

# Security Intelligence

The following topics provide an overview of Security Intelligence, including use of lists for blocking and allowing traffic and basic configuration.


- Security intelligence, on page 1
- License requirements for security intelligence, on page 2
- Requirements and prerequisites for security intelligence, on page 2
- Best practices for security intelligence, on page 2
- Guidelines and limitations for security intelligence, on page 3
- Security intelligence sources, on page 3
- Configure security intelligence, on page 4
- Security intelligence monitoring, on page 11
- Override security intelligence blocking, on page 12
- Troubleshooting security intelligence, on page 13


# Security intelligence

Security Intelligence is an early line of defense mechanism that

- uses reputation intelligence to quickly block connections to or from IP addresses, URLs, and domain names
- operates as the first phase of access control, before the system performs more resource-intensive evaluation, and
- improves performance by quickly excluding traffic that does not require inspection through Security Intelligence block listing.

### Security intelligence features and limitations

Security Intelligence provides access to regularly updated intelligence feeds from Cisco. Sites representing security threats such as malware, spam, botnets, and phishing appear and disappear faster than you can update and deploy custom configurations.

You can refine Security Intelligence Block listing with Do Not Block lists and monitor-only Block lists. These mechanisms exempt traffic from being blocked by a Block list, but do **not** automatically trust or fastpath matching traffic. Traffic added to a Do Not Block list or monitored at the Security Intelligence stage is intentionally subject to further analysis with the rest of access control.

**Note** You cannot use a Block list to block fastpathed traffic. Prefilter evaluation occurs before Security Intelligence filtering. Fastpathed traffic bypasses all further evaluation, including Security Intelligence.

**Related Topics**

Security intelligence

# License requirements for security intelligence

### Threat Defense License

IPS

### Classic License

Protection

# Requirements and prerequisites for security intelligence

### Model support

Any

### Supported domains

Any

### User roles

- Administrator
- Access Admin
- Network Admin

**Important** You must apply the Network Discovery policy on the device for a successful application of the SI policy.

# Best practices for security intelligence

Configure your access control policies to block threats detected by Cisco-provided Security Intelligence feeds. See Configuration example: Security intelligence blocking, on page 10.

If you want to supplement the Cisco-provided Security Intelligence feeds with custom threat data, or manually block emerging threats:

- For IP addresses, use custom Security Intelligence lists and feeds, or Network objects. To create these, see Security intelligence and Networks, and their subtopics. To use them for Security Intelligence, see Configure security intelligence, on page 4. Network objects used in Security Intelligence policy require an IPS license.
- For URLs and domains, use custom Security Intelligence lists and feeds, *not* objects or groups. See details at Manual URL filtering options.
- You can also add entries to a Block list from events. See Global and domain security intelligence lists.

To test new feeds, or for passive deployments, set the action from block to monitor only. See Security intelligence monitoring, on page 11.

If you need to exclude specific sites or addresses from Security Intelligence blocking, see Override security intelligence blocking, on page 12.

If your Firepower deployment is integrated with Cisco XDR and you use custom Security Intelligence lists and feeds, be sure to update Security Services Exchange with these lists and feeds. For details, see instructions for configuring auto-promotion of events in the Security Services Exchange online help.

System-provided Security Intelligence categories may change over time and without notification; you should plan to check periodically for changes, and modify your policies accordingly.

You should also configure URL filtering, a separate feature with separate licensing requirements, for further protection against malicious sites. See URL Filtering Rules.

To reduce latency and CPU overhead, avoid referencing a single, massive SI feed object across your entire security policy. Instead, utilize customized objects to create smaller, targeted subsets of your intelligence data.

Using URL/Domain feeds instead of IP blocklists can reduce CPU overhead because domain filtering is generally more efficient and less resource-intensive than managing massive IP blocklists.

Excluding trusted IPs by adding known good or essential partner IP addresses to an "Do Not Block" list in Security Intelligence (SI) feeds helps reduce CPU overhead as the firewall or security device bypasses unnecessary scanning and deeper inspection for these IPs.

# Guidelines and limitations for security intelligence

Be aware of these limitations when configuring and using Security Intelligence:

- The Security Intelligence configuration that includes detection signatures or malware URLs might lead to false threat alerts when the Firewall Threat Defense troubleshoot files are scanned.
- If a TCP connection attempt is initiated from an IP address that is blocked due to its poor reputation, a TCP reset (RST) packet is sent. This causes the connection to be terminated instantly, preventing the establishment of the TCP session and signalling the rejection to the sender.

