

Context Explorer

The following topics describe how to use the Context Explorer:

- Context explorer, on page 1
- Requirements for the Context Explorer, on page 18
- Reload the context explorer, on page 18
- Set the context explorer time range, on page 19
- Minimize and maximize context explorer sections, on page 19
- Drill down on context explorer data, on page 20
- Filters in the context explorer, on page 21

Context explorer

The **Context Explorer** is a network monitoring tool that

- displays detailed, interactive graphical information about network status, including applications, connections, hosts, security events, and geolocation data
- shows data with line, bar, pie, and donut graphs, as well as detailed lists, to support your analysis
- provides a single, consistent layout that you can explore actively, with manual updates and a broader data context.

Key features and capabilities

The **Context Explorer** provides these key capabilities:

- Create and apply custom filters to fine-tune your analysis.
- Click or hover over graph areas to examine data sections.
- You can configure time ranges from one hour to one year.

The Context Explorer differs from the dashboard in these ways:

Table 1: Context explorer versus dashboard

Dashboard	Context Explorer
Highly customizable and compartmentalized	Single, consistent layout

Dashboard	Context Explorer
Updates in real time	Manually updated
Monitors real-time activity according to specific needs	Investigates predefined set of recent data in granular detail
Compact, narrowly focused widgets	Visual representations help you view broader context

Data availability depends on your licensing, how you deploy your managed devices, and which features are configured. In multidomain deployments, the **Context Explorer** aggregates and displays data from all subdomains for ancestor domains. Leaf domains contain only domain-specific data.

You need an **Administrator**, **Security Analyst**, or **Security Analyst (Read Only)** user role to access **Context Explorer**.

Differences between the dashboard and the context explorer

This table summarizes some of the key differences between the **Dashboard** and the **Context Explorer**.

Table 2: Comparison: dashboard and context explorer

Feature	Dashboard	Context explorer
Displayable data	Anything monitored by the system	Applications, application statistics, geolocation, host indications of compromise, intrusion events, files (including malware files), hosts, Security Intelligence events, servers, users, and URLs
Customizability	• Selection of widgets for a dashboard is customizable • Individual widgets can be customized to varying degrees	• Cannot change base layout • Applied filters appear in explorer URL and can be bookmarked for later use
Data update frequency	Automatic (default); user-configured	Manual
Data filtering	Possible for some widgets (must edit widget preferences)	Possible for all parts of the explorer, with support for multiple filters
Graphical context	Some widgets (particularly Custom Analysis) can display data in graph form	Extensive graphical context for all data, including uniquely detailed donut graphs
Links to relevant web interface pages	In some widgets	In every section
Time range of displayed data	User-configured	User-configured

Related Topics

Dashboards

Traffic and intrusion event counts time graph

A traffic and intrusion event counts time graph is a line chart that displays traffic in kilobytes and intrusion event counts over configurable time intervals. This graph displays at the top of the **Context Explorer** page.

This section draws data primarily from the **Intrusion Events** and **Connection Events** tables.

The graph uses specific time interval processing and display behaviors:

- The X-axis plots time intervals (which range from five minutes to one month, depending on the selected time window).
- The Y-axis plots traffic in kilobytes (blue line) and intrusion event count (red line).
- The smallest X-axis interval is five minutes. To accommodate this, Firewall Management Center will round the beginning and ending points in your selected time range down to the nearest five-minute interval.

Filter behavior affects graph display:

- By default, this section shows all network traffic and all generated intrusion events for the selected time range. This graph adapts dynamically to show filtered data when **Context Explorer** filters are applied. For example, filtering on the **OS Name** of Windows causes the time graph to display only traffic and events associated with hosts using Windows operating systems.
- If you filter the **Context Explorer** on intrusion event data (such as a **Priority** of `High`), the blue Traffic line is hidden to allow greater focus on intrusion events alone.

You can interact with the graph to gain deeper insights into network activity:

- Place your pointer over any point on the graph lines to view exact information about traffic and event counts.
- Place your pointer over one of the colored lines to bring that line to the forefront of the graph and get clearer context.

Indications of compromise section

An Indications of Compromise (IOC) section is a **Context Explorer** feature that contains two interactive sections that provide an overall picture of potentially compromised hosts on your monitored network.

It provides a proportional view of the most prevalent IOC types triggered, as well as a view of hosts by number of triggered indications.

For more information about IOCs, see Indications of compromise data.

Hosts by indication graph

The **Hosts by Indication** graph is adonut-form chart that displays a proportional view of the Indications of Compromise (IOC) triggered by hosts on your monitored network.

This graph divides data by IOC category in the inner ring, such as `CnC Connected` or `Malware Detected`.

it further divides that data by specific event type in the outer ring, such as `Impact 2 Intrusion Event — attempted-admin` or `Threat Detected in File Transfer`.

This graph draws data primarily from the Hosts and Host Indications of Compromise tables.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view detailed information.
- Click on any part of the graph to filter or drill down into specific event data.

