

# Threat Intelligence Director

The topics in this chapter describe how to configure and use Threat Intelligence Director.


- Secure Firewall Threat Intelligence Director, on page 1
- Requirements and prerequisites for threat intelligence director, on page 4
- Set up Threat Intelligence Director, on page 6
- Analyze Threat Intelligence Director incident and observation data , on page 16
- View and change Threat Intelligence Director configurations , on page 28
- Troubleshoot Threat Intelligence Director, on page 44
- History for Threat Intelligence Director, on page 46


# Secure Firewall Threat Intelligence Director

Secure Firewall Threat Intelligence Director is a threat defense feature that

- operationalizes threat intelligence data to help aggregate intelligence data and configure defensive actions,
- analyzes threats in your environment, and
- supplements other Secure Firewall functionality, offering an additional line of defense against threats.

### Threat intelligence data flow and components

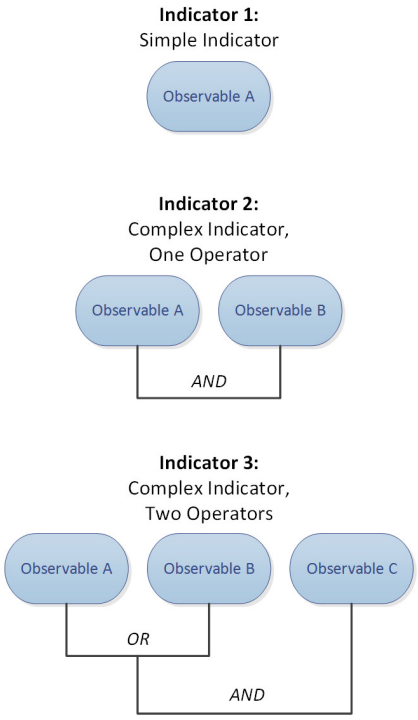
When configured on your hosting platform, Threat Intelligence Director ingests data from threat intelligence *sources* and publishes the data to all configured managed devices (*elements*.) For more information about the hosting platforms and elements supported in this release, refer to Platform, element, and license requirements, on page 4.

Sources contain *indicators*, which contain *observables*. An indicator conveys all characteristics associated with a threat. Individual observables represent specific characteristics associated with the threat, such as an SHA-256 value.

- **Simple indicators**: Contain a single observable
- **Complex indicators**: Contain two or more observables

Observables and the AND/OR operators between them form an indicator's *pattern*, as illustrated in this example.

*Figure 1: Example: indicator patterns*



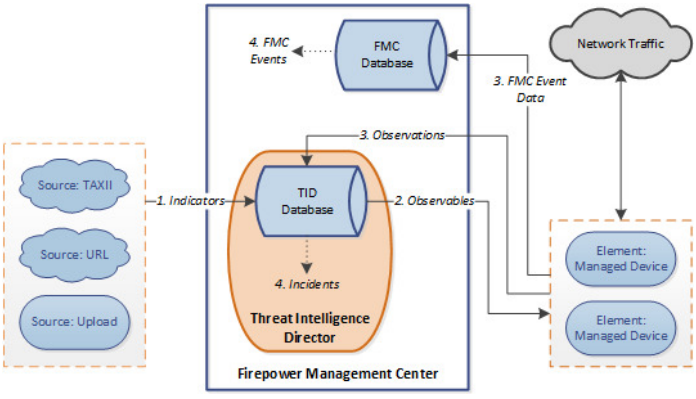

After the observables are published to the elements, the elements monitor traffic and report *observations* to the Firewall Management Center when the system identifies observables in traffic.

The Firewall Management Center collects observations from all elements, evaluates the observations against Threat Intelligence Director 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 16.

This diagram shows data flow in a sample system configuration.

*Figure 2: Firewall Management Center Data Flow*



When a Threat Intelligence Director incident is fully or partially realized, the system takes the configured *action* (monitor, block, partially block, or no action). For details, refer to Factors that affect the action taken, on page 24.

# Threat Intelligence Director and Security Intelligence

Security Intelligence is a threat blocking feature that uses reputation intelligence to quickly block connections to or from IP addresses, URLs, and domains as part of your access control policy.

Security Intelligence uniquely provides access to industry-leading threat intelligence from Talos Intelligence Group. For more information on Security Intelligence, refer to Security intelligence.

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

- **Threat Intelligence Director 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. Threat Intelligence Director also supports filtering by these criteria and adds support for filtering on SHA-256 hash values.
- **Threat Intelligence Director supports additional intelligence ingestion methods**—With both Security Intelligence and Threat Intelligence Director, 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. Threat Intelligence Director provides increased flexibility in managing those flat files. In addition, Threat Intelligence Director can retrieve and ingest intelligence provided in Structured Threat Information eXpression (STIX™) format.
- **Threat Intelligence Director provides granular control of filtering actions**—With Security Intelligence, you can specify filtering criteria by network, URL, or DNS object. Security Intelligence objects, especially lists 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 on individual components of an object. With Threat Intelligence Director, you can configure filtering actions for individual criteria (that is, simple indicators or individual observables).
- **Threat Intelligence Director 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 Threat Intelligence Director, 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 Threat Intelligence Director data to the elements.

For information about what the system does when either Security Intelligence or Threat Intelligence Director could handle a particular incident, refer to Threat Intelligence Director - Firewall Management Center action prioritization , on page 25.

# Performance impact of Threat Intelligence Director

This reference provides information about the performance impacts that may occur when using Threat Intelligence Director with your security infrastructure.

### Secure Firewall 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 Threat Intelligence Director data down to elements.

### Managed device

There is no exceptional performance impact. Threat Intelligence Director impacts performance identically to the Secure Firewall Management Center Security Intelligence feature.

# Requirements and prerequisites for threat intelligence director

Model support

Any

Supported domains

Any

User roles

Admin

Threat Intelligence Director User

### Additional requirements

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

# Platform, element, and license requirements

This reference provides the specific requirements for hosting platforms, managed elements, and licensing necessary to deploy and operate Threat Intelligence Director in your environment.

### Hosting platforms

You can host Threat Intelligence Director on physical and virtual Secure Firewall Management Centers

- running version 6.2.2 or later,
- configured with a minimum of 15 GB of memory, and
- configured with REST API access enabled. See *Enabling REST API Access* in the *Cisco Secure Firewall Management Center Administration Guide*.

### Elements

You can use any Secure Firewall Management Center-managed device as a Threat Intelligence Director element if the device is running version 6.2.2 or later.

### Licensing

To configure the file policies for SHA-256 observable publishing, you need licensed devices with specific requirements:

- For smart licensed devices:
  - IPS License: For IPv4, IPv6, URL, and DNS detection and observables
  - Malware Defense License: For SHA-256 detection and observables
- For classic licensed devices:
  - Protect License: For IPv4, IPv6, URL, and DNS detection and observables
  - Malware License: For SHA-256 detection and observables

For more information, refer to Configure policies to support Threat Intelligence Director, on page 7 and the *Licenses* chapter in the *Cisco Secure Firewall Management Center Administration Guide*.

# Source requirements

This reference provides the specific requirements for different source types including STIX files and flat files that can be used for threat intelligence indicators.

