td>Monitor</td>
<td>No TID incident</td>
<td>Reason as determined by system analysis; see Security Intelligence Categories</td>
</tr>
<tr>
<td>Block</td>
<td>Blocked</td>
<td>Block</td>
<td>Reason TID URL Block</td>
</tr>
</tbody>
</table>

**Table 9: TID IPv4/IPv6 Observable Action vs. Security Intelligence Action**

<table>
<thead>
<tr>
<th>Setting: Security Intelligence Action</th>
<th>Setting: TID Observable Action</th>
<th>TID Incidents Field: Action Taken</th>
<th>Security Intelligence Events Fields:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whitelist</td>
<td>Monitor or Block</td>
<td>No TID incident</td>
<td>No Security Intelligence event</td>
</tr>
<tr>
<td>Block</td>
<td>Monitor</td>
<td>Blocked</td>
<td>Action as determined by system analysis; see Security Intelligence Categories</td>
</tr>
<tr>
<td>Block</td>
<td>No TID incident</td>
<td>Block</td>
<td>Action as determined by system analysis; see Security Intelligence Categories</td>
</tr>
</tbody>
</table>
### Table 10: TID Domain Name Observable Action vs. DNS Policy Action

<table>
<thead>
<tr>
<th>Setting: DNS Policy Action</th>
<th>Setting: TID Domain Name Observable Action</th>
<th>TID Incidents Field: Action Taken</th>
<th>Security Intelligence Events Fields:</th>
</tr>
</thead>
<tbody>
<tr>
<td>Whitelist</td>
<td>Monitor or Block</td>
<td>No TID incident</td>
<td>No Security Intelligence event</td>
</tr>
<tr>
<td>Drop, Domain Not Found</td>
<td>Monitor</td>
<td>Blocked</td>
<td>as determined by system analysis; see Security Intelligence Categories</td>
</tr>
<tr>
<td>Sinkhole—Log</td>
<td></td>
<td>Block</td>
<td>DNS Block</td>
</tr>
<tr>
<td>Sinkhole—Block and Log</td>
<td>Block</td>
<td>Blocked</td>
<td>DNS Block</td>
</tr>
<tr>
<td>Monitor</td>
<td>Monitor</td>
<td>Monitored</td>
<td>as determined by system analysis; see Security Intelligence Categories</td>
</tr>
<tr>
<td></td>
<td>Block</td>
<td>Blocked</td>
<td>DNS Monitor</td>
</tr>
</tbody>
</table>

### Table 11: TID SHA-256 Observable Action vs. Malware Cloud Lookup File Policy

<table>
<thead>
<tr>
<th>File Disposition</th>
<th>TID SHA-256 Observable Action</th>
<th>Action Taken in TID Incidents</th>
<th>Action in File Events</th>
<th>Action in Malware Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clean</td>
<td>Monitor or Block</td>
<td>Monitored</td>
<td>Malware Cloud Lookup</td>
<td>n/a</td>
</tr>
<tr>
<td>File Disposition</td>
<td>TID SHA-256 Observable Action</td>
<td>Action Taken in TID Incidents</td>
<td>Action in File Events</td>
<td>Action in Malware Events</td>
</tr>
<tr>
<td>------------------</td>
<td>--------------------------------</td>
<td>-------------------------------</td>
<td>----------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Malware</td>
<td>Monitor or Block</td>
<td>Monitored</td>
<td>Malware Cloud Lookup</td>
<td>n/a</td>
</tr>
</tbody>
</table>
| Custom           | Monitor or Block               | Monitored                     | • Malware Cloud Lookup, if SHA-256 is not in a custom detection list.  
 • Custom Detection, if SHA-256 is in a custom detection list. | • Malware Cloud Lookup, if SHA-256 is not in a custom detection list.  
 • Custom Detection, if SHA-256 is in a custom detection list. |
| Unknown          | Monitor or Block               | Monitored                     | Malware Cloud Lookup | n/a                      |

**Note**

TID matching occurs before the system sends a file for dynamic analysis.

