Introduction

As part of your Cox Business Managed Router service, you have access to the Managed Service Activator (MSA) portal, which is a web-based portal application where you can view information and generate reports about Adaptive Security Appliance (ASA) or Integrated Services Routers (ISR) routers located at Cox’s customer sites.

All events sent by MSA-managed or-monitored devices are collected, classified, and analyzed in one place. You can use the MSA portal to see management statistics, security dashboards, and detailed reports to facilitate operations management and troubleshooting.

When devices are added or upgraded using the Cisco Services Fulfillment Portal (CSFP or SFP), the device data is automatically sent to the MSA portal to ensure that your device data is consistent across all Cisco platforms.

MSA portal features include:

<table>
<thead>
<tr>
<th>Performance Monitoring</th>
<th>Default and custom Key Performance Indicator (KPI) monitoring, Simple Network Management Protocol (SNMP), threshold-crossing alarms, history, and trending.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Management</td>
<td>Log collection and aggregation, event alerting, and long-term, tamper-proof archiving.</td>
</tr>
<tr>
<td>Security Reporting</td>
<td>Virtual Private Network (VPN) activity reports, Unified Threat Management (UTM) detailed reports, and web-proxy detailed reports.</td>
</tr>
<tr>
<td>Vulnerability Assessment</td>
<td>Trigger penetration testing using an embedded vulnerability assessment scanner.</td>
</tr>
<tr>
<td>Asset Management</td>
<td>Firmware and software—history and network inventory.</td>
</tr>
</tbody>
</table>

Audience

This guide is intended for Cox Business operators. It provides information about how to access the portal, the types of information available, and how to generate reports.

Scope

This document contains information about the MSA portal features and functionality that apply to the Cox Business configuration for MSA and FireSight Manager only. It is not intended for use by any other Cisco client.
Sign In to the MSA Portal

Supported Browsers

The MSA portal is best viewed in the following browsers:

- Firefox®
- Chrome®
- Internet Explorer® (PC only)
- Safari® (MAC only)

To sign in to the MSA portal using Single Sign On

Step 1. Sign in to the Cox MyAccount portal.

Step 2. After you sign in, click the MSA portal link in the MyAccount portal.

The MSA portal opens.
To sign in to the MSA portal without Single Sign On

Warning: To sign in to the MSA portal without signing in to the Cox My Account portal is not recommended. Before you can sign in directly to the MSA portal, your credentials must be set up by Cisco. If you do not know what User ID and password to use, contact Technical Support.

Step 3. Go to the following URL.
https://retail-prod-mrs.coxbusiness.com
Step 4. Type your User ID and Password in the boxes and click Sign In.
The MSA portal opens.
The Customer Care Dashboard

When you sign in to the MSA portal, the first page you see is the Customer Care Dashboard. The Customer Care dashboard displays a list of all the Cox end customers that have Cisco ASA or ISR devices installed.

Note: Depending on how you are set up as an MSA portal user, the Customer Care dashboard that you see might look different. If you do not see the information you need, contact your system administrator.

Navigation

At the top of every page in the MSA portal, you will see navigation and information tools.

From here you can:

- Go to the Cox Business or Cox Residential Home page
- Search for a customer or business name
- View Status Indicators to immediately understand what is happening in your device population (Manager role only)
View alerts for your devices
View your profile or sign out

Search

In the Customer Quick Search box, type the name of the customer or business that you are looking for; names are case-sensitive and should match the names used in the SFP portal.

Status

Point to the status icons to quickly understand what is going on with your devices and how many devices are affected. Click a status indicator to see a list of the affected devices.

Note: Depending on how you are set up in the MSA portal, this information might not display on your screen.

The status icons indicate one of the following:

- **Green**: Available and working correctly. Continue to monitor.
- **Yellow**: Critical, there is a performance issue with this device, such as operating at too high of a temperature. Check the device alarms and log. If the condition persists, contact Customer Support.
- **Red**: The device is unreachable. Ensure your equipment is turned on, connected to a power source and all cables are securely connected. If your device is connected and powered but you do not have service, contact Customer Support.
- **Gray**: The device has been provisioned but not activated in the portal and has, therefore, never been reached.
- **Black**: The total device population, regardless of status.
Alert

The Alert icon shows the number of devices that need your attention. Click any item in the Alert list to see details about a specific device.

Your Profile

To view your Profile in the MSA portal, click the Profile link at the top of any page. Your user information is displayed, including your name, role, address, user name, a password field (masked), and your Customer ID.
Note: Contact your system administrator to change your profile information.

### Change Password

The ability to change your password depends on how you open the MSA portal.

- If you use single sign on, you can change your password in the Cox MyAccount portal and your new password is updated automatically in the MSA portal.
- If you do not use single sign on and instead sign on locally, you can change your password in the MSA portal.

#### To change your password in the MSA portal

1. Click Change Password.
2. Type your current password and your new password twice in the Change Password box.
3. Click Save.

### Customer Care Dashboard—Customers Overview Tab

On the Customers Overview tab, you will see a list of Cox customers, contact information, and the status of all the devices installed at each customer’s site.

#### Sorting

- To quickly sort the list of businesses and devices by status, select a filter from the All Filters list.
- To see a list of all the devices at a particular business, click the business name.
- To see a list of devices at a business with a particular status, click a status icon next to a business name.
Customer Care Dashboard—Devices Overview Tab

The Devices Overview tab on the Customer Care dashboard shows the entire device population for Cox's end customers. The device list is sorted by Business Name, and each device at the business or end-customer location has a separate entry.

- To see a list of all the devices at a particular business, click the business name.
- To see the Devices—Overview subtab for a specific device, click the device name or the IP address.

Note: Your user role and permissions control how many end customers you see on the Devices Overview list. If you need information for an end customer that is not on the list, contact your system administrator.
## Customer Care Dashboard

