Logging Connections in Network Traffic

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

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.

Saving connection events to the Defense Center database allows you to take advantage of many reporting, analysis, and data correlation features of the FireSIGHT System; see Working with Connection & Security Intelligence Data, page 39-1. Or, you can send connection data to an external system log (syslog) or SNMP trap server.

To supplement the connection data gathered by your managed devices, you can use records generated by NetFlow-enabled devices to generate connection events. This is especially useful if you have NetFlow-enabled devices deployed on networks that your FireSIGHT System managed devices cannot monitor.

Note Because NetFlow data collection is not linked to access control, you do not have granular control over which NetFlow connections you want to log. FireSIGHT System managed devices detect records exported by NetFlow-enabled devices, generate unidirectional end-of-connection events based on the data in those records, and finally send those events to the Defense Center to be logged in the database. NetFlow records cannot generate Security Intelligence events, nor be logged to an external server. For more information, see Understanding NetFlow, page 45-16.

For more information on logging connection data, see:

- Deciding Which Connections To Log, page 38-2
- Logging Security Intelligence (Blacklisting) Decisions, page 38-11
- Logging Encrypted Connections, page 38-13
- Logging Connections Based on Access Control Handling, page 38-15
- Logging URLs Detected in Connections, page 38-19

Deciding Which Connections To Log

License: Any

Using various settings in access control and SSL policies, you can log any non-fast-pathed connection that your devices monitor. In most cases, you can log a connection at its beginning or its end, or both. 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.

When you log a connection event, you can save it to the Defense Center database for further analysis using the FireSIGHT System. Or, you can send connection data to an external syslog or SNMP trap server.

Tip To perform detailed analysis of connection data using the FireSIGHT System, Cisco recommends you log the ends of critical connections to the Defense Center database.

For more information, see:

- Logging Critical Connections, page 38-3
- Logging the Beginning or End of Connections, page 38-4
- Logging Connections to the Defense Center or External Server, page 38-5
- Understanding How Access Control and SSL Rule Actions Affect Logging, page 38-6
- License and Model Requirements for Connection Logging, page 38-9

Logging Critical Connections

License: Any

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.

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 a Block rule, consider whether the rule monitors traffic on an Internet-facing interface or other interface vulnerable to DoS attack.

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 using the system policy, regardless of your other logging configurations, the system saves these end-of-connection events to the Defense Center database for further analysis. All connection events reflect why they were automatically logged using the Action and Reason fields; see Action, page 39-5 and Reason, page 39-8.

Security Intelligence Blacklisting Decisions (Optional)

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. For more information, see Logging Security Intelligence (Blacklisting) Decisions, page 38-11.

Encrypted Connections (Optional)

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. For more information, see Logging Encrypted Connections, page 38-13.

Access Control Handling (Optional)

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. For more information, see Logging Connections Based on Access Control Handling, page 38-15.

Connections Associated with Intrusions (Automatic)

When an intrusion policy invoked by an access control rule (see Tuning Traffic Flow Using Access Control Rules, page 14-1) detects an intrusion and generates an intrusion event, the system automatically logs the end of the connection where the intrusion occurred to the Defense Center database, regardless of the logging configuration of the rule.

However, when an intrusion policy associated with the access control default action (see Setting Default Handling and Inspection for Network Traffic, page 12-6) 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.

Tip To disable this connection logging on Series 3 or virtual devices, use the CLI; see log-ips-connections, page D-31.

Connections Associated with File and Malware Events (Automatic)

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 Defense 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).

Logging the Beginning or End of Connections

License: Any

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; see Understanding Logging for Monitored Connections, page 38-6.

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

Table 38-1 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: • 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: • 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: • 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

Logging Connections to the Defense Center or External Server

License: Any

You can log connection events to the Defense Center database, as well as to an external syslog or SNMP trap server. Before you can log connection data to an external server, you must configure a connection to that server called an *alert response*; see Working with Alert Responses, page 43-2.