*Table 12: TID SHA-256 Observable Action vs. Block Malware File Policy*

<table>
<thead>
<tr>
<th>File Disposition</th>
<th>TID SHA-256 Observable Action</th>
<th>Action Taken in TID Incidents</th>
<th>Action in File Events</th>
<th>Action in Malware Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>Clean or Unknown</td>
<td>Monitor</td>
<td>Monitored</td>
<td>Malware Cloud Lookup</td>
<td>n/a</td>
</tr>
</tbody>
</table>
| Block            |                                | Blocked                       | • TID Block, if SHA-256 is not in a custom detection list.  
 Modified file disposition is Custom.  
 • Custom Detection Block, if SHA-256 is in a custom detection list. | TID Block  
 Modified file disposition is Custom. |
### View and Change Threat Intelligence Director Configurations

Use the following information to review and fine-tune your configuration as needed.

#### View TID Status of Elements (Managed Devices)

All devices that are registered to the Firepower Management Center as managed devices appear automatically on the Elements page. All properly-configured elements (as specified in Configure Policies to Support TID, on page 7) will receive all currently-published observables, including those ingested before the element was added.

**Procedure**

| Step 1 | Choose Intelligence > Elements. |
| Step 2 | To see whether the element is connected and TID is enabled, hover over the icon beside the element name. |

#### View and Manage Sources

The Sources page displays summary information about all configured sources; see Source Summary Information, on page 27.

**Procedure**

| Step 1 | Choose Intelligence > Sources. |
Step 2

View your sources:

- To filter the sources displayed on the page, click Filter. For more information, see Filter TID Data in Table Views, on page 33.

- To view detailed ingestion status, hover the cursor over the text in the Status column. For more information, see Source Status Details, on page 28.

Step 3

Manage your sources:

- To edit the Action setting, see Edit TID Actions at the Source, Indicator, or Observable Level, on page 35. If an action is fixed, it is the only supported action for the source Type.

- To edit the Publish setting, click Slider. For more information, see Pause or Publish TID Data at the Source, Indicator, or Observable Level, on page 37.

- To pause or resume TID updating the source, click Pause Updates or Resume Updates. If you pause updates, updating is paused but existing indicators and observables remain in TID.

- To delete the source, click Delete. Delete is greyed out if the source is still processing. Deleting a source deletes all indicators associated with that source. Associated observables may also be deleted; they are retained if they are associated with indicators remaining in the system.

Source Summary Information

The Sources page displays summary information for all configured sources. The table below provides brief descriptions of the fields in the summary display. For detailed information on these fields, see descriptions in the relevant configuration topic for the source: See Options for Ingesting Data Sources, on page 8.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The source name.</td>
</tr>
<tr>
<td>Type</td>
<td>The data format of the source (STIX or Flat File).</td>
</tr>
<tr>
<td>Delivery</td>
<td>The method TID uses to retrieve the source.</td>
</tr>
<tr>
<td>Action</td>
<td>The action (Block or Monitor) that the system is configured to perform on traffic matching the data contained within this source. For more information about TID actions, including availability, inheritance, and overriding inheritance, see Factors That Affect the Action Taken, on page 21.</td>
</tr>
<tr>
<td>Publish</td>
<td>On or Off toggle specifying whether TID publishes data from the source to registered elements (managed devices configured to support TID). Indicators can inherit Publish settings from a parent source, and observables can inherit Publish settings from a parent indicator. For more information, see Inheritance in TID Configurations, on page 34.</td>
</tr>
<tr>
<td>Last Updated</td>
<td>The date and time TID last updated the source.</td>
</tr>
</tbody>
</table>
**Source Status Details**

When you hover over a source's Status value in the Sources summary page, TID provides the additional details described below.