<table>
<thead>
<tr>
<th>Business Name</th>
<th>Status</th>
<th>Device Name</th>
<th>Router Host Name</th>
<th>Type</th>
<th>License</th>
<th>IP Address</th>
<th>Model</th>
</tr>
</thead>
<tbody>
<tr>
<td>A1 DEMO</td>
<td></td>
<td>COX_LAB_992_MS_...</td>
<td>COX_LAB_992_MSA_...</td>
<td>Managed</td>
<td>CISCO-UNIVERSAL...</td>
<td>192.168.100.10</td>
<td>Cisco 2911/K9</td>
</tr>
<tr>
<td>COX BUSINESS</td>
<td></td>
<td>COX_LAB_992_MS_...</td>
<td>CiscoTrainTest</td>
<td>Managed</td>
<td>COX_LAB_992_MSA_...</td>
<td>192.168.100.10</td>
<td></td>
</tr>
<tr>
<td>COX BUSINESS</td>
<td></td>
<td>COX_LAB_992_MS_...</td>
<td>CiscoTrainTest</td>
<td>Managed</td>
<td>COX_LAB_992_MSA_...</td>
<td>192.168.100.10</td>
<td></td>
</tr>
<tr>
<td>COX BUSINESS</td>
<td></td>
<td>COX_LAB_992_MS_...</td>
<td>CiscoTrainTest</td>
<td>Managed</td>
<td>COX_LAB_992_MSA_...</td>
<td>192.168.100.10</td>
<td></td>
</tr>
<tr>
<td>COX BUSINESS</td>
<td></td>
<td>COX_LAB_992_MS_...</td>
<td>CiscoTrainTest</td>
<td>Managed</td>
<td>COX_LAB_992_MSA_...</td>
<td>192.168.100.10</td>
<td></td>
</tr>
<tr>
<td>COX BUSINESS</td>
<td></td>
<td>COX_LAB_992_MS_...</td>
<td>CiscoTrainTest</td>
<td>Managed</td>
<td>COX_LAB_992_MSA_...</td>
<td>192.168.100.10</td>
<td></td>
</tr>
<tr>
<td>COX BUSINESS</td>
<td></td>
<td>COX_LAB_992_MS_...</td>
<td>CiscoTrainTest</td>
<td>Managed</td>
<td>COX_LAB_992_MSA_...</td>
<td>192.168.100.10</td>
<td></td>
</tr>
<tr>
<td>COX BUSINESS</td>
<td></td>
<td>COX_LAB_992_MS_...</td>
<td>CiscoTrainTest</td>
<td>Managed</td>
<td>COX_LAB_992_MSA_...</td>
<td>192.168.100.10</td>
<td></td>
</tr>
<tr>
<td>COX BUSINESS</td>
<td></td>
<td>COX_LAB_992_MS_...</td>
<td>CiscoTrainTest</td>
<td>Managed</td>
<td>COX_LAB_992_MSA_...</td>
<td>192.168.100.10</td>
<td></td>
</tr>
<tr>
<td>COX BUSINESS</td>
<td></td>
<td>COX_LAB_992_MS_...</td>
<td>CiscoTrainTest</td>
<td>Managed</td>
<td>COX_LAB_992_MSA_...</td>
<td>192.168.100.10</td>
<td></td>
</tr>
<tr>
<td>COX BUSINESS</td>
<td></td>
<td>COX_LAB_992_MS_...</td>
<td>CiscoTrainTest</td>
<td>Managed</td>
<td>COX_LAB_992_MSA_...</td>
<td>192.168.100.10</td>
<td></td>
</tr>
<tr>
<td>COX BUSINESS</td>
<td></td>
<td>COX_LAB_992_MS_...</td>
<td>CiscoTrainTest</td>
<td>Managed</td>
<td>COX_LAB_992_MSA_...</td>
<td>192.168.100.10</td>
<td></td>
</tr>
</tbody>
</table>
Devices Tab

After a device is installed and working at a customer site, you can monitor the device and the data it is collecting by selecting the specific device from a list of installed devices at the end-customer location.

Select a Device

On the Customers tab, select the business name where the device is located.

The Devices tab opens and shows either a list of devices at the location or a single device. Click the name of the device.
Devices Tab Views

You can change how the Devices tab looks by selecting one of the display buttons next to the Sort By list at the top of the Devices list.

Tile View

The Tile view displays summary information about the devices at an end-customer location, including device names, statuses, and serial numbers.

Note: The Tile View is the default view.

In Tile view, you can see the following device information:

- Status indicator: A color-coded icon that lets you quickly see the status of the device connection.
- Serial Number: The serial number on the actual device; entered during the provisioning process.
- IP address: Cox Business assigns the IP address during provisioning.
- Firmware: The IOS version of the operating system on the device.
- IP Address: The IP address for the device.
- Model: The model identifier assigned to the device by the equipment manufacturer.
- License: The IOS image name of the device, if available.
List View

In List view you can see the following information:

- **Status indicator**: A color-coded icon that lets you quickly see the status of the device connection.
- **Device Name**: A name assigned when the device is set up that differentiates the device from any others at an end-customer location.
- **Router Host Name**: The name assigned to the router during provisioning in the SFP.
- **Type**: Indicates whether the device is managed.
- **License**: The IOS image name of the device, if available.
- **Serial Number**: The serial number on the actual device; entered during the provisioning process.
- **IP address**: Cox Business assigns the IP address during provisioning.
- **Service Address**: The physical location of the device.
Map View

Click the device icons to open the Device Overview tab for a location or for a piece of equipment.

Device Status

The easiest way to check how a device is doing is to look at the indicator in the Status column. Devices can be in any of the following states:

- **Green**: Available and working correctly. Continue to monitor.
- **Yellow**: Critical, there is a performance issue with this device, such as operating at too high of a temperature. Check the device alarms and log. If the condition persists, contact Customer Support.
- **Red**: The device is unreachable. Ensure your equipment is on, connected to a power source, and that all cables are securely connected. If your device is connected and powered, but you do not have service, contact Customer Support.
- **Gray**: The device has been provisioned but not activated in the MSA portal. There is no information to report.
Device Graphs

The Devices tab also contains the following graphs that show you at a high level how a particular device is performing. The graphs you can see in the Tile (default) view are:

- Traffic Analysis
- Router Availability
- View All

Traffic Analysis

This graph shows the amount of incoming and outgoing traffic, in millions of bytes, on a particular device over time. As you hover over points on the graph, you will see additional information.

Router Availability

This graph shows the amount of time a router was available during a particular period. As you hover over points on the graph, you will see router availability at a specific date and time.
View All

Selecting View All displays the SNMP Graphs (Simple Network Management Protocol) section. The following graphs are on the View All tab:

- Traffic Analysis—Shows the amount of incoming and outgoing traffic, in millions of bytes, on a particular device over time.
- Device CPU Usage—Shows the CPU usage of the device, over time.
- Router Availability—Shows the amount of time a device was available, over time.
- Active VPN Tunnels—Shows when a VPN is established on the device. (VPN Service must be ordered.)
- Firewall—Shows the number of firewall events over time. This graph displays for ASA devices only.

Note: Click a time period button to view the reports by Day, Week, Month, Year, or a Custom period.

Note: If a graph contains no content, it means that the device has not sent any event data that applies to the specific graph.

Detailed Security Metrics

For ASA devices only, clicking the Detailed Security Metrics button opens the FireSight Manager tabs and graphs set up for Cox Business. To learn more about the information available to Cox Business from within FireSight Manager, go to the FireSight Manager section beginning on page 26.
Note: Access to FireSight Manager and access to the graphs within Cox’s FireSight Manager setup is controlled by user roles and permissions. If you do not have this access and need it, contact your system administrator, who will contact Cisco if necessary to get your user role and permissions set up.

Ping Device

To quickly establish that a device is available, on the Device Details—Overview tab, click the Ping button.

Devices Details Subtab

Note: Depending on the profile or role assigned to you, some of the information in this section might not appear to you. If you do not see the information you need, contact your system administrator.
Network Configuration

The Network Configuration section displays the configuration type, the interface name for the type of connection, the IP Address, and the mask for the IP Address.

Click Show More to see the following additional information:

- Additional Interface
- Enable DHCP Server
- Optional Card

Note: Click Show Less to hide this information.

Status of Update

The Status of Update section displays information about the updates that are applicable to this device, including a summary of each update, the date of the last update attempt and information about whether the update was successful.

If you do not see an update in the list, click the Update button to update the section with the latest information.

Additional Information

When MSA connects to a particular device, there are some commands that run in the background and collect the following information.

Note: The information you see depends on what services are provisioned on the device and the type of device.

- Asset Identifier
- Board Revision
- Chassis Serial Number
- Deviation Number
- FastEthernet0
- FastEthernet2
- FastEthernet4
- Fast Ethernet Interface
- Hardware Revision
- MAC Address Block Size
- Non-volatile Configuration Memory
- PCB Serial Number
- ATA System CompactFlash (Read/Write)
- Chassis MAC Address
- CLEI Code
- Fab Version
- FastEthernet1
- FastEthernet3
- FastEthernet4.802
- Gigabit Ethernet interface
- Tunnel0
- Memory
- Part Number
- Processor Type
The Logs Subtab

This page lets you view, sort and filter the logs for this device. It contains information about the date an event was logged, the type of event, the level of severity, a reference number, and the count of records in the log.

