Context Explorer

The following topics describe how to use the Context Explorer:

About the Context Explorer

The Context Explorer displays detailed, interactive graphical information in context about the status of your monitored network, including data on applications, application statistics, connections, geolocation, indications of compromise, intrusion events, hosts, servers, Security Intelligence, users, files (including malware files), and relevant URLs. Distinct sections present this data in the form of vivid line, bar, pie, and donut graphs, accompanied by detailed lists. The first section, a line chart of traffic and event counts over time, provides an at-a-glance picture of recent trends in your network's activity.

You can easily create and apply custom filters to fine-tune your analysis, and you can examine data sections in more detail by simply clicking or hovering your cursor over graph areas. You can also configure the explorer's time range to reflect a period as short as the last hour or as long as the last year. Only users with the Administrator, Security Analyst, or Security Analyst (Read Only) user roles have access to the Context Explorer.

The dashboard is highly customizable and compartmentalized and updates in real time. In contrast, the Context Explorer is manually updated, designed to provide broader context for its data, and has a single, consistent layout designed for active user exploration.

You use the dashboard to monitor real-time activity on your network and appliances according to your own specific needs. Conversely, you use the Context Explorer to investigate a predefined set of recent data in granular detail and clear context: for example, if you notice that only 15% of hosts on your network use Linux, but account for almost all YouTube traffic, you can quickly apply filters to view data only for Linux hosts, only for YouTube-associated application data, or both. Unlike the compact, narrowly focused dashboard widgets, the Context Explorer sections are designed to provide striking visual representations of system activity in a format useful to both expert and casual users.

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. You can also apply filters to constrain the data that appears in all Context Explorer sections.

In a multidomain deployment, the Context Explorer displays aggregated data from all subdomains when you view it in an ancestor domain. In a leaf domain, you can view data specific to that domain only.

Differences Between the Dashboard and the Context Explorer

The following table summarizes some of the key differences between the dashboard and the Context Explorer.

Table 1: 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

About Dashboards

The Traffic and Intrusion Event Counts Time Graph

At the top of the Context Explorer is a line chart of traffic and intrusion events over time. 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).

Note that the smallest X-axis interval is five minutes. To accommodate this, the system will round the beginning and ending points in your selected time range down to the nearest five-minute interval.

By default, this section shows all network traffic and all generated intrusion events for the selected time range. If you apply filters, the chart changes to display only traffic and intrusion events associated with the criteria

specified in the filters. 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 hover your pointer over any point on the graph lines to view exact information about traffic and event counts. Hovering your pointer over one of the colored lines also brings that line to the forefront of the graph, providing clearer context.

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

The Indications of Compromise Section

The Indications of Compromise (IOC) section of the Context Explorer contains two interactive sections that provide an overall picture of potentially compromised hosts on your monitored network: 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.

The Hosts by Indication Graph

The Hosts by Indication graph, in donut form, displays a proportional view of the Indications of Compromise (IOC) triggered by hosts on your monitored network. The inner ring divides by IOC category (such as `CnC Connected` or `Malware Detected`), while the outer ring further divides that data by specific event type (such as `Impact 2 Intrusion Event — attempted-admin` or `Threat Detected in File Transfer`).

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

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

The Indications by Host Graph

The Indications by Host graph, in bar form, displays counts of unique Indications of Compromise (IOC) triggered by the 15 most IOC-active hosts on your monitored network.

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

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

The Network Information Section

The Network Information section of the Context Explorer contains six interactive graphs that display an overall picture of connection traffic on your monitored network: sources, destinations, users, and security zones associated with traffic, a breakdown of operating systems used by hosts on the network, as well as a proportional view of access control actions that have been performed on network traffic.

The Operating Systems Graph

The Operating Systems graph, in donut form, displays a proportional representation of operating systems detected on hosts on your monitored network. The inner ring divides by OS name (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`). Some closely related operating systems (such as Windows 2000, Windows XP, and

Windows Server 2003) are grouped together. Very scarce or unrecognized operating systems are grouped under **Other**.