### 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/.

STIX files can include complex indicators.

The maximum size for a STIX file is 40 MB when configured via URL download or file upload. If you have STIX files larger than this, we recommend using a TAXII server.

### Flat file

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

Flat files include only simple indicators, with one observable for each indicator.

Flat files can be up to 500 MB.

Threat Intelligence Director does **not** support:

- Delimiter characters separating observable values, for example, `observable,` are invalid.
- Enclosing characters around observable values, for example, `"observable"`, are 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** Threat Intelligence Director normalizes any URLs that contain port, protocol, or authentication information, and uses the normalized version when detecting indicators. For example, Threat Intelligence Director normalizes any of these 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, Threat Intelligence Director normalizes this URL:

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

as

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

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

  Threat Intelligence Director does not accept CIDR blocks.

- `IPv6`—IPv6 addresses as defined in RFC 4291.

  Threat Intelligence Director does not accept prefix lengths.

## Source content limitations

The system ingests and matches on only the first 1,000 characters of a URL observable.

# Set up Threat Intelligence Director

This task establishes a fully functional Threat Intelligence Director deployment by ensuring proper installation requirements, policy configuration, and intelligence source integration.

Setting up Threat Intelligence Director involves configuring multiple components in a specific sequence to ensure optimal threat intelligence capabilities.

**Note** If you encounter an issue during Threat Intelligence Director configuration or operation, refer to Troubleshoot Threat Intelligence Director, on page 44.

### Procedure

**Step 1** Ensure that your installation meets the requirements for running Threat Intelligence Director.

See Platform, element, and license requirements, on page 4

**Step 2** For each managed device, configure the policies required to support Threat Intelligence Director and deploy those policies to the devices.

See Configure policies to support Threat Intelligence Director, on page 7.

You can configure elements before or after you ingest intelligence data sources.

**Step 3** Configure the intelligence sources that you want Threat Intelligence Director 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 Threat Intelligence Director data at the source, indicator, or observable Level, on page 41.

### What to do next

- Include Threat Intelligence Director in your regularly scheduled backups. See About backing up and restoring Threat Intelligence Director data, on page 15.

  If your Secure Firewall Management Center deployment is a high availability configuration, see also *Firewall Management Center High Availability Disaster Recovery* in the *Cisco Secure Firewall Management Center Administration Guide*.

- (Optional) Grant administrative access to Threat Intelligence Director functionality as desired. See User roles with Threat Intelligence Director access, on page 15 and the *Users* chapter in the *Cisco Secure Firewall Management Center Administration Guide*.

- 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 28.

# Configure policies to support Threat Intelligence Director

This task configures access control policies to publish Threat Intelligence Director data from the Firewall Management Center to your managed devices and maximize observation and event generation.

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

For each managed device that you want to support Threat Intelligence Director, perform these steps to configure the associated access control policy.

Elements that are configured to use Threat Intelligence Director 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 **General Settings** of the access control policy. To navigate to **General Settings**, choose **Policies** > **Access Control heading** > **Access Control**, and click **Edit** > **More** > **Advanced Settings**. This option is enabled by default.

For more information, see General settings.

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

Because Threat Intelligence Director 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 a decryption policy with the access control policy; see Associate prefilter, decryption, and identity policies with an access control.

**Step 4** If you want **SHA-256** observables to generate observations and Secure Firewall 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* in the *Cisco Secure Firewall Management Center Administration Guide*.

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* in the *Cisco Secure Firewall Management Center Administration Guide*.

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

### What to do next

Complete the remaining action items in 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, refer to Source requirements, on page 5.

*Table 1: Options for ingesting data sources*

| Data Type | Ingestion Options |
|---|---|
| STIX | • Ingest STIX feeds from a TAXII server.<br>Refer to Fetch TAXII feeds to use as sources, on page 9<br>• Download STIX data from a URL.<br>Refer to Fetch sources from a URL, on page 10<br>• Upload a STIX file.<br>Refer to Upload a local file to use as a source, on page 12 |
| Flat file | • Download data from a URL.<br>Refer to Fetch sources from a URL, on page 10<br>• Upload a flat file.<br>Refer to Upload a local file to use as a source, on page 12 |

## Fetch TAXII feeds to use as sources

This task establishes TAXII feeds as threat intelligence sources to automatically retrieve STIX data for threat detection and analysis.

TAXII feeds provide structured threat intelligence data that can enhance your security posture by automatically updating threat indicators. If you encounter an issue during TID configuration or operation, see Troubleshoot Threat Intelligence Director, on page 44.

**Before you begin**

Before configuring TAXII feeds, ensure your source meets the requirements in Source requirements, on page 5.

Follow these steps to fetch TAXII feeds to use as sources:

### Procedure

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

**Step 2** Click **Add** (+).

**Step 3** Choose `TAXII` as the **Delivery** method for the source.

**Step 4** Enter information.

- If the host server requires an encrypted connection, configure the **SSL Settings** as described in Configure TLS/SSL settings for a Threat Intelligence Director source, on page 13.
- 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 Threat Intelligence Director actions at the source, indicator, or observable Level, on page 39.

- It may take some time for the list of feeds to load.
- The **Update Every** interval specifies the frequency that Threat Intelligence Director 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**, Threat Intelligence Director deletes:
  - all indicators for the source that are not included in subsequent source updates.
  - all observables not referenced by a surviving indicator.

**Note**
If the source contains no updates for the number of days specified for TTL and the source checksum remains unchanged, downloads are treated as feeds with no updates. For observables to receive a new TTL value, the source must contain a few updates.

**Step 5** 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 Threat Intelligence Director data at the source, indicator, or observable Level, on page 41.

**Step 6** 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 Threat Intelligence Director configuration, return to Set up Threat Intelligence Director, on page 6.

## Fetch sources from a URL

Configure a URL source if you want Threat Intelligence Director to fetch files from a host.

If you encounter an issue during TID configuration or operation, refer to Troubleshoot Threat Intelligence Director, on page 44.

### Before you begin

Follow these steps to fetch sources from a URL:

### Procedure

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

**Step 2** Choose **Integration** > **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 Threat Intelligence Director source, on page 13.
- For Name: To simplify sorting and handling of incidents based on Threat Intelligence Director 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 Threat Intelligence Director actions at the source, indicator, or observable Level, on page 39.
- Set an update frequency that makes sense for how often the data source is updated. For example, if the source is updated three 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, Threat Intelligence Director deletes:
  - all indicators from the source that are not included in subsequent source updates.
  - all observables not referenced by a surviving indicator.

**Note**
If the source contains no updates for the number of days specified for TTL and the source checksum remains unchanged, downloads are treated as feeds with no updates. For observables to receive a new TTL value, the source must contain a few updates.

**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 Threat Intelligence Director data at the source, indicator, or observable Level, on page 41.

**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 Threat Intelligence Director configuration, return to Set up Threat Intelligence Director, on page 6.

## Upload a local file to use as a source

This task allows you to manually upload a local STIX or flat file to create threat intelligence indicators in Threat Intelligence Director.

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

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

When ingesting a flat file, Threat Intelligence Director creates a simple indicator for each observable value in the file.

