



Connection Logging

The following topics describe how to configure the Firepower System to log connections made by hosts on your monitored network:

- [Connection Logging Basics, page 1](#)
- [Connection Logging Strategies, page 2](#)
- [Security Intelligence Logging, page 8](#)
- [SSL Policy Connection Logging, page 10](#)
- [Access Control Policy Connection Logging, page 12](#)
- [Limiting Logging of Long URLs, page 14](#)

Connection Logging Basics

As managed devices monitor traffic generated by the hosts on your network, they can generate logs of the connections they detect. Various settings in access control and SSL policies give you granular control over which connections you log, when you log them, and where you store the data. An access control rule's specific logging configuration also determines whether you log file and malware events associated with the connection.

In most cases, you can log a connection at its beginning or its end, or both. When you log a connection, the system generates a *connection event*. You can also log a special kind of connection event, called a *Security Intelligence event*, whenever a connection is blacklisted (blocked) by the reputation-based Security Intelligence feature.

Connection events contain data about the detected sessions. The information available for any individual connection event depends on several factors, but in general includes:

- basic connection properties: timestamp, source and destination IP address, ingress and egress zones, the device that handled the connection, and so on
- additional connection properties discovered or inferred by the system: applications, requested URLs, or users associated with the connection, and so on
- metadata about why the connection was logged: which access control rule (or other configuration) in which policy handled the traffic, whether the connection was allowed or blocked, details about encrypted and decrypted connections, and so on

**Note**

You can supplement the connection data gathered by your managed devices with connection data generated from exported NetFlow records. This is especially useful if you have NetFlow-enabled routers or other devices deployed on networks that your Firepower System managed devices cannot monitor.

Connection Logging Strategies

You should log connections according to the security and compliance needs of your organization. You can log **any** connection except those that are fast-pathed at the device level before they reach access control.

**Tip**

To perform detailed analysis of connection data, Cisco recommends you log the ends of critical connections to the Firepower Management Center database.

Optional vs Automatic Logging

You should log connections according to the security and compliance needs of your organization. If your goal is to limit the number of events you generate and improve performance, only enable logging for the connections critical to your analysis. However, if you want a broad view of your network traffic for profiling purposes, you can enable logging for additional connections. Various settings in access control and SSL policies give you granular control over which connections you log, when you log them, and where you store the data.

Optional Connection Logging

Security Intelligence Blacklisting Decisions

You can log a connection whenever it is blacklisted (blocked) by the reputation-based Security Intelligence feature. Optionally, and recommended in passive deployments, you can use a monitor-only setting for Security Intelligence filtering. This allows the system to further analyze connections that would have been blacklisted, but still log the match to the blacklist. Security Intelligence monitoring also allows you to create traffic profiles using Security Intelligence information.

When you enable Security Intelligence logging, blacklist matches generate Security Intelligence events as well as connection events. A Security Intelligence event is a special kind of connection event that you can view and analyze separately, and that is also stored and pruned separately.

Encrypted Connections

You can log a connection when the system blocks an encrypted session according to the settings in an SSL policy. You can also force the system to log connections that it passes for further evaluation by access control rules, regardless of whether you decrypt the traffic, and regardless of how the system later handles or inspects the traffic. You configure this logging on a per-SSL rule basis so that you only log critical connections.

Access Control Handling

You can log a connection when it is handled by an access control rule or the access control default action. You configure this logging on a per-access control rule basis so that you only log critical connections.

Automatic Connection Logging

In addition to the logging that you configure, the system automatically logs most connections where the system detects a prohibited file, malware, or intrusion attempt. Unless you disable connection event storage entirely for the Firepower Management Center, regardless of your other logging configurations, the system saves these end-of-connection events to the Firepower Management Center database for further analysis. All connection events reflect why they were automatically logged.

Connections Associated with Intrusions

When an intrusion policy invoked by an access control rule detects an intrusion and generates an intrusion event, the system automatically logs the end of the connection where the intrusion occurred to the Firepower Management Center database, regardless of the logging configuration of the rule.

However, when an intrusion policy associated with the access control default action generates an intrusion event, the system does **not** automatically log the end of the associated connection. Instead, you must explicitly enable default action connection logging. This is useful for intrusion prevention-only deployments where you do not want to log any connection data.

For connections where an intrusion was blocked, the action for the connection in the connection log is `Block`, with a reason of `Intrusion Block`, even though to perform intrusion inspection you must use an Allow rule.