To open a log, click the magnifying glass icon next to the Count column. Click Download Logs to save the log on your computer.
Filtering the log files for a device

There are multiple ways to filter the Logs list. To quickly sort the logs in chronological order, click the arrow in the Date column.

To apply more filters, select the checkboxes on the left side of the Device Logs tab that match the logs you want to see. Only the records that meet the criteria you select will display in the Device Logs list. You can filter based on the following:

- Logs
- Alarms
- Events
- Date Range
- Day
- Week
- Month
- Year
- Custom
- Type
- Syslog
- IPS
- Anti-Virus
- Anti-Spam
- URL Filtering
- IP Phone
- Asset
- Management
- Monitoring
- Trap
- Level
- Emergency
- Alert
- Critical
- Error
- Warning
- Notice
- Informational
- Debug
- Informational

Note: When you are finished, click Reset Filters to clear the filters and display the entire list.
Reports Subtab

This page contains options to view and download reports about a device.

Click the Download link next to the report name to save a copy of the report on your computer.
VPN Activity Report
for an ASA Device

Shows the status of VPN activity on the device.

ASA Device commands
The output of the following commands is shown in the VPN Activity report:

- show version
- show crypto isakmp sa
- show crypto ipsec sa
- dir flash

ISR Device commands

- show version
- show logging
- show crypto isakmp sa
- show crypto ipsec sa

Complete Activity Report

Shows the status of most the activities on the device, such as HSRP (gateway) and QoS.

ASA Device commands

- show version
- show traffic
- show xlate
- show crypto isakmp stats
- show crypto isakmp sa
- show crypto ipsec sa
- dir flash

ISR Device commands

- show version
- show logging
- show crypto isakmp sa
- show crypto ipsec sa
- show standby brief
- show policy-map interface
- dir flash
Running Configuration

Shows the actual configuration file running on the device.

History Subtab

This page provides details about updates to the device’s firmware and hardware.

Device Information

This section lists the model name, the serial number, firmware version, certificate expiration date, license, memory, IPS version and the IPS expiration date.

Firmware Inventory

Lists section lists the dates when firmware was installed, the firmware attributes, and the firmware’s old and new version numbers.

Hardware Inventory

Lists the dates when new hardware was installed, the hardware attributes and the hardware’s old and new models.
FireSight Manager

In FireSight, you will see two tabs—the Overview tab and the Analysis tab. Within each tab there are subtabs that contain one or more widgets in a three-column layout. Widgets are small, self-contained components (usually some type of graph) that provide different information about your managed devices.

Overview Tab—Summary Dashboard

After you click the FireSight button in the MSA portal, the first tab you see is the Overview—Summary Dashboard tab, which contains widgets and graphs that together offer a complete overview of FireSight data on your monitored network.

There are four subtabs that give you an at-a-glance picture of recent trends in your network’s activity. The four subtabs are:

- Network
- Threats
- Intrusion Events
- Geolocation

Network Subtab

Unique Applications Over Time

Displays a graph of total unique applications detected on your monitored network over the dashboard time range.
Traffic by Application Risk
Displays estimated business relevance levels of applications on your monitored network, based on total kilobytes of data transmitted on your monitored network by applications at each level over the dashboard time range.

Traffic by Business Relevance
Displays estimated business relevance levels of applications on your monitored network, based on total kilobytes of data transmitted on your monitored network by applications at each level over the dashboard time range.
Traffic by Application Category

Displays application categories on your monitored network, based on total kilobytes of data transmitted on your monitored network by applications in each category over the dashboard time range.

Top Web Applications Seen

Displays web applications on your monitored network, based on total kilobytes of data transmitted by the client application.
Top Server Applications Seen

Displays server applications on your monitored network, based on the number of hosts running the service.

Risky Applications with Low Business Relevance

Displays all application connections on your monitored network that have both high application risk level and low estimated business relevance.
Connections by URL Reputation
Displays all application connections on your monitored network, grouped by URL reputation.

<table>
<thead>
<tr>
<th>Reputation</th>
<th>Total Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>Well known</td>
<td>40,876</td>
</tr>
<tr>
<td>Penng sites</td>
<td>2,891</td>
</tr>
<tr>
<td>Penng sites with security risks</td>
<td>1,310</td>
</tr>
<tr>
<td>Suspicious sites</td>
<td>35</td>
</tr>
<tr>
<td>High risk</td>
<td>10</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 50 minutes ago

Top Client Applications Seen
Displays client applications on your monitored network, based on total kilobytes of data transmitted by the client application.

<table>
<thead>
<tr>
<th>Application</th>
<th>Total Bytes (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet Explorer</td>
<td>2,090,044.59</td>
</tr>
<tr>
<td>Firefox</td>
<td>767,745.47</td>
</tr>
<tr>
<td>Google Toolbar</td>
<td>70,982.86</td>
</tr>
<tr>
<td>PHP</td>
<td>51,137.52</td>
</tr>
<tr>
<td>Yahoo</td>
<td>34,929.15</td>
</tr>
<tr>
<td>Warst</td>
<td>27,115.84</td>
</tr>
<tr>
<td>ABC</td>
<td>25,888.38</td>
</tr>
<tr>
<td>Links</td>
<td>25,123.07</td>
</tr>
<tr>
<td>Flipboard</td>
<td>23,935.41</td>
</tr>
<tr>
<td>TSP</td>
<td>22,055.09</td>
</tr>
<tr>
<td>Twitter</td>
<td>14,424.63</td>
</tr>
<tr>
<td>Facebook</td>
<td>11,227.47</td>
</tr>
<tr>
<td>Advanced Packaging Tool</td>
<td>9,931.36</td>
</tr>
<tr>
<td>Amazon Web Services</td>
<td>7,405.41</td>
</tr>
<tr>
<td>iHeartRadio</td>
<td>3,365.53</td>
</tr>
</tbody>
</table>

Last updated 3 hours, 4 minutes ago
Top Operating Systems Seen

Displays operating systems on your monitored network, based on the number of network hosts with the operating system.

Connections by URL Category

Displays all application connections on your monitored network, grouped by URL category.
**Threats Subtab**

**Indications of Compromise by Host**
Displays number of triggered indications of compromise, grouped by associated host IP address

![Indications of Compromise by Host](image)

**Malware Threats**
Displays the number of malware threats detected either in network traffic by the system or by FireAMP Connectors, grouped by threat name.

Note: When a graph contains no data, it means that the device did not send any information to FireSight Manager for the time range selected; it does not indicate a problem with the device itself.

![Malware Threats](image)
New Indications of Compromise Over Time

Displays a graph of new indications of compromise detected over the dashboard time range.

Intrusion Events

The Intrusion Events widget shows the intrusion events that occurred over the time period specified on the Dashboard, organized by priority. This includes statistics on intrusion events with dropped packets. On managed devices, the widget can display statistics for dropped (or, on passively deployed devices, would have dropped) intrusion events, all intrusion events, or both.
Intrusion Events Subtab

Top Attackers
Displays attacking host IP addresses on your monitored network, based on the number of intrusion events where the listed IP address was the attacker in the connection that caused the event.