Indications by host graph

The **Indications by Host** graph is a bar graph that displays counts of unique Indications of Compromise (IOC) triggered by the 15 most IOC-active hosts on your monitored network.

This graph draws data primarily from the Hosts and Indications of Compromise tables.

Graph interaction features

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view detailed information.
- Click on any part of the graph to filter or drill down into specific event data.

Network information section

The **Network Information** section is a **Context Explorer** component that contains six interactive graphs that display an overall picture of connection traffic on your monitored network.

The **Network Information** section displays information about:

- Sources associated with traffic.
- Destinations associated with traffic.
- Users associated with traffic.
- Security zones associated with traffic.
- Operating systems used by hosts on the network.
- Proportional view of access control actions performed on network traffic.

Operating systems graph

The **Operating Systems** graph is a donut-form chart that

- displays a proportional representation of operating systems detected on hosts on your monitored network
- divides by OS name in the inner ring (such as `Windows` or `Linux`) while the outer ring further divides that data by specific operating system version (such as `Windows Server 2008` or `Linux 11.x`), and
- groups closely related operating systems, such as Windows 2000, Windows XP, and Windows Server 2003 together, and
- groups infrequent applications under **Other**.

This graph draws data primarily from the **Hosts** table.

This graph reflects all available data regardless of date and time constraints. Adjusting the explorer time range does not update the graph.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view detailed information.
- Click on any part of the graph to filter or drill down into specific event data.

Traffic by source IP graph

The **Traffic by Source IP** graph is a bar graph that displays counts of network traffic (in kilobytes per second) and unique connections for the top 15 most active source IP addresses on your monitored network. It uses blue bars to represent traffic data and red bars to represent connection data for each source IP address listed.

This graph draws data primarily from the Connection Events table.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view more detailed information.
- Click on any part of the graph to filter or drill down into specific event data.



Note If you filter on intrusion event information, the **Traffic by Source IP** graph is hidden.

Traffic by source user graph

A Traffic by Source User graph is bar chart that displays counts of network traffic (in kilobytes per second) and unique connections for the top 15 most active source users on your monitored network. It uses blue bars to represent traffic data and red bars to represent connection data for each source IP address.

This graph draws data primarily from the **Connection Events** table.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view more detailed information.
- Click on any part of the graph to filter or drill down into specific event data.



Note If you filter on intrusion event information, the **Traffic by Source User** graph is hidden.

Connections by access control action graph

The connections by access control action graph is a pie chart that displays a proportional view of access control actions (such as `Block` or `Allow`) taken on monitored traffic.

This graph draws data primarily from the Connection Events table.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view detailed information.

- Click on any part of the graph to filter or drill down into specific event data.

Note If you filter on intrusion event information, the **Traffic by Source User** graph is hidden.

Traffic by destination IP graph

A traffic by destination IP graph is a bar chart that displays counts of network traffic in kilobytes per second and unique connections for the top 15 most active destination IP addresses on your monitored network. This graph draws data primarily from the **Connection Events** table.

For each destination IP address listed, blue bars represent traffic data and red bars represent connection data.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view more detailed information.
- Click on any part of the graph to filter or drill down into specific event data.

Note If you filter on intrusion event information, the **Traffic by Destination IP** graph is hidden.

Traffic by ingress or egress security zone graphs

The traffic by ingress or egress security zone graph is a bar graph that displays counts of incoming or outgoing network traffic (in kilobytes per second) and unique connections for each security zone configured on your monitored network. This graph draws data primarily from the **Connection Events** table.

For each security zone listed, blue bars represent traffic data and red bars represent connection data.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view more detailed information.
- Click on any part of the graph to filter or drill down into specific event data.
- You can configure this graph to display either ingress (the default) or egress security zone information. To display only traffic by egress security zone in the graph, complete these steps:
  1. Move your pointer over the graph, then click **Egress** on the toggle button that appears.
  2. Click **Ingress** to return to the default view.

     If you navigate away from the **Context Explorer**, the graph returns to the default view.

Note If you filter on intrusion event information, the **Traffic by Ingress or Egress Security Zone** graph is hidden.

Application information section

The **Application Information** section is a component of context explorer that

- contains three interactive graphs and one table-format list that display an overall picture of application activity on your monitored network
- displays traffic, intrusion events, and hosts associated with applications, further organized by the estimated risk or business relevance assigned to each application, and
- provides the Application Details list as an interactive list of each application and its risk, business relevance, category, and host count.

Application types

For all instances of **application** in this section, the **Application Information** graph, by default, specifically examines application protocols (such as DNS or SSH). You can also configure the **Application Information** section to specifically examine client applications (such as PuTTY or Firefox) or web applications (such as Facebook or Pandora).

Change the focus of Application Protocol Information section

View and select the specific application protocol data types most relevant to your analysis in Context Explorer.

The **Application Protocol Information** section lets you switch between available application data type options in this section to focus on relevant protocol, client, or web application data.

In a multidomain deployment, you can view data for the current domain and for any descendant domains. You cannot view data from higher level or sibling domains.

Procedure

Step 1 Choose **Analysis** > **Context Explorer**.