# Security intelligence sources

Security Intelligence sources are data providers that

- supply regularly updated intelligence feeds for domains, URLs and IP addresses
- enable custom blocking and allow lists for specific sites or addresses, and

- provide global lists for immediate event-based blocking and allowing.

### Types of security intelligence sources

Security Intelligence uses these source types:

- **System-provided feeds**: Cisco provides access to regularly updated intelligence feeds for domains, URLs and IP addresses. For more information, see Security intelligence.
- **Third-party feeds**: Optionally, supplement Cisco-provided feeds with third-party reputation feeds, which are dynamic lists that the Cloud-Delivered Firewall Management Center downloads from the internet on a regular basis. See Custom security intelligence feeds.
- **Custom Block lists or feeds (or objects)**: Block specific IP addresses, URLs, or domain names using a manually-created list or feed (for IP addresses, you can also use network objects.)

  For example, if you become aware of malicious sites or addresses that are not yet blocked by a feed, add these sites to a custom Security Intelligence list and add this custom list to the Block list in the Security Intelligence tab of your access control policy, as described in Custom Security Intelligence lists and Configure security intelligence, on page 4.

  For IP addresses, you can optionally use network objects rather than lists or feeds for this purpose; for information, see Networks. (For URLs, using lists and feeds is strongly recommended over other methods.)
- **Custom Do Not Block lists or feeds**: Override Security Intelligence blocking for specific sites or addresses. See Override security intelligence blocking, on page 12.
- **Global Block lists (one each for Network, URL and DNS)**: While reviewing events, you can immediately add an event's IP address, URL, or domain to the applicable Global Block List so that Security Intelligence will handle future traffic from that source. See Global and domain security intelligence lists.
- **Global Do Not Block lists (one each for Network, URL and DNS)**: While reviewing events, you can immediately add an event's IP address, URL, or domain to the applicable Global Do Not Block List if you do not want Security Intelligence to block future traffic from that source. See Global and domain security intelligence lists.

# Configure security intelligence

Configure Security Intelligence filtering to automatically block or monitor traffic based on threat intelligence feeds and custom block or allow lists. This provides an additional layer of security by filtering known malicious IP addresses, URLs, and domains before they reach your network resources.

Each access control policy has Security Intelligence options. You can add network objects, URL objects and lists, and Security Intelligence feeds and lists to a Block list or Do Not Block list, and constrain any of these by security zone. You can also associate a DNS policy with your access control policy, and add domain names to a Block or Do Not Block list.

The number of objects in the Do Not Block lists plus the number in the Block lists cannot exceed 125 network objects, or 32767 URL objects and lists.

**Before you begin**

- Tip: For guidance on minimum configuration recommendations, see also Configuration example: Security intelligence blocking, on page 10.

- To ensure that ALL options are available to select, add at least one managed device to your management center.
- In passive deployments, or if you want to set Security Intelligence filtering to monitor-only, enable logging
- Configure a DNS policy to take Security Intelligence action for domains. For more information, see DNS Policies for Security Intelligence.

Follow these steps to configure Security Intelligence filtering in an access control policy:

## Procedure

**Step 1** In the access control policy editor, click **Security Intelligence**.

If the controls are dimmed, settings are inherited from an ancestor policy, or you do not have permission to modify the configuration. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

**Step 2** Choose the type of objects to configure.

- Click **Networks** to add network objects (IP addresses).

**Note** Network objects used in a Security Intelligence policy require a IPS license.

- Click **URLs** to add URL objects.

**Step 3** Find the **Available Objects** you want to add to the Block or Do Not Block list.

- Search the available objects by typing in the **Search by name or value** field. Clear the search string by clicking **Reload** ( ) or **Clear** ( ).
- If no existing list or feed meets your needs, click **Add** ( ), select **New Network List** or **New URL List**, and proceed as described in Create custom security intelligence feeds or Upload new custom security intelligence lists to the Cloud-Delivered Firewall Management Center.
- If no existing object meets your needs, click **Add** ( ), select **New Network Object** or **New URL Object**, and proceed as described in Create a network object.