<table>
<thead>
<tr>
<th>Source IP</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>70.62.115.162</td>
<td>149</td>
</tr>
<tr>
<td>96.10.162.4</td>
<td>103</td>
</tr>
<tr>
<td>97.77.44.5</td>
<td>60</td>
</tr>
<tr>
<td>96.10.39.66</td>
<td>49</td>
</tr>
<tr>
<td>69.75.199.3</td>
<td>41</td>
</tr>
<tr>
<td>98.101.163.122</td>
<td>29</td>
</tr>
<tr>
<td>108.176.89.227</td>
<td>25</td>
</tr>
<tr>
<td>24.106.177.194</td>
<td>23</td>
</tr>
<tr>
<td>173.198.143.98</td>
<td>22</td>
</tr>
<tr>
<td>24.97.220.68</td>
<td>14</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 6 minutes ago

Top Targets
Displays host IP addresses on your monitored network, based on the number of intrusion events where that address was targeted in the connection that caused the event.

<table>
<thead>
<tr>
<th>Destination IP</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>69.48.211.170</td>
<td>143</td>
</tr>
<tr>
<td>125.209.230.195</td>
<td>56</td>
</tr>
<tr>
<td>185.17.184.11</td>
<td>30</td>
</tr>
<tr>
<td>162.220.223.28</td>
<td>17</td>
</tr>
<tr>
<td>162.220.223.28</td>
<td>14</td>
</tr>
<tr>
<td>46.137.81.66</td>
<td>13</td>
</tr>
<tr>
<td>104.129.204.40</td>
<td>13</td>
</tr>
<tr>
<td>178.77.120.6</td>
<td>12</td>
</tr>
<tr>
<td>52.71.189.2</td>
<td>11</td>
</tr>
<tr>
<td>69.75.199.3</td>
<td>11</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 6 minutes ago
Dropped Intrusion Events
Displays counts for intrusion events, by classification, where the packet was dropped.

<table>
<thead>
<tr>
<th>Classification</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Potential Corporate Policy Violation</td>
<td>278</td>
</tr>
<tr>
<td>Attempted Administrator Privilege Gain</td>
<td>253</td>
</tr>
<tr>
<td>A Network Trojan was Detected</td>
<td>84</td>
</tr>
<tr>
<td>Attempted Information Leak</td>
<td>6</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 6 minutes ago

All Intrusion Events
Displays a graph of the total number of intrusion events on your monitored network over the dashboard time range.

Last updated 2 hours, 7 minutes ago
Intrusion Events

The Intrusion Events widget shows the intrusion events that occurred over the time period specified on the Dashboard, organized by priority. This includes statistics on intrusion events with dropped packets. On managed devices, the widget can display statistics for dropped (or, on passively deployed devices, would have dropped) intrusion events, all intrusion events, or both.

Total Events by Application Protocol

Displays application protocols on your monitored network, based on the number of intrusion events associated with the application protocol.
Displays number of events of estimated impact level 1 grouped by application protocol.

<table>
<thead>
<tr>
<th>Application</th>
<th>Impact 1 Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>84</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 6 minutes ago

---

**Impact 2 Events by Application Protocol**

Displays number of events of estimated impact level 2 grouped by application protocol.

<table>
<thead>
<tr>
<th>Application</th>
<th>Impact 2 Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>416</td>
</tr>
<tr>
<td>TeamViewer</td>
<td>95</td>
</tr>
<tr>
<td>DnGate</td>
<td>95</td>
</tr>
<tr>
<td>HTTPS</td>
<td>4</td>
</tr>
<tr>
<td>HL7</td>
<td>4</td>
</tr>
<tr>
<td>Snapchat</td>
<td>3</td>
</tr>
<tr>
<td>SSL</td>
<td>1</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 6 minutes ago
### Geolocation Subtab

#### Intrusion Events by Source Country
Displays countries where intrusion events originated, based on the number of events originated from each country.

<table>
<thead>
<tr>
<th>Source Country</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA (United States)</td>
<td>550</td>
</tr>
<tr>
<td>NLD (Netherlands)</td>
<td>22</td>
</tr>
<tr>
<td>CHN (China)</td>
<td>20</td>
</tr>
<tr>
<td>BRA (Brazil)</td>
<td>6</td>
</tr>
<tr>
<td>DEU (Germany)</td>
<td>4</td>
</tr>
<tr>
<td>ECU (Ecuador)</td>
<td>4</td>
</tr>
<tr>
<td>KAZ (Kazakhstan)</td>
<td>4</td>
</tr>
<tr>
<td>RUS (Russian Federation)</td>
<td>3</td>
</tr>
<tr>
<td>FRA (France)</td>
<td>2</td>
</tr>
<tr>
<td>MEX (Mexico)</td>
<td>2</td>
</tr>
</tbody>
</table>

Last updated 1 hour, 42 minutes ago

#### Intrusion Events by Destination Country
Displays countries targeted by intrusion events, based on the number of events associated with each country.

<table>
<thead>
<tr>
<th>Destination Country</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA (United States)</td>
<td>420</td>
</tr>
<tr>
<td>DEU (Germany)</td>
<td>109</td>
</tr>
<tr>
<td>KOR (South Korea)</td>
<td>56</td>
</tr>
<tr>
<td>IRL (Ireland)</td>
<td>25</td>
</tr>
<tr>
<td>BRA (Brazil)</td>
<td>3</td>
</tr>
<tr>
<td>GBR (United Kingdom)</td>
<td>3</td>
</tr>
<tr>
<td>NLD (Netherlands)</td>
<td>3</td>
</tr>
<tr>
<td>AUT (Austria)</td>
<td>2</td>
</tr>
<tr>
<td>DNK (Denmark)</td>
<td>1</td>
</tr>
<tr>
<td>POL (Poland)</td>
<td>1</td>
</tr>
</tbody>
</table>

Last updated 1 hour, 42 minutes ago
**Intrusion Events by Source Continent**

Displays continents where intrusion events originated, based on the number of events originated from each continent.

<table>
<thead>
<tr>
<th>Source Continent</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>552</td>
</tr>
<tr>
<td>Europe</td>
<td>31</td>
</tr>
<tr>
<td>Asia</td>
<td>26</td>
</tr>
<tr>
<td>South America</td>
<td>10</td>
</tr>
</tbody>
</table>

Last updated 1 hour, 42 minutes ago

**Intrusion Events by Destination Continent**

Displays continents targeted by intrusion events, based on the number of events associated with each continent.

<table>
<thead>
<tr>
<th>Destination Continent</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>420</td>
</tr>
<tr>
<td>Europe</td>
<td>145</td>
</tr>
<tr>
<td>Asia</td>
<td>57</td>
</tr>
<tr>
<td>South America</td>
<td>3</td>
</tr>
</tbody>
</table>

Last updated 1 hour, 42 minutes ago
Overview Tab—Application Statistics Dashboard

Connections Subtab

Allowed Connections by Application
Displays allowed application connections on your monitored network, grouped by application.