Connections Associated with File and Malware Events

When a file policy invoked by an access control rule detects a prohibited file (including malware) and generates a file or malware event, the system automatically logs the end of the connection where the file was detected to the Firepower Management Center database, regardless of the logging configuration of the access control rule. You **cannot** disable this logging.

**Note**

File events generated by inspecting NetBIOS-ssn (SMB) traffic do not immediately generate connection events because the client and server establish a persistent connection. The system generates connection events after the client or server ends the session.

For connections where a file was blocked, the action for the connection in the connection log is `Block` even though to perform file and malware inspection you must use an Allow rule. The connection's Reason is either `File Monitor` (a file type or malware was detected), or `Malware Block` or `File Block` (a file was blocked).

Beginning vs End-of-Connection Logging

When the system detects a connection, in most cases you can log it at its beginning or its end.

However, because blocked traffic is immediately denied without further inspection, in most cases you can log only beginning-of-connection events for blocked or blacklisted traffic; there is no unique end of connection to log. An exception occurs when you block encrypted traffic. When you enable connection logging in an SSL policy, the system logs end-of-connection rather than beginning-of-connection events. This is because the system cannot determine if a connection is encrypted using the first packet in the session, and thus cannot immediately block encrypted sessions.



Note

For a single non-blocked connection, the end-of-connection event contains all of the information in the beginning-of-connection event, as well as information gathered over the duration of the session.

To optimize performance, log either the beginning or the end of any connection, but not both. You can trigger correlation rules based on either beginning or end-of-connection events. Note that monitoring a connection for any reason forces end-of-connection logging.

The following table details the differences between beginning and end-of-connection events, including the advantages to logging each.

Table 1: Comparing Beginning and End-of-Connection Events

	Beginning-of-Connection Events	End-of-Connection Events
Can be generated...	when the system detects the beginning of a connection (or, after the first few packets if event generation depends on application or URL identification)	when the system: <ul style="list-style-type: none"> • detects the close of a connection • does not detect the end of a connection after a period of time • can no longer track the session due to memory constraints
Can be logged for...	all connections evaluated by Security Intelligence or access control rules, though you may not be able to configure end-of-connection logging in all places	all connections, though you may not be able to configure end-of-connection logging in all places
Contain...	only information that can be determined in the first packet (or the first few packets, if event generation depends on application or URL identification)	all information in the beginning-of-connection event, plus information determined by examining traffic over the duration of the session, for example, the total amount of data transmitted or the timestamp of the last packet in the connection
Are useful...	if you want to log: <ul style="list-style-type: none"> • blocked connections, including Security Intelligence blacklisting decisions • only the beginning of a connection because the end-of-connection information does not matter to you 	if you want to: <ul style="list-style-type: none"> • log encrypted connections handled by an SSL policy • perform any kind of detailed analysis on, or trigger correlation rules using, information collected over the duration of the session • view connection summaries (aggregated connection data) in custom workflows, view connection data in graphical format, or create and use traffic profiles

Firepower Management Center vs External Logging

You can log connection and Security Intelligence events to the Firepower Management Center database, as well as to an external syslog or SNMP trap server. The number of events a Firepower Management Center can store depends on its model. Before you can log connection data to an external server, you must configure a connection to that server called an *alert response*.

Logging to the Firepower Management Center database allows you to take advantage of many reporting, analysis, and data correlation features of the Firepower System. For example:

- Dashboards and the Context Explorer provide you with graphical, at-a-glance views of the connections logged by the system.
- Event views present detailed information on the connections logged by the system, which you can display in a graphical or tabular format or summarize in a report.
- Traffic profiling uses connection data to create a profile of your normal network traffic that you can then use as a baseline against which to detect and track anomalous behavior.
- Correlation policies allow you to generate events and trigger responses (such as alerts or external remediations) to specific types of connections or traffic profile changes.

**Note**

To use these features, you **must** log connections (and in most cases, the end of those connections rather than the beginning) to the Firepower Management Center database. This is why the system automatically logs critical connections—those associated with logged intrusions, prohibited files, and malware.

Rule Actions and Connection Logging

Every access control and SSL rule has an *action* that determines not only how the system inspects and handles the traffic that matches the rule, but also when and how you can log details about matching traffic.