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

- Dashboards and the Context Explorer provide you with graphical, at-a-glance views of the connections logged by the system; see Using Dashboards, page 55-1 and Using the Context Explorer, page 56-1.

- 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; see Working with Connection & Security Intelligence Data, page 39-1.
- 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; see Creating Traffic Profiles, page 53-1.
- 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; see Creating Rules for Correlation Policies, page 51-2.

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

The number of connection and Security Intelligence events a Defense Center can store depends on its model. For a list of those limits, and for information on disabling connection event storage, see Configuring Database Event Limits, page 63-15.

Understanding How Access Control and SSL Rule Actions Affect Logging

License: feature dependent

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.

Note Logging connections allowed by the access control and SSL policy default actions is handled slightly differently; see Logging Connections Handled by the Access Control Default Action, page 38-17 and Setting Default Logging for Encrypted and Undecryptable Connections, page 38-14.

For more information, see:

- Using Rule Actions to Determine Traffic Handling and Inspection, page 14-7
- Using Rule Actions to Determine Encrypted Traffic Handling and Inspection, page 21-8
- Understanding Logging for Monitored Connections, page 38-6
- Understanding Logging for Trusted Connections, page 38-7
- Understanding Logging for Blocked and Interactively Blocked Connections, page 38-7
- Understanding Logging for Allowed Connections, page 38-8
- Disabling File and Malware Event Logging for Allowed Connections, page 38-9

Understanding Logging for Monitored Connections

License: feature dependent

The system always logs the ends of the following connections to the Defense 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; see Logging Security Intelligence (Blacklisting) Decisions, page 38-11.

Because monitored traffic is always later handled by another rule or by the default action, the action associated with a connection 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; see Action, page 39-5.

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 Defense 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. For more information, see Specifying Correlation Rule Trigger Criteria, page 51-5.

Understanding Logging for Trusted Connections

License: feature dependent

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 Series 3 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.

Understanding Logging for Blocked and Interactively Blocked Connections

License: feature dependent

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; see Understanding Logging for Allowed Connections, page 38-8.

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 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.

Understanding Logging for Allowed Connections

License: feature dependent

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 Defense 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 Defense 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; see Action, page 39-5 and Reason, page 39-8. 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.

Disabling File and Malware Event Logging for Allowed Connections

License: Protection or Malware

Supported Devices: feature dependent

Supported Defense Centers: feature dependent

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; see Tuning Intrusion Prevention Performance, page 18-8. Note that because you cannot use a Malware license with a DC500, nor enable a Malware license on a Series 2 device or Cisco NGIPS for Blue Coat X-Series, you cannot use those appliances for malware protection.

When the system detects a prohibited file, it automatically logs one of the following types of event to the Defense 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 by clearing the **Log Files** check box on the Logging tab of the access control rule editor. For information on disabling file and malware event storage entirely, see Configuring Database Event Limits, page 63-15.

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 Defense Center database, regardless of the logging configuration of the invoking access control rule; see Connections Associated with File and Malware Events (Automatic), page 38-4.

License and Model Requirements for Connection Logging

License: feature dependent

Because you configure connection logging in access control and SSL policies, you can log any connection that those policies can successfully handle.

Although you can create access control and SSL policies regardless of the licenses on your Defense Center, certain aspects of access control require that you enable specific licensed capabilities on target devices before you can apply the policy. Additionally, some features are only available on certain models.

Note that with a FireSIGHT license, which is included with your Defense Center, you can add host, user, and application data to the network map based on the information in connection logs, as well as view indications of compromise (IOC) information associated with connection events. Except on the DC500, you can also view geolocation data (source or destination country or continent) associated with connections.

The following table explains the licenses you must have to successfully configure access control, and therefore to log connections handled by an access control policy.