<table>
<thead>
<tr>
<th>Application</th>
<th>Allowed Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>DNS</td>
<td>870</td>
</tr>
<tr>
<td>HTTP</td>
<td>346</td>
</tr>
<tr>
<td>POLITICO.com</td>
<td>342</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>216</td>
</tr>
<tr>
<td>Firefox</td>
<td>90</td>
</tr>
<tr>
<td>Google Toolbar</td>
<td>10</td>
</tr>
<tr>
<td>Web browser</td>
<td>10</td>
</tr>
<tr>
<td>Flipboard</td>
<td>6</td>
</tr>
<tr>
<td>PHP</td>
<td>6</td>
</tr>
<tr>
<td>Links</td>
<td>4</td>
</tr>
</tbody>
</table>

Last updated less than a minute ago

Denied Connections by Application
Displays denied connections on your monitored network, grouped by application.

<table>
<thead>
<tr>
<th>Application</th>
<th>Denied Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>35</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>23</td>
</tr>
<tr>
<td>AddThis</td>
<td>8</td>
</tr>
<tr>
<td>Firefox</td>
<td>7</td>
</tr>
<tr>
<td>HTTPS</td>
<td>5</td>
</tr>
<tr>
<td>PHP</td>
<td>3</td>
</tr>
<tr>
<td>Google Toolbar</td>
<td>2</td>
</tr>
</tbody>
</table>

Last updated less than a minute ago
Unique Applications over Time
Displays a graph of total unique applications detected on your monitored network over the dashboard time range.

Allowed Connections by Application Risk
Displays allowed application connections on your monitored network, grouped by application risk level.
Allowed Connections by Business Relevance

Displays allowed application connections on your monitored network, grouped by estimated relevance to business activity.

Traffic by Application

Displays applications on your monitored network, based on total kilobytes of data transmitted on your monitored network by the application over the dashboard time range.
Traffic by Application Category

Displays application categories on your monitored network, based on total kilobytes of data transmitted on your monitored network by applications in each category over the dashboard time range.

Intrusion Events Subtab

Dropped Events by Application

Displays dropped intrusion events, grouped by application.
### Impact 3 Events by Application

Displays number of events of estimated impact level 3 grouped by application.

<table>
<thead>
<tr>
<th>Application</th>
<th>Impact 3 Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>14</td>
</tr>
<tr>
<td>TeamViewer</td>
<td>7</td>
</tr>
<tr>
<td>PynGate</td>
<td>7</td>
</tr>
<tr>
<td>Web browser</td>
<td>6</td>
</tr>
<tr>
<td>Media Stream Daemon</td>
<td>1</td>
</tr>
</tbody>
</table>

Last updated 32 minutes ago

### Impact 1 Events by Application

Displays number of events of estimated impact level 1 grouped by application.

<table>
<thead>
<tr>
<th>Application</th>
<th>Impact 1 Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>94</td>
</tr>
<tr>
<td>Web browser</td>
<td>62</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>32</td>
</tr>
</tbody>
</table>

Last updated 32 minutes ago
**Impact 4 Events by Application**

Displays number of events of estimated impact level 4 grouped by application.

<table>
<thead>
<tr>
<th>Application</th>
<th>Impact 4 Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>94</td>
</tr>
<tr>
<td>Mobile Safari</td>
<td>32</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>32</td>
</tr>
<tr>
<td>TeamViewer</td>
<td>19</td>
</tr>
<tr>
<td>DynGate</td>
<td>19</td>
</tr>
<tr>
<td>Web browser</td>
<td>5</td>
</tr>
<tr>
<td>Chrome</td>
<td>4</td>
</tr>
<tr>
<td>Safari</td>
<td>2</td>
</tr>
<tr>
<td>Forbes</td>
<td>2</td>
</tr>
<tr>
<td>ZergNet</td>
<td>1</td>
</tr>
</tbody>
</table>

Last updated 32 minutes ago

**Total Events by Application**

Displays applications on your monitored network, based on the number of intrusion events generated by the application.

Note: When a graph contains no data, it means that the device did not send any information to FireSight Manager for the time range selected; it does not indicate a problem with the device itself.

**Total Events by Application**

No Data

Last updated 2 minutes ago
Impact 2 Events by Application

Displays number of events of estimated impact level 2 grouped by application.

<table>
<thead>
<tr>
<th>Application</th>
<th>Impact 2 Events</th>
</tr>
</thead>
<tbody>
<tr>
<td>HTTP</td>
<td>416</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>162</td>
</tr>
<tr>
<td>TeamViewer</td>
<td>95</td>
</tr>
<tr>
<td>DynGate</td>
<td>95</td>
</tr>
<tr>
<td>Web browser</td>
<td>72</td>
</tr>
<tr>
<td>Mobile Safari</td>
<td>42</td>
</tr>
<tr>
<td>Chrome</td>
<td>29</td>
</tr>
<tr>
<td>Media Stream Daemon</td>
<td>8</td>
</tr>
<tr>
<td>Safari</td>
<td>5</td>
</tr>
<tr>
<td>HTTPS</td>
<td>4</td>
</tr>
</tbody>
</table>

Last updated 32 minutes ago

Impact 0 Events by Application

Displays number of events of estimated impact level 0 grouped by application.

Note: When a graph contains no data, it means that the device did not send any information to FireSight Manager for the time range selected; it does not indicate a problem with the device itself.

No Data

Last updated 2 minutes ago
Overview Tab—Connection Summary Dashboard

Connections Subtab

Connections by Initiator IP
Displays host IP addresses on your monitored network, based on the number of connections where that IP address on a host initiated the session.
Connections by Responder IP

Displays host IP addresses on your monitored network, based on the number of connections where the responder in that session was that IP address on a host. The output of this widget varies according to your connection logging configuration.

<table>
<thead>
<tr>
<th>Responder IP</th>
<th>Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>64.94.1.1</td>
<td>833</td>
</tr>
<tr>
<td>164.26.143.96</td>
<td>224</td>
</tr>
<tr>
<td>164.26.143.115</td>
<td>209</td>
</tr>
<tr>
<td>64.94.1.33</td>
<td>19</td>
</tr>
<tr>
<td>172.29.199.241</td>
<td>3</td>
</tr>
<tr>
<td>91.189.91.157</td>
<td>2</td>
</tr>
<tr>
<td>96.17.170.8</td>
<td>1</td>
</tr>
<tr>
<td>96.17.170.18</td>
<td>1</td>
</tr>
<tr>
<td>208.68.240.126</td>
<td>1</td>
</tr>
</tbody>
</table>

Last updated 4 minutes ago

Connections Over Time

Displays a graph of the total number of connections on your monitored network, over the dashboard time range.

Connections over Time

Last updated 5 minutes ago
Connections by Port
Displays ports on your monitored network, based on the number of detected connections.

Connections by Applications
Displays applications on your monitored network, based on the number of detected connections.
Traffic Subtab

Traffic by Initiator IP
Displays host IP addresses on your monitored network, based on total kilobytes of data transmitted on your monitored network from the IP address over the dashboard time range.

Traffic by Responder IP
Displays IP addresses on your monitored network, based on total kilobytes of data received by the IP addresses (on hosts) over the dashboard time range. The output of this widget varies according to your connection logging configuration.
Traffic Over Time
Displays a graph of total kilobytes of data transmitted on your monitored network over the dashboard time range.

Traffic by Port
Displays responder ports on your monitored network, based on total kilobytes of data transmitted on your monitored network via each port over the dashboard time range. The output of this widget varies according to your connection logging configuration.
Traffic by Application

Displays applications on your monitored network, based on total kilobytes of data transmitted on your monitored network by the application over the dashboard time range.

Geolocation Subtab

Connections by Source Country

Displays countries communicating with your monitored network, based on the number of connections initiated from each country.
Connections by Destination Country

Displays countries to which connections were sent from your monitored network, based on the number of connections.