Logging for Monitored Connections

The system always logs the ends of the following connections to the Firepower Management Center database, regardless of the logging configuration of the rule or default action that later handles the connection:

- connections matching a Security Intelligence blacklist set to monitor
- connections matching an SSL Monitor rule
- connections matching an access control Monitor rule

In other words, if a packet matches a Monitor rule or Security Intelligence monitored blacklist, the connection is always logged, even if the packet matches no other rules and you do not enable logging on the default action. Whenever the system logs a connection event as the result of Security Intelligence filtering, it also logs a matching Security Intelligence event, which is a special kind of connection event that you can view and analyze separately.

Because monitored traffic is always later handled by another rule or by the default action, the Action field for a connection event logged due to a monitor rule is never `Monitor`. Rather, it reflects the action of the rule or default action that later handles the connection.

The system does **not** generate a separate event each time a single connection matches an SSL or access control Monitor rule. Because a single connection can match multiple Monitor rules, each connection event logged to the Firepower Management Center database can include and display information on the first eight Monitor access control rules that the connection matches, as well as the first matching Monitor SSL rule.

Similarly, if you send connection events to an external syslog or SNMP trap server, the system does not send a separate alert each time a single connection matches a Monitor rule. Rather, the alert that the system sends at the end of the connection contains information on the Monitor rules the connection matched.


Tip

Even though the rule action in the connection log can never be `Monitor`, you can still trigger correlation policy violations on connections that match Monitor rules.

Logging for Trusted Connections

A trusted connection is one that is handled by a Trust access control rule or the default action in an access control policy. You can log the beginnings and ends of these connections, however, keep in mind that trusted connections, regardless of whether they are encrypted, are not inspected for discovery data, intrusions, or prohibited files and malware. Therefore, connection events for trusted connections contain limited information.

Note that the system logs TCP connections handled by a Trust access control rule differently depending on the device that detected the connection:

- For 7000 and 8000 Series devices, TCP connections detected by a Trust rule on the first packet generate different events depending on the presence of a preceding enabled Monitor rule. If the Monitor rule is active, the system evaluates the packet and generates both a beginning and end-of-connection event. If no Monitor rule is active, the system only generates an end-of-connection event.
- For all other models, TCP connections detected by a Trust rule on the first packet only generate an end-of-connection event. The system generates the event one hour after the final session packet.

Logging for Blocked and Interactively Blocked Connections

When you log a blocked connection, how the system logs it depends on why the connection was blocked; this is important to keep in mind when configuring correlation rules based on connection logs:

- For SSL rules and SSL policy default actions that block encrypted traffic, the system logs **end**-of-connection events. This is because the system cannot determine if a connection is encrypted using the first packet in the session.
- For access control rules and access control policy default actions that block decrypted or unencrypted traffic (including interactive blocking rules), the system logs **beginning**-of-connection events. Matching traffic is denied without further inspection.

Connection events for sessions blocked by an access control or SSL rule have an action of `Block` or `Block with reset`. Blocked encrypted connections have a reason of `SSL Block`.

Interactive blocking access control rules, which cause the system to display a warning page when a user browses to a prohibited website, allow you to configure end-of-connection logging. This is because if the user clicks through the warning page, the connection is considered a new, allowed connection which the system can monitor and log.

Therefore, for packets that match an Interactive Block or Interactive Block with reset rule, the system can generate the following connection events:

- a beginning-of-connection event when a user's request is initially blocked and the warning page is displayed; this event has an associated action of `Interactive Block` or `Interactive Block with reset`
- multiple beginning- or end-of-connection events if the user clicks through the warning page and loads the originally requested page; these events have an associated action of `Allow` and a reason of `User Bypass`

Note that only devices deployed inline (that is, using routed, switched, or transparent interfaces, or inline interface pairs) can block traffic. Because blocked connections are not actually blocked in passive deployments, the system may report multiple beginning-of-connection events for each blocked connection.

**Caution**

Logging blocked TCP connections during a Denial of Service (DoS) attack can affect system performance and overwhelm the database with multiple similar events. Before you enable logging for an `Block` rule, consider whether the rule monitors traffic on an Internet-facing interface or other interface vulnerable to DoS attack.

Logging for Allowed Connections

The `Decrypt SSL` rules, `Do not decrypt SSL` rules, and `Allow access control` rules permit matching traffic to pass to the next phase of inspection and traffic handling.

Regardless of whether you decrypt encrypted traffic using an SSL rule, the traffic continues to be evaluated by access control rules. If you enable logging for this SSL rule, the system logs the end of matching connections, regardless of the logging configuration of the access control rules or default action that later handles them.