Security Intelligence ignores IP address blocks using a `/0` netmask.

**Step 4** Choose one or more **Available Objects** to add.

**Step 5** (Optional) Choose an **Available Zone** to constrain the selected objects by zone.

You cannot constrain system-provided Security Intelligence lists by zone.

**Note** The **Any** zone for an SI list applies only to interfaces that are part of a security zone. However, an exception is that if a device does not have any interfaces associated with a security zone, then the **Any** zone will match any interface.

For example, if you have five interfaces on a device and none of them are associated with a security zone, any SI list that is assigned to the **Any** zone will be inspected against traffic on ALL interfaces on the device. If you add one interface to a security zone on that device, it effectively would remove SI inspection on the other four interfaces, where the zone is set to **Any** for an SI list. If you add the other four interfaces to a security zone, they will be evaluated by the SI list attached to the **Any** zone.

**Step 6** Click **Add to Do Not Block list** or **Add to Block list**, or click and drag the selected objects to either list.

To remove an object from a Block or Do Not Block list, click **Delete** ( ) To remove multiple objects, choose the objects and right-click to **Delete Selected**.

**Step 7** (Optional) Set objects on the Block list to monitor-only by right-clicking the object under **Block List**, then choosing **Monitor-only (do not block)**.

You cannot set system-provided global Security Intelligence lists to monitor only.

**Step 8** Choose a DNS policy from the **DNS Policy** drop-down list.

**Step 9** Click **Save**.

Security Intelligence filtering is now configured for your access control policy. The system will automatically block or monitor traffic based on the configured Block and Do Not Block lists, providing enhanced protection against known threats.

### What to do next

- Deploy configuration changes.

### Related Topics

Security intelligence
Snort restart scenarios

# Security intelligence options

Use the Security Intelligence tab in the access control policy editor to configure network (IP address) and URL Security Intelligence, and to associate the access control policy with a DNS policy in which you have configured Security Intelligence for domains.

### Available objects

Available objects include:

- Security Intelligence categories populated by the system-provided feed.

  For details, see Security intelligence categories, on page 8.

- System-provided Global Block and Do Not Block lists.

For descriptions, see Security intelligence sources, on page 3.

- Security Intelligence lists and feeds that you create under Object > Object Management > Security Intelligence.

  For descriptions, see Security intelligence sources, on page 3.

- Network and URL objects that are configured on the respective pages under Object > Object Management. These are different from the Security Intelligence objects in the previous bullet.

  For details about network objects, see Networks. (For URLs, use Security Intelligence lists or feeds rather than objects.)

  Note that range and group network object types are not supported in Security Intelligence policy.

### Available zones

Except for the system-provided Global lists, you can constrain Security Intelligence filtering by zone.

For example, to improve performance, you might want to target enforcement to specific zones rather than all interfaces. As a more specific example, you can block spam only for a security zone that handles email traffic.

To enforce Security Intelligence filtering for an object on multiple zones, you must add the object to the Block or Do Not Block list separately for each zone.

Note that range and group network object types are not supported in Security Intelligence policy.

### DNS policy

In order to match DNS traffic using Security Intelligence, you must select a DNS policy for your Security Intelligence configuration.

Using Block or Do Not Block lists, or monitoring traffic based on a DNS list or feed, also requires that you:

- Configure DNS Security Intelligence lists and feeds. See Security intelligence.
- Create a DNS policy. See Create basic DNS policies for more information.
- Configure DNS rules that reference your DNS lists or feeds. See Create and edit DNS rules for more information.
- Because you deploy the DNS policy as part of your access control policy, you must associate both policies. See Requirement: deploy DNS policy configuration changes for more information.

### Do not block list

See Override security intelligence blocking, on page 12.

To select all objects in the list, right-click an object.

### Block list

See Configuration example: Security intelligence blocking, on page 10 and other topics in this chapter.

For explanations of the visual indicators in the Block list, see Block list icons, on page 10.

To select all objects in the list, right-click an object.

### Logging

Security Intelligence logging, enabled by default, logs all blocked and monitored connections handled by an access control policy's assigned devices. However, the system does not log Do Not Block list matches; logging of connections on the Do Not Block list depends on their eventual disposition. Logging must be enabled for connections on the Block list before you can set objects on that list to monitor-only.