### Connections by Destination Country

<table>
<thead>
<tr>
<th>Responder Country</th>
<th>Total Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA (United States)</td>
<td>2,758</td>
</tr>
<tr>
<td>GBR (United Kingdom)</td>
<td>5</td>
</tr>
</tbody>
</table>

Last updated 3 minutes ago

Connections by Source Continent

Displays continents communicating with your monitored network, based on the number of connections initiated from each continent.

### Connections by Source Continent

<table>
<thead>
<tr>
<th>Initiator Continent</th>
<th>Total Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>88,638</td>
</tr>
<tr>
<td>South America</td>
<td>5,278</td>
</tr>
<tr>
<td>Europe</td>
<td>147</td>
</tr>
<tr>
<td>Asia</td>
<td>37</td>
</tr>
<tr>
<td>Australia</td>
<td>31</td>
</tr>
</tbody>
</table>

Last updated 3 minutes ago

Connections by Destination Continent
Displays continents to which connections were sent from your monitored network, based on the number of connections.

**Connections by Destination Continent**

<table>
<thead>
<tr>
<th>Responder Continent</th>
<th>▼ Total Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>North America</td>
<td>2,758</td>
</tr>
<tr>
<td>Europe</td>
<td>5</td>
</tr>
</tbody>
</table>

Last updated 4 minutes ago

**Traffic by Source Continent**

Displays continents transmitting data to your monitored network, based on total kilobytes of data on your monitored network transmitted from each continent over the dashboard time range.

Note: When a graph contains no data, it means that the device did not send any information to FireSight Manager for the time range selected; it does not indicate a problem with the device itself.
Traffic by Destination Continent

Displays continents contacted from your monitored network, based on total kilobytes of data transmitted on your monitored network to each continent over the dashboard time range.

Traffic by Source Country

Displays countries transmitting data to your monitored network, based on total kilobytes of data on your monitored network transmitted from each country over the dashboard time range.
### Traffic by Destination Country
Displays countries contacted from your monitored network, based on total kilobytes of data transmitted on your monitored network to each country over the dashboard time range.

<table>
<thead>
<tr>
<th>Responder Country</th>
<th>Total Bytes (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>USA (United States)</td>
<td>86,702.83</td>
</tr>
<tr>
<td>GBR (United Kingdom)</td>
<td>2.57</td>
</tr>
</tbody>
</table>

Last updated 2 minutes ago

### URL Subtab

### Allowed Connections by URL Category
Displays allowed application connections on your monitored network, grouped by URL category.

<table>
<thead>
<tr>
<th>Category</th>
<th>Allowed Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>News and Media</td>
<td>434</td>
</tr>
<tr>
<td>Business and Economy</td>
<td>3</td>
</tr>
<tr>
<td>Educational Institutions</td>
<td>1</td>
</tr>
</tbody>
</table>

Last updated 2 minutes ago
Denied Connections by URL Category

Displays denied connections on your monitored network, grouped by URL category.

<table>
<thead>
<tr>
<th>Category</th>
<th>Denied Connections</th>
</tr>
</thead>
<tbody>
<tr>
<td>News and Media</td>
<td>12</td>
</tr>
<tr>
<td>Computer and Internet Info</td>
<td>5</td>
</tr>
<tr>
<td>Job Search</td>
<td>2</td>
</tr>
</tbody>
</table>

Last updated 2 minutes ago

Traffic by URL Category

Displays application URL categories on your monitored network, based on total kilobytes of data exchanged with URLs of each category over the dashboard time range.

<table>
<thead>
<tr>
<th>Category</th>
<th>Total Bytes (KB)</th>
</tr>
</thead>
<tbody>
<tr>
<td>News and Media</td>
<td>79,168.79</td>
</tr>
<tr>
<td>Business and Economy</td>
<td>152.91</td>
</tr>
<tr>
<td>Educational Institutions</td>
<td>28.95</td>
</tr>
<tr>
<td>Computer and Internet Info</td>
<td>3.75</td>
</tr>
<tr>
<td>Job Search</td>
<td>1.01</td>
</tr>
</tbody>
</table>

Last updated 3 minutes ago
Traffic by URL Reputation
Displays application URL reputation types on your monitored network, based on total kilobytes of data exchanged with URLs of each reputation over the dashboard time range.

Allowed connections by URL Reputation
Displays allowed application connections on your monitored network, grouped by URL reputation.
Denied Connections by URL Reputation

Displays denied connections on your monitored network, grouped by URL reputation.

**Overview Tab—Detailed Dashboard**

*Intrusion Events Subtab*

**Intrusion Events**

The Intrusion Events widget shows the intrusion events that occurred over the time period specified on the Dashboard, organized by priority. This includes statistics on intrusion events with dropped packets. On managed devices, the widget can display statistics for dropped (or, on passively deployed devices, would have dropped) intrusion events, all intrusion events, or both.
**All Intrusion Events**

Displays a graph of the total number of intrusion events on your monitored network over the dashboard time range.

**All Intrusion Events (Not Dropped)**

Displays the most frequently occurring types of intrusion events, by classification, where the packet was not dropped as part of the event.
Dropped Intrusion Events

Displays counts for intrusion events, by classification, where the packet was dropped.

<table>
<thead>
<tr>
<th>Classification</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Attempted Administrator Privilege Gain</td>
<td>952</td>
</tr>
<tr>
<td>Potential Corporate Policy Violation</td>
<td>653</td>
</tr>
<tr>
<td>A Network Trojan was Detected</td>
<td>464</td>
</tr>
<tr>
<td>Attempted Information Leak</td>
<td>2</td>
</tr>
<tr>
<td>Web Application Attack</td>
<td>2</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 7 minutes ago

Intrusion Events Requiring Analysis

Displays a count of intrusion events requiring analysis, based on event classification.

Note: When a graph contains no data, it means that the device did not send any information to FireSight Manager for the time range selected; it does not indicate a problem with the device itself.

Last updated 3 minutes ago
**Context Subtab**

**Servers**
Displays servers, by number of hosts.

![Servers Table]

**Operating Systems**
Displays operating systems, based on the number of hosts running each operating system within your network.

![Operating Systems Table]
Clients
Displays clients on your monitored network, by type.

Traffic by Application
Displays applications on your monitored network, based on total kilobytes of data transmitted on your monitored network by the application over the dashboard time range.
Traffic by Initiator IP

Displays host IP addresses on your monitored network, based on total kilobytes of data transmitted on your monitored network from the IP address over the dashboard time range.

Traffic by Responder IP

Displays IP addresses on your monitored network, based on total kilobytes of data received by the IP addresses (on hosts) over the dashboard time range. The output of this widget varies according to your connection logging configuration.
Traffic Over Time
Displays a graph of total kilobytes of data transmitted on your monitored network over the dashboard time range.

Overview Tab—Files Dashboard
Malware Subtab

Hosts Receiving Malware
Displays the number of malware files received by host IP addresses on your network, grouped by IP address.
**Hosts Sending Malware**

Displays the number of malware files sent from host IP addresses on your network, grouped by IP address.

![Hosts Sending Malware](image)

**Application Protocols Introducing Malware**

Displays the number of malware files transmitted over your network, grouped by the application protocol used to transmit the files.

![Application Protocols Introducing Malware](image)
### Client Applications introducing Malware

Displays the applications, or parent files, that accessed or created malware detected by FireAMP Connectors.