If you encounter an issue during Threat Intelligence Director configuration or operation, refer to Troubleshoot Threat Intelligence Director, on page 44

### Procedure

**Step 1** Make sure your file meets the requirements in Source requirements, on page 5

**Step 2** Choose **Integration** > **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 Threat Intelligence Director 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 Threat Intelligence Director actions at the source, indicator, or observable Level, on page 39.

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

**Note**
If the source contains no updates for the number of days specified for TTL and the source checksum remains unchanged, downloads are treated as feeds with no updates. For observables to receive a new TTL value, the source must contain a few updates.

**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 Threat Intelligence Director data at the source, indicator, or observable Level, on page 41.

**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 Threat Intelligence Director configuration, return to Set up Threat Intelligence Director, on page 6.

## Handling of duplicate indicators

If a single indicator is included in multiple sources:

Each instance of the indicator generates an incident, so one encounter with a particular threat may generate multiple incidents.

To avoid future duplicate incidents, pause publishing of all but one of the duplicated indicators. Refer to Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 41.

## Configure TLS/SSL settings for a Threat Intelligence Director source

Configure TLS/SSL settings to establish secure encrypted connections with host servers that require certificate-based authentication.

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

**Before you begin**

- Configure a `TAXII` or `URL` source, as described in Fetch TAXII feeds to use as sources, on page 9 or Fetch sources from a URL, on page 10.

Follow these steps to configure TLS/SSL settings for a Threat Intelligence Director source:

### Procedure

**Step 1** In the **Edit Source** dialog box, 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`—Threat Intelligence Director requires the source **URL** to match the hostname provided in the server certificate.

  If the hostname includes a wildcard, TID cannot match more than one subdomain.

- `Browser Compatible`—Threat Intelligence Director requires the source **URL** to match the hostname provided in the server certificate.

  If the hostname includes a wildcard, TID matches all subdomains.

- `Allow All`—Threat Intelligence Director does not require 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, Threat Intelligence Director 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 9
  - Fetch sources from a URL, on page 10

# User roles with Threat Intelligence Director access

You can use Firewall Management Center user accounts to access the Threat Intelligence Director menus and pages.

The user roles that can access Threat Intelligence Director menus and pages are:

- 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 Firewall Management Center user accounts with the **Admin**, **Access Admin**, or **Network Admin** user role to enable or disable Threat Intelligence Director in your access control policies.

For more information about user accounts, refer to the *Users for the Firewall Management Center* chapter in the *Cisco Secure Firewall Management Center Administration Guide*.

# About backing up and restoring Threat Intelligence Director data

You can use the Firewall Management Center to back up and restore all of the data needed for Threat Intelligence Director: Element data, security intelligence events, connection events, Threat Intelligence Director configurations, and Threat Intelligence Director data. For more information, refer to the *Backup/Restore* chapter in the *Cisco Secure Firewall Management Center Administration Guide*.

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

Before you attempt to restore the Threat Intelligence Director data on the active Firewall Management Center, pause synchronization on the active peer. For more information, see *Pausing Communication Between Paired Firepower Management Centers* in the *Cisco Secure Firewall Management Center Administration Guide*.

***Table 2: Threat Intelligence Director-Related Backup and Restore File Contents***

| Threat Intelligence Director-Related File Contents | Backup Selection | Restore Selection |
|---|---|---|
| Element data | **Back Up Configuration** | **Restore Configuration Data** |

| Threat Intelligence Director-Related File Contents | Backup Selection | Restore Selection |
|---|---|---|
| Secure Firewall Management Center event data | **Back Up Events** | **Restore Event Data** |
| Threat Intelligence Director configurations and Threat Intelligence Director data | **Back Up Threat Intelligence Director** | **Restore Threat Intelligence Director Data** |

# Analyze Threat Intelligence Director incident and observation data

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

## Observation and incident generation

Observation and incident generation is a threat detection process that

- generates an incident when the first observable for an indicator is seen in traffic,
- fully realizes simple indicators after a single observation,
- partially realizes complex indicators until additional observations fulfill their pattern, and
- triggers new incidents for subsequent observations after an incident is fully realized.

### How observation and incident generation works

Threat Intelligence Director 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, Threat Intelligence Director ignores unsupported and invalid objects and observables on the Do Not Block list.

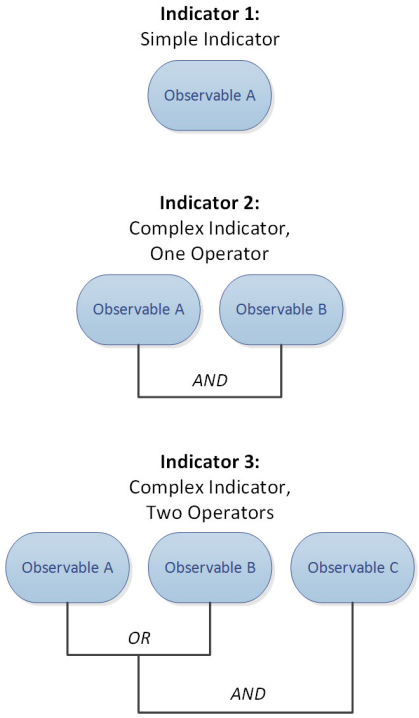
After an incident is fully realized, subsequent observations trigger new incidents.

If a particular indicator exists in multiple sources, you may see duplicate incidents. For more information, see Troubleshoot Threat Intelligence Director, on page 44.

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.

### Indicator pattern processing example

***Figure 3: Indicator patterns***




If Threat Intelligence Director 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, Threat Intelligence Director:
   - 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, Threat Intelligence Director:
   - 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, Threat Intelligence Director:
   - 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, Threat Intelligence Director:
   - Generates a new fully-realized incident for Indicator 1.
   - Generates new partially-realized incidents for Indicator 2 and Indicator 3.

# View and manage incidents

This task allows you to view and manage incidents to monitor security threats and track investigation progress.

The Incidents page displays summary information for up to 1.1 million of the most recent Threat Intelligence Director incidents. Refer to Incident summary information, on page 19.

**Before you begin**

- Configure the feature as described in Set up Threat Intelligence Director, on page 6.
- Understand observation and incident generation, as described in Observation and incident generation, on page 16.

Follow these steps to view and manage incidents:

## Procedure

**Step 1** Choose **Integration** > **Intelligence** > **Incidents**.

**Step 2** View your incidents:

- Click **Filter** ( ) to add one or more filters. The default filter duration is six hours. For more information, refer to Filter Threat Intelligence Director data in table views, on page 36.
- To view the date and time an incident was last updated by Threat Intelligence Director, 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. Refer to View and manage indicators, on page 32.

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

For an explanation of the details you see, refer to Incident details, on page 19.

- 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:

To maximize consistency and usefulness of the options listed, 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 Threat Intelligence Director incidents.