To enable, disable, or view logging settings, right-click an object in the Block list.

### Related Topics

Global and domain security intelligence lists
Security intelligence lists and multitenancy

# Security intelligence categories

Security Intelligence categories are determined by the system-provided feeds described in Security intelligence.

These categories are used in the following locations:

- The Networks sub-tab on the Security Intelligence tab of an access control policy
- The URLs sub-tab beside the Networks tab on the Security Intelligence tab of an access control policy
- In a DNS policy on the DNS tab in the DNS rule configuration page
- In events generated when traffic matches Block or Monitor configurations in the above locations

**Note** If your organization is using Secure Firewall Threat Intelligence Director: When viewing events, you may see categories that indicate that the action was taken by TID, such as `TID URL Block`.

Categories are updated by Talos from the cloud, and this list may change independently of Firepower releases.

***Table 1:***

| Security Intelligence Category | Description |
|---|---|
| Attackers | Active scanners and hosts known for outbound malicious activity |
| Banking_fraud | Sites that engage in fraudulent activities that relate to electronic banking |
| Bogon | Bogon networks and unallocated IP addresses |
| Bots | Sites that host binary malware droppers |
| CnC | Sites that host command-and-control servers for botnets |
| Cryptomining | Hosts providing remote access to pools and wallets for the purpose of mining cryptocurrency |

| Security Intelligence Category | Description |
|---|---|
| Dga | Malware algorithms used to generate a large number of domain names acting as rendezvous points with their command-and-control servers |
| Exploitkit | Software kits designed to identify software vulnerabilities in clients |
| High_risk | Domains and hostnames that match against the OpenDNS predictive security algorithms from security graph |
| Ioc | Hosts that have been observed to engage in Indicators of Compromise (IOC) |
| Link_sharing | Websites that share copyrighted files without permission |
| Malicious | Sites exhibiting malicious behavior that do not necessarily fit into another, more granular, threat category |
| Malware | Sites that host malware binaries or exploit kits |
| Newly_seen | Domains that have recently been registered, or not yet seen via telemetry.<br>**Attention**<br>Currently, this category does not have any active feed and is reserved for future use. |
| Open_proxy | Open proxies that allow anonymous web browsing |
| Open_relay | Open mail relays that are known to be used for spam |
| Phishing | Sites that host phishing pages |
| Response | IP addresses and URLs that are actively participating in malicious or suspicious activity |
| Spam | Mail hosts that are known for sending spam |
| Spyware | Sites that are known to contain, serve, or support spyware and adware activities |
| Suspicious | Files that appear to be suspicious and have characteristics that resemble known malware |
| Tor_exit_node | Hosts known to offer exit node services for the Tor Anonymizer network |

# Block list icons

The visual indicators may appear in the Block list on the Security Intelligence tab in an access control policy.

| Icon or Visual Indicator | Description |
|---|---|
| **Block** ( ) | The object is set to block. |
| **Monitor** ( ) | The object is set to monitor-only.<br>See Security intelligence monitoring, on page 11 |
| An object is displayed in strikethrough text | The same object is also on the Do Not Block list, which overrides the block. |

# Configuration example: Security intelligence blocking

Configure Security Intelligence blocking to protect your network from known malicious IP addresses, URLs, and domains using regularly updated threat intelligence feeds.

Configure your access control policy to block all threats detectable by the system's regularly updated Security Intelligence feeds.

The number of objects in the Block lists plus the number in the Do Not Block lists cannot exceed 125 network objects, or 32767 URL objects and lists.

**Before you begin**

- To ensure that all options are available to select, add at least one managed device to your management center.
- Configure a DNS policy to block all Security Intelligence threat categories for domains. For more information, see DNS Policies for Security Intelligence.
- If you have, or will have, custom lists of entities to block, create a Security Intelligence object of each type (URLs, DNS, Networks.) See Security intelligence.

## Procedure

**Step 1** Click **Policies** > **Security policies** > **Access Control**.

**Step 2** Create a new access control policy or edit an existing policy.

**Step 3** In the access control policy editor, click **Security Intelligence**.

If the controls are dimmed, settings are inherited from an ancestor policy, or you do not have permission to modify the configuration. If the configuration is unlocked, uncheck **Inherit from base policy** to enable editing.