<table>
<thead>
<tr>
<th>Client</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wget</td>
<td>3,248</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 12 minutes ago

### Web Applications Introducing Malware

Displays web applications on your monitored network that accessed or created malware detected by FireAMP Connectors.

<table>
<thead>
<tr>
<th>Web Application</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Browsing</td>
<td>3,252</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 14 minutes ago
Possible ZeroDay Malware

Displays the captured files most likely to be zero-day malware, with a file disposition of unknown and either High or Very High threat scores, based on the number of times the file was seen.

Note: When a graph contains no data, it means that the device did not send any information to FireSight Manager for the time range selected; it does not indicate a problem with the device itself.
Malware Threats

Displays the number of malware threats detected either in network traffic by the system or by FireAMP Connectors, grouped by threat name.

Note: When a graph contains no data, it means that the device did not send any information to FireSight Manager for the time range selected; it does not indicate a problem with the device itself.
Threat Detections Over Time

Displays a graph of the total number of malware threats detected either in network traffic by the system or by FireAMP Connectors, over the dashboard time range.

Top Threats

Displays the distribution of threat scores, based on the number of stored files with that threat score.

Note: When a graph contains no data, it means that the device did not send any information to FireSight Manager for the time range selected; it does not indicate a problem with the device itself.
**Malware Intrusions**

Displays intrusion events, based on the number of intrusion events occurring in connections transmitting malware.

**Note:** When a graph contains no data, it means that the device did not send any information to FireSight Manager for the time range selected; it does not indicate a problem with the device itself.

---

**File Types Infected with Malware**

Displays the number of malware detected either in network traffic by the system or by FireAMP Connectors, grouped by file type.
Processes Introducing Malware

Displays the system processes that accessed or created malware detected by FireAMP Connectors.

Note: When a graph contains no data, it means that the device did not send any information to FireSight Manager for the time range selected; it does not indicate a problem with the device itself.

Files Subtab

Hosts Receiving Files

Displays the number of files received (downloaded) by host IP addresses on your network, grouped by IP address.
Hosts Sending Files
Displays the number of files sent (uploaded) from host IP addresses on your network, grouped by IP address.

Applications Protocols Transferring File
Displays the number of files transmitted over your network, grouped by the application protocol used to transmit the files.
Client Applications Transferring files

Displays the applications, or parent files, that transmitted files over your network.

<table>
<thead>
<tr>
<th>Client</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Wget</td>
<td>3,259</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>80</td>
</tr>
<tr>
<td>Firefox</td>
<td>33</td>
</tr>
<tr>
<td>Web browser</td>
<td>2</td>
</tr>
<tr>
<td>Flipboard</td>
<td>1</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 19 minutes ago

Web Applications Transferring Files

Displays the number of files transmitted over your network, grouped by the web application used to transmit the files.

<table>
<thead>
<tr>
<th>Web Application</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Web Browsing</td>
<td>3,316</td>
</tr>
<tr>
<td>RealClearPolitics</td>
<td>38</td>
</tr>
<tr>
<td>CNN.com</td>
<td>16</td>
</tr>
<tr>
<td>Amazon Web Services</td>
<td>2</td>
</tr>
<tr>
<td>C-SPAN</td>
<td>1</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 20 minutes ago
File Transfers Over Time

Displays a graph of the total number of file transfers detected in network traffic by the system, over the dashboard time range.

File Dispositions

Displays the number of files detected in network traffic as a result of Malware Cloud Lookup file rules, grouped by malware disposition.
File Actions

Displays the number of files transmitted over your network, grouped by the file rule actions used to handle the files.

<table>
<thead>
<tr>
<th>Action</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Malware Block</td>
<td>3,250</td>
</tr>
<tr>
<td>Malware Cloud Lookup</td>
<td>117</td>
</tr>
<tr>
<td>Archive (Failed to Inspect)</td>
<td>3</td>
</tr>
<tr>
<td>Cloud Lookup Timeout</td>
<td>1</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 20 minutes ago

File Categories

Displays the number of files transmitted over your network, grouped by file category.

<table>
<thead>
<tr>
<th>Category</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>Executables</td>
<td>3,259</td>
</tr>
<tr>
<td>PDF files</td>
<td>117</td>
</tr>
<tr>
<td>Archive</td>
<td>3</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 22 minutes ago
**File Types**

Displays the number of files transmitted over your network, grouped by file type.

<table>
<thead>
<tr>
<th>Type</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>EICAR</td>
<td>3,259</td>
</tr>
<tr>
<td>PDF</td>
<td>117</td>
</tr>
<tr>
<td>GZ</td>
<td>3</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 22 minutes ago

**File Names**

Displays the number of files transmitted over your network, grouped by file name.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Count</th>
</tr>
</thead>
<tbody>
<tr>
<td>eicar.com</td>
<td>3,248</td>
</tr>
<tr>
<td>3bebb2_b53ca6b673c14cdab9d68832bd7e74cb....</td>
<td>12</td>
</tr>
<tr>
<td>3bebb2_dd59ad4faff34206969d7d6f07995e2....</td>
<td>8</td>
</tr>
<tr>
<td>2016 Reuters Tracking - Core Political 9...</td>
<td>6</td>
</tr>
<tr>
<td>BGGWTarranceGroupLakeResearch.pdf</td>
<td>6</td>
</tr>
</tbody>
</table>

Last updated 2 hours, 21 minutes ago
Analysis Tab

The Analysis tab in FireSight is divided into sections that show you even more details about events and trends you might see on the dashboards on the Overview tab.

The Analysis tab includes the following subtabs:

- Context Explorer
- Connections
- Intrusions
- Files
- Hosts

Context Explorer Tab

The Context Explorer tab contains details that help you to understand more information and gather data to determine the best needs for your company. This section explains the parts of the Context Explorer and the graphs contained in each section.

Traffic and Intrusion Events Over Time

At the top of the Context Explorer is a line chart of traffic and intrusion events over time. The X-axis (horizontal line) plots time intervals, which range from five minutes to one month, depending on the selected time window. The Y-axis (vertical line) plots traffic in kilobytes (blue line) and intrusion event counts (red line).

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 specified filters.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
Indications of Compromise

Hosts by Indication

The Hosts by Indication pie chart displays a proportional view of the IoCs triggered by hosts on your monitored network.

- The inner ring divides by category (such as CnC Connected or Malware Detected).
- The outer ring divides data by specific event type.

Point to any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.

Indications by Host

Indications by Host bar graph displays the IP addresses and counts of unique Indications of Compromise triggered by the top 15 most active users on your monitored network.

Point to any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.
The other sections are sets of interactive graphs that you can click to see lists that provide greater detail for indications of compromise, network, application, intrusion, file, geolocation, and URL data.

Note: All the sections on the Analysis tab combined together are called the Context Explorer.

**Network Information**

This section contains interactive graphs on monitored network information.

**Operating Systems**

The Operating Systems pie graph shows you the operating systems running on your network.

- Inner ring shows groups of operating systems, such as Windows.
- Outer ring shows details about versions of the operating systems, such as Windows XP.

Point to any part of the graph to view more detailed information. Double-click the graph to choose specific actions, such as applying filters. Click any part of the graph to drill down on that information.
Traffic by Source IP

The Traffic by Source IP bar graph shows you the IP addresses of the users on your network who generate the most traffic. Blue bars represent source IP address and red bars represent connection data.