Step 2 Place your pointer over the **Application Protocol Information** section.

Note
If you have previously changed this setting in the same **Context Explorer** session, title of this section may appear as **Client Application Information** or **Web Application Information** instead.

Step 3 Click **Application Protocol**, **Client Application**, or **Web Application** from the toggle that appears.

Traffic by Risk or Business relevance and application graph

The **Traffic by Risk or Business Relevance and Application** graph is a donut-form chart that displays a proportional representation of application traffic detected on your monitored network, arranged by the applications' estimated risk (the default) or estimated business relevance.

The inner ring separates data by estimated risk or business relevance level (such as `Medium` or `High`), while the outer ring further separates that data by specific application (such as `SSH` or `NetBIOS`). The system groups infrequently detected applications under **Other**.

This graph draws data primarily from the **Connection Events** and Application Statistics tables.



Note This graph reflects all available data regardless of date and time constraints. Adjusting the **Content Explorer** time range does not update the graph.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view more detailed information.
- Click on any part of the graph to filter or drill down into specific event data.
- To display traffic by business relevance and application in the graph, complete these steps:
  1. Move your pointer over the graph, then click **Business Relevance** on the toggle button that appears.
  2. Click **Risk** to return to the default view.

     If you navigate away from the **Context Explorer**, the graph returns to the default view.



Note If you filter on intrusion event information, the **Traffic by Risk or Business and Application** graph is hidden.

Intrusion events by risk or business relevance and application graph

The intrusion events by risk or business relevance and application graph is a donut-form chart that

- displays a proportional representation of intrusion events detected on your monitored network and the applications associated with those events
- arranges data by the applications' estimated risk (the default) or estimated business relevance
- divides information using an inner ring for estimated risk or business relevance level (such as `Medium` or `High`) and an outer ring for specific applications (such as `SSH` or `NetBIOS`), and
- groups infrequent applications under **Other**.

This graph draws data primarily from the **Intrusion Events** and **Application Statistics** tables.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view detailed information.
- Click on any part of the graph to filter or drill down into specific event data.
- To display intrusion events by business relevance and application in this graph, place your pointer over the graph, then click **Business Relevance** on the toggle button that appears. Click **Risk** to return to the default view. If you navigate away from **Context Explorer**, the graph retursn to the default view.

Hosts by risk or business relevance and application graph

The **Hosts by Risk or Business Relevance and Application** graph is a donut-shaped chart that

- displays a proportional representation of hosts detected on your monitored network and the applications associated with those hosts
- arranges data by the applications' estimated risk (the default) or estimated business relevance
- divides information using an inner ring for estimated risk or business relevance level (such as `Medium` or `High`) and an outer ring for specific applications (such as `SSH` or `NetBIOS`), and
- groups infrequent applications under **Other**.

This graph draws data primarily from the **Applications** table.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view detailed information.
- Click on any part of the graph to filter or drill down into specific event data.
- To displays hosts by business relevance and application in this graph, place your pointer over the graph, then click **Business Relevance** on the toggle button that appears. Click **Risk** to return to the default view. If you navigate away from **Context Explorer**, the graph returns to the default view.

Application details list

The **Application Details** list is a table that provides estimated risk, estimated business relevance, category, and hosts count information for each application detected on your monitored network.

This table draws data primarily from the Applications table.

The **Application Details** list has these features:

- The **Application Details** list table is not sortable, but you can click on any table entry to filter or drill down on that information, or (where applicable) to view application information.
- Displays applications in descending order of associated host count.
- The list displays all available data regardless of date and time constraints. Adjusting the **Context Explorer** time range does not update the list.

Security intelligence section

Security Intelligence is a section in **Context Explorer** that

- contains three interactive bar graphs that display an overall picture of traffic on your monitored network
- shows traffic that is blocked or monitored by Security Intelligence, and
- sorts traffic by category, source IP address, and destination IP address with both traffic amount (in kilobytes per second) and number of applicable connections.

Security intelligence traffic by category graph

The **Security Intelligence Traffic by Category** graph is a bar graph that displays counts of network traffic (in kilobytes per second) and unique connections for the top Security Intelligence categories of traffic on your monitored network. It uses blue bars to represent traffic data and red bars to represent connection data for each category listed.

This graph draws data primarily from the **Security-Related Connection Events** table.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view detailed information.
- Click on any part of the graph to filter or drill down into specific event data.



Note If you filter on intrusion event information, the **Security Intelligence Traffic by Category** graph is hidden.

Security intelligence traffic by source IP graph

A Security Intelligence Traffic by Source IP graph is a bar chart that displays counts of network traffic (in kilobytes per second) and unique connections for the top source IP addresses of Security Intelligence-monitored traffic on your network. For each category listed, blue bars represent traffic data and red bars represent connection data.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view detailed information.
- Click on any part of the graph to filter or drill down into specific event data.



Note If you filter on intrusion event information, the **Security Intelligence Traffic by Source I**P graph is hidden.