Table 38-2 License and Model Requirements for Connection Logging in Access Control Policies

To log connections...	License	Supported Defense Centers	Supported Devices
for traffic handled using, network, VLAN, port, or literal URL criteria	Any	Any	Any, except: • Series 2 devices cannot perform URL filtering • ASA FirePOWER devices cannot perform VLAN filtering
for traffic handled using geolocation data	FireSIGHT	Any except DC500	Any except Series 2 or X-Series
associated with: • IP addresses with a poor reputation (Security Intelligence filtering) • intrusions or prohibited files in unencrypted or decrypted traffic	Protection	Any	Any, except Series 2 devices cannot perform Security Intelligence filtering
associated with malware detected in unencrypted or decrypted traffic	Malware	Any except DC500	Any except Series 2 or X-Series
for traffic handled by user control or application control	Control	Any, except the DC500 cannot perform user control	Any except Series 2 or X-Series
for traffic that the system filters using URL category and reputation data, and to display URL category and URL reputation information for URLs requested by monitored hosts	URL Filtering	Any except DC500	Any except Series 2

The following table explains the licenses you must have to successfully configure SSL inspection, and therefore to log connections handled by an SSL policy. Keep in mind that even if an encrypted connection is not logged (or even examined) by an SSL policy, it still may be logged for other reasons.

Table 38-3 License and Model Requirements for Connection Logging in SSL Policies

To log connections...	License	Supported Defense Centers	Supported Devices
for encrypted traffic handled using zone, network, VLAN, port, or SSL-related criteria	Any	Any	Series 3
for encrypted traffic handled using geolocation data	FireSIGHT	Any except DC500	Series 3
for encrypted traffic handled using application or user criteria	Control	Any, except the DC500 cannot perform user control	Series 3
for encrypted traffic that the system filters using URL category and reputation data	URL Filtering	Any except DC500	Series 3

Logging Security Intelligence (Blacklisting) Decisions

License: Protection

Supported Devices: Any except Series 2

Supported Defense Centers: Any except DC500

As a first line of defense against malicious Internet content, the FireSIGHT 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** any other policy-based inspection, analysis, or traffic handling, although it does occur after hardware-level handling, such as fast-pathing.

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.

Note If you want to create traffic profiles based on Security Intelligence information, or trigger correlation rules using Security Intelligence information in end-of-connection events, you **must** log this information to the Defense Center database. First, enable Security Intelligence logging. Then, build a blacklist using monitor-only Security Intelligence objects. For more information, see Blacklisting Using Security Intelligence IP Address Reputation, page 13-1.

Enabling Security Intelligence logging logs all blocked and monitored connections handled by an access control policy's target devices. However, the system does not log whitelist matches; 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` and the reason is `IP Block`.

`IP 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 Defense 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`, as well as 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.

To log blacklisted connections:

Access: Admin/Access Admin/Network Admin

Step 1 Select **Policies > Access Control**.

The Access Control Policy page appears.

Step 2 Click the edit icon ( ) next to the access control policy you want to configure.

The access control policy editor appears.

Step 3 Select the Security Intelligence tab.

Security Intelligence settings for the access control policy appear.

Step 4 Click the logging icon ( ).

The Blacklist Options pop-up window appears.

Step 5 Select the **Log Connections** check box.

Step 6 Specify where to send connection and Security Intelligence events. You have the following choices:

- To send events to the Defense Center, select **Defense Center**.
- To send events to an external syslog server, select **Syslog**, then select a syslog alert response from the drop-down list. Optionally, you can add a syslog alert response by clicking the add icon ( ); see Creating a Syslog Alert Response, page 43-5.
- To send connection events to an SNMP trap server, select **SNMP Trap**, then select an SNMP alert response from the drop-down list. Optionally, you can add an SNMP alert response by clicking the add icon ( ); see Creating an SNMP Alert Response, page 43-4.

You **must** send events to the Defense Center if you want to set blacklisted objects to monitor-only, or perform any other Defense Center-based analysis on connection events generated by Security Intelligence filtering. For more information, see Logging Connections to the Defense Center or External Server, page 38-5.

Step 7 Click **OK** to set your logging options.

The Security Intelligence tab appears again.

Step 8 Click **Save**.

You must apply the access control policy for your changes to take effect; see Applying an Access Control Policy, page 12-15.