<table>
<thead>
<tr>
<th>Data</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status Message</td>
<td>Briefly describes the current status of the source.</td>
</tr>
<tr>
<td>Last Updated</td>
<td>Specifies the date and time TID last updated the source.</td>
</tr>
<tr>
<td>Next Update</td>
<td>For TAXII and URL sources, this value specifies when TID will update the source next.</td>
</tr>
<tr>
<td>Indicators</td>
<td>Specifies indicator counts:</td>
</tr>
<tr>
<td></td>
<td>- Consumed—The number of indicators TID processed during the most recent source update. This number represents all indicators contained in the update, regardless of whether they were ingested or discarded.</td>
</tr>
<tr>
<td></td>
<td>- Discarded—The number of malformed indicators that the system did not add to TID during the most recent update.</td>
</tr>
</tbody>
</table>

**Note**  
For TAXII sources, TID provides separate Last Update and Total indicator counts, because TAXII updates add incremental data, rather than replacing existing data. For indicators from other source types, TID provides only the Last Update count, because updates from those sources replace the existing data set entirely.

If all of an indicator's observables are Invalid, TID discards the indicator.
### Data | Description
--- | ---
**Observables** | Specifies observable counts:
- **Consumed**—The number of observables TID processed during the most recent source update. This number represents all observables contained in the update, regardless of whether they were ingested or discarded.
- **Unsupported**—The number of unsupported observables that the system did not add to TID during the most recent update.

For more information about supported observable types, see information about content types in Source Requirements, on page 5.
- **Invalid**—The number of invalid observables that the system did not add to TID during the most recent update.

An observable is invalid if it is improperly constructed. For example, 10.10.10.10.123 is not a valid IPv4 address.

**Note** For TAXII sources, TID provides separate Last Update and Total observable counts, because TAXII updates add incremental data, rather than replacing existing data. For observables from other source types, TID provides only the Last Update count, because updates from those sources replace the existing data set entirely.

---

### View and Manage Indicators

Indicators are generated automatically from ingested sources. For more information about information on this page, see Indicator Summary Information, on page 30.

**Procedure**

**Step 1** Choose **Intelligence > Sources**.

**Step 2** Click **Indicators**.

**Step 3** View your current indicators:

- To filter the indicators displayed on the page, click **Filter**. For more information, see Filter TID Data in Table Views, on page 33.
- To view additional details about an indicator (including associated observables), click the indicator name. For more information, see Indicator Details, on page 31.
- In the **Incidents** column, click the number to view information about incidents associated with an indicator, or hover the cursor over Incidents to view whether the incidents are fully- or partially-realized.
- To determine whether TID finished ingesting an indicator from the source, view the **Status** column.

**Step 4** Manage your current indicators:

- To edit the **Action**, see Edit TID Actions at the Source, Indicator, or Observable Level, on page 35. If an action is fixed, it is the only supported action for the source **Type**.
To edit the Publish setting, see Pause or Publish TID Data at the Source, Indicator, or Observable Level, on page 37.

To add one or more of an indicator's observables to the Do Not Block list, click the indicator name to access the Indicator Details page. For more information, see About Adding TID Observables to the Do Not Block List, on page 38.

**Indicator Summary Information**

The Indicators page displays summary information for all indicators associated with configured sources.

**Table 14: Indicators Summary Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Type</td>
<td>• Indicators that have a single observable list the data type of that observable (URL, SHA-256, etc.)&lt;br&gt;• Indicators that have two or more observables are listed as Complex. Hover over the type to see the specific observable.</td>
</tr>
<tr>
<td>Name</td>
<td>The indicator name.</td>
</tr>
<tr>
<td>Source</td>
<td>The source that contained the indicator (the parent source).</td>
</tr>
<tr>
<td>Incidents</td>
<td>Information about any incidents associated with the indicator:&lt;br&gt;• an icon specifying whether the incident is Partially or Fully realized&lt;br&gt;• the number of incidents associated with the indicator</td>
</tr>
<tr>
<td>Action</td>
<td>The action associated with the indicator. For more information, see Edit TID Actions at the Source, Indicator, or Observable Level, on page 35. Indicators can inherit Action settings from a parent source, and observables can inherit Action settings from a parent indicator. For more information, see Inheritance in TID Configurations, on page 34.</td>
</tr>
<tr>
<td>Publish</td>
<td>The publish setting for the indicator. For more information, see Pause or Publish TID Data at the Source, Indicator, or Observable Level, on page 37. Indicators can inherit Publish settings from a parent source, and observables can inherit Publish settings from a parent indicator. For more information, see Inheritance in TID Configurations, on page 34.</td>
</tr>
<tr>
<td>Last Updated</td>
<td>The date and time TID last updated the indicator.</td>
</tr>
</tbody>
</table>
The current status of the indicator:

- **Pending** — TID is ingesting the indicator's observables.
- **Completed** — TID successfully ingested all of the indicator's observables.
- **Completed With Errors** — TID finished ingesting the indicator, but some observables are unsupported or invalid.