Security intelligence traffic by destination IP graph

The Security Intelligence Traffic by Destination IP Graph is a bar graph that displays counts of network traffic (in kilobytes per second) and unique connections for the top destination IP addresses of Security Intelligence-monitored traffic on your monitored network. It uses blue bars to represent traffic data and red bars to represent connection data for each category listed.

This graph draws data primarily from the Security Intelligence Events table.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view more detailed information.
- Click any part of the graph to drill down on that information.



Note If you filter on intrusion event information, the **Security Intelligence Traffic by Destination IP** graph is hidden.

Intrusion information section

The **Intrusion Information** section is a **Context Explorer** component that

- contains six interactive graphs and one table-format list that display an overall picture of intrusion events on your monitored network
- shows impact levels, attack sources, target destinations, users, priority levels, and security zones associated with intrusion events, and
- provides a detailed list of intrusion event classifications, priorities, and counts.

Intrusion events by impact graph

The **Intrusion Events by Impact** graph is a pie chart that displays a proportional view of intrusion events on your monitored network. It groups events by estimated impact level from 0 to 4.

This graph draws data primarily from the intrusion detection (IDS Statistics) and Intrusion Events tables.

Interactive features

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view detailed information.
- Click on any part of the graph to filter or drill down into specific event data.

The top attackers graph

The top attackers graph is a bar chart that displays counts of intrusion events for the top attacking host IP addresses on your monitored network.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view more detailed information.
- Click on any part of the graph to filter or drill down into specific event data.

The Top Users Graph

The **Top Users** graph is a bar chart that displays users on your monitored network that are associated with the highest intrusion event counts, by event count.

This graph draws data primarily from the intrusion detection (IDS) User Statistics and **Intrusion Events** tables.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view more detailed information.
- Click on any part of the graph to filter or drill down into specific event data.

Intrusion events by priority graph

The Intrusion Events by Priority Graph is a pie chart visualization that displays a proportional view of intrusion events on your monitored network, grouped by estimated priority level (such as `High`, `Medium`, or `Low`).

This graph draws data primarily from the **Intrusion Events** table.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view detailed information.
- Click on any part of the graph to filter or drill down into specific event data.

Top targets graph

The **Top Targets** graph is a bar chart that displays counts of intrusion events for the top target host IP addresses (targeted in the connections causing those events) on your monitored network.

This graph draws data primarily from the **Intrusion Events** table.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view more detailed information.
- Click on any part of the graph to filter or drill down into specific event data.

Top ingress or egress security zones graph

The **Top Ingress or Egress Security Zones** graph is a bar graph that displays counts of intrusion events associated with each security zone (ingress or egress, depending on graph settings) configured on your monitored network. This graph draws data primarily from the **Intrusion Events** table.

You can configure this graph to display either ingress (the default) or egress security zone information, according to your needs.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view more detailed information.
- Click on any part of the graph to filter or drill down into specific event data.
- To display only traffic by egress security zone in the graph, complete these steps:
  1. Move your pointer over the graph, then click **Egress** on the toggle button that appears.
  2. Click **Ingress** to return to the default files view.

     If you navigate away from the **Context Explorer**, the graph returns to the default files view.

Intrusion event details list

The **Intrusion Event Details** list is a table that provides classification, estimated priority, and event count information for each intrusion event detected on your monitored network.

This table draws data primarily from the Intrusion Events table.

You can interact with the graph to gain deeper insights into network activity:

- Click on any part of the graph to filter or drill down into specific event data.
- This table lists events in descending order of event count and it does not support sorting the data.

Files information section

The **Files Information** section is a Context Explorer component that contains six interactive graphs and displays an overall picture of file and malware events on your monitored network.

Five of the graphs display data related to malware defense (formerly called AMP for Firepower):

- File types detected in network traffic
- File names detected in network traffic
- Malware dispositions of the files detected in network traffic
- Hosts sending (uploading) files
- Hosts receiving (downloading) files

The final graph displays all malware threats detected in your organization, whether by malware defense or Secure Endpoint.



Note If you filter on intrusion information, the entire **Files Information** section is hidden.

The Top File Types Graph

The **Top File Types** graph is a donut chart that provides a proportional view of file types detected in network traffic, categorized by their specific file group. The outer ring displays individual file types and the inner ring displays file categories. This graph draws information primarily from the **File Events** table.



Note You must have a Malware license for this graph to display malware defense data.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view detailed information.
- Click on any part of the graph to filter or drill down into specific event data.

Top file names graph

The **Top File Names** graph is a bar chart that displays counts of the top unique file names detected in network traffic. This graph draws data primarily from the **File Events** table.



Note You must have a Malware license to for this graph to display malware defense data.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view more detailed information.
- Click on any part of the graph to filter or drill down into specific event data.

Files by disposition graph

The **Files by Disposition** Graph is a pie chart that displays proportional malware dispositions for files detected by the malware defense feature (formerly called AMP for Firepower).

This graph draws data primarily from the **File Events** table.



Note You must have a Malware license for this graph to display malware defense data.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view detailed information.
- Click on any part of the graph to filter or drill down into specific event data.