Note that this graph reflects all available data regardless of date and time constraints. If you change the explorer time range, the graph does not change.

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

This graph draws data primarily from the Hosts table.

The Traffic by Source IP Graph

The Traffic by Source IP graph, in bar form, 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. For each source IP address listed, blue bars represent traffic data and red bars represent connection data.

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

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

This graph draws data primarily from the Connection Events table.

The Traffic by Source User Graph

The Traffic by Source User graph, in bar form, displays counts of network traffic (in kilobytes per second) and unique connections for the top 15 most active source users on your monitored network. For each source IP address listed, blue bars represent traffic data and red bars represent connection data.

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

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

This graph draws data primarily from the Connection Events table. It displays authoritative user data.

The Connections by Access Control Action Graph

The Connections by Access Control Action graph, in pie form, displays a proportional view of access control actions (such as `Block` or `Allow`) taken on monitored traffic.

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

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

This graph draws data primarily from the Connection Events table.

The Traffic by Destination IP Graph

The Traffic by Destination IP graph, in bar form, 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. For each destination IP address listed, blue bars represent traffic data and red bars represent connection data.

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

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

This graph draws data primarily from the Connection Events table.

The Traffic by Ingress/Egress Security Zone Graph

The Traffic by Ingress/Egress Security Zone graph, in bar form, displays counts of incoming or outgoing network traffic (in kilobytes per second) and unique connections for each security zone configured on your monitored network. You can configure this graph to display either ingress (the default) or egress security zone information, according to your needs.

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

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information

Tip To constrain the graph so it displays only traffic by egress security zone, hover your pointer over the graph, then click **Egress** on the toggle button that appears. Click **Ingress** to return to the default view. Note that navigating away from the Context Explorer also returns the graph to the default Ingress view.

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

This graph draws data primarily from the Connection Events table.

The Application Information Section

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

For all instances of "application" in this section, the Application Information graph set, 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).

Focusing the Application Information Section

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 Hover your pointer over the **Application Protocol Information** section.

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

Step 3 Click **Application Protocol**, **Client Application**, or **Web Application**.

The Traffic by Risk/Business Relevance and Application Graph

The Traffic by Risk/Business Relevance and Application graph, in donut form, 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 divides by estimated risk/business relevance level (such as `Medium` or `High`), while the outer ring further divides that data by specific application (such as `SSH` or `NetBIOS`). Scarcely detected applications are grouped under **Other**.

Note that this graph reflects all available data regardless of date and time constraints. If you change the explorer time range, the graph does not change.

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Tip To constrain the graph so it displays traffic by business relevance and application, hover your pointer over the graph, then click **Business Relevance** on the toggle button that appears. Click **Risk** to return to the default view. Note that navigating away from the Context Explorer also returns the graph to the default Risk view.

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

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

The Intrusion Events by Risk/Business Relevance and Application Graph

The Intrusion Events by Risk/Business Relevance and Application graph, in donut form, displays a proportional representation of intrusion events detected on your monitored network and the applications associated with those events, arranged by the applications' estimated risk (the default) or estimated business relevance. The inner ring divides by estimated risk/business relevance level (such as `Medium` or `High`), while the outer ring further divides that data by specific application (such as `SSH` or `NetBIOS`). Scarcely detected applications are grouped under **Other**.

Hover your pointer over any part of the donut graph to view more detailed information. Click any part of the graph to filter or drill down on that information, or (where applicable) to view application information.

Tip To constrain the graph so it displays intrusion events by business relevance and application, hover your pointer over the graph, then click **Business Relevance** on the toggle button that appears. Click **Risk** to return to the default view. Note that navigating away from the Context Explorer also returns the graph to the default Risk view.

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

The Hosts by Risk/Business Relevance and Application Graph

The Hosts by Risk/Business Relevance and Application graph, in donut form, displays a proportional representation of hosts detected on your monitored network and the applications associated with those hosts, arranged by the applications' estimated risk (the default) or estimated business relevance. The inner ring divides by estimated risk/business relevance level (such as `Medium` or `High`), while the outer ring further divides that data by specific application (such as `SSH` or `NetBIOS`). Very scarce applications are grouped under **Other**.