***Table 3: Incident summary information***

| Field | Description |
|---|---|
| **Last Updated** | 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. |
| **Incident ID** | The unique identifier for the incident. This ID has the format:<br>`<type>-<date>-<number>`<br>• `<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`.<br>• `<date>`—The date (*yyyymmdd*) on which the incident was created.<br>• `<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.<br>Next to the identifier, the system displays an icon that indicates whether the incident is **Partially Realized** or **Fully Realized**. For more information, refer to Observation and incident generation, on page 16. |
| **Indicator Name** | The name of the indicator involved in the incident. To view additional information about the indicator, click the value in this column. Refer to View and manage indicators, on page 32. |
| **Type** | The type of indicator involved in the incident.<br>• Indicators that contain a single observable display the data type (`URL`, `SHA-256`, etc.)<br>• 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, refer to Incident details, on page 19. |
| **Status** | The status of your investigation into the incident. For more information, refer to Incident details, on page 19. |
| **Delete** ( ) | Clicking this icon permanently deletes the incident. |

## Incident details

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

• Incident details: Basic information, on page 20
• Incident details: Indicators and observations, on page 21

## Incident details: Basic information

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

***Table 4: Basic incident information fields***

| Field | Description |
|---|---|
| **Partially-Realized** *IncidentID* or **Fully-Realized** *IncidentID* | An icon indicating the status of the incident (partially-realized or fully-realized), as well as the unique identifier for the incident.<br>**Note**<br>When determining the status of an incident, Threat Intelligence Director 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.<br>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.<br>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`.<br>`Partially Blocked` indicates that the incident contained both `Monitored` and `Blocked` observations.<br>**Note**<br>The **Action Taken** indicates the action taken by the system, not necessarily the action selected in Threat Intelligence Director. For more information, see Threat Intelligence Director - Firewall Management Center action prioritization , on page 25. |
| **Category** | A custom, optional tag or keyword that you manually add to the incident. |

| Field | Description |
|---|---|
| **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.<br>This field is optional. Depending on the needs of your organization, consider using the status values as follows:<br>• `New`—The incident requires investigation, but you have not started investigating.<br>• `Open`—You are currently investigating the incident.<br>• `Closed`—You investigated the incident and took action.<br>• `Rejected`—You investigated the incident and determined there was no action to take. |
| **Delete** ( ) | Clicking this icon permanently deletes this incident. |

## Incident details: Indicators and observations

The lower section of the Incident Details window provides an in-depth view of 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***

| Field | Description |
|---|---|
| **Description** | The indicator description provided by the source. |
| **SOURCE** | The source that contained the indicator. Click this link to access full source details. |
| **Expires** | The date and time the incident will expire, based on the source's **TTL** value. |
| **Action** | The action associated with the indicator. For more information, see Edit Threat Intelligence Director actions at the source, indicator, or observable Level, on page 39. |
| **Publish** | The publish setting for the indicator. For more information, see Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 41. |
| **Download STIX** | If the source type is **STIX**, click this button to download the STIX file. |

### 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 **Add to Do-Not-Block List** 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 Adding Threat Intelligence Director observables to the Do Not Block list, on page 43.
- 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, Threat Intelligence Director 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 these fields:

***Table 6: Observation detail fields***

| Field | Description |
|---|---|
| **SOURCE** | The source IP address and port for the traffic that triggered the observation. |

| Field | Description |
|---|---|
| **DESTINATION** | The destination IP address and port for the traffic that triggered the observation. |
| **ADDITIONAL INFORMATION** | DNS and authentication information related to the traffic that triggered the observation. |
| **Events** | This clickable link displays if the observation generated connection, security intelligence, file, or malware events. Click the link to view the events in the Secure Firewall Management Center event table; see *Cisco Secure Firewall Management Center Administration Guide*. |

# View events for a Threat Intelligence Director observation

View events associated with Threat Intelligence Director observations to analyze security incidents and understand system actions taken.

For more information about the Secure Firewall Management Center events that Threat Intelligence Director observations generate, refer to Threat Intelligence Director observations in Secure Firewall Management Center events, on page 24.

The system action logged for Threat Intelligence Director-related events can vary, depending on the interaction of Threat Intelligence Director and other Secure Firewall Management Center features. For more information about action prioritization, refer to Threat Intelligence Director - Firewall Management Center action prioritization , on page 25.

**Before you begin**

- Configure the feature as described in Set up Threat Intelligence Director, on page 6.
- Confirm that you enabled event logging required for Threat Intelligence Director in your access control policy, as described in Configure policies to support Threat Intelligence Director, on page 7.

**Procedure**

**Step 1** Choose **Integration** > **Intelligence** > **Incidents**.

**Step 2** Click the **Incident ID** value for the incident.

**Step 3** Click the observation in the **Indicator** section to display the observation box.

**Step 4** Expand the observation box by clicking the arrow in the upper-left corner of the box.

**Step 5** Click the **Events** link in the observation information. For more information on the Security Intelligence display, refer to the *Connection and Security Intelligence Events* chapter in the *Cisco Secure Firewall Management Center Administration Guide*.

## Threat Intelligence Director observations in Secure Firewall Management Center events

If you fully configure your access control policy, Threat Intelligence Director observations generate specific Secure Firewall Management Center events.

***Table 7: Secure Firewall Management Center Events Generated by Observations***

| Observation Content | Connection Events Table | Security Intelligence Events Table | File Events Table | Malware Events Table |
|---|---|---|---|---|
| **SHA-256** | Yes | No | Yes | Yes, if disposition is Malware or Custom Detection. |
| **Domain Name**, **URL**, or **IPv4/IPv6** | Yes<br>Threat Intelligence Director-related connection events are identified with a Threat Intelligence Director-related **Security Intelligence Category** value. | Yes<br>Threat Intelligence Director-related security intelligence events are identified with a Threat Intelligence Director-related **Security Intelligence Category** value. | No | No |

# Factors that affect the action taken

Factors that affect the action taken are system conditions that determine when the system takes action and what action the system takes when it detects traffic that matches a Threat Intelligence Director observable.

### Action determination factors

The system considers these factors when determining actions:

- Features like Security Intelligence take action before Threat Intelligence Director does. For details, refer to Threat Intelligence Director - Firewall Management Center action prioritization , on page 25.
- 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 Structured Threat Information eXpression (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. Refer to Inheritance in Threat Intelligence Director configurations, on page 37 and Edit Threat Intelligence Director actions at the source, indicator, or observable Level, on page 39.
- Traffic that might otherwise be actionable might be on a Do Not Block list. For details, refer to Add Threat Intelligence Director observables to a Do Not Block list, on page 43.
- 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.

- The actions the system takes are affected when publishing is paused. Refer to Pausing publishing, on page 40 and Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 41.
- Pausing the Threat Intelligence Director feature prevents all actions. After you resume the feature, actionable data may be different from before. For details, refer to Pause Threat Intelligence Director and purge Threat Intelligence Director data from elements, on page 41.