When you allow traffic with an access control rule, you can use an associated intrusion or file policy (or both) to further inspect traffic and block intrusions, prohibited files, and malware before the traffic can reach its final destination. Note, however, that by default file and intrusion inspection is disabled for encrypted payloads.

Connections for traffic matching an `Allow` access control rule are logged as follows:

- When an intrusion policy invoked by an access control rule detects an intrusion and generates an intrusion event, the system automatically logs the end of the connection where the intrusion occurred to the Firepower Management Center database, regardless of the logging configuration of the rule.
- When a file policy invoked by an access control rule detects a prohibited file (including malware) and generates a file or malware event, the system automatically logs the end of the connection where the file was detected to the Firepower Management Center database, regardless of the logging configuration of the access control rule.
- Optionally, you can enable beginning- and end-of-connection logging for any allowed traffic, including traffic that the system deems safe or that you do not inspect with an intrusion or file policy.

For all of the resulting connection events, the `Action` and `Reason` fields reflect why the events were logged. Note that:

- An action of `Allow` represents explicitly allowed and user-bypassed interactively blocked connections that reached their final destination.
- An action of `Block` represents a connection that was at first allowed by an access control rule, but where an intrusion, prohibited file, or malware was detected.

File and Malware Event Logging for Allowed Connections

When you allow unencrypted or decrypted traffic with an access control rule, you can use an associated file policy to inspect transmitted files, and block prohibited files and malware before it can reach its destination.

When the system detects a prohibited file, it automatically logs one of the following types of event to the Firepower Management Center database:

- *file events*, which represent detected or blocked files, including malware files
- *malware events*, which represent detected or blocked malware files only
- *retrospective malware events*, which are generated when the malware disposition for a previously detected file changes

If you do not want to log file or malware events, you can disable this logging on a per-access-control-rule basis. Or, you can disable file and malware event storage entirely in the Firepower Management Center configuration.



Note

Cisco recommends you leave file and malware event logging enabled.

Regardless of whether you save file and malware events, when network traffic violates a file policy, the system automatically logs the end of the associated connection to the Firepower Management Center database, regardless of the logging configuration of the invoking access control rule.

Security Intelligence Logging

As a first line of defense against malicious Internet content, the Firepower System includes the Security Intelligence feature, which allows you to immediately blacklist (block) connections based on the latest reputation intelligence, removing the need for a more resource-intensive, in-depth analysis. This traffic filtering takes place **before** most other policy-based inspection, analysis, or traffic handling, although it does occur after hardware-level handling, such as fast-pathing.

Enabling Security Intelligence logging logs all blocked and monitored connections handled by an access control policy's target devices. Logging monitored connections allows the system to further analyze connections that would have been blacklisted, but still log the match to the blacklist. The system does not log whitelist matches, however; logging of whitelisted connections depends on their eventual disposition.

When the system logs a connection event as the result of Security Intelligence filtering, it also logs a matching Security Intelligence event, which is a special kind of connection event that you can view and analyze separately. Both types of events use the **Action** and **Reason** fields to reflect the blacklist match. Additionally, so that you can identify the blacklisted IP address in the connection, host icons next to blacklisted and monitored IP addresses look slightly different in the event viewer.

Logging Blocked Blacklisted Connections

For a blocked connection, the system logs beginning-of-connection Security Intelligence and connection events. Because blacklisted traffic is immediately denied without further inspection, there is no unique end of connection to log. For these events, the action is `Block`. The reason is:

- `IP Block` if the system blocked traffic based on the IP address.

- **DNS Block** if the system blocked traffic based on the domain name.
- **URL Block** if the system blocked traffic based on the URL.

IP Block, **DNS Block**, and **URL Block** connection events have a threshold of 15 seconds per unique initiator-responder pair. That is, once the system generates an event when it blocks a connection, it does not generate another connection event for additional blocked connections between those two hosts for the next 15 seconds, regardless of port or protocol.

Logging Monitored Blacklisted Connections

For connections monitored—rather than blocked—by Security Intelligence, the system logs end-of-connection Security Intelligence and connection events to the Firepower Management Center database. This logging occurs regardless of how the connection is later handled by an SSL policy, access control rule, or the access control default action.

For these connection events, the action depends on the connection’s eventual disposition. The **Reason** field contains **IP Monitor**, **DNS Monitor**, or **URL Monitor**. It also contains any other reason why the connection may have been logged.