Hover your pointer over any part of the donut graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Tip To constrain the graph so it displays hosts by business relevance and application, hover your pointer over the graph, then click **Business Relevance** on the toggle button that appears. Click **Risk** to return to the default view. Note that navigating away from the Context Explorer also returns the graph to the default Risk view.

This graph draws data primarily from the Applications table.

The Application Details List

At the bottom of the Application Information section is the Application Details List, a table that provides estimated risk, estimated business relevance, category, and hosts count information for each application detected on your monitored network. The applications are listed in descending order of associated host count.

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. This table draws data primarily from the Applications table.

Note that this list reflects all available data regardless of date and time constraints. If you change the explorer time range, the list does not change.

The Security Intelligence Section

The Security Intelligence section of the Context Explorer contains three interactive bar graphs that display an overall picture of traffic on your monitored network that is blocked or monitored by Security Intelligence. The graphs sort such traffic by category, source IP address, and destination IP address, respectively; both the amount of traffic (in kilobytes per second) and the number of applicable connections appear.

The Security Intelligence Traffic by Category Graph

The Security Intelligence Traffic by Category graph, in bar form, displays counts of network traffic (in kilobytes per second) and unique connections for the top Security Intelligence categories of traffic on your monitored network. For each category listed, blue bars represent traffic data and red bars represent connection data.

Hover 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 Category graph is hidden.

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

The Security Intelligence Traffic by Source IP Graph

The Security Intelligence Traffic by Source IP graph, in bar form, 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 monitored network. For each category listed, blue bars represent traffic data and red bars represent connection data.

Hover 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 Source IP graph is hidden.

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

The Security Intelligence Traffic by Destination IP Graph

The Security Intelligence Traffic by Destination IP graph, in bar form, 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. For each category listed, blue bars represent traffic data and red bars represent connection data.

Hover 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.

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

The Intrusion Information Section

The Intrusion Information section of the Context Explorer contains six interactive graphs and one table-format list that display an overall picture of intrusion events on your monitored network: impact levels, attack sources, target destinations, users, priority levels, and security zones associated with intrusion events, as well as a detailed list of intrusion event classifications, priorities, and counts.

The Intrusion Events by Impact Graph

The Intrusion Events by Impact graph, in pie form, displays a proportional view of intrusion events on your monitored network, grouped by estimated impact level (from 0 to 4).

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

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

The Top Attackers Graph

The Top Attackers graph, in bar form, displays counts of intrusion events for the top attacking host IP addresses (causing those events) on your monitored network.

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

This graph draws data primarily from the Intrusion Events table.

The Top Users Graph

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

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

This graph draws data primarily from the intrusion detection (IDS) User Statistics and Intrusion Events tables. It displays authoritative user data.

The Intrusion Events by Priority Graph

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

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

This graph draws data primarily from the Intrusion Events table.

The Top Targets Graph

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

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

This graph draws data primarily from the Intrusion Events table.

The Top Ingress/Egress Security Zones Graph

The Top Ingress/Egress Security Zones graph, in bar form, displays counts of intrusion events associated with each security zone (ingress or egress, depending on graph settings) configured on your monitored network.

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Tip To constrain the graph so it displays only traffic by egress security zone, hover your pointer over the graph, then click **Egress** on the toggle button that appears. Click **Ingress** to return to the default view. Note that navigating away from the Context Explorer also returns the graph to the default Ingress view.

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.

The Intrusion Event Details List

At the bottom of the Intrusion Information section is the Intrusion Event Details List, a table that provides classification, estimated priority, and event count information for each intrusion event detected on your monitored network. The events are listed in descending order of event count.

The Intrusion Event Details List table is not sortable, but you can click on any table entry to filter or drill down on that information. This table draws data primarily from the Intrusion Events table.

The Files Information Section

The Files Information section of the Context Explorer contains six interactive graphs that display 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): the file types, file names, and malware dispositions of the files detected in network traffic, as well as the hosts sending (uploading) and receiving (downloading) those 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, in donut form, displays a proportional view of the file types detected in network traffic (outer ring), grouped by file category (inner ring).