Disposition types

The graph displays specific disposition categories:

- The files for which Secure Firewall Management Center performed a malware cloud lookup have dispositions.
- Files that did not trigger a cloud lookup have a disposition of `N/A`.
- The disposition `Unavailable` indicates that the Secure Firewall Management Center could not perform a malware cloud lookup.

Top hosts sending files graph

The **Top Hosts Sending Files** graph is a bar chart that displays counts of the number of files detected in network traffic for the top file-sending host IP addresses. It provides specialized filtering capabilities for malware detection. This graph draws data primarily from the **File Events** table.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view more detailed information.
- Toggle between the files view and the malware view using the controls that appear when you place your pointer over the graph.
- Click on any part of the graph to filter or drill down into specific event data.
- To display only hosts receiving malware in the graph, complete these steps:
  1. Move your pointer over the graph, then click **Malware** on the toggle button that appears.
  2. Click **Files** to return to the default files view.

     If you navigate away from the **Context Explorer**, the graph returns to the default files view.



Note Note that you must have a Malware license to for this graph to display malware defense data.

Top hosts receiving files graphs

The **Top Hosts Receiving Files** graph is a bar chart that displays counts of the number of files detected in network traffic for the top file-receiving host IP addresses. This graph draws data primarily from the **File Events** table.

Note You must have a Malware license for this graph to display malware defense data.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view more detailed information.
- Toggle between the files view and the malware view using the controls that appear when you place your pointer over the graph.
- Click on any part of the graph to filter or drill down into specific event data.
- To display only hosts receiving malware in the graph, complete these steps:
  1. Move your pointer over the graph, then click **Malware** on the toggle button that appears.
  2. Click **Files** to return to the default files view.

     If you navigate away from the **Context Explorer**, the graph returns to the default files view.

Top malware detections graph

The **Top Malware Detections** graph is a bar chart visualization that displays counts of the top malware threats detected in your organization from both malware defense and Secure Endpoint.

This graph draws data primarily from the **File Events** and **Malware Events** tables.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view more detailed information.
- Click on any part of the graph to filter or drill down into specific event data.

Note Note that you must have a Malware license to for this graph to display malware defense data.

Geolocation information section

The **Geolocation Information** is a section in **Context Explorer** that contains three interactive donut-form graphs displaying an overall picture of countries with which hosts on your monitored network are exchanging data.

The three graphs in **Geolocation Information** section displays these data:

- Unique connections by initiator or responder country
- Intrusion events by source or destination country

- File events by sending or receiving country.

Connections by Initiator or Responder country graph

The **Connections by Initiator or Responder Country** graph is a donut-form chart that displays a proportional view of the countries involved in connections on your network as either the initiator (the default) or the responder. The inner ring groups these countries together by continent.

This graph draws data primarily from the **Connection Summary** data table.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view detailed information.
- Click on any part of the graph to filter or drill down into specific event data.
- To display only countries acting as the responder in connections, place your pointer over the graph, then click **Responder** on the toggle button that appears. Click **Initiator** to return to the default view. If you navigate away from **Context Explorer**, the graph returns to the default view.

Intrusion events by Source or Destination country graph

The Intrusion Events by Source or Destination Country graph is a donut-form chart that displays a proportional view of countries involved in intrusion events on your network as either the source or destination.

This graph draws data primarily from the **Intrusion Events** table.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view detailed information.
- Click on any part of the graph to filter or drill down into specific event data.
- To display only countries acting as the destinations of intrusion events in this graph, place your pointer over the graph, then click **Destination** on the toggle button that appears. Click **Source** to return to the default view. If you navigate away from **Context Explorer**, the graph returns to the default view.

File events by sending or receiving country graph

The file events by sending or receiving country graph is a donut-form chart that displays a proportional view of the countries detected in file events on your network as either sending (the default) or receiving files. The inner ring groups these countries together by continent.

This graph draws data primarily from the File Events table.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view detailed information.
- Click on any part of the graph to filter or drill down into specific event data.
- To display only countries receiving files in this graph, place your pointer over the graph, then click **Receiver** on the toggle button that appears. Click **Sender** to return to the default view. If you navigate away from **Context Explorer**, the graph returns to the default view.

URL information section

URL Information is a section of the **Context Explorer** that displays an overall view of URLs with which hosts on your monitored network are exchanging data. It uses three interactive bar graphs to display traffic and unique connections associated with URLs, sorted by individual URL, URL category, and URL reputation.



Note

- If you filter on intrusion event information, the entire **URL Information** section is hidden.
- You must have a URL Filtering license for this graph to include URL category and reputation data.

Traffic by URL graph

The **Traffic by URL** graph is a bar chart that displays counts of network traffic (in kilobytes per second) and unique connections for the top 15 most requested URLs on your monitored network. It uses blue bars to represent traffic data and red bars to represent connection data for each URL listed.

This graph draws data primarily from the Connection Events table.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view more detailed information.
- Click on any part of the graph to filter or drill down into specific event data.



Note

- If you filter on intrusion event information, the **Traffic by URL** graph is hidden.
- You must have a URL Filtering license for this graph to include URL category and reputation data.