Logging Encrypted Connections

License: SSL

Supported Devices: Series 3

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. You can force the system to log these decrypted connections, regardless of how the system later handles or inspects the traffic. You can also log connections when you block encrypted traffic, or when you allow it to pass to access control rules without decryption.

Connection logs for encrypted sessions contain details about the encryption, such as the certificate used to encrypt that session. You configure connection logging for encrypted sessions in the SSL policy on a per-SSL rule basis so that you only log critical connections.

For more information, see the following sections:

- Logging Decryptable Connections with SSL Rules, page 38-13
- Setting Default Logging for Encrypted and Undecryptable Connections, page 38-14

Logging Decryptable Connections with SSL Rules

License: SSL

Supported Devices: Series 3

Within an SSL policy, *SSL rules* provide a granular method of handling encrypted traffic across multiple managed devices. So that you can log only critical connections, you 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.

For encrypted connections inspected by an SSL policy, you can log connection events to the Defense Center database, or to an external syslog or SNMP trap server. You can log only end-of-connection events, however:

- 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

For more information, see Understanding How Access Control and SSL Rule Actions Affect Logging, page 38-6.

To log decryptable connections:

Access: Admin/Access Admin/Network Admin/Security Approver

Step 1 Select **Policies > SSL**.

The SSL Policy page appears.

Step 2 Click the edit icon ( ) next to the SSL policy you want to edit.

The SSL policy editor appears, focused on the Rules tab.

Step 3 Click the edit icon ( ) next to the rule where you want to configure logging.

The SSL rule editor appears.

Step 4 Select the Logging tab.

The Logging tab appears.

Step 5 Select **Log at End of Connection**.

Step 6 Specify where to send connection events. You have the following choices:

- To send connection events to the Defense Center, select **Defense Center**. When your rule action is **Monitor**, you must log connections to the Defense Center.
- To send events to an external syslog, select **Syslog**, then select a syslog alert response from the drop-down list. Optionally, you can add a syslog alert response by clicking the add icon ( ); see Creating a Syslog Alert Response, page 43-5.
- To send events to an SNMP trap server, select **SNMP Trap**, then select an SNMP alert response from the drop-down list. Optionally, you can add an SNMP alert response by clicking the add icon ( ); see Creating an SNMP Alert Response, page 43-4.

You **must** send events to the Defense Center if you want to perform Defense Center-based analysis on these connection events. For more information, see Logging Connections to the Defense Center or External Server, page 38-5.

Step 7 Click **Add** to save your changes.

You must apply the access control policy the SSL policy is associated with for your changes to take effect; see Applying an Access Control Policy, page 12-15.

Setting Default Logging for Encrypted and Undecryptable Connections

License: SSL

Supported Devices: Series 3

You can log connections for the traffic handled by the default action of your SSL policy. These logging settings also govern how the system logs undecryptable sessions.

The SSL policy default action determines how the system handles encrypted traffic that matches none of the SSL rules in the policy (except Monitor rules, which match and log—but do not handle or inspect—traffic). If your SSL policy does not contain any SSL rules, the default action determines how all encrypted sessions on your network are logged. For more information, see Setting Default Handling and Inspection for Encrypted Traffic, page 20-3.

You can configure the SSL policy default action to log connection events to the Defense Center database, or to an external syslog or SNMP trap server. You can log only end-of-connection events, however:

- for blocked connections (Block, Block with reset), the system immediately ends the sessions and generates an event
- for connections that you allow to pass unencrypted to access control rules (Do not decrypt), the system generates an event when the session ends

Note that even if you disable logging for the SSL policy default action, end-of-connection events may still be logged to the Defense 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.

To set the default handling for encrypted and undecryptable traffic:

Access: Admin/Access Admin/Network Admin/Security Approver

Step 1 Select **Policies > SSL**.

The SSL Policy page appears.

Step 2 Click the edit icon ( ) next to the SSL policy you want to edit.

The SSL policy editor appears, focused on the Rules tab.