## Indicator Details

The Indicator Details page displays indicator and observable data for an incident.

**Table 15: Indicator Details Information**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Name</td>
<td>The indicator name.</td>
</tr>
<tr>
<td>Description</td>
<td>The indicator description provided by the source.</td>
</tr>
<tr>
<td>Source</td>
<td>The source that contained the indicator.</td>
</tr>
<tr>
<td>Expires</td>
<td>The date and time the indicator will expire, based on the source's TTL value.</td>
</tr>
<tr>
<td>Action</td>
<td>The action associated with the indicator. For more information, see Edit TID Actions at the Source, Indicator, or Observable Level, on page 35. Indicators can inherit the Action setting from a parent source, and observables can inherit the Action setting from a parent indicator. For more information, see Inheritance in TID Configurations, on page 34.</td>
</tr>
<tr>
<td>Publish</td>
<td>The publish setting for the indicator. For more information, see Pause or Publish TID Data at the Source, Indicator, or Observable Level, on page 37. Indicators can inherit the Publish setting from a parent source, and observables can inherit the Publish setting from a parent indicator. For more information, see Inheritance in TID Configurations, on page 34.</td>
</tr>
<tr>
<td>Indicator Pattern</td>
<td>The observables and operators that form the indicator's pattern. Operators link the observables within the indicator. AND relationships are indicated with the AND operator. OR relationships are indicated with the OR operator or by a close grouping of several observables. Optionally, click the Whitelist button to add an observable to the Do Not Block list. For more information, see About Adding TID Observables to the Do Not Block List, on page 38.</td>
</tr>
</tbody>
</table>

## View and Manage Observables

The Observables page displays all successfully ingested observables; see Observable Summary Information, on page 32.
Before you begin

- Configure one or more sources as described in Fetch TAXII Feeds to Use as Sources, on page 8, Fetch Sources from a URL, on page 9, or Upload a Local File to Use as a Source, on page 10.

Procedure

Step 1
Choose **Intelligence > Sources**.

Step 2
Click **Observables**.

Step 3
View your current observables:
- To filter the observables displayed on the page, click **Filter (Ω)**. For more information, see Filter TID Data in Table Views, on page 33.
- If the information in the **Value** column is cut off, hover over the value.
- To view indicators that contain the observable, click the number in the **Indicators** column. The Incidents page opens with the observable value as the filter. For more information, see View and Manage Indicators, on page 29.

Step 4
Manage your current observables:
- To edit the **Action**, see Edit TID Actions at the Source, Indicator, or Observable Level, on page 35.
- To edit an observable's **Publish** setting, see Pause or Publish TID Data at the Source, Indicator, or Observable Level, on page 37.
- To change an observable's expiration date, modify the **TTL** for the parent source. For more information, see View and Manage Sources, on page 26.
- To add an observable to the Do Not Block list, click the **Whitelist** button. For more information, see About Adding TID Observables to the Do Not Block List, on page 38.

Observable Summary Information

The Observables page displays summary information for all ingested observables.

*Table 16: Observables Summary Information*

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Type</strong></td>
<td>The type of observable data: SHA-256, Domain, URL, IPv4, or IPv6.</td>
</tr>
<tr>
<td><strong>Value</strong></td>
<td>The data that comprises the observable.</td>
</tr>
<tr>
<td><strong>Indicators</strong></td>
<td>The number of parent indicators containing the observable.</td>
</tr>
</tbody>
</table>
### Field Description

**Action**
The action configured for the observable. For more information, see Edit TID Actions at the Source, Indicator, or Observable Level, on page 35. Indicators can inherit Action settings from a parent source, and observables can inherit Action settings from a parent indicator. For more information, see Inheritance in TID Configurations, on page 34.