Traffic by URL category graphs

A **Traffic by URL Category** graph is a bar graph that displays counts of network traffic (in kilobytes per second) and unique connections for the most requested URL categories (such as `Search Engines` or `Streaming Media`) on your monitored network. It uses blue bars to represent traffic data and red bars to represent connection data for each URL category listed.

This graph draws data primarily from the URL Statistics and Connection Events tables.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view more detailed information.
- Click on any part of the graph to filter or drill down into specific event data.



Note

- If you filter on intrusion event information, the **Traffic by URL Category** graph is hidden.
- You must have a URL Filtering license for this graph to include URL category and reputation data.

Traffic by URL reputation graph

The **Traffic by URL Reputation** graph is a bar chart that displays counts of network traffic (in kilobytes per second) and unique connections for the most requested URL reputation groups (such as Trusted or Neutral) on your monitored network. It uses blue bars to represent traffic data and red bars to represent connection data for each URL reputation listed.

This graph draws data primarily from the **URL Statistics** and **Connection Events** tables.

You can interact with the graph to gain deeper insights into network activity:

- Move your pointer over any part of the graph to view more detailed information.
- Click on any part of the graph to filter or drill down into specific event data.



Note

- If you filter on intrusion event information, the **Traffic by URL Reputation** graph is hidden.
- You must have a URL Filtering license for this graph to include URL category and reputation data.

Requirements for the Context Explorer

You must meet these requirements to access and use the **Context Explorer** feature in Firewall Management Center.

- Configure and deploy your devices to generate events, and enable event logging so that Firewall Management Center can display that data.
- Ensure your devices are properly licensed so relevant event data is available in Firewall Management Center. You must have a Malware license to view Malware Defense data and a URL Filtering license to view URL category and reputation data.
- Ensure that you have one of these user roles assigned:
  - Admin
  - Security Analyst
  - Security Analyst (Read Only)

Reload the context explorer

The Context Explorer does not update information automatically. Reload the explorer to view new data.



Note If you reload the Context Explorer by refreshing the browser or by leaving and returning to the Context Explorer, all displayed information is refreshed. Changes to section configuration, such as the ingress or egress graphs and the **Application Protocol Information** section, are not preserved. This process may also cause loading delays.

In a multidomain deployment, you can view data for the current domain and for any descendant domains. You cannot view data from higher level or sibling domains.

Procedure

Step 1 Choose **Analysis** > **Context Explorer**.

Step 2 Click **Reload** at the upper right.

Reload is dimmed until your refresh is finished.

Set the context explorer time range

Configure the Context Explorer time range to display data from as little as the past hour (the default) to up to the past year.

When you change the time range, the Context Explorer does not automatically update to reflect the change. You must manually reload the explorer to apply the new time range.

Changes to the time range persist even if you navigate away from the Context Explorer or end your login session.

In a multidomain deployment, you can view data for the current domain and for any descendant domains. You cannot view data from higher level or sibling domains.

Procedure

Step 1 Choose **Analysis** > **Context Explorer**.

Step 2 From the **Show the last** drop-down list, choose a time range.

Step 3 To reload the Context Explorer and view data from the new time range, click **Reload**.

Alternatively, clicking **Apply Filters** will also apply any updates to the time range.

Minimize and maximize context explorer sections

Minimizing and maximizing Context Explorer sections helps you focus on specific areas. Hiding sections you do not need creates a simpler view.

You cannot minimize the **Traffic** and **Intrusion Event Counts Time** graph. Context Explorer sections keep their minimized or maximized states, even if you refresh the page or log out of the appliance.

In a multidomain deployment, you can view data for the current domain and for any descendant domains. You cannot view data from higher level or sibling domains.

Procedure

Step 1 Choose **Analysis** > **Context Explorer**.

Step 2 To minimize a section, click **Collapse Arrow** ( ) in a section's title bar.

Step 3 To maximize a section, click maximize **Expand Arrow** ( ) in a minimized section's title bar.

Drill down on context explorer data

Drilling down allows you to examine graph or list data in more detail than the Context Explorer allows by accessing table views of relevant data.

If you want to examine graph or list data in more detail than the Context Explorer allows, you can drill down to the table views of the relevant data. (Note that you cannot drill down on the Traffic and Intrusion Events over Time graph.) For example, drilling down on an IP address in the Traffic by Source IP graph displays the Connections with Application Details view of the Connection Events table, including only data associated with the source IP address you selected.

Depending on the type of data you examine, additional options can appear in the context menu. Data points that are associated with specific IP addresses offer the option to view host or whois information on the IP address you select. Data points associated with specific applications offer the option to view application information on the application you select. Data points associated with a specific user offer the option to view that user's user profile page. Data points associated with an intrusion event message offer the option to view the rule documentation for that event's associated intrusion rule, and data points associated with a specific IP address offer the option to add that address to a Block or Do Not Block list. For more information about these lists, see *Global and Domain Security Intelligence List* in the *Cisco Secure Firewall Management Center Device Configuration Guide*.