Step 3 Click the logging icon ( ) next to the **Default Action** drop-down list.

The Logging pop-up window appears.

Step 4 Select **Log at End of Connection** to enable logging connection events.

Step 5 Specify where to send connection events. You have the following choices:

- To send connection events to the Defense Center, select **Defense Center**.
- To send events to an external syslog server, select **Syslog**, then select a syslog alert response from the drop-down list. Optionally, you can configure a syslog alert response by clicking the add icon ( ); see Creating a Syslog Alert Response, page 43-5.
- To send events to an SNMP trap server, select **SNMP Trap**, then select an SNMP alert response from the drop-down list. Optionally, you can configure an SNMP alert response by clicking the add icon ( ); see Creating an SNMP Alert Response, page 43-4.

You **must** send events to the Defense Center if you want to perform Defense 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. For more information, see Logging Connections to the Defense Center or External Server, page 38-5.

Step 6 Click **OK** to save your changes.

You must apply the access control policy the SSL policy is associated with for your changes to take effect; see Applying an Access Control Policy, page 12-15.

Logging Connections Based on Access Control Handling

License: Any

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.

You can also 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 all access control rules and the default action, end-of-connection events may still be logged to the Defense Center database if the connection matches an access control rule and contains an intrusion attempt, prohibited file, or malware, or if it was decrypted by the system and you enabled logging for the connection in the SSL policy.

Depending on the rule or default policy action and the associated inspection options that you configure, your logging options differ. For more information, see:

- Logging Connections Matching an Access Control Rule, page 38-16
- Logging Connections Handled by the Access Control Default Action, page 38-17

Logging Connections Matching an Access Control Rule

License: Any

To log only critical connections, you enable connection logging on a per-access-control-rule basis. If you enable 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; see Understanding How Access Control and SSL Rule Actions Affect Logging, page 38-6. Also, 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 Defense Center database if the connection:

- contains an intrusion attempt, prohibited file, or malware
- was inspected and logged by an SSL policy
- previously matched at least one access control Monitor rule

To configure an access control rule to log connection, file, and malware information:

Access: Admin/Access Admin/Network Admin

Step 1 Select **Policies > Access Control**.

The Access Control Policy page appears.

Step 2 Click the edit icon ( ) next to the access control policy you want to modify.

The access control policy editor appears, focused on the Rules tab.

Step 3 Click the edit icon ( ) next to the rule where you want to configure logging.

The access control rule editor appears.

Step 4 Select the Logging tab.

The Logging tab appears.

Step 5 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.

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. Because blocked traffic is immediately denied without further inspection, you can log only beginning-of-connection events for Block rules.

Also note that because the purpose of a Monitor rule is to log matching traffic, end-of-connection logging to the Defense Center database is auto-enabled and you cannot disable it. For more information, see Logging the Beginning or End of Connections, page 38-4.

Step 6 Use the **Log Files** check box to specify whether the system should log any file and malware events associated with the connection.

The system automatically enables this option when you associate a file policy with the rule to perform either file control or AMP. Cisco recommends you leave this option enabled; see Disabling File and Malware Event Logging for Allowed Connections, page 38-9.

Step 7 Specify where to send connection events. You have the following choices:

- To send connection events to the Defense Center, select **Defense Center**. You cannot disable this option for Monitor rules.
- To send events to an external syslog server, select **Syslog**, then select a syslog alert response from the drop-down list. Optionally, you can add a syslog alert response by clicking the add icon ( ); see Creating a Syslog Alert Response, page 43-5.
- To send events to an SNMP trap server, select **SNMP Trap**, then select an SNMP alert response from the drop-down list. Optionally, you can add an SNMP alert response by clicking the add icon ( ); see Creating an SNMP Alert Response, page 43-4.

You **must** send events to the database if you want to perform Defense Center-based analysis on connection events. For more information, see Logging Connections to the Defense Center or External Server, page 38-5.

Step 8 Click **Save** to save the rule.

Your rule is saved. You must apply the access control policy for your changes to take effect; see Applying an Access Control Policy, page 12-15.