**Publish**
The publish setting for the observable; see Pause or Publish TID Data at the Source, Indicator, or Observable Level, on page 37. Indicators can inherit Publish settings from a parent source, and observables can inherit Publish settings from a parent indicator. For more information, see Inheritance in TID Configurations, on page 34.

**Updated At**
The date and time TID last updated the observable.

**Expires**
The date that the observable will be automatically purged from TID based on TTL for the parent indicator.

**Whitelist button**
Clicking this button adds the observable to the Do Not Block list; see About Adding TID Observables to the Do Not Block List, on page 38.

---

## Filter TID Data in Table Views

### Procedure

**Step 1** Choose one of the following TID table views:
- Intelligence > Incidents
- Intelligence > Sources
- Intelligence > Sources > Indicators
- Intelligence > Sources > Observables

**Step 2** Click Filter (🔍) and choose a filter attribute.

**Step 3** Choose or enter a value for that filter attribute.
Filters are case-sensitive.

**Step 4** (Optional) To filter by multiple attributes, click Filter (🔍) and repeat Step 2 and Step 3.

**Step 5** To cancel the changes you have made since you last applied the filter, click Cancel.

**Step 6** Click Apply to refresh the table with the filter applied.

**Step 7** To remove a filter attribute individually, click Remove (✗) next to the filter attribute and click Apply to refresh the table.
Inheritance in TID Configurations

When TID ingests intelligence data from a source, it creates indicators and observables as child objects of that source. On creation, these child objects inherit Action and Publish settings from the parent configuration.

An indicator inherits these settings from the parent source. An indicator can only have one parent source.

An observable inherits these settings from the parent indicator(s). An observable can have multiple parent indicators.

For more information, see:
- Inheritance of TID Settings from Multiple Parents, on page 34
- About Overriding Inherited TID Settings, on page 34

Inheritance of TID Settings from Multiple Parents

If an observable has multiple parent indicators, the system compares the inherited settings from all the parents and assigns the most secure option to the observable. Thus:

- **Action**: Block is more secure than Monitor
- **Publish**: On is more secure than Off

For example, SourceA might contribute IndicatorA and related ObservableA:

<table>
<thead>
<tr>
<th>Setting</th>
<th>SourceA</th>
<th>IndicatorA</th>
<th>ObservableA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Block</td>
<td>Block</td>
<td>Block</td>
</tr>
<tr>
<td>Publish</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
</tbody>
</table>

If SourceB later contributes IndicatorB, which also includes ObservableA, the system modifies ObservableA as follows:

<table>
<thead>
<tr>
<th>Setting</th>
<th>SourceB</th>
<th>IndicatorB</th>
<th>ObservableA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Action</td>
<td>Monitor</td>
<td>Monitor</td>
<td>Block (inherited from IndicatorA)</td>
</tr>
<tr>
<td>Publish</td>
<td>On</td>
<td>On</td>
<td>On (inherited from IndicatorB)</td>
</tr>
</tbody>
</table>

In this example, ObservableA has two parents: one parent for its Action setting and one parent for its Publish setting. If you manually edit the settings for the observable and then revert the settings, the system sets the Action setting to the IndicatorA value and the Publish setting to the IndicatorB value.

About Overriding Inherited TID Settings

To override an inherited setting, change the setting at the child level; see Edit TID Actions at the Source, Indicator, or Observable Level, on page 35 and Pause or Publish TID Data at the Source, Indicator, or Observable Level, on page 37. After you override an inherited setting, the child object retains that setting despite changes to the parent object(s).