# Threat Intelligence Director - Firewall Management Center action prioritization

If Threat Intelligence Director observable actions conflict with Firewall Management Center policy actions, the system prioritizes actions as follows:

- Security Intelligence Do Not Block
- TID Block
- Security Intelligence Block
- TID Monitor
- Security Intelligence Monitor

Specifically:

***Table 8: Threat Intelligence Director URL Observable Action vs. Security Intelligence Action***

| Setting: Security Intelligence Action | Setting: Threat Intelligence Director Observable Action | Threat Intelligence Director Incidents Field: Action Taken | Security Intelligence Events Fields: | | |
|---|---|---|---|---|---|
| | | | Action | Security Intelligence Category | Reason |
| `Do Not Block` | `Monitor` or `Block` | No TID incident | No Security Intelligence event | | |
| `Block` | `Monitor` | `Blocked` | `Block` | as determined by system analysis; see Security intelligence categories | `URL Block` |
| | `Block` | `Blocked` | `Block` | `TID URL Block` | `URL Block` |
| `Monitor` | `Monitor` | `Monitored` | Determined by access control rules processed after Security Intelligence and TID. | `TID URL Monitor` | `URL Monitor` |
| | `Block` | `Blocked` | `Block` | `TID URL Block` | `URL Block` |

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

| Setting: Security Intelligence Action | Setting: Threat Intelligence Director Observable Action | Threat Intelligence Director Incidents Field: Action Taken | Security Intelligence Events Fields: | | |
|---|---|---|---|---|---|
| | | | Action | Security Intelligence Category | Reason |
| Do Not Block | Monitor or Block | No TID incident | No Security Intelligence event | | |
| Block | Monitor | No TID incident | Block | as determined by system analysis; see Security intelligence categories | IP Block |
| | Block | Blocked | Block | TID IPv4 Block<br>TID IPv6 Block | IP Block |
| Monitor | Monitor | Monitored | Determined by access control rules processed after Security Intelligence and TID. | TID IPv4 Monitor<br>TID IPv6 Monitor | IP Monitor |
| | Block | Blocked | Block | TID IPv4 Block<br>TID IPv6 Block | IP Block |

*Table 10: Threat Intelligence Director Domain Name Observable Action vs. DNS Policy Action*

| Setting: DNS Policy Action | Setting: Threat Intelligence Director Domain Name Observable Action | Threat Intelligence Director Incidents Field: Action Taken | Security Intelligence Events Fields: | | |
|---|---|---|---|---|---|
| | | | Action | Security Intelligence Category | Reason |
| Do Not Block | Monitor or Block | No TID incident | No Security Intelligence event | | |
| Drop, Domain Not Found<br>Sinkhole—Log<br>Sinkhole—Block and Log | Monitor | Blocked | Block | as determined by system analysis; see Security intelligence categories | DNS Block |
| | Block | Blocked | Block | TID Domain Name Block | DNS Block |

| Setting: DNS Policy Action | Setting: Threat Intelligence Director Domain Name Observable Action | Threat Intelligence Director Incidents Field: Action Taken | Security Intelligence Events Fields: | | |
|---|---|---|---|---|---|
| | | | Action | Security Intelligence Category | Reason |
| Monitor | Monitor | Monitored | Determined by access control rules processed after Security Intelligence and TID. | TID Domain Name Monitor | DNS Monitor |
| | Block | Blocked | Block | TID Domain Name Block | DNS Block |

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

| File Disposition | Threat Intelligence Director SHA-256 Observable Action | Action Taken in Threat Intelligence Director Incidents | Action in File Events | Action in Malware Events |
|---|---|---|---|---|
| Clean | Monitor or Block | Monitored | Malware Cloud Lookup | n/a |
| Malware | Monitor or Block | Monitored | Malware Cloud Lookup | n/a |
| Custom | Monitor or Block | Monitored | • Malware Cloud Lookup , if SHA-256 is not in a custom detection list.<br>• Custom Detection , if SHA-256 is in a custom detection list. | • Malware Cloud Lookup , if SHA-256 is not in a custom detection list.<br>• Custom Detection , if SHA-256 is in a custom detection list. |
| Unknown | Monitor or Block | Monitored | Malware Cloud Lookup | n/a |

**Note** Threat Intelligence Director matching occurs before the system sends a file for dynamic analysis.

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

| File Disposition | Threat Intelligence Director SHA-256 Observable Action | Action Taken in Threat Intelligence Director Incidents | Action in File Events | Action in Malware Events |
|---|---|---|---|---|
| Clean or Unknown | Monitor | Monitored | Malware Cloud Lookup | n/a |
| | Block | Blocked | • TID Block, if SHA-256 is not in a custom detection list.<br>Modified file disposition is Custom.<br>• Custom Detection Block, if SHA-256 is in a custom detection list. | TID Block<br>Modified file disposition is Custom. |
| Malware or Custom | Monitor | Blocked | Block Malware | Block Malware |
| | Block | Blocked | • TID Block, if SHA-256 is not in a custom detection list.<br>Modified file disposition is Custom.<br>• Custom Detection Block, if SHA-256 is in a custom detection list. | TID Block<br>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 Threat Intelligence Director status of elements (managed devices)

This task allows you to monitor the status of managed devices and confirm that Threat Intelligence Director is properly enabled on elements.

All devices that are registered to the Firewall Management Center as managed devices appear automatically on the Elements page. All properly configured elements (as specified in Configure policies to support Threat Intelligence Director, on page 7) will receive all currently published observables, including those ingested before the element was added.

### Procedure

**Step 1** Choose **Integration** > **Intelligence** > **Elements**.

**Step 2** To see whether the element is connected and Threat Intelligence Director is enabled, hover over the icon beside the element name.

**Note**
After deploying, it may take up to five minutes for information on this page to update, including the applied access control policy and whether TID is enabled.

# View and manage sources

View summary information about all configured sources and manage their settings, including actions, publish status, updates, and deletion.

The Sources page displays summary information about all configured sources. Refer to Source summary information, on page 30.

### Procedure

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

**Step 2** View your sources.

- To filter the sources displayed on the page, click **Filter** (). For more information, refer to Filter Threat Intelligence Director data in table views, on page 36.
- To view detailed ingestion status, hover the cursor over the text in the **Status** column. For more information, refer to Source status details, on page 31.

**Step 3** Manage your sources.

- To edit the **Action** setting, refer to Edit Threat Intelligence Director actions at the source, indicator, or observable Level, on page 39. 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, refer to Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 41.

- To pause or resume Threat Intelligence Director 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** ( ). The Delete option is unavailable if the source is still processing. Removing a source removes 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. This reference 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. Refer to Options for ingesting data sources, on page 8.

***Table 13: Sources summary information***

| Field | Description |
|---|---|
| **Name** | The source name. |
| **Type** | The data format of the source, such as**STIX** or **Flat File**. |
| **Delivery** | The method Threat Intelligence Director uses to retrieve the source. |
| **Action** | The action (**Block** or **Monitor**) that the system is configured to perform on traffic matching the data contained within this source.<br>For more information about Threat Intelligence Director actions, including availability, inheritance, and overriding inheritance, refer to Factors that affect the action taken, on page 24. |
| **Publish** | **On** or **Off** toggle specifying whether Threat Intelligence Director publishes data from the source to registered elements (managed devices configured to support Threat Intelligence Director).<br>Indicators can inherit **Publish** settings from a parent source, and observables can inherit **Publish** settings from a parent indicator. For more information, refer to Inheritance in Threat Intelligence Director configurations, on page 37. |
| **Last Updated** | The date and time Threat Intelligence Director last updated the source. |

| Field | Description |
|---|---|
| **Status** | The current status of the source:<br>• **New**—The source is newly created.<br>• **Scheduled**—The initial download or subsequent update is scheduled, but not yet in progress.<br>• **Downloading**—Threat Intelligence Director is performing the initial download or update refresh.<br>• **Parsing** or **Processing**—Threat Intelligence Director is ingesting the source.<br>• **Completed**—Threat Intelligence Director finished ingesting the source.<br>• **Completed with Errors**—Threat Intelligence Director finished ingesting the source, but some observables are unsupported or invalid.<br>• **Error**—Threat Intelligence Director experienced a problem. If the source is a TAXII or URL source with an **Update Frequency** specified, and updates are not paused, Threat Intelligence Director retries on the next scheduled update.<br>Refresh the page to update the status. |
| **Edit** ( ) | Clicking this icon allows you to edit settings for the source. |
| **Delete** ( ) | Clicking this icon permanently deletes the source. |