Logging Connections Handled by the Access Control Default Action

License: Any

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); see Setting Default Handling and Inspection for Network Traffic, page 12-6.

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

Table 38-4 Access Control Default Action Logging Options

Default Action	Compare To	See...
Access Control: Block All Traffic	Block rules	Understanding Logging for Blocked and Interactively Blocked Connections, page 38-7
Access Control: Trust All Traffic	Trust rules	Understanding Logging for Trusted Connections, page 38-7

Table 38-4 Access Control Default Action Logging Options (continued)

Default Action	Compare To	See...
Intrusion Prevention	Allow rules with associated intrusion policies	Understanding Logging for Allowed Connections, page 38-8
Network Discovery Only	Allow rules without associated intrusion policies	

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.

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 Defense Center database if the connection previously matched at least one access control Monitor rule, or was inspected and logged by an SSL policy.

To log connections in traffic handled by the access control default action:

Access: Admin/Access Admin/Network Admin

Step 1 Select **Policies > Access Control**.

The Access Control Policy page appears.

Step 2 Click the edit icon ( ) next to the access control policy you want to modify.

The access control policy editor appears, focused on the Rules tab.

Step 3 Click the logging icon ( ) next to the **Default Action** drop-down list.

The Logging pop-up window appears.

Step 4 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 these connections, but not both. 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. Because blocked traffic is immediately denied without further inspection, you can log only beginning-of-connection events for the Block All Traffic default action.

Step 5 Specify where to send connection events. You have the following choices:

- To send connection events to the Defense Center, select **Defense Center**. You cannot disable this option for Monitor rules.
- To send events to an external syslog server, select **Syslog**, then select a syslog alert response from the drop-down list. Optionally, you can add a syslog alert response by clicking the add icon ( ); see Creating a Syslog Alert Response, page 43-5.

- To send events to an SNMP trap server, select **SNMP Trap**, then select an SNMP alert response from the drop-down list. Optionally, you can add an SNMP alert response by clicking the add icon ( ); see Creating an SNMP Alert Response, page 43-4.

You **must** send events to the database if you want to perform Defense Center-based analysis on connection events. For more information, see Logging Connections to the Defense Center or External Server, page 38-5.

Step 6 Click **Save** to save the policy.

Your policy is saved. You must apply the access control policy for your changes to take effect; see Applying an Access Control Policy, page 12-15.

Logging URLs Detected in Connections

License: FireSIGHT

When you log an end-of-connection event to the Defense Center database for HTTP traffic, the system records the URL requested by the monitored host during the session.

By default, the system stores the first 1024 characters of the URL in the connection log. However, you can configure the system to store up to 4096 characters per URL to make sure you capture the full URLs requested by monitored hosts. Or, if you are uninterested in the individual URLs visited, you can disable URL storage entirely by storing zero characters. Depending on your network traffic, disabling or limiting the number of stored URL characters may improve system performance.

Note that disabling URL logging does not affect URL filtering. Access control rules properly filter traffic based on requested URLs, their categories, and reputations, even though the system does not record the individual URLs requested in the traffic handled by those rules. For more information, see Blocking URLs, page 16-8.

To customize the number of URL characters you store:

Access: Admin/Access Admin/Network Admin

Step 1 Select **Policies > Access Control**.

The Access Control Policy page appears.

Step 2 Click the edit icon ( ) next to the access control policy you want to configure.

The access control policy editor appears.

Step 3 Select the Advanced tab.

Advanced settings for the access control policy appear.

Step 4 Click the edit icon ( ) next to General Settings.

The General Settings pop-up window appears.

Step 5 Type the **Maximum URL characters to store in connection events**.

You can specify any number from zero to 4096. Storing zero characters disables URL storage without disabling URL filtering.

Step 6 Click **OK**.

Advanced settings for the access control policy appear.

Step 7 Click **Save** to save the policy.

Your policy is saved. You must apply the access control policy for your changes to take effect; see Applying an Access Control Policy, page 12-15.