Note that the system may also generate beginning-of-connection events for monitored connections, depending on the logging settings in the access control rule or default action that later handles the connection.

Logging Blacklisted Connections

Smart License	Classic License	Supported Devices	Supported Domains	Access
Threat	Protection	Any	Any	Admin/Access Admin/ Network Admin

When you create an access control policy, the system enables Security Intelligence logging by default. You can configure Security Intelligence logging based on IP address, URL, domain name, or any combination. The system logs blocked and monitored connections handled by an access control policy's target devices.

Procedure

- Step 1** In the access control policy editor, click the **Security Intelligence** tab.
- Step 2** You have the following options:

- To log blocked and monitored connections based on IP address, click the logging icon (📄) next to **Networks**.
- To log blocked and monitored connections based on URL, click the logging icon (📄) next to **URLs**.
- To log blocked and monitored connections based on domain name, click the logging icon (📄) next to the **DNS Policy** drop-down list.

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 3 Check the **Log Connections** check box.

Step 4 Specify where to send connection and Security Intelligence events.

Note You **must** send events to the Firepower Management Center if you want to perform Firepower Management Center-based analysis, or if you want to set blacklisted objects to monitor-only.

Step 5 Click **OK** to set your logging options.

Step 6 Click **Save**.

What to Do Next

- Deploy configuration changes; see [Deploying Configuration Changes](#).

SSL Policy Connection Logging

As part of access control, the *SSL inspection* feature allows you to use an SSL policy to decrypt encrypted traffic for further evaluation by access control rules. In the SSL policy, you can log end-of-connection events for encrypted connections, as follows:

- for blocked connections (Block, Block with reset), the system immediately ends the session and generates an event
- for monitored connections (Monitor) and connections that you pass to access control rules (Decrypt, Do not decrypt), the system generates an event when the session ends, regardless of the logging configuration of the access control rule or default action that later handles it

Connection logs for encrypted sessions contain details about the encryption, such as the certificate used to encrypt that session.

Logging Decryptable Connections with SSL Rules

Smart License	Classic License	Supported Devices	Supported Domains	Access
Threat	Protection	Any	Any	Admin/Access Admin/Network Admin/Security Approver

So that you log only critical connections, you can enable connection logging on a per-SSL-rule basis. If you enable connection logging for a rule, the system logs all connections handled by that rule.

Procedure

-
- Step 1** In the SSL policy editor, click the edit icon () next to the rule where you want to configure logging. If a view icon () appears instead, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.

- Step 2** Select the **Logging** tab.
- Step 3** Check **Log at End of Connection**.
- Step 4** Specify where to send connection events.
Note You **must** send events to the Firepower Management Center if you want to perform Management Center-based analysis on these connection events, or if the rule action is **Monitor**.
- Step 5** Click **Add** to save your changes.

What to Do Next


- Deploy configuration changes; see [Deploying Configuration Changes](#).

Logging Encrypted and Undecryptable Connections with the SSL Policy Default Action

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Access Admin/Network Admin/Security Approver

Logging settings for the SSL policy default action also govern how the system logs undecryptable sessions. Note that even if you disable logging for the SSL policy default action, end-of-connection events may still be logged to the Firepower Management Center database if the connection previously matched at least one SSL Monitor rule, or later matches an access control rule or the access control policy default action.

Procedure

- Step 1** In the SSL policy editor, click the logging icon () next to the **Default Action** drop-down list.
- Step 2** Select **Log at End of Connection** to enable logging connection events.
If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.
- Step 3** Specify where to send connection events.
Note You **must** send events to the Firepower Management Center if you want to perform Management Center-based analysis on these connection events. However, note that traffic handled by the SSL policy default action is not further inspected for intrusions, malware, or discovery data.
- Step 4** Click **OK** to save your changes.

What to Do Next

- Deploy configuration changes; see [Deploying Configuration Changes](#).

Access Control Policy Connection Logging



Logging Connections with Access Control Rules

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Access Admin/Network Admin

Within an access control policy, access control rules provide a granular method of handling network traffic across multiple managed devices. So that you can log only critical connections, you enable connection logging on a per-access-control-rule basis—if you enable connection logging for a rule, the system logs all connections handled by that rule. Depending on the rule action and intrusion and file inspection configuration of the rule, your logging options differ.

Note that even if you disable logging for an access control rule, end-of-connection events for connections matching that rule may still be logged to the Firepower Management Center database if the connection contains an intrusion attempt, prohibited file, or malware; was inspected and logged by an SSL policy; or previously matched at least one access control Monitor rule.