**Step 4** Click **Networks** to add blocking criteria for IP addresses.

a) Scroll down in the Networks list and select all of the threat categories listed below the Global lists.
b) If applicable, select the security zones for which you want to block these threats.
c) Click **Add to Block List**.

d) If you have created custom lists or feeds with addresses to block, add those to the Block List using the same steps as above.

**Step 5** Click **URLs** to add blocking criteria for URLs, and repeat the steps you followed for Networks.

**Step 6** Choose a DNS policy from the **DNS Policy** drop-down list; see DNS policies.

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

Your access control policy now blocks malicious IP addresses, URLs, and domains based on Security Intelligence threat feeds, providing enhanced protection against known threats.

### What to do next

- Enable logging for these connections
- Deploy configuration changes.
- For additional protection, configure URL filtering to block malicious URLs. See URL Filtering Rules.

# Security intelligence monitoring

Security Intelligence monitoring is a security feature that

- logs connection events for traffic that would have been blocked by Security Intelligence, but does not block the traffic,
- enables testing of feeds before implementation, and
- optimizes performance in passive deployments.

### Use cases for security intelligence monitoring

Monitoring is especially useful for:

- Testing feeds before you implement them.

  Consider a scenario where you want to test a third-party feed before you implement blocking using that feed. When you set the feed to monitor-only, the system allows connections that would have been blocked to be further analyzed by the system, but also logs a record of each of those connections for your evaluation.

- Passive deployments, to optimize performance.

  Managed devices that are deployed passively cannot affect traffic flow; there is no advantage to configuring the system to block traffic. Additionally, because blocked connections are not actually blocked in passive deployments, the system may report multiple beginning-of-connection events for each blocked connection.

**Note** If configured, Secure Firewall Threat Intelligence Director may impact the action taken (Monitor or Block.)

To configure Security Intelligence monitoring:

After you configure Security Intelligence blocking following the instructions in Configuration example: Security intelligence blocking, on page 10, right-click each applicable object in the Block list and choose **Monitor-only**. You cannot set system-provided Security Intelligence lists to monitor only.

# Override security intelligence blocking

Use Do Not Block lists to exempt specific domains, URLs, or IP addresses from being blocked by Security Intelligence lists or feeds.

You can use Do Not Block lists for various purposes:

- Override the occasional false-positive block in a reputable Security Intelligence feed
- Inspect specific traffic in depth instead of blocking it early based on reputation
- Exempt otherwise-restricted transactions based on zone from Security Intelligence blocking

  For example, you can add an improperly classified URL to a Do Not Block list, but then restrict the Do Not Block list object using a security zone used by those in your organization who need to access those URLs. That way, only those with a business need can access the URLs on the Do Not Block list.



**Note** Entries on a Do Not Block list are simply exemptions from the block list. Any connection that passes the Security Intelligence policy is subject to the access control rules. Thus, an entry in the Do Not Block list can subsequently be blocked by an access control rule or intrusion policy. Your Do Not Block entries should always be exemptions from your block lists.

### Procedure

**Step 1** Option 1: Add an IP address, URL, or domain from an event to the Global Do Not Block List. See Global and domain security intelligence lists.

**Step 2** Option 2: Use a custom Security Intelligence list or feed.

a) Create the custom Security Intelligence list or feed. See Custom Security Intelligence lists or Create custom security intelligence feeds.

b) For IP addresses (Networks) and URLs: Edit your access control policy, click the Security Intelligence tab, then click the custom list or feed in the Networks or URLs sub-tab, then click **Add to Do Not Block List**.

c) Save your changes.

d) For domains (DNS): See the "DNS Policy" section in the Security intelligence options, on page 6 topic.

e) Deploy your changes.

The specified domains, URLs, or IP addresses are now exempted from Security Intelligence blocking and will be subject to access control rules instead.

# Troubleshooting security intelligence

See the following topics for troubleshooting Security Intelligence.

## Security intelligence categories missing from the Available Options List

Security Intelligence categories (such as CnC or Exploitkit) display in the Networks tab under Available Options only after you add at least one managed device to your management center.

You must add a device in order to pull all TALOS feeds that provide the Security Intelligence categories.

If the expected category does not appear in Security Intelligence, verify that it is not a URL filtering category, which uses a different set of categories.

To see URL filtering categories, look at the **URLs** tab in an access control rule.