Point to any part of the graph to view more detailed information. Double-click the graph to choose specific actions, such as applying filters. Click any part of the graph to drill down on that information.
Traffic by Destination IP

The Traffic by Destination IP bar graph shows you the top destination addresses for traffic leaving your network. Blue bars represent the destination IP address and red bars represent connection data.

Point to any part of the graph to view more detailed information. Double-click the graph to choose specific actions, such as applying filters. Click any part of the graph to drill down on that information.
Connections by Access Control Action

The Connections by Access Control Action pie graph, displays a proportional view of the access control actions (determined when the security policy is defined) taken the most regarding your network traffic.

Point to any part of the graph to view more detailed information. Double-click the graph to choose specific actions, such as applying filters. Click any part of the graph to drill down on that information.
Traffic by Source User

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.

Application Protocol Information

The Application Protocol Information section displays application groups together by type. Charts are color-coded to indicate the risk level and business relevance for each type of application.

For example, there can be traffic that is exposing your network to risk, but has little or no business relevance. This could lead to policies and decisions about what types of traffic to keep out of your network.
Intrusion Events by Risk and Application

The Intrusion Events by Risk and Application donut graph displays the applications by intrusion events and is arranged by the applications’ estimated risk (default) or by estimated business relevance.

- The inner ring represents estimated risk- or business-relevance level (such as Medium or High).
- The outer ring shows you the actual applications that represent the risk.

Point to any part of the graph to view more detailed information. Double-click the graph to choose specific actions, such as applying filters. Click any part of the graph to drill down on that information.
Hosts by Risk and Application

The Hosts by Risk and Application donut graph displays the applications used most by your users and is arranged by the applications’ estimated risk (default) or by estimated business relevance.

- The inner ring represents estimated risk- or business-relevance level (such as Medium or High).
- The outer ring shows you the actual applications that represent the risk.

Point to any part of the graph to view more detailed information. Double-click the graph to choose specific actions, such as applying filters. Click any part of the graph to drill down on that information.

Application Details List

The Application Detail List displays below the Risk and Application graphs. In this list you can see all the identified applications from each graph with the application’s name, Risk, Business Relevance, Category, and numbers of hosts.

<table>
<thead>
<tr>
<th>Application</th>
<th>Risk</th>
<th>Business Relevance</th>
<th>Category</th>
<th>Hosts</th>
</tr>
</thead>
<tbody>
<tr>
<td>Firefox</td>
<td>Medium</td>
<td>Medium</td>
<td>web browser</td>
<td>1381</td>
</tr>
<tr>
<td>Chrome</td>
<td>Medium</td>
<td>Medium</td>
<td>web browser</td>
<td>21</td>
</tr>
<tr>
<td>Google Analytics</td>
<td>Very low</td>
<td>High</td>
<td>web services provider</td>
<td>20</td>
</tr>
<tr>
<td>TiVoMP</td>
<td>Very low</td>
<td>Very High</td>
<td>security management, web services provider</td>
<td>9</td>
</tr>
<tr>
<td>Microsoft Cryptval</td>
<td>Medium</td>
<td>Medium</td>
<td>web services provider</td>
<td>9</td>
</tr>
<tr>
<td>Google Accounts Authentication</td>
<td>Low</td>
<td>Low</td>
<td>web services provider</td>
<td>8</td>
</tr>
<tr>
<td>Adobe Flash</td>
<td>Very low</td>
<td>High</td>
<td>browser plugins, business, software updates</td>
<td>7</td>
</tr>
<tr>
<td>Facebook</td>
<td>Very High</td>
<td>Low</td>
<td>email, gaming, instant messaging, mobile app</td>
<td>7</td>
</tr>
<tr>
<td>Internet Explorer</td>
<td>Medium</td>
<td>Medium</td>
<td>web browser</td>
<td>7</td>
</tr>
</tbody>
</table>
**Intrusion Information**

**Intrusion Events by Impact**

The Intrusion Events by Impact pie chart displays a proportional view of intrusion events on your monitored network, grouped by estimated impact level (from 0 to 4, with 0 being the least and 4 being the most impactful).

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
Top Attackers Graph

The Top Attackers bar graph shows the IP addresses sorted by the number of intrusion events (targeted in the connections causing those events) on your monitored network.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
Intrusion Events by Priority

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).

Point to 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.

Top Targets Graph

The Top Targets bar graph shows the top 10 target host IP addresses sorted by number of intrusion events (targeted in the connections causing those events) on your monitored network.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
File Information

Top File Types
The Top File Types donut graph displays a view of detected file types associated with malware.

- The outer ring shows file types detected in network traffic.
- The inner ring shows the file types grouped by category.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
**Top Hosts Sending Files**

The Top Hosts Sending Files or Malware graph shows the top IP addresses of users sending malware or the top users sending files across your network.

To switch between the number of files and the number of files containing malware, point to the graph and select the option that shows what you want to see.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
Top File Names

The Top File Names bar graph shows the names of the files affected by malware that were detected in network traffic.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.

Top Hosts Receiving Files

The Top Hosts Receiving Files graph shows the IP addresses of the users who receive the most files.

To switch between the number of files and the number of files containing malware, point to the graph and select the option that shows what you want to see.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
Files by Disposition

Shows the status of the files that were detected by the network.

Point to any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.

Top Malware Detections

Point to a bar in the graph to see detailed information about the malware, such as the threat name and the number of files that contain the selected malware.
Geolocation Information

Geolocation Information section 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.

Connections by Initiator Country

The Connections by Initiator/Responder Country donut graph 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 the connections by continent.
- The outer ring groups the connections by country.

Point to 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: You must install the Malware License to see this information.
Intrusion Events by Source Country

The Intrusion Events by Source Country donut graph displays countries targeted by intrusion events, based on the number of events associated with each country.

- The inner ring groups the connections by continent.
- The outer ring groups the connections by country.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
File Events by Sending Country

The File Events by Sending/Receiving Country donut graph 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 the connections by continent.
- The outer ring groups the connections by country.

Point to any part of the graph to view more detailed information. Click any part of the graph to filter or drill down on that information.
**Anti-Malware**

File Information section of the Context Explorer contains interactive graphs that display an overall picture of file and malware events on monitored network.

**URL Information**

The URL Information section contains three interactive bar graphs that display an overall picture of the URLs that the hosts on your monitored network use to exchange data.

These graphs show you traffic and unique connections associated with URLs, sorted by:

- Separate URLs
- URL category
- URL reputation

Note: You must have a URL Filtering license and enable URL Filtering for these graphs to include URL category and URL reputation data. Contact Cisco to set up these filtering options for you.

**Traffic by URL**

The Traffic by URL bar graph shows network traffic in kilobytes per second and unique connections for most-requested URLs on your monitored network. For each URL listed, blue bars represent traffic data and red bars represent connection data.

Point to any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.
Traffic by URL Category

The Traffic by URL Category bar graph shows network traffic in kilobytes per second and unique connections for the most-requested URL categories on your monitored network. For each URL category listed, blue bars represent traffic data and red bars represent connection data.

Point to any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.
Traffic by URL Reputation

The Traffic by URL Reputation bar graph shows network traffic in kilobytes per second and unique connections for the most requested URL reputation groups on your monitored network. For each URL reputation listed, blue bars represent traffic data and red bars represent connection data.

The URL reputations are:

- Well known
- Benign site
- Benign with Security Risk
- Suspicious Site
- High Risk

Point to any part of the graph to view more detailed information. Click any part of the graph to drill down on that information.