Procedure

-
- Step 1** In the access control policy editor, click the edit icon () next to the rule where you want to configure logging. If a view icon () appears instead, the configuration is inherited from an ancestor policy, belongs to an ancestor domain, or you do not have permission to modify the configuration.
- Step 2** Click the **Logging** tab.
- Step 3** Specify whether you want to **Log at Beginning of Connection** or **Log at End of Connection**. To optimize performance, log either the beginning or the end of any connection, but not both.
- Step 4** Check the **Log Files** check box to specify whether the system should log any file and malware events associated with the connection. Cisco recommends you leave this option enabled if the rule invokes file or malware inspection.
- Step 5** Specify where to send connection events. You **must** send events to the Firepower Management Center if you want to perform Management Center-based analysis on these connection events, or if the rule action is **Monitor**.
- Step 6** Click **Save** to save the rule.
-

What to Do Next

- Deploy configuration changes; see [Deploying Configuration Changes](#).

Logging Connections with the Access Control Policy Default Action

The mechanisms and options for logging connections handled by the access control policy’s default action largely parallel the options for logging connections handled by individual access control rules. That is, except for blocked traffic, you can log the beginning and end of connections, and you can send connection events to the Firepower Management Center database, or to an external syslog or SNMP trap server.

Table 2: Access Control Default Action Logging Options

Default Action	Compare To
Access Control: Block All Traffic	Block rules
Access Control: Trust All Traffic	Trust rules
Intrusion Prevention	Allow rules with associated intrusion policies
Network Discovery Only	Allow rules without associated intrusion policies
Inherit from base policy	Any of the above, as indicated by the policy editor

However, there are some differences between logging connections handled by access control rules versus the default action:

- The default action has no file logging options. You cannot perform file control or AMP using the default action.
- When an intrusion policy associated with the access control default action generates an intrusion event, the system does **not** automatically log the end of the associated connection. This is useful for intrusion detection and prevention-only deployments, where you do not want to log any connection data.

An exception to this rule occurs if you enable beginning-of-connection logging for the default action. In that case, the system **does** log the end of the connection when an associated intrusion policy triggers, in addition to logging the beginning of the connection.


Logging Connections Handled by the Access Control Default Action

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin/Access Admin/Network Admin

You can log connections for the traffic handled by the default action of your access control policy. The default action determines how the system handles traffic that matches none of the access control rules in the policy (except Monitor rules, which match and log—but do not handle or inspect—traffic).

Note that even if you disable logging for the default action, end-of-connection events for connections matching that rule may still be logged to the Firepower Management Center database if the connection was inspected and logged by an SSL policy or previously matched at least one access control Monitor rule.

Procedure

-
- Step 1** In the access control policy editor, click the logging icon () next to the **Default Action** drop-down list.
- Step 2** Specify whether you want to **Log at Beginning of Connection** or **Log at End of Connection**. If the controls are dimmed, the configuration belongs to an ancestor domain, or you do not have permission to modify the configuration.
- Tip** To optimize performance, log either the beginning or the end of any connection, but not both.
- Step 3** Specify where to send connection events.
- Note** You **must** send events to the Firepower Management Center if you want to perform Firepower Management Center-based analysis on these connection events.
- Step 4** Click **Save** to save the policy.
-

What to Do Next

- Deploy configuration changes; see [Deploying Configuration Changes](#).



Limiting Logging of Long URLs

Smart License	Classic License	Supported Devices	Supported Domains	Access
Any	Any	Any	Any	Admin Access Admin Network Admin

End-of-connection events for HTTP traffic record the URL requested by monitored hosts. Depending on your network traffic, disabling or limiting the number of stored URL characters may improve system performance.

Disabling URL logging (storing zero characters) does not affect URL filtering. Access control rules properly filter traffic based on requested URLs even though the system does not record them.

Procedure

-
- Step 1** In the access control policy editor, click the **Advanced** tab, then click the edit icon () next to **General Settings**.
- If a view icon () appears instead, the configuration is inherited from an ancestor policy, belongs to an ancestor domain, 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** Type the **Maximum URL characters to store in connection events**. Storing zero characters disables URL storage without disabling URL filtering.
- Step 3** Click **OK**.
- Step 4** Click **Save** to save the policy.
-

What to Do Next

- Deploy configuration changes; see [Deploying Configuration Changes](#).