In a multidomain deployment, you can view data for the current domain and for any descendant domains. You cannot view data from higher level or sibling domains.

Procedure

Step 1 Choose **Analysis** > **Context Explorer**.

Step 2 In any section except **Traffic and Intrusion Events over Time**, click a data point that you want to investigate.

Step 3 Depending on the data point you selected, you have several options:

- To view more details of this data in a table view, choose **Drill into Analysis**.
- If you chose a data point associated with a specific IP address and want more information about the associated host, choose **View Host Information**.
- If you chose a data point with a specific IP address and want to make a whois search on that address, choose **Whois**.
- If you chose a data point associated with a specific application and want more information about that application, choose **View Application Information**.

- If you chose a data point associated with a specific user and want more information about that user, choose **View User Information**.
- If you chose a data point associated with a specific intrusion event message and want more information about the associated intrusion rule, choose **View Rule Documentation**; optionally, then click **Rule Documentation** to view more-specific rule details
- If you chose a data point associated with a specific IP address and want to add that IP address to the Security Intelligence global Block or Do Not Block list, choose the appropriate option.

The system displays the requested detailed view, host information, application information, user information, rule documentation, or adds the IP address to the specified list based on your selection.

Filters in the context explorer

The **Filter** option in the Context Explorer enables you to filter the wide-ranging data that the Context Explorer initially displays for more granular contextual analysis of activity on your network. The **Filter** option provides these capabilities:

- Encompasses all types of system data except URL information.
- Supports exclusion as well as inclusion criteria.
- Supports adding up to 20 filters simultaneously.

Filter application methods AND behavior

You can add filters to Context Explorer data in several ways:

- from the Add Filter dialog
- from the context menu, when you select a data point in the explorer
- from the text links that appear in certain detail view pages (Application Detail, Host Profile, Rule Detail, AND User Profile). Clicking these links automatically opens AND filters the Context Explorer according to the relevant data on the detail view page. For example, clicking the Context Explorer link on a user detail page for the user **jenkins** constrains the explorer to show only data associated with that user

Some filter types are incompatible with others: for example, filters that relate to intrusion events (such as **Device** AND **Inline Result**) cannot be applied at the same time as connection event-related filters (such as **Access Control Action**) because the system cannot sort connection event data by intrusion event data. The system automatically prevents incompatible filters from simultaneously applying; when one filter type is more recently activated, filters of the incompatible type are hidden as long as the incompatibility exists.

When multiple filters are active, values for the same data type are treated as OR search criteria: all data that matches at least one of the values appears. Values for different data types are treated as AND search criteria: to appear, data must match at least one value for each filtered data type. For example, data that appears for the filter set of **Application: 2channel**, **Application: Reddit**, AND **User: edickinson** must be associated with the user **edickinson AND** either the application **2channel OR** the application **Reddit**.

In a multidomain deployment, you can filter by multiple descendant domains when viewing the Context Explorer in an ancestor domain. In such cases, use caution when also adding **IP Address** filters. The system

builds a separate network map for each leaf domain. Using literal IP addresses to constrain this configuration can have unexpected results.

Note that the data displayed depends on such factors as how you license AND deploy your managed devices AND whether you configure features that provide the data.

Note Filters function as a simple, agile tool to get the precise data context you need at any given time. They are not intended as permanent configuration settings, AND disappear when you navigate away from the Context Explorer OR end your session. To preserve filter settings for later use, see Save filtered context explorer views, on page 25.

Data type field options

This table provides a comprehensive list of data types that can be used as filters to refine and manage network event data.

Table 3: Filter data types

Type	Example values	Definition
Access Control Action	`Allow` , `Block`	Action taken by your access control policy to allow or block traffic.
Application Category	`web browser` , `email`	General classification of an application's most essential function.
Application Name	`Facebook` , `HTTP`	Name of an application.
Application Risk	`Very High` , `Medium`	Estimated security risk of an application.
Application Tag	`encrypts communications` , `sends mail`	Additional information about an application; applications can have any number of tags, including none.
Application Type	`Client` , `Web Application`	Type of an application: application protocol, client, or web application.
Business Relevance	`Very Low` , `High`	Estimated relevance of an application to business activity (as opposed to recreation).
Continent	`North America` , `Asia`	Continent associated with a routable IP address detected on your monitored network.
Country	`Canada` , `Japan`	Country associated with a routable IP address detected on your monitored network.
Device	`device1.example.com` , `192.168.1.3`	Name or IP address of a device on your monitored network.
Domain	`Asia Division` , `Europe Division`	The domain of the device whose network activity you want to graph. This data type is only present in a multidomain deployment.