## Source status details

When you hover over the **Status** value of a source in the Sources summary page, Threat Intelligence Director provides additional details about the source status.

| Data | Description |
|---|---|
| **Status Message** | Briefly describes the current status of the source. |
| **Last Updated** | Specifies the date and time Threat Intelligence Director last updated the source. |
| **Next Update** | For TAXII and URL sources, this value specifies when Threat Intelligence Director will update the source next. |

| Data | Description |
|---|---|
| **Indicators** | Specifies indicator counts.<br>• **Consumed**—The number of indicators Threat Intelligence Director processed during the most recent source update. This number represents all indicators contained in the update, regardless of whether they were ingested or discarded.<br>• **Discarded**—The number of malformed indicators that the system did not add to Threat Intelligence Director during the most recent update.<br>**Note**<br>For `TAXII` sources, Threat Intelligence Director 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, Threat Intelligence Director provides only the **Last Update** count, because updates from those sources replace the existing data set entirely.<br>If all observables of an indicator are **Invalid**, Threat Intelligence Director discards the indicator. |
| **Observables** | Specifies observable counts.<br>• **Consumed**—The number of observables Threat Intelligence Director processed during the most recent source update. This number represents all observables contained in the update, regardless of whether they were ingested or discarded.<br>• **Unsupported**—The number of unsupported observables that the system did not add to Threat Intelligence Director during the most recent update.<br>For more information about supported observable types, see information about content types in Source requirements, on page 5.<br>• **Invalid**—The number of invalid observables that the system did not add to Threat Intelligence Director during the most recent update.<br>An observable is invalid if it is improperly constructed. For example, `10.10.10.10.123` is not a valid IPv4 address.<br>**Note**<br>For `TAXII` sources, Threat Intelligence Director 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, Threat Intelligence Director provides only the **Last Update** count, because updates from those sources replace the existing data set entirely. |

# View and manage indicators

This task enables you to view current indicators and manage their configuration settings including actions and publish status.

Indicators are generated automatically from ingested sources. For more information about the contents of this page, refer to Indicator summary information, on page 33.

### Procedure

**Step 1** Choose **Integration** > **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, refer to Filter Threat Intelligence Director data in table views, on page 36.
- To view additional details about an indicator, including associated observables, click the indicator name. For more information, refer to Indicator details, on page 34.
- 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 realized or partially realized.
- To determine whether Threat Intelligence Director finished ingesting an indicator from the source, view the **Status** column.

**Step 4** Manage your current indicators.

- To edit the **Action**, refer to Edit Threat Intelligence Director actions at the source, indicator, or observable Level, on page 39. If an action is fixed, that is the only supported action for the source **Type**.
- To edit the **Publish** setting, refer to Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 41.
- To add one or more observables for an indicator to the Do Not Block list, click the indicator name to access the Indicator Details page. For more information, refer to Adding Threat Intelligence Director observables to the Do Not Block list, on page 43.

## Indicator summary information

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

***Table 14: Indicators summary information***

| Field | Description |
|---|---|
| **Type** | • Indicators that have a single observable list the data type of that observable (URL, SHA-256, etc.)<br>• Indicators that have two or more observables are listed as **Complex**.<br>Hover over the type to see the specific observable. |
| **Name** | The indicator name. |
| **Source** | The source that contained the indicator (the parent source). |

| Field | Description |
|---|---|
| **Incidents** | Information about any incidents associated with the indicator:<br>• an icon specifying whether the incident is **Partially** or **Fully** realized<br>• the number of incidents associated with the indicator |
| **Action** | The action associated with the indicator. For more information, refer to Edit Threat Intelligence Director actions at the source, indicator, or observable Level, on page 39.<br>Indicators can inherit **Action** settings from a parent source, and observables can inherit **Action** settings from a parent indicator. For more information, refer to Inheritance in Threat Intelligence Director configurations, on page 37. |
| **Publish** | The publish setting for the indicator. For more information, refer to Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 41.<br>Indicators can inherit **Publish** settings from a parent source, and observables can inherit **Publish** settings from a parent indicator. For more information, refer to Inheritance in Threat Intelligence Director configurations, on page 37. |
| **Last Updated** | The date and time Threat Intelligence Director last updated the indicator. |
| **Status** | The current status of the indicator:<br>• **Pending**—Threat Intelligence Director is ingesting the observables of the indicator.<br>• **Completed**—Threat Intelligence Director successfully ingested all observables for the indicator.<br>• **Completed With Errors**—Threat Intelligence Director 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***

| Field | Description |
|---|---|
| **Name** | The indicator name. |
| **Description** | The indicator description provided by the source. |
| **Source** | The source that contained the indicator. |
| **Expires** | The date and time the indicator will expire, based on the source's **TTL** value. |
| **Action** | The action associated with the indicator. For more information, refer to Edit Threat Intelligence Director actions at the source, indicator, or observable Level, on page 39.<br>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 Threat Intelligence Director configurations, on page 37. |

| Field | Description |
|---|---|
| **Publish** | The publish setting for the indicator. For more information, refer to Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 41.<br><br>Indicators can inherit the **Publish** setting from a parent source, and observables can inherit the **Publish** setting from a parent indicator. For more information, refer to Inheritance in Threat Intelligence Director configurations, on page 37. |
| **Indicator Pattern** | 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.<br><br>Optionally, click the **Add to Do-Not-Block List** button to add an observable to the Do Not Block list. For more information, refer to Adding Threat Intelligence Director observables to the Do Not Block list, on page 43. |

# View and manage observables

This task allows you to view all successfully ingested observables and perform management operations such as editing actions, modifying publish settings, and adding observables to the Do Not Block list.

The Observables page displays all successfully ingested observables. Refer to Observable summary information, on page 36.

**Before you begin**

- Configure one or more sources as described in Fetch TAXII feeds to use as sources, on page 9, Fetch sources from a URL, on page 10, or Upload a local file to use as a source, on page 12.

Follow these steps to view and manage observables:

**Procedure**

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

**Step 2** Click **Observables**.

**Step 3** View your current observables.

- To filter the observables displayed on the page, click **Filter** (). For more information, refer to Filter Threat Intelligence Director data in table views, on page 36.
- 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, refer to View and manage indicators, on page 32.

**Step 4** Manage your current observables.

- To edit the **Action**, refer to Edit Threat Intelligence Director actions at the source, indicator, or observable Level, on page 39.