For example, you might start with the following original settings, with no overrides set:
If you override the setting for IndicatorA, the settings would be the following:

<table>
<thead>
<tr>
<th>Setting</th>
<th>SourceA</th>
<th>IndicatorA</th>
<th>ObservableA1</th>
<th>ObservableA2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publish</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
<td>Off</td>
</tr>
</tbody>
</table>

In this case, any changes to the Publish setting for SourceA no longer cascade automatically to IndicatorA. However, inheritance from IndicatorA to ObservableA1 and ObservableA2 continues, because the observable settings are not currently set to override values.

If you later override the setting for ObservableA1:

<table>
<thead>
<tr>
<th>Setting</th>
<th>SourceA</th>
<th>IndicatorA</th>
<th>ObservableA1</th>
<th>ObservableA2</th>
</tr>
</thead>
<tbody>
<tr>
<td>Publish</td>
<td>Off</td>
<td>On</td>
<td>Off</td>
<td>On</td>
</tr>
</tbody>
</table>

Any changes to the Publish setting for IndicatorA no longer cascade automatically to ObservableA1. However, those changes continue to cascade to ObservableA2, because it is not set to an override value.

At the observable level, you can revert from an override setting to the inherited setting, and the system resumes cascading setting changes automatically from the parent indicator to that observable.

**Edit TID Actions at the Source, Indicator, or Observable Level**

Note:

- Editing the action for a parent sets the action for all children. If you edit the action at the source level, you set the action for all its indicators. If you edit the action at the indicator level, you set the action for all of its observables.

- Editing the action for a child interrupts inheritance. If you edit the action at the indicator level, and subsequently edit it at the source level, the indicator's action is retained until you edit the action for the individual indicator. If you edit the action at the observable level, and subsequently edit it at the indicator level, the observable's action is retained until you edit the action for the individual observable. At the observable level, you can revert automatically to the parent indicator's action. For more information about inheritance, see Inheritance in TID Configurations, on page 34.

You may also want to review other Factors That Affect the Action Taken, on page 21.

**Procedure**

**Step 1** Choose any of the following:

- **Intelligence > Sources**

  **Note** TID does not support blocking TAXII sources at the source level. If the TAXII source contains a simple indicator, you can block at the indicator or observable level.

- **Intelligence > Sources > Indicators**
TID does not support blocking complex indicators. Instead, block individual observables within the complex indicator.

- **Intelligence > Sources > Observables**

**Step 2** Use the **Action** dropdown to choose **Monitor** or **Block**.

**Step 3** (Observables only) If you want to resume inheriting the action setting from the parent indicator, click **Revert** next to the **Action** setting for the observable.

---

### About Pausing Publishing

- If you pause publishing at the feature level, the system purges all TID observables stored on your elements. This means that TID cannot detect, monitor or block threats. Other security features on your system are not affected.

- If you pause publishing at the source, indicator, or observable level, the system removes the paused TID observables from your elements, preventing them from matching traffic.

- Pausing publication for a parent pauses all children. If you pause publishing at the source level, you pause publishing for all its indicators. If you pause publishing at the indicator level, you pause publishing for all of its observables.

- Pausing publication for a child interrupts inheritance. If you pause publishing at the indicator level, and subsequently publish at the source level, publishing for the indicator remains paused until you change the individual setting for the indicator. If you pause publishing at the observable level, and subsequently publish at the indicator level, publishing for the observable remains paused until you change the individual setting for the observable. At the observable level, you can revert automatically to the parent indicator’s publishing status. For more information about inheritance, see Inheritance in TID Configurations, on page 34.

- Publishing for Uploaded sources can only be paused at the indicator level.

- For a comparison of pausing publishing for an observable vs adding the observable to the Do Not Block list, see About Adding TID Observables to the Do Not Block List, on page 38.

- If you have specified a publish/pause setting for an individual observable or indicator, source updates do not change that setting if the update contains the same observable or indicator.

- Publishing can be disabled on the object management pages. See Modify the Observable Publication Frequency, on page 38.

- The option on the Sources page to pause updates is not related to publishing data to elements; it applies to updating sources on the Firepower Management Center from feeds.
**Pause TID and Purge TID Data from Elements**

**Caution**

This setting pauses publishing to all elements, purges all TID observables stored on your elements, and stops inspecting traffic using the TID feature.