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

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

This graph draws data primarily from the File Events table.

The Top File Names Graph

The Top File Names graph, in bar form, displays counts of the top unique file names detected in network traffic.

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

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

This graph draws data primarily from the File Events table.

The Files by Disposition Graph

The Top File Types graph, in pie form, displays a proportional view of the malware dispositions for files detected by the malware defense feature (formerly called AMP for Firepower). Note that only files for which the 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.

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

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

This graph draws data primarily from the File Events table.

The Top Hosts Sending Files Graph

The Top Hosts Sending Files graph, in bar form, displays counts of the number of files detected in network traffic for the top file-sending host IP addresses.

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Tip To constrain the graph so it displays only hosts sending malware, hover your pointer over the graph, then click **Malware** on the toggle button that appears. Click **Files** to return to the default files view. Note that navigating away from the Context Explorer also returns the graph to the default files view.

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

This graph draws data primarily from the File Events table.

The Top Hosts Receiving Files Graph

The Top Hosts Receiving Files graph, in bar form, displays counts of the number of files detected in network traffic for the top file-receiving host IP addresses.

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Tip To constrain the graph so it displays only hosts receiving malware, hover your pointer over the graph, then click **Malware** on the toggle button that appears. Click **Files** to return to the default files view. Note that navigating away from the Context Explorer also returns the graph to the default files view.

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

This graph draws data primarily from the File Events table.

The Top Malware Detections Graph

The Top Malware Detections graph, in bar form, displays counts of the top malware threats detected in your organization, whether by malware defense or Secure Endpoint.

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

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

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

The Geolocation Information Section

The Geolocation Information section of the Context Explorer contains three interactive donut graphs that display an overall picture of countries with which hosts on your monitored network are exchanging data: unique connections by initiator or responder country, intrusion events by source or destination country, and file events by sending or receiving country.

The Connections by Initiator/Responder Country Graph

The Connections by Initiator/Responder Country graph, in donut form, 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.

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Tip To constrain the graph so it displays only countries acting as the responder in connections, hover your pointer over the graph, then click **Responder** on the toggle button that appears. Click **Initiator** to return to the default view. Note that navigating away from the Context Explorer also returns the graph to the default Initiator view.

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

The Intrusion Events by Source/Destination Country Graph

The Intrusion Events by Source/Destination Country graph, in donut form, displays a proportional view of the countries involved in intrusion events on your network as either the source of the event (the default) or the destination. The inner ring groups these countries together by continent.

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Tip To constrain the graph so it displays only countries acting as the destinations of intrusion events, hover your pointer over the graph, then click **Destination** on the toggle button that appears. Click **Source** to return to the default view. Note that navigating away from the Context Explorer also returns the graph to the default Source view.

This graph draws data primarily from the Intrusion Events table.

The File Events by Sending/Receiving Country Graph

The File Events by Sending/Receiving Country graph, in donut form, 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.

Hover your pointer over any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Tip To constrain the graph so it displays only countries receiving files, hover your pointer over the graph, then click **Receiver** on the toggle button that appears. Click **Sender** to return to the default view. Note that navigating away from the Context Explorer also returns the graph to the default Sender view.

This graph draws data primarily from the File Events table.

The URL Information Section

The URL Information section of the Context Explorer contains three interactive bar graphs that display an overall picture of URLs with which hosts on your monitored network are exchanging data: traffic and unique connections associated with URLs, sorted by individual URL, URL category, and URL reputation. You cannot filter on URL information.

Note If you filter on intrusion event information, the entire URL Information Section is hidden.

Note that you must have a URL Filtering license for this graph to include URL category and reputation data.

The Traffic by URL Graph

The Traffic by URL graph, in bar form, displays counts of network traffic (in kilobytes per second) and unique connections for the top 15 most requested URLs on your monitored network. For each URL listed, blue bars represent traffic data and red bars represent connection data.

Hover 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 Traffic by URL graph is hidden.