- To edit the **Publish** setting for an observable, refer to Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 41.
- To change the expiration date for an observable, modify the **TTL** for the parent source. For more information, refer to View and manage sources, on page 29.
- To add an observable to the Do Not Block list, click the **Add to Do-Not-Block List** button. For more information, refer to Adding Threat Intelligence Director observables to the Do Not Block list, on page 43.

## Observable summary information

The Observables page displays summary information for all ingested observables.

***Table 16: Observables summary information***

| Field | Description |
|---|---|
| **Type** | The type of observable data: `SHA-256`, `Domain`, `URL`, `IPv4`, or `IPv6`. |
| **Value** | The data that comprises the observable. |
| **Indicators** | The number of parent indicators containing the observable. |
| **Action** | The action configured for the observable. For more information, refer to Edit Threat Intelligence Director actions at the source, indicator, or observable Level, on page 39.<br>Indicators can inherit **Action** settings from a parent source, and observables can inherit **Action** settings from a parent indicator. For more information, refer to Inheritance in Threat Intelligence Director configurations, on page 37. |
| **Publish** | The publish setting for the observable. Refer to Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 41.<br>Indicators can inherit **Publish** settings from a parent source, and observables can inherit **Publish** settings from a parent indicator. For more information, refer to Inheritance in Threat Intelligence Director configurations, on page 37. |
| **Updated At** | The date and time Threat Intelligence Director last updated the observable. |
| **Expires** | The date that the observable will be automatically purged from Threat Intelligence Director based on **TTL** for the parent indicator. |
| **Add to Do-Not-Block List** button | Clicking this button adds the observable to the Do Not Block list. Refer to Adding Threat Intelligence Director observables to the Do Not Block list, on page 43. |

# Filter Threat Intelligence Director data in table views

Filter table views to narrow down and display only the Threat Intelligence Director data that matches your specific criteria.

Use this procedure when you need to focus on specific data within Threat Intelligence Director table views by applying attribute-based filters.

**Procedure**

**Step 1** Choose one of these Threat Intelligence Director table views.

- **Integration** > **Intelligence** > **Incidents**
- **Integration** > **Intelligence** > **Sources**
- **Integration** > **Intelligence** > **Sources**, and click **Indicators**
- **Integration** > **Intelligence** > **Sources**, and click **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 Threat Intelligence Director configurations

Inheritance in Threat Intelligence Director configurations is a hierarchical configuration mechanism that

- creates indicators and observables as child objects when Threat Intelligence Director ingests intelligence data from a source,
- ensures child objects automatically inherit **Action** and **Publish** settings from their parent configuration on creation, and
- maintains parent-child relationships where indicators inherit from source configurations and observables inherit from parent indicators.

### Inheritance relationships

The inheritance hierarchy follows these parent-child relationships:

- 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 indicators. An observable can have multiple parent indicators.

For more information, refer to:

• Inheritance of TID settings from multiple parents, on page 38
• Overriding inherited TID settings, on page 38

## 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:

| Setting | SourceA | IndicatorA | ObservableA |
|---|---|---|---|
| **Action** | `Block` | `Block` | `Block` |
| **Publish** | `Off` | `Off` | `Off` |

If SourceB later contributes IndicatorB, which also includes ObservableA, the system modifies ObservableA in this way:

| Setting | SourceB | IndicatorB | ObservableA |
|---|---|---|---|
| **Action** | `Monitor` | `Monitor` | `Block` (inherited from IndicatorA) |
| **Publish** | `On` | `On` | `On` (inherited from IndicatorB) |

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.

## Overriding inherited TID settings

An overriding inherited TID setting is a configuration change that

- changes the inherited setting at the child level,
- retains the child object setting despite changes to parent objects, and
- breaks automatic cascading of setting changes from parent to child for that specific setting.

### Override behavior and inheritance

To override an inherited setting, change the setting at the child level. Refer to Edit Threat Intelligence Director actions at the source, indicator, or observable Level, on page 39 and Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 41. After you override an inherited setting, the child object retains that setting despite changes to the parent object(s).

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.

### Override inheritance scenarios

For example, you might start with these original settings, with no overrides set:

| Setting | SourceA | IndicatorA | ObservableA1 | ObservableA2 |
|---|---|---|---|---|
| **Publish** | Off | Off | Off | Off |

If you override the setting for IndicatorA, the settings would be these:

| Setting | SourceA | IndicatorA | ObservableA1 | ObservableA2 |
|---|---|---|---|---|
| **Publish** | Off | On | On | On |

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:

| Setting | SourceA | IndicatorA | ObservableA1 | ObservableA2 |
|---|---|---|---|---|
| **Publish** | Off | On | Off | On |

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.

# Edit Threat Intelligence Director actions at the source, indicator, or observable Level

Configure action settings at the source, indicator, or observable level to control how threat intelligence data is handled within your security policies.

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, refer to Inheritance in Threat Intelligence Director configurations, on page 37.

You may also want to review other Factors that affect the action taken, on page 24.

### Procedure

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

- **Integration** > **Intelligence** > **Sources**

**Note**

Threat Intelligence Director 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.

- **Integration** > **Intelligence** > **Sources**, and click **Indicators**

  **Note**
  Threat Intelligence Director does not support blocking complex indicators. Instead, block individual observables within the complex indicator.

- **Integration** > **Intelligence** > **Sources**, and click **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.

# Pausing publishing

- If you pause publishing at the feature level, the system purges all Threat Intelligence Director observables stored on your elements. This means that Threat Intelligence Director 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 Threat Intelligence Director observables from your elements, preventing them from matching traffic.
- If you pause publication for a parent, the system pauses all children. For example, pausing publishing at the source level pauses publishing for all its indicators; pausing publishing at the indicator level pauses 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 Threat Intelligence Director configurations, on page 37.
- 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 Adding Threat Intelligence Director observables to the Do Not Block list, on page 43.
- If you have specified a publish or 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 42.
- The option on the Sources page to pause updates is not related to publishing data to elements; it applies to updating sources on the Firewall Management Center from feeds.

# Pause Threat Intelligence Director and purge Threat Intelligence Director data from elements

This task allows you to pause Threat Intelligence Director operations across all elements and purge existing data when necessary.

**Caution** This setting pauses publishing to all elements, purges all Threat Intelligence Director observables stored on your elements, and stops inspecting traffic using the Threat Intelligence Director feature.

To disable observables at a more granular level, see Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 41.

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 **Integration** > **Intelligence** > **Settings**.

**Step 2** Click **Pause**.

#### What to do next

When you are ready to resume synchronizing Threat Intelligence Director 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 Threat Intelligence Director data at the source, indicator, or observable Level

This task allows you to control the publishing of Threat Intelligence Director data by pausing or enabling publication 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 Threat Intelligence Director observables at once from your devices (elements), see Pause Threat Intelligence Director and purge Threat Intelligence Director data from elements, on page 41.

### Before you begin

Before pausing publishing, review the ramifications described in Pausing publishing, on page 40.

### Procedure

**Step 1** Choose any of these options.

- **Integration** > **Intelligence** > **Sources**
- **Integration** > **Intelligence** > **Sources**, and click **Indicators**
- **Integration** > **Intelligence** > **Sources**, and click **Observables**

**Step 2** Locate the **Publish Slider** () 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 ten 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. Refer to Modify the observable publication frequency, on page 42.