To disable observables at a more granular level, see Pause or Publish TID Data at the Source, Indicator, or Observable Level, on page 37.

Data on the management center (existing incidents and configured sources, indicators, and observables, and ingestion of sources) is not affected by this setting.

**Procedure**

**Step 1**
Choose Intelligence > Settings.

**Step 2**
Click Pause.

**What to do next**

When you are ready to resume synchronizing TID data on your elements and generating observations, manually Resume publishing from this page. Existing observables on the management center are published to all elements.

**Pause or Publish TID Data at the Source, Indicator, or Observable Level**

If publishing is enabled at the Source level, the system automatically publishes the initial source data and any subsequent changes including:

- changes from periodic source refreshes
- changes resulting from system action (for example, TTL expiration)
- any user-initiated changes (for example, a change in the Action setting for an indicator or observable)

**Note**

To purge all TID observables at once from your devices (elements), see Pause TID and Purge TID Data from Elements, on page 37.

**Before you begin**

Before pausing publishing, understand the ramifications described in About Pausing Publishing, on page 36.

**Procedure**

**Step 1**
Choose any of the following:
• Intelligence > Sources
• Intelligence > Sources > Indicators
• Intelligence > Sources > Observables

Step 2 Locate the Publish Slider (ıldığı) and use it to toggle publishing to elements.
Step 3 (Observables only) If you want to resume inheriting the publication setting from the parent indicator, click Revert next to the Publish setting for the observable.

What to do next
• Wait at least 10 minutes for elements to receive changes. Changes involving large sources will take longer.
• (Optional) Change the publication frequency for TID data at the observable level; see Modify the Observable Publication Frequency, on page 38.

Modify the Observable Publication Frequency

By default, the system publishes observables to TID elements every 5 minutes. Use this procedure to set this interval to a different value.

Before you begin
• Enable publication of TID data at the observable level; see Pause or Publish TID Data at the Source, Indicator, or Observable Level, on page 37.

Procedure

Step 1 Choose Objects > Object Management.
Step 2 Choose Security Intelligence > Network Lists and Feeds.
Step 3 Click edit next to the Cisco-TID-Feed.
Step 4 Choose a value from the Update Frequency drop-down list:
  • Choose Disable to stop publication of observable data to elements.
  • Choose any other value to set the interval for observable publication.
Step 5 Click Save.

About Adding TID Observables to the Do Not Block List

If you want to exempt an observable in a simple indicator from the specified Action (let the traffic pass without monitoring or blocking), you can add the observable to a Do Not Block list.
In a complex indicator, TID ignores observables on the Do Not Block list when evaluating traffic, but other observables in that indicator are still evaluated. For example, if an indicator includes Observable 1 and Observable 2 linked by the AND operator, and you add Observable 1 to a Do Not Block list, TID generates a fully realized incident when Observable 2 is seen.

By comparison, in the same complex indicator, if you disable publishing of Observable 1 instead of adding it to the Do Not Block list, TID generates a partially-realized incident when Observable 2 is seen.

The **Whitelist** button ( ![Whitelist](image)) appears on the indicator details page and the observables page. If you want to add an observable to the Do Not Block list, click the icon.

---

**Note**

If you add an observable to the Do Not Block list, this always takes precedence over the **Action** setting, whether the setting in the observable is an inherited or override value.

Source updates do not affect the Do Not Block list setting for individual observables if the update contains the same observable.

### Add TID Observables to a Do Not Block List

For detailed information about using Do Not Block lists, see About Adding TID Observables to the Do Not Block List, on page 38.

**Tip**

An "Add to Do Not Block List" button ( ![Add to Do Not Block List](image)) can appear in several places in the web interface. You can add an observable to a Do Not Block list in any of those locations by clicking this button.

#### Procedure

**Step 1**
Click **Intelligence > Sources > Observables**.

**Step 2**
Navigate to the observable that you want to allow.

**Step 3**
Click ![Whitelist](image) for that observable.

---

**What to do next**

(Optional) If you need to remove an observable from the Do Not Block list, click the button again.