Note that you must have a URL Filtering license for this graph to include URL category and reputation data.

This graph draws data primarily from the Connection Events table.

The Traffic by URL Category Graph

The Traffic by URL Category graph, in bar form, 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. For each URL category listed, blue bars represent traffic data and red bars represent connection data.

Hover 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 Traffic by URL Category graph is hidden.

Note that you must have a URL Filtering license for this graph to include URL category and reputation data.

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

The Traffic by URL Reputation Graph

The Traffic by URL Reputation graph, in bar form, 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. For each URL reputation listed, blue bars represent traffic data and red bars represent connection data.

Hover 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 Traffic by URL Reputation graph is hidden.

Note that you must have a URL Filtering license for this graph to include URL category and reputation data.

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

Requirements and Prerequisites for the Context Explorer

Model Support

Any.

Supported Domains

Any

User Roles

- Admin
- Security Analyst

Refreshing the Context Explorer

The Context Explorer does not automatically update the information it displays. To incorporate new data, you must manually refresh the explorer.

Note that, although reloading the Context Explorer itself (by refreshing the browser program or navigating away from, then back to, the Context Explorer) refreshes all displayed information, this does not preserve any changes you made to section configuration (such as the Ingress/Egress graphs and the Application Information section) and may cause delays in loading.

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.

Setting the Context Explorer Time Range

You can configure the Context Explorer time range to reflect a period as short as the last hour (the default) or as long as the last year. Note that when you change the time range, the Context Explorer does not automatically update to reflect the change. To apply the new time range, you must manually refresh the explorer.

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 Optionally, to view data from the new time range, click **Reload**.

Tip Clicking **Apply Filters** also applies any time range updates.

Minimizing and Maximizing Context Explorer Sections

You can minimize and hide one or more sections of the Context Explorer. This is useful if you want to focus on only certain sections, or if you want a simpler view. You cannot minimize the Traffic and Intrusion Event Counts Time Graph.

Context Explorer sections retain the minimized or maximized states that you configure 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.

Drilling Down on Context Explorer 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.

Filters in the Context Explorer

Beyond the basic, wide-ranging data that the Context Explorer initially displays, you have the option to filter that data for a more granular contextual picture of activity on your network. Filters encompass all types of system data except URL information, support exclusion as well as inclusion, can be applied quickly by clicking on Context Explorer graph data points, and affect the entire explorer. You can apply up to 20 filters at a time.

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 Saving Filtered Context Explorer Views, on page 21.

Data Type Field Options

The following table lists the data types available as filters, with examples and brief definitions of each.

Table 2: 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.
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.

Type	Example Values	Definition
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.

Creating a Filter from the Add Filter Window

Use this procedure to create filters from scratch with the Add Filter window. (You can also use the context menu to create quick filters.)

The Add Filter window, which you access by clicking **Plus** (+) under **Filters** at the top left of the Context Explorer, contains only two fields:

- The **Data Type** drop-down list contains many different types of data you can use to constrain the Context Explorer. After you select a data type, you then enter a specific value for that type in the **Filter** field (for example, a value of `Asia` for the type **Continent**). To assist you, the Filter field presents several grayed-out example values for the data type you select. (These are erased when you enter data in the field.)

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

Note Filters that you add are not automatically applied; you must click **Apply Filters** to see the filtering in the Context Explorer.

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 Under **Filters** at the top left, click **Plus** ( ).

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.

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 18
Search Constraints

Creating a Quick Filter 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 a widget information that links to the relevant detail page for that data type (such as Application Detail for application data). Note that you cannot filter on URL data.

You can also use the context menu to investigate specific graph or list data in more detail.

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 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 two 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.

Saving Filtered Context Explorer Views

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. Because applied filters are incorporated in the Context Explorer page URL, loading a bookmark of that page also loads the corresponding filters.

Procedure

Create a browser bookmark of the Context Explorer with your preferred filters applied.

Viewing 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.

Deleting a Filter

Procedure

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

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

Tip If you want to delete all filters at once, you can click **Clear**.