# Modify the observable publication frequency

This task allows you to set a custom publication interval for observables to TID elements, replacing the default 5-minute interval.

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. Refer to Pause or publish Threat Intelligence Director data at the source, indicator, or observable Level, on page 41.

Follow these steps to modify the observable publication frequency:

### Procedure

**Step 1** Choose **Objects** > **Object Management** > **Security Intelligence** > **Network Lists and Feeds**.

**Step 2** Click **Edit** () next to the **Cisco-TID-Feed**.

**Step 3** 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 4** Click **Save**.

# Adding Threat Intelligence Director observables to the Do Not Block list

A Do Not Block list is a security feature that

- exempts observables in indicators from specified actions, allowing traffic to pass without monitoring or blocking,
- ignores listed observables when evaluating traffic in complex indicators while still evaluating other observables, and
- takes precedence over action settings regardless of whether they are inherited or override values.

### Do not block list behavior

The Do Not Block list affects simple and complex indicators differently:

- Simple indicators: If you add an observable to the Do Not Block list, traffic passes without monitoring or blocking.
- Complex indicators: Threat Intelligence Director ignores observables on the Do Not Block list when evaluating traffic, but other observables in that indicator are still evaluated.

In a complex indicator that includes Observable 1 and Observable 2 linked by the AND operator:

- If you add Observable 1 to a Do Not Block list, Threat Intelligence Director generates a fully realized incident when Observable 2 is seen.
- If you disable publishing of Observable 1 instead of adding it to the Do Not Block list, Threat Intelligence Director generates a partially-realized incident when Observable 2 is seen.

**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 Threat Intelligence Director observables to a Do Not Block list

Adding observables to a Do Not Block list allows you to exempt specific items from being blocked, ensuring legitimate traffic is not inadvertently restricted.

For detailed information about using Do Not Block lists, refer to Adding Threat Intelligence Director observables to the Do Not Block list, on page 43.

**Tip** An "Add to Do Not Block List" button ( ) 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** Choose **Integration** > **Intelligence** > **Sources**, and click **Observables**.

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

**Step 3** Click (**Add to Do-Not-Block List**) 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** Choose **Integration** > **Intelligence** > **Sources** , and click **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

This reference describes possible solutions and mitigations for common Threat Intelligence Director 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 **Integration** > **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 Threat Intelligence Director can retrieve a new certificate. For more information, refer to Configure TLS/SSL settings for a Threat Intelligence Director source, on page 13.

### "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.

### Threat Intelligence Director 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 Threat Intelligence Director table views:

- Check your table filter and consider expanding the time window for the **Last Updated** filter attribute. Refer to Filter Threat Intelligence Director data in table views, on page 36.
- Verify that you correctly configured your sources. Refer to Options for ingesting data sources, on page 8.
- Verify that you configured your access control policy and related policies to support Threat Intelligence Director. Refer to Configure policies to support Threat Intelligence Director, 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 Threat Intelligence Director-supporting access control policy and related policies to your elements. Refer to Deploy configuration changes.
- Verify that you did not pause Threat Intelligence Director data publication at the feature level. Refer to Pause Threat Intelligence Director and purge Threat Intelligence Director data from elements, on page 41.

### System is experiencing slowness or decreased performance

For more information about performance impact, refer to Performance impact of Threat Intelligence Director, on page 3.

### Secure Firewall Management Center table views do not show Threat Intelligence Director data

If you are publishing observables to your elements but no Threat Intelligence Director 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, refer to Configure policies to support Threat Intelligence Director, on page 7.

### One or more elements are overwhelmed by Threat Intelligence Director data

If Threat Intelligence Director data is overwhelming one or more of your devices, consider pausing Threat Intelligence Director publishing and purging the data stored on your elements. For more information, refer to Pause Threat Intelligence Director and purge Threat Intelligence Director data from elements, on page 41.

### System is performing a malware cloud lookup instead of a TID block

This is by design. For more information, refer to Threat Intelligence Director - Firewall Management Center action prioritization , on page 25.

### System is performing a security intelligence or DNS policy action instead of a TID action

This is by design. For more information, refer to Threat Intelligence Director - Firewall Management Center action prioritization , on page 25.

### TID is disabled

- Add memory to your appliance. Threat Intelligence Director can only be used on appliances with at least 15 GB of memory.
- Enable REST API access for the Secure Firewall Management Center. For more information, refer to *Enabling REST API Access* in the *Cisco Secure Firewall Management Center Administration Guide*.

### The system does not generate the Threat Intelligence Director incident or take the Threat Intelligence Director action that you expected

- Verify that all of your managed devices are properly enabled and configured for Threat Intelligence Director. Refer to View Threat Intelligence Director status of elements (managed devices), on page 29 and Configure policies to support Threat Intelligence Director, 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. Refer to View and manage observables, on page 35.
- For a list of the other factors that influence the Threat Intelligence Director action that the system takes, refer to Factors that affect the action taken, on page 24.
- Elements (managed devices) may not have the threat data you think they have. Refer to Pausing publishing, on page 40.

### One encounter with a particular threat generates multiple incidents

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

For details, refer to Handling of duplicate indicators, on page 13.

# History for Threat Intelligence Director

This reference provides the complete version history for Threat Intelligence Director features, including implementation details, version requirements, and behavioral changes across different software releases.

| Feature | Minimum Firewall Management Center | Minimum Firewall Threat Defense | Details |
|---|---|---|---|
| Handling of an indicator that is included in multiple STIX feeds | 7.1 | Any | If STIX feeds contain identical indicators, an indicator is created for each feed, which may lead to multiple incidents being generated for the same indicator. Previously, only the feed that was downloaded last took effect. |

| Feature | Minimum Firewall Management Center | Minimum Firewall Threat Defense | Details |
|---|---|---|---|
| Change in action prioritization | 6.5 | Any | These changes apply if more than one Firepower feature could apply to a particular observable.<br>TID blocking/monitoring observable actions now have priority over blocking/monitoring by Security Intelligence.<br>**Important**<br>The system still effectively handles traffic as before. Traffic that was previously blocked is still blocked, and monitored traffic is still monitored. This simply changes the component reported in the event as responsible for the action. You may also see more TID incidents generated.<br>• If you configure the Block TID observable action, even if the traffic also matches a Security Intelligence Block action:<br>  • The Security Intelligence category in the connection event is a variant of TID Block.<br>  • The system generates a TID incident with an action taken of Blocked.<br>• If you configure the Monitor TID observable action, even if the traffic also matches a Security Intelligence Monitor rule:<br>  • The Security Intelligence category in the connection event is a variant of TID Monitor<br>  • The system generates a TID incident with an action taken of Monitored.<br>Previously, in each of these cases, the system reported the category by analysis and did not generate a TID incident. |
| Secure Firewall Threat Intelligence Director | 6.2.2 | Any | Lets you use threat intelligence from external sources to identify and process threats.<br>New screens: A new top-level **Intelligence** menu with multiple tabs.<br>Supported platforms: Secure Firewall Management Center |