### View a STIX Source File

#### Procedure

**Step 1**
Select **Intelligence > Sources > Indicators**.

**Step 2**
Click the indicator name.
Step 3  
Click Download STIX.

Step 4  
Open the file in a text editor.

---

## Troubleshoot Threat Intelligence Director

The sections below describe possible solutions and mitigations for common TID issues.

### Fetching or uploading flat file sources generates an error

If the system fails to fetch or upload a flat file source, check that the data in the flat file matches the Type column on the Intelligence > Sources page.

### TAXII or URL source update generates an error

If a TAXII or URL source update generates a source status error, check that your Server Certificate is not expired. If the certificate has expired, enter a new Server Certificate or delete the existing Server Certificate so TID can retrieve a new certificate. For more information, see Configure TLS/SSL Settings for a TID Source, on page 12.

### "Block" action is not available for an indicator or source, only "Monitor"

You can change the action for individual observables in the indicator or source.

### TID table views return “No results”

Table views include the Sources, Indicators, Observables, and Incidents pages.

If you do not see data in one of the TID table views:

- Check your table filter and consider expanding the time window for the Last Updated filter attribute; see Filter TID Data in Table Views, on page 33.
- Verify that you correctly configured your sources; see Options for Ingesting Data Sources, on page 8.
- Verify that you configured your access control policy and related policies to support TID; see Configure Policies to Support TID, on page 7. For example, if your SHA-256 observables are not generating observations, verify that your deployed access control policy contains one or more access control rules that invoke a Malware Cloud Lookup or Block Malware file policy.
- Verify that you deployed the TID-supporting access control policy and related policies to your elements; see Deploy Configuration Changes.
- Verify that you did not pause TID data publication at the feature level; see Pause TID and Purge TID Data from Elements, on page 37.

### System is experiencing slowness or decreased performance

For more information about performance impact, see Performance Impact of Threat Intelligence Director, on page 3.
Firepower Management Center table views do not show TID data

If you are publishing observables to your elements but no TID data appears in the connection, security intelligence, file, or malware events tables, check the access control and file policies deployed to your elements. For more information, see Configure Policies to Support TID, on page 7.

One or more elements are overwhelmed by TID data

If TID data is overwhelming one or more of your devices, consider pausing TID publishing and purging the data stored on your elements. For more information, see Pause TID and Purge TID Data from Elements, on page 37.

System is performing a Malware Cloud Lookup instead of a TID block

This is by design. For more information, see TID-Firepower Management Center Action Prioritization, on page 22.

System is performing a Security Intelligence or DNS Policy action instead of a TID action

This is by design. For more information, see TID-Firepower Management Center Action Prioritization, on page 22.

TID is disabled

- Add memory to your appliance. Threat Intelligence Director can only be used on appliances with at least 15GB of memory.
- Enable REST API access for the Firepower Management Center. For more information, see Enabling REST API Access.

The system does not generate the TID incident or take the TID action that you expected

- Verify that all of your managed devices are properly enabled and configured for TID. See View TID Status of Elements (Managed Devices), on page 26 and Configure Policies to Support TID, on page 7.
- It takes at least 5-10 minutes for changes to be published to elements, and significantly longer if publishing a large data feed.
- Check the action setting for the observable. See View and Manage Observables, on page 31.
- For a list of the other factors that influence the TID action that the system takes, see Factors That Affect the Action Taken, on page 21.
- Elements (managed devices) may not have the threat data you think they have. See About Pausing Publishing, on page 36.

One encounter with a particular threat generates multiple incidents

This can occur if a single indicator is included in multiple sources.

For details, see Handling of Duplicate Indicators, on page 12.
## History for Threat Intelligence Director

<table>
<thead>
<tr>
<th>Feature</th>
<th>Version</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Intelligence Director</td>
<td>6.2.2</td>
<td>Feature introduced: Lets you use threat intelligence from external sources to identify and process threats.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>New screens: A new top-level Intelligence menu with multiple tabs.</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Supported platforms: Firepower Management Center</td>
</tr>
</tbody>
</table>