Type	Example values	Definition
Event Classification	`Potential Corporate Policy Violation`, `Attempted Denial of Service`	Capsule description of an intrusion event, determined by the classification of the rule, decoder, or preprocessor that triggered it.
Event Message	`dns response`, `P2P`	Message generated by an event, determined by the rule, decoder, or preprocessor that triggered it.
File Disposition	`Malware`, `Clean`	Disposition of a file for which the Secure Firewall Management Center performed a malware cloud lookup.
File Name	`Packages.bz2`	Name of a file detected in network traffic.
File SHA256	any 32-bit string	SHA-256 hash value of a file for which the Secure Firewall Management Center performed a malware cloud lookup.
File Type	`GZ`, `SWF`, `MOV`	File type detected in network traffic.
File Type Category	`Archive`, `Multimedia`, `Executables`	General category of file type detected in network traffic.
IP Address	`192.168.1.3`, `2001:0db8:85a3::0000/24`	IPv4 or IPv6 addresses, address ranges, or address blocks. Note that searching for an IP address returns events where that address was either the source or the destination for the event.
Impact Level	`Impact Level 1`, `Impact Level 2`	Estimated impact of an event on your monitored network.
Inline Result	`dropped`, `would have dropped`	Whether traffic was dropped, would have been dropped, or was not acted upon by the system.
IOC Category	`High Impact Attack`, `Malware Detected`	Category for a triggered Indication of Compromise (IOC) event.
IOC Event Type	`exploit-kit`, `malware-backdoor`	Identifier associated with a specific Indication of Compromise (IOC), referring to the event that triggers it.
Malware Threat Name	`W32.Trojan.a6b1`	The name of a malware threat.
OS Name	`Windows`, `Linux`	Name of an operating system.
OS Version	`XP`, `2.6`	Specific version of an operating system.
Priority	`high`, `low`	Estimated urgency of an event.
Security Intelligence Category	`Malware`, `Spam`	Category of risky traffic, as determined by Security Intelligence.
Security Zone	`My Security Zone`, `Security Zone X`	A set of interfaces through which traffic is analyzed and, in an inline deployment, passes.
SSL	`yes`, `no`	SSL- or TLS-encrypted traffic.
User	`wsmith`, `mtwain`	Identity of a user logged in to a host on your monitored network.

Create a filter from the Add Filter window

Create filters from scratch with the **Add Filter** window to constrain the Context Explorer display.

Alternatively, you can also use the context menu to create quick filters.

In a multidomain deployment, you can view data for the current domain and for any descendant domains. You cannot view data from higher level or sibling domains.

Before you begin

Follow these steps to create a filter from the Add Filter window:

Procedure

Step 1 Choose **Analysis** > **Context Explorer**.

Step 2 Under **Filters** at the top left, click the **Plus** (+) icon.

Step 3 From the **Data Type** drop-down list, choose the data type you want to filter on.

Step 4 In the **Filter** field, enter the data type value you want to filter on.

In the **Filter** field, you can input special search parameters such as * and ! essentially as you can in event searches. You can create exclusion filters by prefixing filter parameters with the ! symbol.

Step 5 Click **OK**.

Step 6 Optionally, repeat the previous steps to add more filters until you have the filter set you need.

Step 7 Click **Apply Filters**.

Related Topics

Data type field options, on page 22
Search constraints

Create a quick filter from the context menu

Create a filter from Context Explorer graph or list data by selecting a data point from the context menu.

While exploring Context Explorer graph and list data, you can click on data points, then use the context menu to quickly create a filter based on that data, either inclusive or exclusive. If you use the context menu to filter on information of data type Application, User, or Intrusion Event Message, or any individual host, the filter widget includes widget information that links to the relevant detail page for that data type (such as Application Detail for application data).

Note Filtering on URL data is not supported.

Procedure

Step 1 Choose **Analysis** > **Context Explorer**.

Step 2 In any Context Explorer section except **Traffic** and **Intrusion Events over Time** or sections that contain URL data, click a data point you want to filter on.

Step 3 You have these options:

- To add a filter for this data, click **Add Filter**.
- To add an exclusion filter for this data, click **Add Exclude Filter**. The filter, when applied, displays all data **not** associated with the excluded value. Exclude filters display an exclamation point (!) before the filter value.

Save filtered context explorer views

You can save specific filter configurations in the Context Explorer by creating browser bookmarks that capture the current page URL.

To preserve filter settings in the Context Explorer after you navigate away from the Context Explorer or end your session, create a browser bookmark of the Context Explorer with your preferred filters applied. When filters are applied in Context Explorer, they are incorporated into the page URL. By creating a browser bookmark with the desired filters set, you can return to the same filtered view by loading the bookmark in their browser. This feature allows for consistent access to customized views without needing to reapply filter settings each time.

View filter data

In a multidomain deployment, you can view data for the current domain and for any descendant domains. You cannot view data from higher level or sibling domains.

Procedure

Step 1 Choose **Analysis** > **Context Explorer** .

Step 2 Click **Information** on any eligible filter widget.

Delete a filter

Delete individual filter widgets or all filters at once in the Context Explorer.

Use this procedure to remove filter widgets that are no longer needed in your Context Explorer view.

Procedure

Step 1 Choose **Analysis** > **Context Explorer**.

Step 2 Under **Filters** at the top left, click **Close** (✕) to delete the filter widget individually.

Tip
To delete all filters at once, click **Clear**.